UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

USABILIDADE NAS SOLUÇÕES DE E-MAIL SEGURO

O MODELO MENTAL DE SEGURANÇA DO USUÁRIO

LUCAS CESAR FERREIRA

ORIENTADORA: DRA. JUNIA COUTINHO ANACLETO

São Carlos - SP
Março/2018

UNIVERSIDADE FEDERAL DE SÃO CARLOS

CENTRO DE CIÊNCIAS EXATAS E DE TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

USABILIDADE NAS SOLUÇÕES DE E-MAIL SEGURO

O MODELO MENTAL DE SEGURANÇA DO USUÁRIO

LUCAS CESAR FERREIRA

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de São Carlos, como parte dos requisitos para a obtenção do título de Mestre em Ciência da Computação, área de concentração: Interação Humano Computador
Orientadora: Dra. Junia Coutinho Anacleto

São Carlos - SP
Março/2018

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Ciência da Computação

Folha de Aprovação

Assinaturas dos membros da comissão examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Lucas Cesar Ferreira, realizada em 06/03/2018:

Profa. Dra. Marilde Terezinha Prado Santos
UFSCar

Profa. Dra. Junia Coutinho Anacleto
UFSCar

Profa. Dra. Renata Pontin de Mattos Fortes
USP

Certifico que a defesa realizou-se com a participação à distância do(s) membro(s) Junia Coutinho Anacleto e, depois das arguições e deliberações realizadas, o(s) participante(s) à distância está(ao) de acordo com o conteúdo do parecer da banca examinadora redigido neste relatório de defesa.

Dedico esta dissertação à minha família, em especial, aos meus pais José Ferreira e Maria José Ferreira, aos meus irmãos Júlio e Atalia Ferreira e a minha namorada Giovana Giacomini pelo apoio, incentivo e auxílio em todos os meus passos

AGRADECIMENTO

Agradeço primeiramente a Deus, por sempre estar presente na minha vida, por me abençoar e por me proporcionar a oportunidade de fazer uma pós-graduação.

A minha família, meus pais **José Antônio** e **Maria José**, pelo apoio e por serem exemplos de perseverança, dedicação, trabalho e honestidade. Eles são minha fonte de inspiração para alcançar os meus objetivos e sonhos. Aos meus irmãos, **Atalia** e **Júlio**, por todo carinho e apoio nos momentos que precisei. Aos meus avós pelo exemplo de vida, carinho e perseverança.

Em especial, a minha namorada, **Giovana Giacomini** por sempre estar ao meu lado me pondo para cima, dividindo os pesos da vida e me fazendo acreditar. Seu companheirismo, compreensão, amizade, apoio e, principalmente, amor me ajudou e ajuda na concretização dos meus projetos e deste trabalho.

A minha orientada e incentivadora, **Júnia Coutinho Anacleto**, pela paciência e confiança. Seu auxílio, ensinamentos e dedicação me proporcionaram determinação e inspiração para o desenvolvimento deste trabalho. Obrigado por todo carinho e por me possibilitar a experiência de ministrar aulas (pelo PESCD) e viagens para eventos de pesquisa.

Aos meus amigos, em especial **Alex Mansano, Flavio Rodrigues, Paulo Fontoura**, **João Paulo, Diego Henrique, Johny Velho e Renato Costa,** pelo apoio, momento de distrações, “roles”, risadas e horas de estudo.

A todos os colegas do Laboratório de Interação Avançada (LIA), por todo companheirismo, auxilio e amizade. Agradeço em especial o **André Bueno**, a **Francielle de Mattos**, o **Marcelo Huffenbaecher**, o **Vinicius Ferreira**, o **Rener Baffa** e o **Paulo Hect** pelos ensinamentos e por transmitirem suas experiências e proporcionarem momentos de alegria.

A CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior) pela bolsa de estudos que me proporcionaram uma dedicação integral a esta pesquisa. Agradeço também ao PPG-CC (Programa de Pós-

graduação em Ciência da Computação) pelo auxílio financeiro que possibilitou a publicação de artigos científicos.

Enfim, a todos que, de alguma forma, contribuíram para essa conquista.

Muito obrigado!

Seja feliz no pouco que no muito
Deus te colocará

RESUMO

A adoção da tecnologia de informação e comunicação em ambientes pessoais, sociais e corporativos é cada vez mais evidente, trazendo complexidade, interdisciplinaridade e diversidade ao estudo sobre segurança da informação em uma era marcada pela descentralização e ubiquidade. À medida que esse fenômeno se torna cada vez mais comum, as preocupações se intensificam em relação a segurança, sigilo, privacidade e governança da informação. Por consequência, ferramentas que provem tais medidas seguras também ganharam mais evidência e novas concepções tem surgido. No entanto, eventos e estudos mostram a dificuldade de uso e adoção dessas soluções seguras, mesmo sendo efetivas para segurança da informação, há evidências da necessidade de modelos mais eficazes de segurança e privacidade na Web, de maneira que possam ser amplamente adotados pelos usuários em geral. Logo, é necessário que as abordagens para desenvolvimento de soluções de segurança e privacidade sejam compreendidas pelos usuários, facilitando sua adoção, sem desconsiderar seus contextos de uso. Neste contexto, este trabalho visa compreender os modelos mentais dos usuários sobre segurança da informação (instanciados para soluções de e-mails seguros) e verificar se o design centrado em tais modelos pode ajudar no uso e adoção das ferramentas de segurança. Para isto, foi feito uma revisão das principais ferramentas encontradas na literatura, visando identificar suas principais características e abordagens de design e, ainda, se tais abordagens estavam em conformidade com as *guidelines* e desafios de Segurança Usável. Além disso, foi feita uma avaliação empírica usando o protótipo Xmail (desenvolvido pelo LIA) e a ferramenta Pwm a fim de extrair evidências qualitativas, a percepção dos usuários e validar a proximidade dos seus modelos mentais ao modelo de tarefa proposto pela ferramenta. Como resultados, este trabalho contribui com um modelo de revisão e avaliação de ferramentas seguras que pode ser estendido para além da instância de e-mail seguro. Além disso, a partir da análise dos resultados, foram encontrados indícios de que a compreensão do modelo mental de segurança dos usuários pode contribuir consideravelmente no processo de concepção de ferramentas de e-mails seguras e usáveis.

Palavras-chave: Segurança e Usabilidade, HCI-Sec, Modelos Mentais, E-mails seguros.

ABSTRACT

The adoption of Information and Communication Technology (ICT) in personal, social and corporate environments is increasingly evident. This fact brings complexity, interdisciplinarity, and diversity into the information security field intensified by decentralization and ubiquity of the actual era. As this phenomenon becomes more common, concerns regarding security, secrecy, privacy, and information governance increase. Consequently, tools to improve the safety in systems gain more evidence and new conceptions have emerged. However, studies and recent events have demonstrated how difficult is to use and adopt these safer solutions. Although these solutions improve the information security, there is evidence of the need for more effective security and privacy models on the Web to make these tools widely adopted by users in general. Therefore, the users need be aware of the approaches used by these security and privacy solutions in order to facilitate their adoption, without disregarding the contexts of use. In this context, this study aims at understanding the users' mental models of information security (e.g., secure e-mail solutions) to investigate if the design focused on such models can support the use and adoption of security tools. For that, a review of the main tools found in the literature was performed to identify the main characteristics and design approaches of these tools. Furthermore, to explore if such approaches are in compliance with Usable Safety guidelines and challenges defined in the literature. Then, an empirical evaluation was carried out using the Xmail prototype (developed at the LIA-UFSCar) and the Pwm tool to extract qualitative evidence from the users' perception and validate the proximity of their mental models to the task model proposed by the tools. As a result, this study contributes with a review and an evaluation model of secure tools that can be extended beyond keeping e-mail safe. In addition, from the analysis of the results, it was found that integrating the understanding of the users' mental security model into the process of designing safe and usable e-mail tools can significantly improve the usability of such tools.

Keywords: Usable security, HCI-Sec, Mental Models and Secure e-mail

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AT – Análise de Tarefas

CNSS – Comitê Nacional de Sistemas de Segurança

CTT – ConcurTaskTree

CTTE – ConcurTaskTreesEnvironment

FBI – Federal Bureau of Investigation

HCI-Sec – Human Computer Interaction and Security

IHC – Interação Humano-Computador

LIA – Laboratório de Interação Avançada

MT – Modelo de Tarefa

NSA – National Security Agency

PGP – Pretty Good Privacy

Pwm – Private WebMail

TICs – Tecnologias de Informação e Comunicação

UFSCar – Universidade Federal de São Carlos

SUMÁRIO

Capítulo 1

INTRODUÇÃO

1.1 Contexto

Vivemos em uma era pautada pelo terceiro paradigma de IHC que foca principalmente em valorizar a experiência dos usuários e a adoção das tecnologias no contexto social, pessoal e profissional, dando ênfase nos aspectos emocionais e culturais (BøDKER, 2006). Com este paradigma, as relações entre os usuários e seus artefatos tecnológicos ganham novas proporções e se diferenciam de uma era pautada pelos fatores humanos e delimitada pelo ambiente de trabalho com ênfase à execução de tarefas.

Alinhadas a este paradigma tecnológico, há grandes mudanças que também estão alterando irrevogavelmente a relação das pessoas com os computadores. A internet das coisas (*Internet of Things* – IoT) e a dependência tecnológica estão cada vez mais presentes na vida das pessoas, tornando-as dependentes de tecnologia em quase todos os aspectos (Figura 1.1). Além disso, o aumento dos serviços em nuvem e a capacidade de armazenamento de dados estão contribuindo para o fim do efêmero, onde todas as interações e atividades das pessoas estão sendo registradas e/ou gravadas e dificilmente serão esquecidas com o tempo (HARPER et al., 2008).

Com todas essas mudanças, juntamente com a vigilância global, o marketing eletrônico (baseado na coleta de informações pessoais) e a atual ênfase na gestão de cidades para sustentabilidade. Atingiu-se uma situação onde a coleta de dados

permeia os espaços pessoais, sociais e de trabalho e está muitas vezes acima dos consentimentos e direitos das pessoas.

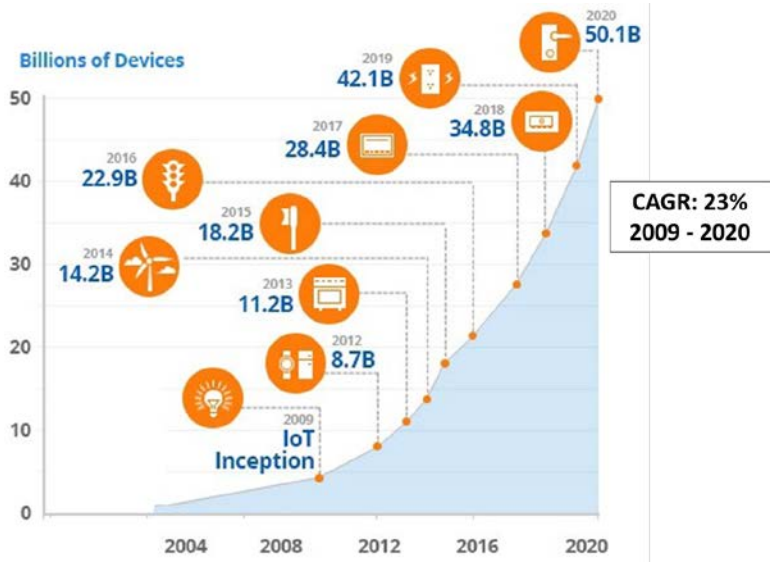


Figura 1.1: Taxa de crescimento do fenômeno internet das coisas desde o seu surgimento até 2020[1]

1.2 Motivação

Se por um lado a adoção generalizada das Tecnologias de Informação e Comunicação (TICs) é um fenômeno inevitável, do outro lado as preocupações se intensificam em relação à segurança, sigilo, privacidade e governança da informação e comunicação em uma era marcada pela descentralização e ubiquidade. Ao adotarem um serviço em nuvem como ferramenta, as pessoas estão colocando em risco sua privacidade e a segurança dos seus dados se não analisarem detalhadamente as políticas adotadas pelos serviços utilizados.

Eventos recentes colocam em evidência a necessidade de modelos mais eficientes de segurança e privacidade na Web. Em Junho de 2013, o jornal britânico *The Guardian* publicou um dos maiores escândalos de espionagem doméstica e internacional envolvendo a agência de inteligência americana *National Security Agency* (NSA) (GREENWALD; MACASKILL, 2013). Documentos confidenciais do governo dos Estados Unidos vazaram para o jornal através de Edward Snowden, um funcionário de uma empresa terceirizada alocado em projetos da NSA.

[1] Disponível em: https://goo.gl/4L9jhn

Ao expor o governo americano, Snowden sai do país e se vê como um procurado da justiça americana. Para se defender e continuar a expor as questões envolvendo o governo e o acesso aos e-mails de milhões de usuários da Google, Snowden se comunica com o advogado e jornalista Glenn Greenwald que, então, se torna seu porta voz (GREENWALD; MACASKILL, 2013). Snowden solicita a Greenwald que estabeleça um canal de segurança para sua comunicação, usando a solução Gpg4win[2], que apoia a comunicação ponta-a-ponta por meio da criptografia de chave publica. Entretanto, Greenwald teve muitas dificuldades em utilizar tal solução e, apesar de um vídeo de 12 minutos publicado por Snowden ensinando a utilizar o Gpg4win, o jornalista demorou sete semanas para finalmente enviar uma mensagem de volta para Snowden (GAYLE, 2014). Mesmo assim, Greenwald desiste e a solução Gpg4win não é adotada. A Figura 1.2 mostra parte do vídeo feito por Snowden para exemplificar o conceito de criptografia de chave pública.

A necessidade de melhor segurança e privacidade na internet é evidente, haja vista o caso Ashley Madison (THOMSEN, 2015) e o caso dos e-mails de Hilary Clinton (YUHAS, 2016). No entanto, grande parte das ferramentas para segurança de e-mails foca nas questões tecnológicas de segurança e suas possibilidades, concentrando-se em modelos centrados nas tecnologias. Entretanto, o resultado dessas abordagens são soluções seguras, mas não são compreendidas pelo usuário, exigindo um esforço cognitivo no seu uso que leva o usuário a não adotá-las ou quando exigida no ambiente de trabalho, boicota-la com os aplicativos já adotados.

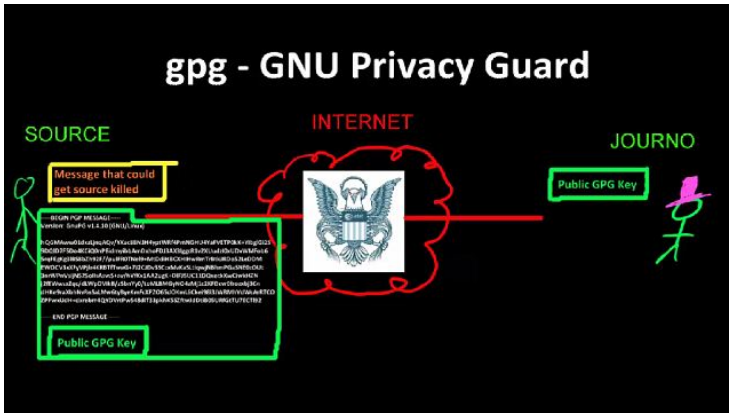


Figura 1.2: Esquema apresentado no vídeo feito por Snowden para explicar o conceito de chave pública a Greenwald[3]

[2] https://www.gpg4win.org/
[3] Disponível em: https://vimeo.com/56881481

1.3 Relevância do trabalho

Como mencionado nos casos anteriores, a possibilidade técnica de se obter privacidade e segurança com o ferramental tecnológico na maioria das vezes já é eficiente, porém os modelos do sistema propostos na maioria dessas ferramentas de segurança não são eficientes para um amplo uso e adoção dos usuários comuns.

Sendo assim, este trabalho busca identificar os principais motivos dessa não adoção e relata todo o processo de identificação, avaliação e análise das ferramentas, enfatizando suas abordagens de design e conformidades com as *guidelines* e desafios de Segurança Usável. Além disso, este trabalho busca evidências qualitativas e avalia a interação dos usuários em uso das ferramentas Xmail e Pwm, enfatizando as rupturas do modelo mental dos participantes. Com isto, espera-se que as lições aprendidas, bem como os relatos e resultados alcançados possam contribuir para a concepção de ferramentas seguras e usáveis.

A questão de pesquisa a ser respondida com este trabalho é:

- “A compreensão do modelo mental dos usuários sobre segurança pode apoiar no design de ferramentas seguras de fácil adoção?”

1.4 Objetivos

Este trabalho tem por objetivo estabelecer estratégias de design para dar poder e autonomia ao usuário final em relação à segurança de seus dados na adoção efetiva dos serviços de e-mail seguros.

Assim, com esta pesquisa, buscou-se:

(i) identificar as soluções/ferramentas que promovem segurança e privacidade em serviços de e-mails;

(ii) identificar os motivos desta não adoção, seja por dificuldades na compreensão dos métodos de segurança ou pelo esforço cognitivo extra envolvendo as tarefas cotidianas dos usuários;

(iii) entender os modelos mentais de segurança dos usuários em uso de ferramentas de e-mails;

(iv) formalizar a metodologia e as lições aprendidas, gerando novas estratégias de design de ferramentas de e-mail seguro baseadas no modelo metal de uso que contextualiza o modo de pensar do usuário.

1.5 Metodologia de Desenvolvimento do Trabalho

Para o desenvolvimento deste projeto foi realizado uma revisão da literatura focando nos três principais referenciais teóricos adotados: (i) a usabilidade para o embasamento de técnicas de avaliação; (ii) modelos mentais para a compreensão da lógica, a fim de estabelecer soluções de segurança úteis e adequadas ao usuário; (iii) modelo de tarefas para a representação do modelos implementados nas soluções oferecidas.

Foram realizadas também uma revisão e análise contínuas dos trabalhos científicos e ferramentas relacionados no contexto de segurança e usabilidade, tendo como objetivo a avaliação de suas abordagens de design ante a percepção dos usuários no seu uso.

Além disso, com objetivo de extrair evidências qualitativas de uso e entender o modelo mental dos usuários em uso de ferramentas seguras. Foram feitos testes de usabilidade, usando o protótipo Xmail (desenvolvido pelo Laboratório de Interação Avançada) e a ferramenta Private WebMail (Pwm). Para isso, questões éticas e de privacidade foram consideradas na forma de coleta de dados. Estas questões foram avaliadas pelo Comitê Ético Brasileiro, para onde o estudo foi enviado para apreciação, certificado pelo número CAAE: 68941717.5.0000.5504

A partir da revisão das ferramentas e dos experimentos envolvendo usuários, evidências qualitativas e quantitativas foram coletadas. Essas evidências foram analisadas procurando responder às questões de pesquisas deste trabalho, por meio da organização, interpretação e categorização dos dados coletados.

1.6 Organização do Trabalho

Este trabalho está organizado em sete capítulos. Neste primeiro capítulo, a introdução, motivação, objetivos e metodologia de desenvolvimento do trabalho foram caracterizados. Os demais são descritos a seguir:

Capítulo 2 É feita uma descrição do referencial teórico necessário para a compreensão do trabalho.

Capítulo 3 O protótipo Xmail, desenvolvido pelo LIA, utilizado para os testes com usuários é detalhado.

Capítulo 4 Uma revisão das principais ferramentas de e-mails seguros é apresentada, juntamente com uma análise de suas abordagens.

Capítulo 5 É apresentado o planejamento e a execução do teste de usabilidade realizado para compreender os usuários em uso das ferramentas seguras.

Capítulo 6 É explicado o processo de análise dos dados coletados no estudo, bem como a discussão dos principais resultados obtidos nas análises.

Capítulo 7 São listados e discutidos os resultados e as contribuições alcançadas deste trabalho, listando os artigos publicados, as limitações e as sugestões de trabalhos futuros.

Capítulo 2

REFERENCIAL TEÓRICO

Destacada a necessidade de abordagens de segurança e privacidade que, além de seguras, também possam ser compreendidas pelos usuários finais, a fim de oferecer poder e autonomia. Este capítulo apresenta os trabalhos mais relevantes juntamente com os conceitos-base para o desenvolvimento do projeto de pesquisa descrito neste trabalho.

Dentre esses conceitos estão: Usabilidade, Segurança da Informação, Segurança Usável, Modelos Mentais e Análise e Modelo de tarefas.

A organização deste capítulo segue da seguinte maneira: O conceito de Usabilidade é apresentado na Seção 2.2, juntamente com os principais métodos de avaliação. Na Seção 2.3, uma breve definição dos conceitos de Segurança e Privacidade é apresentada. A Seção 2.4 descreve o conceito de Segurança Usável, ressaltando as *guidelines* de design. Os conceitos de Modelos Mentais e Conceitual são apresentados na Seção 2.4. A Seção 2.5 apresenta o Modelo de Tarefas *ConcurTaskTree* (CTT), seguido das considerações finais na Seção 2.9.

2.1 Usabilidade

Usabilidade em termos de qualidade de software na norma ISO/IEC 9126 é definida como um conjunto de atributos relacionados com esforço necessário para o uso de um sistema interativo, relacionados com a avaliação individual de tal uso, por um conjunto específico de usuários. Tal conjunto de atributos é composto por: (i)

inteligibilidade: esforço do usuário em compreender o conceito lógico e sua aplicabilidade, (ii) apreensibilidade: esforço do usuário em aprender a usar a aplicação do software, (iii) operacionalidade: esforço do usuário para operar e controlar a operação e (iv) atratividade: satisfação subjetiva dos usuários durante o uso (ISO/IEC 9126, 1991).

Na norma sobre requisitos de ergonomia ISO 9241-11, usabilidade é definida como sendo o grau em que um produto é usado por usuários específicos para atingir objetivos específicos com eficácia, eficiência e satisfação de uso. Nesse contexto, **eficácia** está relacionada com a capacidade dos usuários interagirem com o sistema para alcançar seus objetivos devidamente como o esperado. A **eficiência** tem relação com os recursos necessários para os usuários interagirem com o sistema e alcançarem seus objetivos com o menor esforço possível. Por fim, a **satisfação de uso** refere-se à experiência do usuário ao utilizar o sistema interativo (ISO 9241-11, 1998).

Para Nielsen, usabilidade é um conceito que quantifica a utilidade do sistema interativo, ou seja, o quão bem um usuário pode interagir com o sistema em questão. Os fatores de usabilidade são definidos por um conjunto de cinco atributos (NIELSEN, 1993):

1. **Facilidade de aprendizado (*learnability*).** Refere-se ao tempo e o esforço necessário para que os usuários aprendam a utilizar o sistema efetivamente, independente do nível de habilidade e/ou conhecimento sobre sistemas computacionais.
2. **Eficiência (*efficiency*).** Determina quanto um sistema interativo é eficiente (tempo), a ponto de obter maneiras eficientes aos usuários e obter um nível elevado de produtividade.
3. **Facilidade de memorização (*memorability*).** Refere-se ao esforço cognitivo do usuário necessário para lembrar-se da interação com o sistema interativo. O sistema precisa ser de fácil memorização sem a necessidade de reaprendizado. Fornecer pistas, *affordances* e até metáforas pode ajudar na memorização.
4. **Geração de poucos erros.** Determina à taxa de erros do sistema, visto que o erro é uma ação que leva a um resultado inesperado e o sistema precisa oferecer opções de recuperação sem perda de trabalho.

5. **Satisfação do usuário (*satisfaction*).** Refere-se o quanto o sistema satisfaz os usuários, de maneira que eles se sintam satisfeitos ao usá-lo. A satisfação está diretamente com a experiência do usuário na interação com o sistema.

2.1.1 Métodos de Avaliação de Usabilidade Analíticos

A avaliação analítica ou por inspeção é utilizada para examinar um sistema interativo, focando em identificar os problemas de usabilidade em um projeto de interface com vistas a fazer recomendações para consertá-los. Esses métodos não envolvem diretamente os usuários, ou seja, tratam de experiências de uso potencial e não real. Nesta inspeção, os avaliadores tentam se colocar no lugar dos possíveis usuários da solução simulando e identificando os possíveis problemas na interação com o sistema (BARBOSA; SILVA, 2010).

Mack e Nielsen identificam os principais objetivos deste tipo de avaliação (MACK; NIELSEN, 1994):

- **Identificação de problemas de usabilidade:** identificar, classificar e contar o número de problemas de usabilidade encontrados durante a inspeção;
- **Seleção dos problemas que devem ser corrigidos:** priorizar os problemas de usabilidade de acordo com a sua severidade e custo associado à correção.

A literatura dispõe de vários métodos analíticos, como por exemplo: Avaliação Heurística que visa identificar problemas de usabilidade conforme um conjunto de heurísticas ou diretivas, também conhecidas como *guidelines* (MACK; NIELSEN, 1994); Percurso Cognitivo que avalia a facilidade de aprendizagem da interface através do conceito de aprendizagem por exploração (LEWIS et al. 1997; POLSON et al. 1992).

2.1.2 Métodos de Avaliação de Usabilidade Empíricos

Métodos de avaliação empíricos são utilizados para identificar problemas reais que os usuários enfrentam na interação com sistemas interativos (não apenas problemas potenciais previstos por avaliadores). Em tais métodos, os avaliadores focam na observação dos usuários e como eles interagem com o sistema. Por

envolver usuários, bem como o recrutamento e a gestão, tais testes costumam ser mais custosos e lentos.

A seguir o método Teste de Usabilidade é apresentado e seguirá como base para os capítulos seguintes.

2.1.2.1 Teste de Usabilidade

O teste de usabilidade é um método empírico que avalia a usabilidade de um sistema interativo a partir de experiências de uso dos usuários-alvo (RUBIN, 1994). A partir de objetivos e critérios de medição previamente estabelecidos, um grupo de usuários é convidado a realizar um conjunto de tarefas usando o sistema interativo em laboratórios específicos ou no ambiente real em que o software é utilizado. Durante toda a avaliação, observações são realizadas com o objetivo de coletar dados sobre o desempenho dos participantes na realização das tarefas (NIELSEN, 1993). Esse teste foca principalmente na avaliação quantitativa de critérios de usabilidade. Através da determinação de limites máximos, mínimos e almejados e da observação direta do usuário é possível obter medidas quantificáveis dos critérios estabelecidos.

A seguir são listadas algumas medidas típicas de usabilidade que são quantificáveis (ROCHA et al., 2000):

- O tempo que o usuário gasta para realizar determinada tarefa;
- A razão entre interações de sucesso e erro;
- O número de erros do usuário;
- A frequência de uso de manuais e sistemas de ajuda;
- O tempo gasto com manuais ou sistemas de ajuda;
- A frequência em que o uso dos manuais ou sistemas de ajuda resolveu o problema do usuário;
- A proporção entre comentários favoráveis e desfavoráveis;
- O número de comandos e quais foram utilizados pelos usuários;
- Quais comandos nunca foram utilizados pelos usuários;
- A quantidade de tempo que o usuário não interagiu com o sistema.

A execução de um teste de usabilidade depende de atividades que são comuns a outros testes empíricos, como a determinação dos objetivos, usuários e

experimentadores; geração do material a ser utilizado; preocupações éticas; adequação do ambiente onde o teste será realizado e análise dos dados coletados. A seguir, são descritas algumas etapas que permitem a realização de testes de usabilidade (Tabela 2.1).

Tabela 2.1: Atividades do teste de usabilidade (BARBOSA; SILVA, 2010))

Teste de Usabilidade	
Atividade	**Tarefa**
Preparação	- Definir tarefas para os participantes executarem - Definir o perfil dos participantes e recrutá-los - Preparar material para observar e registrar o uso - Executar um teste-piloto
Coleta de dados	- Observar e registrar o desempenho e a opinião dos participantes durante sessões de uso controladas
Interpretação	- Reunir, contabilizar e sumarizar os dados coletados dos participantes.
Consolidação dos resultados	
Relato dos resultados	- Relatar o desempenho e a opinião dos participantes

Na etapa de **preparação**, são definidos os objetivos, as tarefas, os termos de consentimentos, o ambiente e os dados a serem coletados. De maneira, geral esta etapa esta preocupada em deixar tudo certo para a chegada dos participantes e a coleta de dados.

A **coleta de dados** tem por objetivo coletar as experiências vivenciadas pelos usuários durante o processo de interação com o sistema ou protótipo sendo avaliado, incluindo questionário pré-teste, a sessão de observação e a entrevista pós-teste. Além disso, os avaliadores devem ser atenciosos para coletar diferentes tipos de dados, por exemplo, expressões dos usuários, registro das teclas digitadas e áudio. Nesta etapa, o avaliador deve entender que toda a informação no ambiente de teste é relevante até mesmo a mais simples.

Na etapa de **interpretação** os dados devem ser organizados e agrupados segundo suas relações, e por fim interpretados, visto que a análise conjunta dos dados pode revelar novos aspectos nos quais não seriam identificados por meio de dados separados. No entanto, a interpretação dos dados depende também do tipo de avaliação (qualitativa e quantitativa), de maneira que a visualização de dados qualitativos é diferente de dados quantitativos. Na consolidação recomenda-se que o

avaliador categorize os problemas encontrados durante a interação dos participantes, descrevendo cada problema e explicando as hipóteses dos mesmos.

O **relato dos resultados** descrever o teste de usabilidade, bem com os objetivos, escopo da avaliação, o perfil dos usuários que participaram das tarefas escolhidas, os problemas encontrados e suas hipóteses e, por fim, os resultados sumarizados.

Vale a pena mencionar, que o teste de usabilidade é considerado o método mais eficaz em detectar erros nos sistemas interativos, entretanto, o custo para o teste de usabilidade é cerca de 50 vezes maior do que o custo em métodos de inspeção (DESURVIRE, 1994).

2.2 Segurança da Informação e Privacidade

A definição de segurança da informação no conjunto de normas da ISO/IEC 27000 refere-se genericamente a três atributos básicos: confidencialidade, integridade, disponibilidade. Entretanto, algumas normas se estendem e dizem que a segurança requer outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade (ISO/IEC 27000, 2012).

Para o Comitê Nacional de Sistemas de Segurança (CNSS), segurança da informação é a proteção do acesso, divulgação, alteração, utilização e/ou destruição da informação não autorizada, objetivando a garantia da confidencialidade, integridade e disponibilidade.

A privacidade dentro da computação é centrada na privacidade dos dados pessoais, refletindo o direito do usuário de controlar, usar e o compartilhar informações digitais sobre si (WESTIN, 1970).

Em resumo, segurança e privacidade em computadores é a garantia que pessoas possam preservar seus dados pessoais de maneira que tais dados não serão involuntariamente modificados ou liberados.

2.3 Segurança Usável

Saltzer e Schroeder foram os primeiros a observarem que sistemas de segurança devem ser usáveis aos usuários para serem realmente seguros. Neste trabalho, eles identificaram a “psicologia da aceitabilidade” como um dos oito princípios para a construção de ferramentas seguras (SALTZER; SCHROEDER, 1975):

- Psicologia da aceitabilidade. É essencial que a interface humana seja desenvolvida para fácil uso, de modo que os usuários rotineiramente e automaticamente apliquem corretamente os mecanismos de proteção. Além disso, na medida em que a imagem mental do usuário e dos mecanismos de proteção coincide erros são minimizados.

Zurko e Simon em 1996 publicaram um artigo intitulado de “*User-Centered Security*” onde definiram três categorias de pesquisas para explorar o conceito de segurança e usabilidade: i) aplicação de teste de usabilidade e técnicas de proteção aos sistemas; ii) desenvolvimento de modelos de segurança e mecanismos para sistemas de fácil utilização; iii) e a necessidade dos usuários como um objetivo primário de desenvolvimento de ferramentas seguras. Esse artigo trouxe uma ideia radical para a comunidade de segurança, onde a comunidade viu a necessidade de realizar testes de usabilidade em ferramentas de segurança para estabelecer não somente a usabilidade, mas também a segurança (ZURKO; SIMON, 1996).

Apesar disso, o termo segurança usável ganhou bastante força em 1999 com o trabalho de Whitten e Tygar, onde definiram que um software é seguro e usável se os usuários: i) Estão cientes das tarefas de segurança que necessitam executar; ii) São capazes de descobrir como executar suas tarefas com êxito; iii) Não cometem erros comprometedores; iv) Estão suficientemente confortáveis com a interface (WHITTEN; TYGAR, 1999).

Em resumo, Segurança Usável ou Interação Humano-Computador e Segurança (abreviação em inglês HCI-Sec) é um área de pesquisa que tem por objetivo unir os conceitos Usabilidade e Segurança da Informação a fim de melhorar a experiência de uso dos usuários na interação com soluções de segurança. (Figura 2.1).

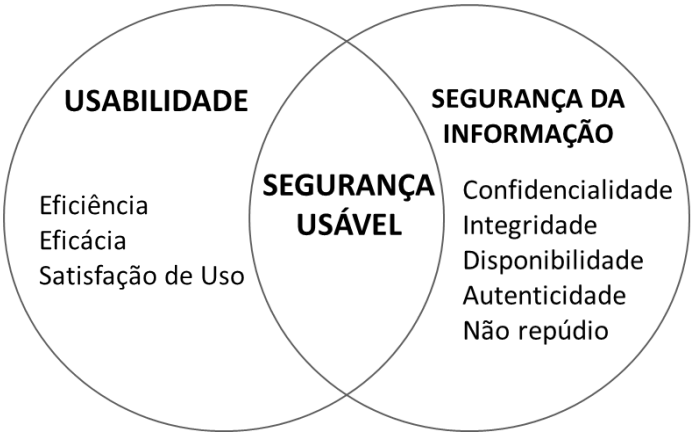


Figura 2.1: Conceito de Segurança Usável representado pela interseção dos conceitos de Usabilidade e Segurança da Informação

2.3.1 A Desmotivação e dos Usuários Comuns em Segurança

A desmotivação dos usuários em aprenderem a utilizar ferramentas e aplicativos complexos não é uma novidade e tal problema já é considerado em *guidelines* de designs (NILSEN, 1993). Entretanto, se tratando de segurança e privacidade digital esta desmotivação se torna ainda maior, visto que a grande maioria dos usuários tratam a segurança e a privacidade como um objetivo secundário e dificilmente estão dispostos há perderem seu tempo com treinamentos e manuais completos (WHITTEN; TYGAR, 1999).

Até mesmo no ambiente corporativo com firewalls e vários mecanismos de segurança de dados, às informações podem ser comprometidas por causa do esforço cognitivo e trabalho extra dos usuários. Por exemplo, para compartilhar um arquivo com um colega em uma estação de trabalho ao lado, um usuário (experiente o suficiente em trocas de e-mails) prefere enviar um e-mail com o arquivo em anexo do que passar pela frustração de configurar pastas compartilhadas na rede corporativa (DIX, 2007).

Devido a essa desmotivação da grande maioria dos usuários, fica evidente que conceber soluções que sejam seguras e também usáveis é uma tarefa complexa e vai além dos padrões de design comuns. Whitten e Tygar destacam os cinco desafios de conceber tais soluções (WHITTEN; TYGAR, 1999):

1. **Desafio do usuário desmotivado:** Segurança é geralmente um objetivo secundário, os usuários geralmente não estão dispostos a perderem tempo para administrar sua segurança. Assim, os designers devem assumir que

qualquer esforço desnecessário (treinamentos e manuais complexo) pode desmotivar completamente o usuário a usar o sistema.

2. **Desafio de abstração:** Usuários não compartilham o mesmo nível de abstração que os desenvolvedores do sistema. Caso este nível não seja considerado, há um risco maximizado da interface não ser intuitiva.
3. **Desafio da falta de *feedback*:** A necessidade de evitar erros comprometedores torna os feedbacks uma tarefa essencial para os usuários, porém, fornecê-los para gestão de segurança nem sempre são adequados.
4. **Desafio da porteira aberta:** Se o "segredo" foi deixado acidentalmente desprotegido, independentemente do período de tempo, não há nenhuma garantia de que ele continua íntegro. A solução deve priorizar e garantir que os usuários entendam esse risco potencial e evitem erros comprometedores.
5. **Desafio do elo mais fraco:** Se tratando de segurança, um único erro pode ser fatal e comprometer toda a integridade da mensagem. Por isso, os usuários devem ser orientados a atender todos os aspectos de segurança, não deixando os "segredos" em lugares que podem ser explorados por outros recursos.

2.3.2 *Guidelines*

Com o objetivo de guiar a concepção de soluções de seguras e usáveis, Yee em 2002 propôs um conjunto de dez *guidelines* criadas por meio de experiências contínuas com usuários (YEE, 2002). Abaixo cada uma é apresentada e servirá de base para capítulos futuros:

1. **Caminho de menor resistência.** A maioria dos usuários não gasta tempo pesando sobre segurança e escolher o "caminho de menor resistência" na maioria das vezes é a opção preferida. Devido a isso, o caminho mais natural (ou padrão) de fazer qualquer tarefa deve ser também o caminho mais seguro.
2. **Limites relevantes.** A interface deve ser consistente e distinguir ações e objetos que são importantes para o usuário, mostrando somente o que é necessário, ou seja, implicações de segurança significativas devem estar visíveis e as insignificantes invisíveis.

3. **Autorização explícita.** Atribuir autorização explícita aos usuários em nível de aquisições de recursos. Essas autorizações explícitas aumentam a probabilidade dos usuários operarem com autoridade necessária.
4. **Visibilidade.** A interface da solução deve sempre mostrar aos usuários o estado do sistema, fornecendo informações necessárias para atualizá-los e informá-los.
5. **Revogabilidade.** A solução deve permitir que os usuários possam revogar ações concebidas sempre que possível tal revogação.
6. **Falsa expectativa.** A solução não deve dar ao usuário a impressão de que é possível fazer algo que não seja realmente possível.
7. **Caminho confiável.** A solução deve fornecer “caminhos confiáveis” para os usuários executarem suas ações na interface, de maneira que esses caminhos não possam ser corruptíveis.
8. **Identificabilidade.** A capacidade de identificar objetos e ações é essencial em sistemas seguros e a interface deve garantir consistência nessa identificação, de maneira que os objetos e as ações não sejam ambíguos.
9. **Expressividade.** Expressar as políticas de segurança, coincidindo com os objetivos dos usuários, definindo as intenções da solução e permitindo os usuários expressarem suas políticas de segurança.
10. **Clareza.** Indicar com clareza as consequências das possíveis decisões dos usuários em uso da solução.

2.3.3 E-mail Seguro

Apesar da pesquisa em HCI-Sec possuir várias vertentes de pesquisa, tais como estudo para melhoria da autenticação e criptografia, ferramentas de gerenciamento de senhas e infraestrutura de chaves publicas (KAINDA; FLECHAIS; ROSCOE, 2010) Este trabalho é instanciado para o estudo de sistemas seguros, em especial para soluções de e-mails seguros. Assim, esta seção apresenta uma breve historia da criptografia em e-mails, juntamente com os trabalhos encontrados na literatura que abordam o conceito de Segurança Usável em e-mails.

2.3.3.1 Criptografia em E-mails

A troca de e-mails é um caso particular em criptografia, caracterizado pela alta latência das mensagens. Dois padrões são predominantes na criptografia de mensagens de e-mails (PGP e S/MIME), ambos dependentes de Infraestruturas de Chaves Públicas, mas com abordagens bastante distintas quanto à operação.

S/MIME

Com a possibilidade de encriptar e assinar conteúdo com criptografia assíncrona, um esquema de criptografia em mensagens de e-mail foi proposto em meados da década de 80, padrão nomeado PEM (Privacy Enhanced Mail). Esse padrão, utilizava a especificação X.509 para a certificação de chaves públicas através de Autoridades de Certificado, mas na ausência de um diretório de chaves públicas online todas as chaves necessárias para verificar a assinatura da mensagem eram incluídas no corpo do e-mail, o cliente então armazenava a chave pública do remetente e a utilizava para encriptar dados na próxima que um e-mail era enviado para esse endereço (GARFINKEL et al., 2005).

Mais tarde em 1999, RFC 2633 definiu Secure/Multipurpose Internet Mail Extensions (S/MIME), que se originou de uma reimplementação do PEM utilizando o novo padrão MIME de e-mails, uma vez que uma Autoridade de Certificados raiz central se mostrou uma alternativa problemática. S/MIME utiliza uma abordagem centralizada para a distribuição de chaves. Nessa distribuição, todos os usuários têm certificados de chaves públicas que são assinadas por uma autoridade de certificação e distribuídos através do envio de e-mails dos usuários (RAMSDELL, 1999). A grande maioria dos clientes de e-mail tem suporte a S/MIME, mas nenhum dos webmails mais utilizados (Gmail, Yahoo, Hotmail) suporta a especificação, apresentando as assinaturas como um arquivo em anexo e deixando as mensagens encriptadas indecifráveis (GARFINKEL et al., 2005).

PGP *(Pretty Good Privacy)*

PGP é um método de criptografia implementado inicialmente como um programa em 1991 por Phil Zimmerman. O método utiliza criptografia hibrida, ou seja, utiliza criptografia assíncrona de modo que cada usuário possui uma chave

pessoal, mas gera uma chave síncrona para cada documento. PGP é agnóstico em relação aos algoritmos de criptografia utilizados e um subconjunto de padrões que não requer nenhum tipo de patente é distribuído como OpenPGP (GARFINKEL, 1995).

PGP descentraliza a emissão de certificados de confiança em chaves públicas e baseia seu modelo em um conceito ponta-a-ponta chamado Cadeia de Confiança (tradução livre de *Web of Trust*). Em uma Cadeia de Confiança, os usuários podem consultar o nível de confiança dos seus colaboradores, assinar e aprovar a autenticidade da chave que são "confiáveis" ao invés de depender de uma autoridade centralizada.

2.3.3.2 Estudos em E-mails Seguros e Usáveis

Whitten e Tygar em seu trabalho seminal "*Why Johnny Can't Encrypt*" de 1999 exploraram a usabilidade da ferramenta de criptografia de e-mail PGP 5.0 (WHITTEN; TYGAR, 1999). O título do artigo é uma referência ao livro "*Why Johnny Can't Read*" de Rudolf Flesch que critica o sistema pedagógico na alfabetização, carregando uma dura crítica já nesse simples trocadilho (que foi mantido em diversas publicações da comunidade de segurança usável das quais muitas serão discutidas nesse trabalho).

Os autores apresentam resultados bastante informativos que explicitam problemas catastróficos da interface e a ineficiência do sistema em conceber um modelo mental adequado para os usuários. Alguns dos resultados são relevantes até mesmo nos dias de hoje, pois correspondem a percepções de sistemas criptográficos em sua essência, não sendo casos particulares da versão do software utilizado, como por exemplo, metáforas visuais e problemas irreversíveis. Com tais resultados, concluíram que o PGP 5.0 não é utilizável o suficiente para fornecer segurança eficaz para a grande maioria dos usuários comuns.

Uma avaliação da nova versão do PGP, o PGP 9.0, foi realizada em 2006 pelo grupo da Carnegie Mellon University e publicada com o titulo de *"Why Johnny Still Can't Encrypt" ("Why Johnny Still Can't Read"* é o título da continuação do livro de Rudolf Flesh) (SHENG et al., 2006). Esse trabalho listou a persistência de muitos problemas detectados na versão 5.0. Os autores apontaram que a transparência das operações do software pode ser problemática, uma vez que a interface não apresentava nenhum *feedback* durante a composição de mensagens para indicar

que a mensagem seria criptografada. A transparência na decriptação também se mostrou problemática, pois possibilita um ataque de *spoof* com o atacante enviando um e-mail que tem forjada uma indicação visual de uma assinatura verificada.

As avaliações no PGP não acabaram na versão 9.0. Em 2015, um grupo de pesquisa da Brigham Young University publicou um estudo intitulado *"Why Johnny Still, Still Can't Encrypt"* (RUOTI et al., 2015). Tal trabalho avaliou a usabilidade de um sistema de PGP moderno (Mailvelope), buscando identificar se os problemas de usabilidade persistiam após 15 anos do primeiro estudo com a versão 5.0. Os concluíram que o PGP moderno, apesar dos avanços em usabilidade, ainda possui usabilidade muito baixa e funcionamento muito complexo para usuários sem conhecimentos de criptografia de chave pública, ou seja, o gerenciamento manual das chaves de criptografia ainda não corresponde ao modelo mental dos usuários.

Outro trabalho que marca a jornada Johnny é intitulado *"Confused Johnny"* (RUOTI et al., 2013). Esse trabalho discute a transparência de segurança no envio de mensagens criptografadas. Os autores notaram que a primeira versão de seu sistema de e-mails seguro (Private WebMail (Pwm)) confundiu os usuários quanto a percepção de segurança, devido a transparência excessiva. Ao realizarem um estudo complementar com um protótipo que mostrava a mensagem cifrada antes de enviá-la, os autores concluíram que esta tarefa adicional não tem efeito significativo sobre a usabilidade e contribuiu para a percepção de segurança dos usuários.

Por fim, o trabalho de Routi et al. em 2016 também marcou as pesquisas e-mails seguros e usáveis. Nesse trabalho, os autores classificam as ferramentas de segurança de e-mails em três modelos (RUOTI et al., 2016):

- ***Integrated Secure Email.*** Para as ferramentas que se integram diretamente como a interface dos webmails (por exemplo, Gmail e Outlook) que os usuários já utilizam e conseguem prover segurança dentro de tais serviços sem a criação de novos domínios.
- ***Depot-Based Secure Email.*** Para as ferramentas que são totalmente desintegradas aos webmails convencionais dos usuários, ou seja, são webmails específicos de segurança e necessitam da criação de novos domínios.
- ***Hybrid Secure Email.*** Para as ferramentas que são integradas aos webmails dos usuários, mas realizam funções específicas (por exemplo, criação de

senhas e gerenciamento de chaves) fora da interface dos serviços de tais webmails.

Os autores avaliaram também a usabilidade de três ferramentas que se diferem nos modelos definidos acima, a ferramenta Private WebMail (*Integrated*), Virtru (Hybrid) e Tutanota (*Depot-Based*). Os resultados do estudo mostram uma ruptura do modelo mental dos usuários em uso da ferramenta Tutanota, pois a maioria dos participantes não concluiu a tarefa com êxito e no tempo pré-estabelecido. Sendo assim, concluíram que os participantes do teste preferiram as soluções integradas aos seus e-mails convencionais e, consequentemente, seriam mais adotadas em casos de envio de e-mails seguros.

Em resumo, na Tabela 2.2 os trabalhos mencionados acima, bem como os outros trabalhos que se destacam no estudo de e-mails seguros e usáveis são destacados juntamente com as suas principais contribuições.

Tabela 2.2: Principais trabalhos e suas contribuições para o estudo de e-mails seguros e usáveis

Ferramentas			
Nº	Autores	Ano	Contribuições
1	DOURISH, P. et al	2004	Reforçam que apesar dos avanços das pesquisas em segurança, sobre suas bases matemáticas e técnicas, serem muito bem sucedidos, há dificuldade em fazer que esses sistemas atenderem às expectativas dos usuários em diversos contextos de uso (ex: e-mails).
2	MATHIASEN, N. R.; BøDKER, S.	2008	
3	RUOTI et al.	2013	Concluíram que transparência excessiva no processo de cifragem dos e-mails pode confundir os usuários.
4	WHITTEN; TYGAR	1999	Concluíram que gerenciamento manual das chaves de criptografia não corresponde ao modelo mental da maioria os usuários.
5	SHENG et al.	2006	
6	RUOTI et al.	2015	
7	GAYLE, D	2014	Relatou a experiência de falta de usabilidade na prática da ferramenta de e-mail seguro Gpg4win.
8	RUOTI et al.	2016	Mostraram indícios de que a avaliação em pares de amigos para testar a troca de e-mails seguros é mais efetiva.

2.4 Modelo Mental

O termo Modelo Mental foi sugerido por Kenneth Craik em 1943, no livro "*A natureza da Explicação*". Para Craik, modelos mentais são representações na mente de situações reais ou imaginárias. Conceitualmente, a mente constrói um modelo de pequena escala da realidade e usa a razão para fundamentar as explicações e

antecipar os eventos. Estes modelos podem ser construídos da percepção, imaginação ou da interpretação do discurso e desempenha um papel importante na cognição, raciocínio e tomada de decisão (CRAIK, 1967).

Apesar de o termo ser cunhado por Craik, Johnson-Laird em 1983 foi um dos principais precursores que contribuíram para criar a fundamentação que serviu de base para o conceito. Para Laird, os modelos mentais utilizam semântica processual para a codificação do mundo real, de modo que a mente adquire informações sobre os novos fenômenos e procura modelos semelhantes para uma semântica de harmonização. Caso não haja tal harmonização, um novo é construído e armazenado como a semântica relevante (JOHNSON-LAIRD, 1983).

Além do Johnson-Laird, outro precursor de destaque dos modelos mentais é o americano CS Peirce, que ao identificar três propriedades dos símbolos em geral (icônico, indicador ou simbólico) esclarece a natureza icônica de artefatos como diagramas e como seu se dá o pareamento da expectativa do funcionamento de um e outro (JOHNSON-LAIRD, 2004).

2.4.1 Modelo Conceitual

Cunhado por Joseph D. Novak em 1972, mapas ou modelos conceituais são estruturas hierárquica utilizadas para representar o conhecimento sobre determinados assuntos, por meio de um conjunto de conceitos e suas relações. Tal mapeamento pode ser entendido como uma representação visual utilizada para partilhar conhecimentos. O mapa conceitual se apoia na teoria da aprendizagem significativa de David Ausubel, que menciona que o ser humano organiza o seu conhecimento através de uma hierarquização dos conceitos (NOVAK; CANAS, 2007).

Tendo em vista a similaridade dos conceitos mencionados acima, convém fazer a distinção entre modelo conceitual e modelo mental. Modelo conceitual é um instrumento que permite a compreensão ou o ensino de conceitos e o modelo mental é uma concepção que as pessoas têm e que as guiam para a compreensão do mundo (GENTNER; STEVENS, 1983).

2.4.2 Modelo Mental e Conceitual em Interação Humano-Computador

Segundo Doyle e Ford, o modelo mental de um sistema interativo é uma representação conceitual relativamente acessível, porém limitada, a partir de um determinado ponto de vista, cuja representação é análoga à estrutura percebida desse sistema (DOYLE; FORD, 1998).

Apesar de Doyle e Ford apresentarem diversas definições de modelo mental para sistemas interativos, o conceito ganhou bastante destaque na área IHC com o livro *"The Design of Everday Things"* de Donald Norman. Para Norman, um modelo mental é o que o usuário acredita sobre o sistema em questão baseando-se em sua crença, ou seja, um modelo mental é o que os usuários sabem (ou pensam que sabem) sobre um sistema interativo. Cada usuário tem seu próprio modelo mental e ele é interno ao cérebro de cada usuário e diferentes usuários podem construir diferentes modelos mentais de uma mesma interface (NORMAN, 2013).

Além disso, Norman divide os papéis chaves para a usabilidade de um sistema em três tipos de modelos: Modelo conceitual do designer, sendo a maneira como o sistema foi concebido pelos designers; Imagem do Sistema, que é o modelo real do funcionamento do sistema no mundo real; e Modelo conceitual do usuário, sendo a ideia que o usuário faz do funcionamento do sistema. Assim, o principal objetivo do designer é conceber interfaces que possam se comunicar com a natureza básica do sistema, de maneira que o sistema possa proporcionar Modelos Conceituais úteis, precisos e que correspondam as expectativas dos usuários. Entretanto, tal objetivo é desafiador e, em grande parte dos designs, não é alcançado visto que a Imagem do Sistema nesses casos corresponde aos Modelos Mentais dos designers não dos usuários do sistema interativo.

2.5 Análise e Modelo de Tarefas

Análise de Tarefas (AT) para Diaper é *"a expressão utilizada no campo da Ergonomia, que inclui IHC, para representar todos os métodos de coleta, classificação e interpretação dos dados sobre o desempenho de um sistema que possui ao menos uma pessoa como componente"* (DIAPER; STANTON, 2003). Em

outras palavras, Análise de Tarefas é um conjunto de métodos para descrever as tarefas dos usuários visando entender como eles as realizam e por quê. Neste tipo de análise, o enfoque básico é descrever a tarefa como tendo um objetivo principal e um conjunto de passos para a sua realização, porém, não se trata apenas de listar ações, mas de entender como o sistema afeta o domínio de aplicação.

Na área de IHC, a AT pode ser utilizada em três diferentes atividades habituais: i) analisar a situação atual (apoiada ou não por um sistema computacional); ii) fazer um *re-design* de um sistema; iii) avaliar um sistema computacional existente (BARBOSA; SILVA, 2010). Além disso, para Diaper, a AT é o núcleo da maior parte do trabalho de IHC, devido ao fato da análise se preocupar com o desempenho do trabalho se distinguindo das outras abordagens (DIAPER; STANTON, 2003).

A análise de tarefas em um domínio específico pode produzir uma descrição explícita das tarefas, chamada de Modelo de Tarefa (MT). Modelos de tarefas são usados para representar os resultados da análise de tarefas, cada modelo enfatizando uma perspectiva. Os modelos de tarefas estão interessados em permitir um entendimento mais detalhado dos passos e dos relacionamentos entre eles e, consequentemente, contribuir para a simplicidade, eficácia e usabilidade do sistema computacional (WINCKLER; PIMENTA, 2004).

Geralmente, um MT é construído utilizando conceitos e relacionamentos representando aspectos relevantes das tarefas e dos usuários. Entre eles, os mais comuns são:

- **Decomposição da tarefa.** Descrição hierárquica da tarefa, onde o nível mais alto contém a tarefa principal gradativamente divida em subtarefas.

- **Relacionamentos causais/temporais.** Descrição do fluxo da tarefa, indicando a ordem em que as subtarefas são executadas, geralmente através de construtores típicos (sequência, simultaneidade, entrelaçamento, etc.).

Diferentes métodos de análise e modelos de tarefas podem ser encontrados na literatura, como por exemplo, Hierarchical Task Analysis (HTA; Annett, 2003), o Goals, Operators, Methods, and Selection Rules (GOMS; Kieras, 2003) e o ConcurTaskTrees (CTT; Paternò, 1999). No entanto, nesse trabalho optou-se pelo CTT por apresentar uma expressividade relativamente positiva em relação à

complexidade e ser bem difundido e utilizado pela comunidade internacional de IHC (LIMBOURG; VANDERDONCKT et al., 2004). Além disso, o CTT possui uma ferramenta de edição e de suporte, nomeada de CTT Environment (CTTE), que facilita a criação, edição e simulação do modelo de tarefa (MORI; PATERNO; SANTORO, 2002).

2.5.1 Árvores de Tarefas Concorrentes (*ConcurTaskTree*)

Proposto por Paternò em 1999, Árvores de Tarefas Concorrentes (no inglês ConcurTaskTrees ou CTT) é um modelo de tarefas que visa auxiliar o design e avaliação em IHC. O CTT fornece um rico conjunto de operadores temporais que descrevem as relações entre as tarefas, permitindo a sequência, simultaneidade e entrelaçamento. Além dos operadores temporais, as tarefas podem ganhar mais informações, tais como tipo, categoria, objetos e atributos (PATERNO, 1999). A Tabela 2.3 destaca as principais características do CTT.

Nos próximas seções, a alocação de tarefas e os relacionamentos do CTT são descritas, bem como um simples exemplo de uma modelagem de tarefa usando o CTT (Figura 2.3). Neste exemplo, a tarefa *"retirar dinheiro de um terminal bancário genérico"* é decomposta em subtarefas e utiliza os operadores temporais para indicar qual a ordem cronológica da tarefa.

Tabela 2.3: Principais características do CTT (tabela baseada em (PATERNO, 1999))

Características	Descrição
Foco nas atividades	Permite aos designers se concentrarem mais nos aspectos relevantes que precisam realizar com o sistema, evitando detalhes de implementação.
Estrutura hierárquica	Fornece vários níveis de granularidade da tarefa, permitindo a decomposição em várias subtarefas.
Representação gráfica	Na maioria dos casos, permite melhorar a interpretação das tarefas.
Notação Concorrente	Permite aos designers expressarem claramente o relacionamento temporal entre as tarefas, de maneira que possam trazer mais expressividade ao modelo de tarefas produzido.
Alocação de tarefas	Permite descrever graficamente os agentes que realizam as tarefas.
Objetivos	Permite identificar os objetos que serão manipulados durante a execução da tarefa.

2.5.1.1 Alocação de Tarefas

Os tipos de tarefas propostos pelo CTT são representados por ícones ou formas geométricas, podendo representar quatro tipos de tarefa (Figura 2.2):

 Tarefas do Usuário		Tarefas cognitivas ou físicas realizadas inteiramente pelo usuário.
 Tarefas da Aplicação		Tarefas completamente realizadas pelo sistema sem a intervenção do usuário.
 Tarefas interativas		Tarefas que o usuário realiza com o sistema, as interações são ativadas pelo usuário e processadas pelo sistema.
 Tarefas Abstratas		Tarefas que requerem ações complexas e que devem ser decompostas em um subtarefas.

Figura 2.2: Tipos de tarefas do CTT representados por ícones e formas geométricas (figura adaptada de (PATERNO, 1999))

2.5.1.2 Relacionamentos Temporais

Os operadores temporais são utilizados para indicar o relacionamento temporal entre as tarefas do mesmo nível hierárquico, podendo modelar o comportamento dos sistemas. A lista de operadores temporais disponíveis em CTT é apresentada na Tabela 2.4. Além dos operadores temporais, o CTT inclui um conjunto de três operadores unários (

Tabela 2.5.) que são aplicáveis a uma tarefa individualmente.

2.6 Considerações Finais

Neste capítulo foram apresentados os conceitos de Usabilidade, Segurança da Informação, Segurança Usável, Modelos Mentais e Análise e Modelo de tarefas. Estes conceitos definem o escopo de pesquisa e serviram de base para todo trabalho.

O capítulo seguinte é destinado ao protótipo de segurança Xmail, desenvolvido pelo Laboratório de Interação Avançada (LIA). Nesse capítulo, as principais características, conceitos e arquitetura do protótipo são descritos.

Tabela 2.4: Operadores temporais (PATERNO, 1999)

Operador	Símbolo	Forma	Descrição
Escolha	[ ]	T1 [ ] T2	É possível escolher uma tarefa entre outras, mas quando iniciada as outras se tornam indisponíveis até a tarefa escolhida terminar.
Independência de ordem	|=|	T1 |=| T2	Ambas as tarefas devem ser realizadas, em qualquer ordem, mas devem ser executadas de maneira individual.
Concorrência independente	|||	T1 ||| T2	Especifica que as tarefas podem ser realizadas em qualquer ordem ou ao mesmo tempo.
Concorrência com troca de informações	|[]|	T1 |[]| T2	As tarefas poderem ser executadas concorrentemente, mas elas devem sincronizar para troca de informações.
Desativação	[>	T1 [>T2	(T1) é completamente interrompida por (T2).
Suspende / continua	|>	T1 |>T2	(T1) pode ser interrompida por (T2) e é retomada do ponto em que parou assim que (T2) terminar.
Habilitação	>>	T1 >>T2	(T2) só é iniciada quando (T1) terminar
Habilitação com passagem de informação	[] >>	T1 [] >>T2	Quando a (T1) termina ela envia a informação produzida para inicio da (T2).

Tabela 2.5: Operadores unários (PATERNO, 1999)

Operador	Símbolo	Forma	Descrição
Iteração	*	T *	Tarefa é iterativa, somente terminará se interrompida por outra tarefa.
Opcionalidade	[ ]	[T]	Tarefa é indicada como opcional.
Conexão entre modelos	↔	T ↔	Tarefa pode ser usada em modelo cooperativo onde participam vários usuários.

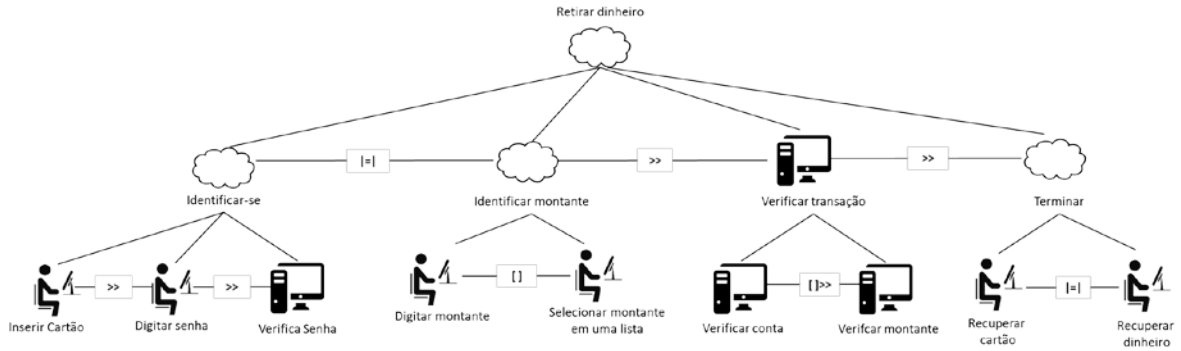


Figura 2.3: Modelagem da tarefa Retirar Dinheiro em um terminal bancário genérico usando o CTT.

Capítulo 3

PROTÓTIPO XMAIL

Mirando alcançar os objetivos do presente trabalho, o protótipo da ferramenta de segurança Xmail[4] foi escolhido para validar tais objetivos. O Xmail é um protótipo de uma extensão do Google Chrome criado pelo Laboratório de Interação Avançada[5] (LIA) que se integra com a interface do serviço de webmail Gmail[6], oferecendo segurança e privacidade aos usuários no envio de e-mails. Tal protótipo fornece segurança através da criptografia ponta-a-ponta e certificados digitais, tendo como foco principal a usabilidade (HECHT; FELS; ANACLETO, 2015).

Nas próximas seções deste capítulo, a arquitetura do Xmail é brevemente apresentada, bem como as diretrizes de usabilidade e conceitos de design utilizados em sua concepção.

3.1 Arquitetura

Como já dito, Xmail é uma extensão do Google Chrome criada a partir de tecnologias baseadas em Web, tais como HTML5, CSS3, Javascript e Coffeescript. Essas tecnologias, bem como o uso da extensão integrada, foram escolhidas devido a sua portabilidade, eficiência de uso e integração direta da ferramenta com o provedor de e-mails, possibilitando o uso da ferramenta em diversos sistemas operacionais, bastando apenas acessar um endereço num navegador.

[4] https://xmail.shwyz.ca/
[5] http://lia.dc.ufscar.br/
[6] www.gmail.com

Além das tecnologias de *front-end*, também foram adotadas a linguagem de programação Ruby, o framework Rails e, para efetuar o armazenamento de dados, o banco de dados MySQL. Tecnicamente, a ferramenta funciona como um Webservice que se integra com a interface do provedor Gmail e tem o propósito parecido como uma Autoridade Certificadora, ou seja, a ferramenta é responsável por armazenar, certificar e distribuir as chaves públicas. Abaixo a Figura 3.1 mostra a arquitetura da ferramenta.

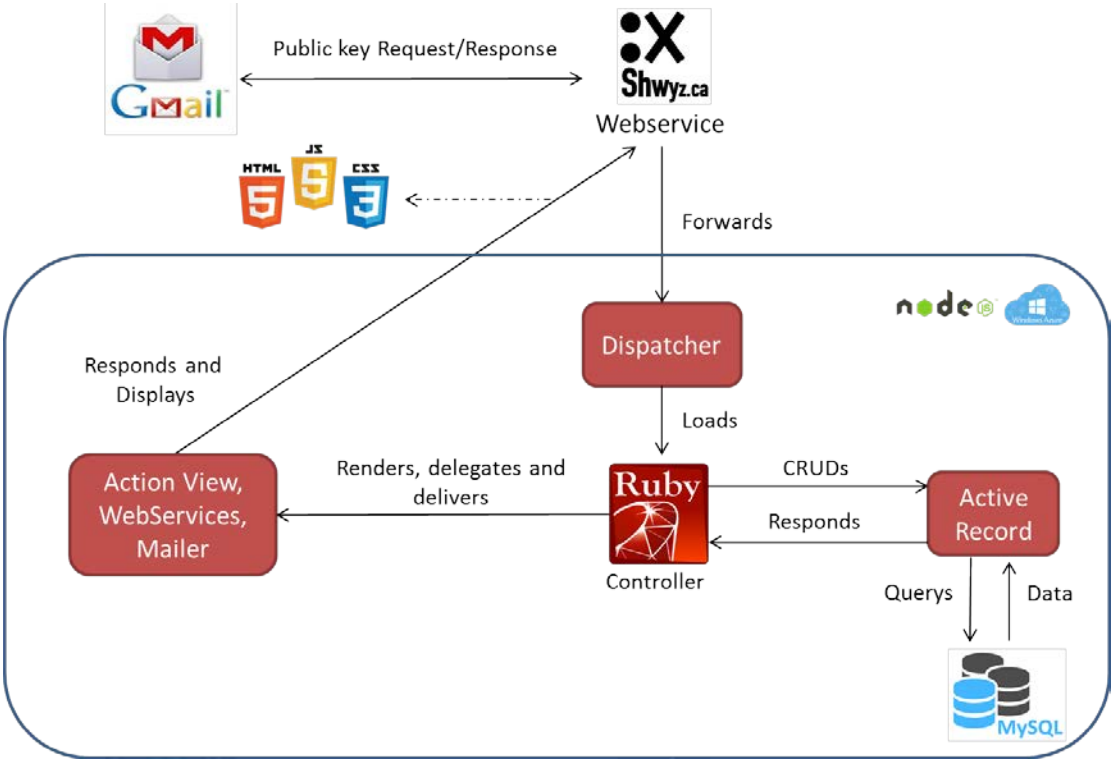


Figura 3.1: Arquitetura do Xmail

3.2 Usabilidade

O design do Xmail teve como principal objetivo a usabilidade e foi conduzido para abordar três desafios de Segurança Usável listados por Whitten e Tygar. Sendo eles, abstração, falta de *feedback* e usuário desmotivado (HECHT; FELS; ANACLETO, 2015). Esses desafios são tratados no design seguindo um conjunto de diretrizes (Tabela 3.1). A seguir, as diretrizes usadas para alcançar os desafios de Segurança Usável.

Tabela 3.1: Diretrizes de design do protótipo Xmail

Desafios de Whitten e Tygar	Diretrizes de Hecht et al.
Abstração	Manter os usuários seguros por padrão sempre que possível, eles não pesam sobre isso, é melhor deixa-los seguros.
Usuário desmotivado	Metáforas de uso com base em modelo mental dos usuários, em vez de detalhes técnicos.
	Não deixar a segurança distrair os usuários da sua tarefa principal.
Falta de feedback	Sempre informar o usuário sobre o status de segurança.
	Alertar os usuários sobre um risco potencial.

3.2.1 Abstração - Camada *Always-on Security*

Como visto anteriormente, os usuários não compartilham o mesmo nível de abstração dos designers e caso esta abstração não seja considerada, há um risco maximizado da interface não ser intuitiva. Para tentar solucionar este desafio, o protótipo Xmail propõe a camada ***Always-on Security.***

Always-on Security é uma camada de segurança *seamless* (não disruptiva) que se integra diretamente com o provedor de webmail Gmail e mantém o conteúdo do e-mail criptografado por padrão, ou seja, na medida em que os usuários vão escrevendo o conteúdo do e-mail esta camada é responsável por manter estas informações íntegras.

A Figura 3.2 mostra parte do modelo de tarefas da ferramenta Xmail usando a camada *Always-on Security,* modelada pelo modelo de tarefas CTT. Pode-se notar que a camada de segurança é criada antes de qualquer ação do usuário e se mantém em paralelo com a criptografia do conteúdo (usando o operador temporal |[]|) durante todo processo de escrita do e-mail. É possível notar também que mesmo que o usuário escolha a opção “envio sem segurança”, em qualquer momento da escrita do e-mail, a camada irá proteger os dados até o momento da ação “enviar e-mail”. Neste caso, antes do envio o e-mail será decriptografado e enviado aos destinatários.

3.2.2 Usuário desmotivado - Conceito *Seamless*

O conceito ***Seamless*** pode ser definido como sendo uma mudança não disruptiva, ou seja, uma mudança que não altera o fluxo natural (ou padrão) da

interface. Em segurança, tal conceito é, basicamente, utilizado para “esconder” funções e processos de segurança, de maneira que os usuários possam utilizar as ferramentas seguras de forma natural sem a preocupação com detalhes avançados de segurança.

No Xmail, este conceito é utilizado para tornar a camada *Always-on Security* não disruptiva e a experiência do usuário tão próxima quanto possível à experiência do Gmail. Como mostra a Figura 3.2, a maioria das alterações no design da interface padrão do Gmail envolvem o ator “aplicação”, ou seja, o protótipo se integra com a interface alterando o mínimo possível do fluxo natural do provedor.

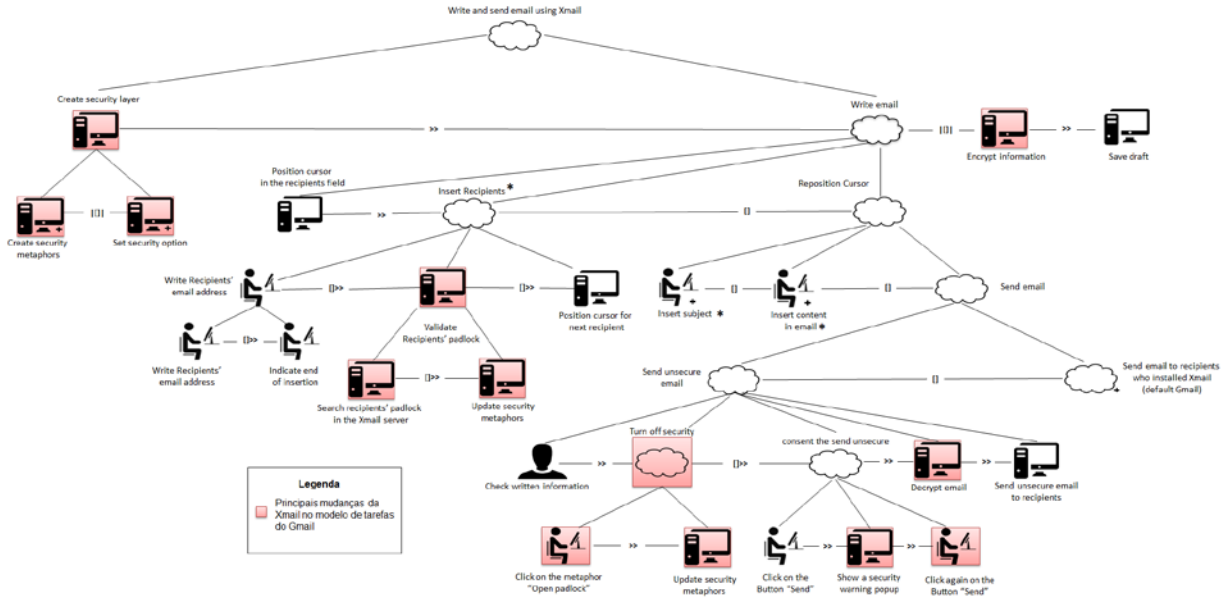


Figura 3.2: Parte do modelo de tarefas do Xmail destacando as principais mudança entre tal e o modelo do provedor Gmail (modelo completo https://goo.gl/xGQRRw)

3.2.3 Usuário desmotivado - Metáforas e Analogias

Como mencionado durante todo o texto, o Xmail busca aproximar a segurança de dados da usabilidade e, diferentemente da maioria das ferramentas de e-mails seguros, o protótipo informa aos usuários como funciona o processo de segurança utilizando analogias que se aproximam de suas experiências de vida. Ao invés de termos técnicos como, chaves públicas e privadas, certificados digitais e etc., o protótipo propõem analogias de “chaves” e “cadeados”.

No protótipo, os usuários que acessam pela primeira vez, são convidados a forjar uma “chave” e um “cadeado”, que, respectivamente, representam a chave pública e privada (Figura 3.3). Além disso, eles são informados que o envio de e-

mails é feito por meio do “cadeado” forjado, onde tais “cadeados” são distribuídos para os interlocutores e fechados com os segredos e, uma vez fechado, somente podem ser aberto pelo seu dono, ou seja, o usuário com a chave. A história canônica de Alice e Bob usando esta analogia é representada abaixo e ilustrada na Figura 3.4:

1. Imagine que Bob queira enviar um segredo para Alice e Eve é o provedor de e-mails que pode acessar todos os dados.
2. Bob solicita, por meio do Xmail, o cadeado aberto de Alice.
3. Após receber o cadeado de Alice, Bob trava seu segredo com o cadeado de Alice e envia de volta usando o serviço de entrega Eve.
4. Eve entrega o cadeado trancado para Alice.
5. Alice, com a sua chave, abre o cadeado e lê o conteúdo enviado por Bob.

Além das analogias, o protótipo propõem também as metáforas de segurança que basicamente traduzem as analogias para a interface e dão visibilidade do status de segurança do sistema. As Figura 3.5 e Figura 3.6 mostram as principais abordagens design adicionadas no design padrão do provedor.

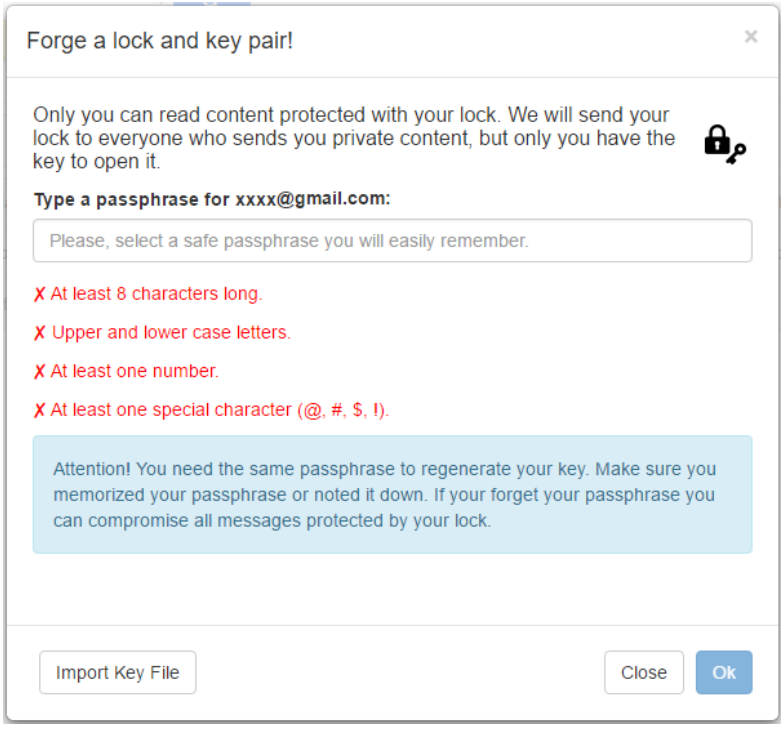


Figura 3.3: Criação da chave e cadeado no protótipo Xmail

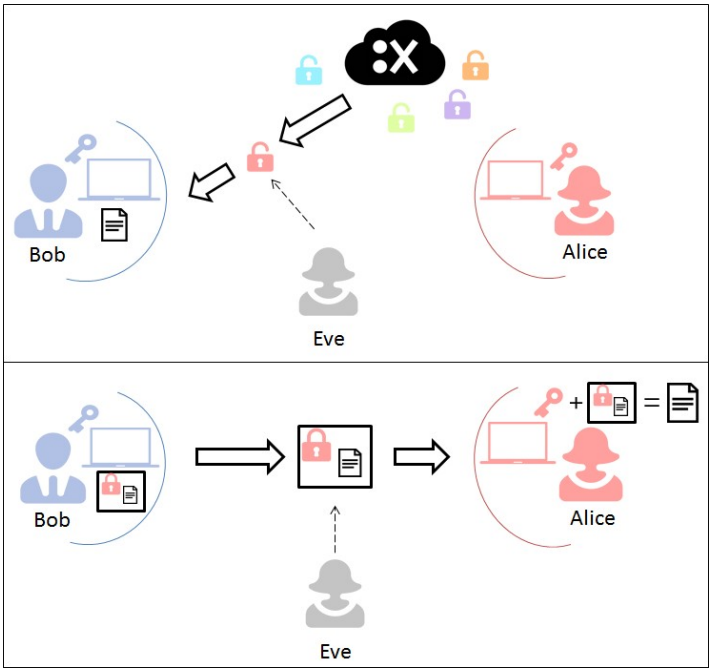


Figura 3.4: História canônica de Alice e Bob representando a analogia de troca de e-mails no Xmail

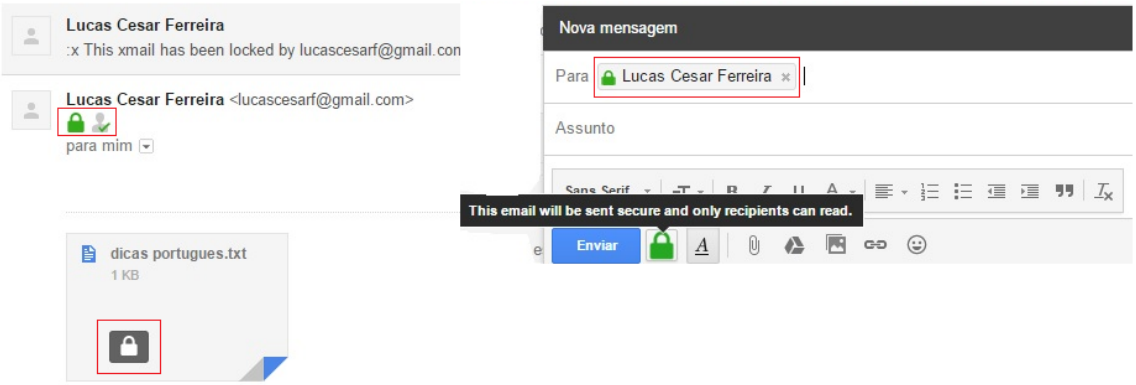


Figura 3.5: Metáforas de segurança adicionadas na interface padrão do Gmail

3.2.4 Falta de *Feedback*

Mediar entre oferecer e não oferecer *feedbacks* para os usuários em sistema interativo que promove segurança de dados é uma tarefa difícil. Para tratar esse desafio, o protótipo Xmail propõe *feedbacks* unindo metáforas visuais (seção anterior) e texto informativos e alertas.

Exemplos do uso desses alertas são mostrados na Figura 3.6. No primeiro caso, o destinatário ainda não possui um “cadeado” para ser distribuído e trancado com os segredos a serem enviados. Por isso, o protótipo avisa sobre o risco potencial e oferece a opção de convidar os destinatários. Já no segundo caso, o destinatário possui o “cadeado”, mas o usuário optou pelo envio sem segurança e,

neste caso, a ferramenta também informa o risco potencial e espera uma nova confirmação de envio.

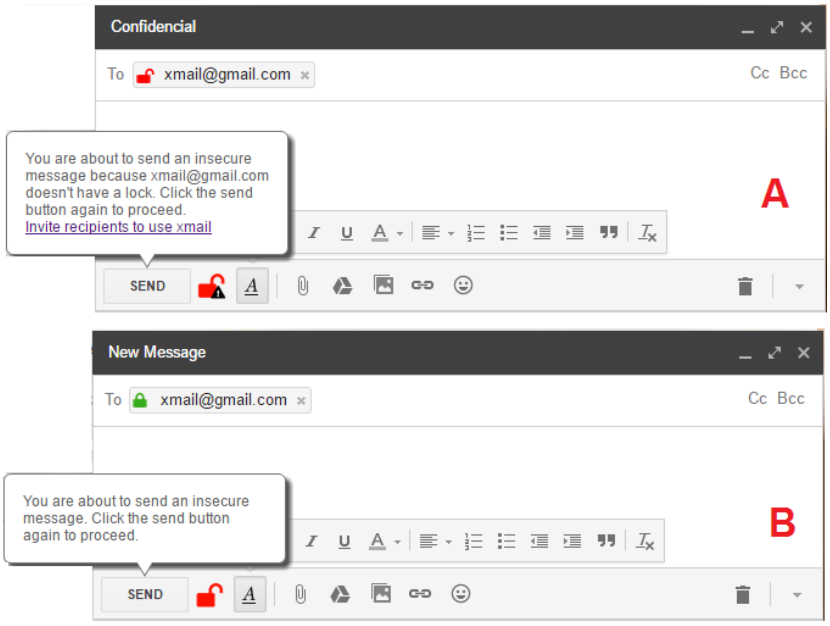


Figura 3.6: *Feedbacks* apresentados pelo protótipo Xmail informando um risco potencial

3.3 Considerações Finais

Neste capítulo, o protótipo de segurança Xmail, bem como sua arquitetura, principais conceitos e abordagens de design foram descritos e serviram de base para comparações e avaliações com os usuários nos próximos capítulos.

O capítulo seguinte é destinado a uma revisão das principais ferramentas e/ou protótipos que se assemelham com o Xmail ao promoverem segurança em e-mails. Nesse capítulo, serão apresentados estudos e acontecimentos que evidenciam a falta de privacidade dos usuários em serviços Web e, por fim, uma a revisão das principais ferramentas e suas principais características e abordagens de design.

Capítulo 4

REVISÃO DAS FERRAMENTAS

A adoção dos serviços em nuvem tem sido escolhida pelos usuários e cresce muito nos últimos anos (MCKENDRICK, 2016). No entanto, a segurança dos dados e a privacidade dos usuários é algo questionável em tais soluções, visto que é uma prática padrão de termos de uso de serviços na Web se garantirem o direito de modificar os próprios termos e coletar informações dos usuários.

Este capítulo tem por objetivo apresentar estudos e acontecimentos que evidenciam a falta de privacidade dos usuários em serviços Web e, também, uma revisão das principais ferramentas e/ou protótipos que fornecem segurança e privacidade em e-mails.

A organização deste capítulo segue da seguinte maneira: na Seção 4.1 são apresentados os casos que demonstram os problemas de Segurança da Informação e seus impactos. Na Seção 4.2 a revisão das ferramentas das principais ferramentas de e-mails seguros e, por fim, a Seção 4.3 apresenta as considerações finais do capítulo.

4.1 Segurança da Informação nos Últimos Anos

Para Sun Tzu, espionagem e vigilância de informações é a prática de obter dados de caráter sigiloso relativa a governos ou organizações, a fim de obter vantagens políticas, econômicas, científicas e/ou sociais (TZU, 1988). Essa prática não é incomum entre países em guerra ou mesmo em situações de paz. Nos últimos

anos, diversos casos de vazamento de informações e espionagem vieram à tona. Assim, esta seção tem por objetivo apresentar tais eventos e seus principais impactos.

4.1.1 Caso 1: Edward Snowden

Em Junho de 2013, o jornal britânico The Guardian publicou um dos maiores escândalos de espionagem doméstica e internacional envolvendo a National Security Agency (NSA) (GREENWALD; MACASKILL, 2013). Documentos confidenciais vazaram para o jornal através de Edward Snowden, um funcionário de uma empresa terceirizada alocado em projetos da NSA. Um dos principais documentos foi uma série de slides em PowerPoint que introduziam o programa PRISM. Um programa de vigilância digital que possibilitava a coleta de dados diretamente de servidores dos maiores provedores de serviços da internet, entre eles Google, Yahoo!, Microsoft, Facebook e Skype (Figura 4.1).

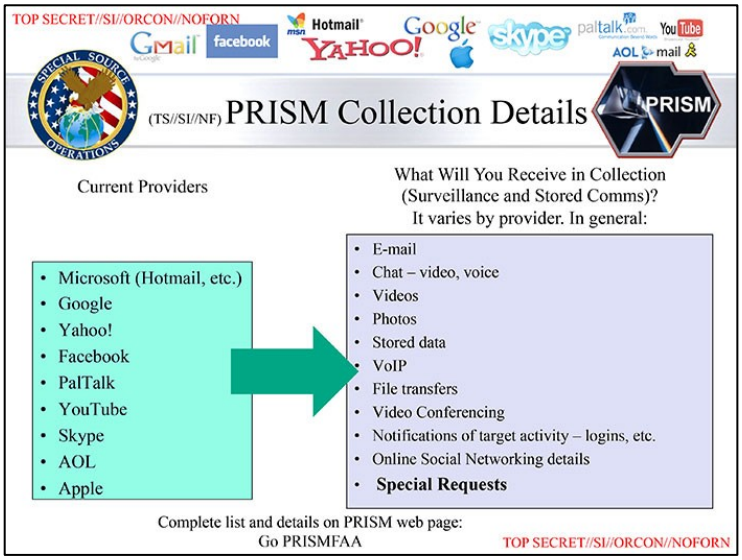


Figura 4.1: Slide do programa PRISM vazado em 2013 no jornal The Guardian

Não tardou até que novas revelações de Snowden denunciassem evidências de espionagem injustificáveis no âmbito da segurança pública, ficando claro que as práticas da agência de inteligência se estendem ao domínio de espionagem industrial, tendo como alvo empresas brasileiras, como a Petrobras (BCC, 2013). Essas revelações tiveram um enorme dano colateral econômico quando, em função dos casos de espionagem, a presidente Dilma Rousseff decidiu não fechar um

acordo de 4 bilhões de dólares com a empresa americana BOEING (WINTER, 2013).

4.1.2 Caso 2: Disputa de Criptografia entre Apple Inc. e FBI

Em Fevereiro de 2016 a Justiça Federal dos Estados Unidos ordenou a empresa Apple Inc. a quebrar a criptografia do seu aparelho iPhone. Em nota, o tribunal determinou que a empresa fornecesse ao Federal Bureau of Investigation (FBI) todas as informações necessárias do celular do atirador no caso de terrorismo em San Bernadinho em Dezembro de 2015.

A Apple se pronunciou dizendo que lamentava profundamente pelo ato terrorista, mas se recusaria a criar mecanismos para quebrar seu próprio sistema de segurança, justamente pelo fato da empresa ser referência em seus mecanismos de segurança (THIELMAN, 2016).

Novos pedidos foram feitos pelo FBI, exigindo até uma nova versão do sistema operacional da Apple, que pudesse descriptografar qualquer aparelho solicitado pela Justiça Federal, criando uma espécie de *"backdoor"* no sistema de segurança (THIELMAN, 2016). Após isso, o CEO da Apple, Tim Cook, publicou uma carta dizendo que a privacidade é um direito dos seus consumidores e não se oporia a essas condições do FBI (COOK, 2016).

Esta disputa gerou muita repercussão na internet envolvendo opiniões divididas, entre elas a opinião do Presidente Barack Obama, Mark Zuckerberg, Edward Snowden e John McAfee (THE GUARDIAN, 2016; JUNIOR, 2016; PAGLIERY, 2016).

4.1.3 Demais Casos

Com objetivo de adotar medidas contra o terrorismo, o Parlamento russo aprovou em Junho de 2016 a "*lei Yarovaya*", que obriga as operadoras de telefonia celular e internet a armazenarem todos os dados de comunicação durante seis meses e ajudarem nos serviços de decodificação de mensagens. (LUHN, 2016). Apesar da vigilância em massa parecer uma solução contra os problemas de segurança e terrorismo na Rússia, Edward Snowden acredita que essa solução não

funciona e viola os direitos de liberdade dos cidadãos sem melhora na segurança (SNOWDEN, 2016).

Semelhante à disputa da Apple e FBI mencionada acima, no Brasil em Dezembro de 2015, a Justiça brasileira intimou as principais operadoras de telefonia a suspenderem o aplicativo WhatsApp em todo território nacional por 48 horas. Tal suspensão foi devida ao descumprimento da empresa Facebook Inc. (empresa proprietária do WhatsApp) em compartilhar informações que ajudariam a Polícia Federal em investigações criminais. O processo se estendeu levando a deliberação de novas suspensões e até a prisão do vice-presidente do Facebook da América Latina, Diego Dzodan (GLOBO.COM, 2016).

4.2 Revisão das Ferramentas de E-mails Seguros

Como consequência dos casos de vigilância global e vazamento de informação, o conceito de Segurança da Informação tem ganhado mais evidência nos últimos anos e novas propostas computacionais para prover mais segurança e privacidade aos usuários têm surgido (Figura 4.2). Porém, como experienciado por Greenwald (GAYLE, 2014) conceber ferramentas seguras e também usáveis não é uma tarefa trivial, indo além das técnicas gerais de criptografia, arquitetura e engenharia, bem como design de softwares de segurança. É necessário o uso de abordagens específicas de usabilidade e segurança (WHITTEN; TYGAR, 1999).

Sendo assim, esta seção apresenta uma revisão das principais ferramentas de e-mail seguro, buscando verificar se a usabilidade delas é suficiente para o uso dos usuários comuns. Essa revisão é divida em quatro partes, sendo elas: (i) identificação das ferramentas; (ii) descrição e categorização das suas principais características; (iii) refinamento das ferramentas; (iv) percepção do usuários comuns e avaliação das ferramentas. Vale ressaltar que esta revisão se baseia nas *guidelines*, modelos de interação e desafios de Segurança Usável (ver Capítulo 2).

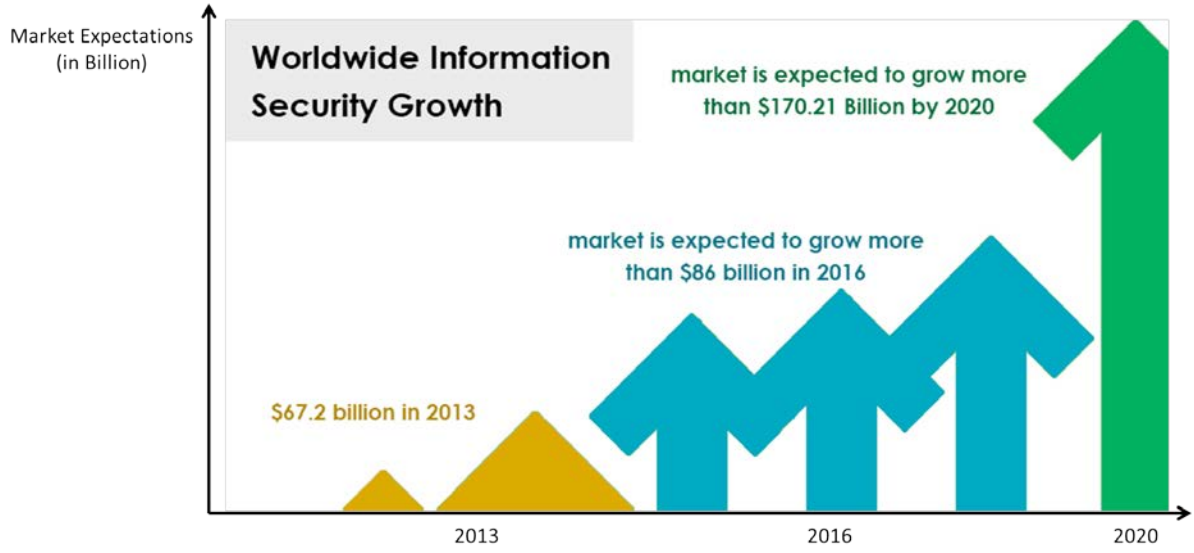


Figura 4.2: Crescimento do investimento em Segurança da Informação nos últimos anos (acesso em: https://goo.gl/uHys66)

4.2.1 Identificação das Ferramentas/Soluções de E-mail Seguros

A primeira etapa desta revisão consistiu na definição dos argumentos de busca pelos trabalhos científicos que tratam deste assunto (*string* de busca), baseando-se em palavras-chave que descrevem ferramentas/protótipos de segurança em e-mails e seus sinônimos. A *string* de busca utilizada para procurar tais ferramentas em diversos mecanismos de busca foi:

```
(("email encryption" OR "encrypted email" OR "safe email" OR "secure email"
OR "email security" OR "email safety") AND (usability OR usable) AND (tool
OR system OR solution OR implementation OR prototype) NOT (phishing))
```

Usando tal *string*, o resultado final de todas as buscas resultou em mais de 100 artigos científicos. No entanto, devido a grande maioria dos artigos estarem relacionadas aos métodos de segurança e suas possíveis melhorias, viu-se a necessidade de utilizar critérios de inclusão (I) e exclusão (E) que são apresentados a seguir:

- **I1.** Artigos publicados que apresentam, avaliam, ou implementam as ferramentas/soluções de e-mail seguro;
- **I2.** Artigos publicados somente em português e inglês;
- **I3.** Artigos publicados na área de informática ou afins;
- **E1.** Artigos publicados que tratam somente de novos métodos criptográficos ou a eficiência dos mesmos.

Além da procura nas bibliotecas digitais usando os motores acadêmicos (por exemplo, ACM, IEEE, Springer e Google Scholar) também foram feitas pesquisas

pela comunidade de segurança no site Quora[7], busca geral na internet e nas lojas de aplicativos e extensões.

Foram identificadas 11 ferramentas de que proveem segurança no envio de e-mails. Porém, vale mencionar que esta revisão não faz uma busca exaustiva às ferramentas disponíveis, mas apenas as principais soluções recomendadas pela comunidade e fóruns. A Tabela 4.1 mostra a lista de ferramentas identificadas.

Tabela 4.1: Soluções de e-mail seguro identificadas na revisão das ferramentas

Ferramentas			
1	Enlocked	7	SecureGmail
2	Jumble Mail	8	Startmail
3	Mailvelope	9	Tutanota
4	Private WebMail (Pwm)	10	Virtru
5	ProtonMail	11	Xmail
6	SCRYPTmail		

4.2.2 Introdução e Categorização das Soluções Selecionadas

Com objetivo de identificar as abordagens de design e as principais características de cada solução selecionada. Esta seção apresenta uma breve introdução (focada na usabilidade e percepção dos usuários) e uma categorização das principais características de cada solução identificada na Tabela 4.1.

4.2.2.1 Introdução e Abordagens de Design das Soluções Selecionadas

Cada ferramenta possui suas particularidades e abordagens de design diferentes para informar aos usuários sobre a segurança. Deste modo, cada uma dessas ferramentas e suas abordagens de design serão introduzidas, bem como as metáforas e analogias utilizadas por tais.

Vale mencionar que o protótipo Xmail já foi introduzido no Capitulo 3. Além disso, as soluções que são integradas aos provedores serviços mais convencionais (Gmail, Outlook e Yahoo!) serão comparadas com a interface padrão desses serviços, preferencialmente com o provedor Gmail (Figura 4.3).

[7] https://www.quora.com/

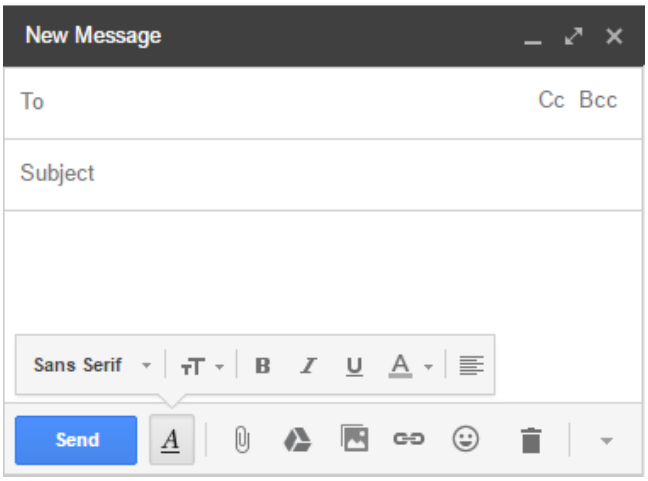


Figura 4.3: Interface padrão da janela de escrita e envio de e-mails do provedor Gmail usada para comparação com as ferramentas de extensão

1- Enlocked

Enlocked[8] é uma solução de e-mail criptográfico fundado em 2011 por uma equipe de tecnologia da informação e veteranos de segurança. Esta solução promove segurança e privacidade por meio da criptografia de chave pública e oferece duas opções de uso; i) integração direta com a interface dos provedores de e-mails convencionais (extensão); ii) provedor de e-mails totalmente desintegrado, usando o endereço de e-mail já existente.

Quando integrado com a interface do Gmail, o serviço faz pequenas mudanças, adicionando a opção de segurança através de um simples botão (Figura 4.4). No entanto, independente da opção de uso escolhida pelos usuários, todo processo de criação de senhas é feito fora da extensão (provedor da ferramenta).

2- Jumble Mail

Jumble Mail[9] é uma solução de e-mail seguro criada por Gavin Kearney e lançado no ano de 2014. Essa solução se integra com os provedores de e-mails convencionais, tanto na versão web quanto no software instalado. Jumble utiliza a criptografia de chave pública e o processo de criação de chaves é feito no website da ferramenta, entretanto, após a criação a distribuição e centralizada e não necessita de importações de chaves públicas. O status de segurança na Jumble é traduzido utilizando metáforas e modelo de cores, mas um novo fluxo é adicionado para a tarefa de enviar e-mails seguros, como mostra a Figura 4.5.

[8] https://www.enlocked.com/
[9] https://www.jumble.io/

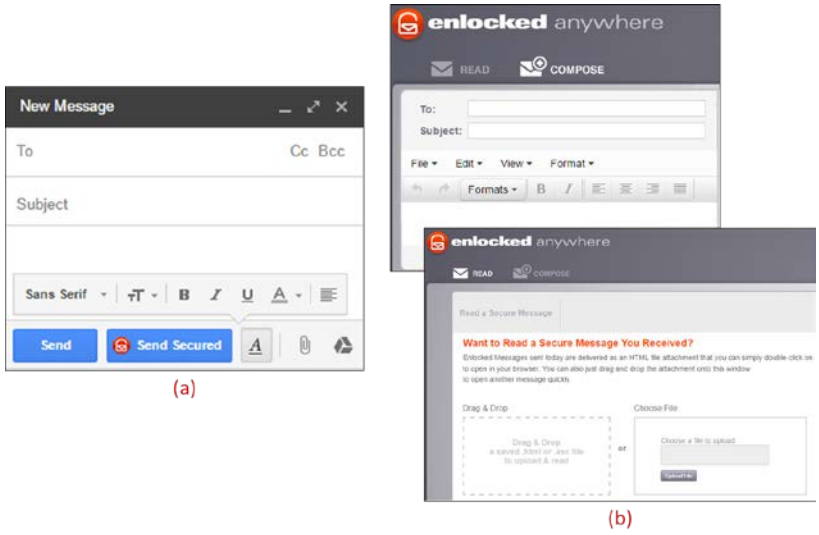


Figura 4.4: (a) Enlocked integrado a interface do Gmail e (b) como um provedor desintegrado

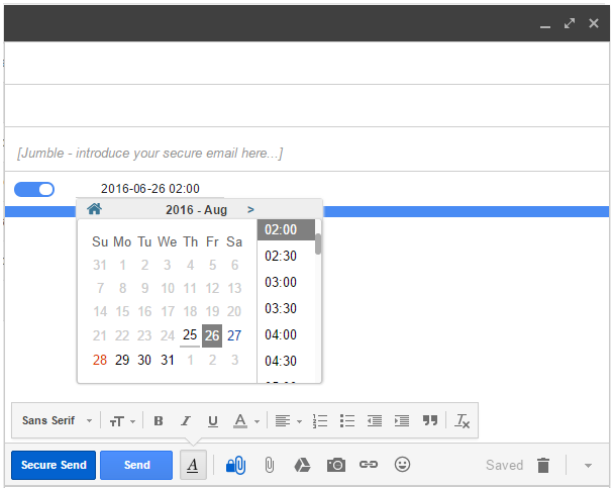


Figura 4.5: Abordagens de design da ferramenta Jumble Mail adicionadas na interface padrão do Gmail

3- Mailvelope

Mailvelope[10] é uma extensão dos browsers (Google Chorme e Firefox) criada por Thomas Oberndörfer e lançada no ano de 2012. Tal extensão se integra com a interface dos provedores de e-mails mais convencionais e promove segurança e privacidade aos usuários por meio da criptografia de chave pública. Apesar de possuir integração com os provedores, todo o processo de criação e gerenciamento das chaves é feito na própria extensão (fora dos provedores).

[10] https://www.mailvelope.com/

Na interface padrão do Gmail, a Mailvelope adiciona botões e metáforas que quando acionados abrem janelas (pop-ups) para a escrita do conteúdo. A Figura 4.6 mostra o fluxo de tarefas para o envio de e-mails seguros na extensão.

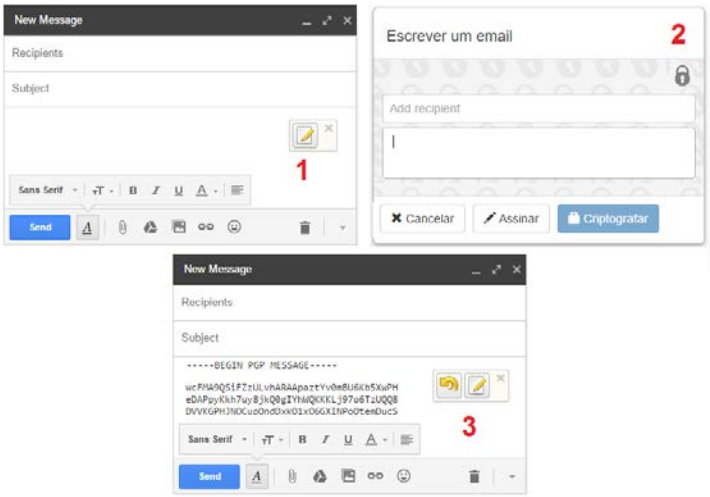


Figura 4.6: Fluxo de tarefa para enviar e-mails seguros usando Mailvelope no provedor de e-mails Gmail

4- *Private WebMail (Pwm)*

Private WebMail (Pwm)[11] é um protótipo de uma extensão do Google Chorme criada por Scott Routi et al. em 2013. Esse protótipo se integra com a interface do provedor Gmail e utiliza a criptografia de chave pública para promover privacidade e integridade na troca de e-mails (ROUTI et al., 2013). Pwm propõe um gerenciamento automatizado das chaves através de um servidor centralizado apoiado em sistemas criptográficos baseados em identidade (SCBI) (SHAMIR, 1985) possibilitando, o envio de e-mails para usuários que não possuem chaves registradas.

A usabilidade da ferramenta é baseada em modelo de cores, botões personalizados e *feedback* textuais que indicam o status do sistema. No entanto, como mostra a Figura 4.7, a interface é disruptiva e muda praticamente todo o design padrão do Gmail.

[11] https://pwm.byu.edu/home/

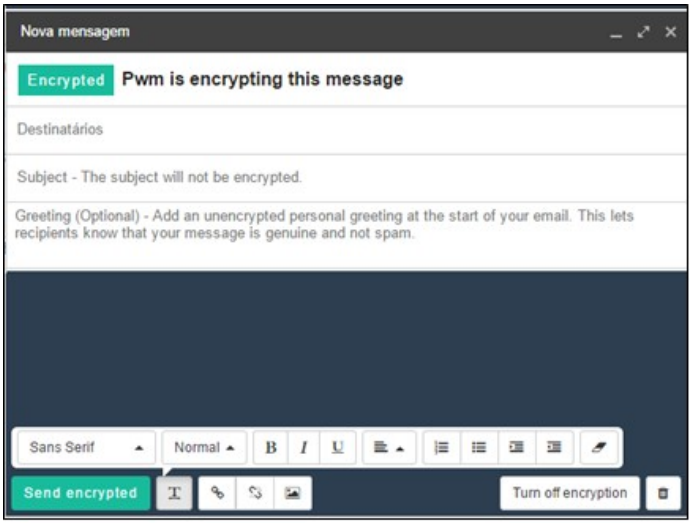


Figura 4.7: Interface da Pwm e suas modificações na interface padrão do Gmail

5- ProtonMail

ProtonMail[12] é um provedor de e-mails criptográfico criado por Jason Stockman et al. em 2013. Tal provedor é baseado na criptografia de chave pública e tem a usabilidade semelhante aos provedores mais convencionais (Figura 4.8). Para a segurança, o ProtonMail utiliza dois tipos de senhas: i) senha de acesso; ii) senha para a criação da chave pública e privada.

Por ser um provedor de e-mails seguro desenvolvido em um ambiente propício a segurança, o envio de e-mail entre usuários do ProtonMail segue o fluxo normal. No entanto, o envio de e-mails para outros domínios é feito por meio de uma senha previamente estabelecida entre as partes (criptografia simétrica).

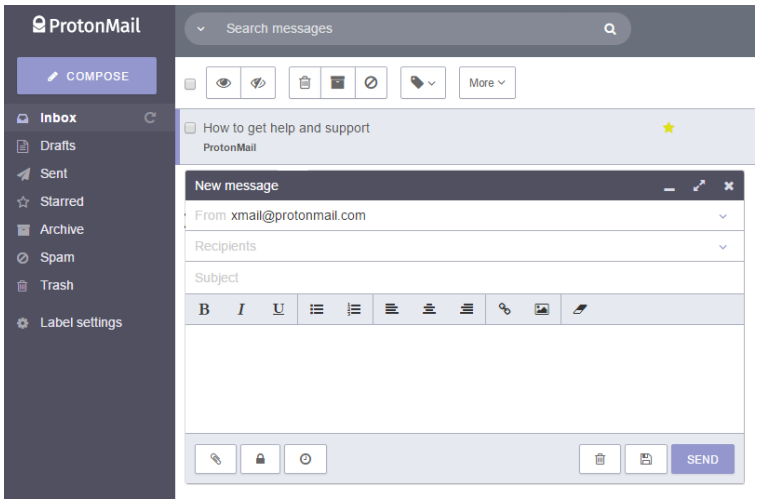


Figura 4.8: Interface de usuário do provedor de e-mails seguros ProtonMail

[12] https://protonmail.com

6- SCRYPTmail

SCRYPTmail[13] é um provedor de e-mail seguros criado por Sergei Krutov em 2014. Esse provedor se baseia na criptografia de chave pública para oferecer segurança e integridade aos seus usuários. Entretanto, como no caso do ProtonMail, os e-mails para o mesmo domínio são seguros por padrão, mas para outros domínios o envio é baseado em criptografia de chave simétrica com chave, ou seja, uma senha ou PIN previamente acordado. A Figura 4.9 a interface do SCRYPTmail, juntamente com o envio de e-mails para outros domínios.

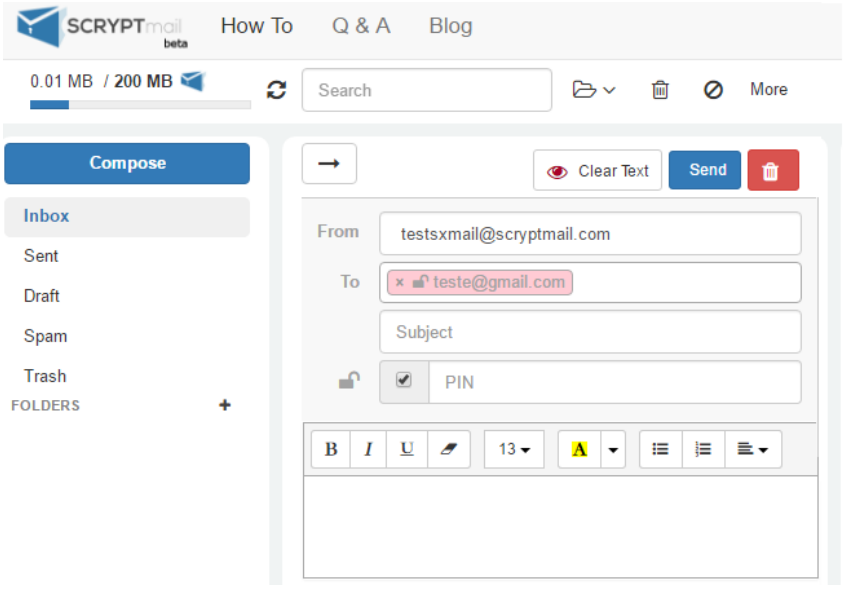


Figura 4.9: Interface do provedor SCRYPTmail e envio de e-mails para domínios externos

7- SecureGmail

SecureGmail[14] é uma extensão do Google Chorme criada pelo grupo Streal Inc. em 2014. Tal extensão se integra com a interface do provedor Gmail e utiliza criptografia simétrica para garantir a privacidade e segurança dos usuários. A extensão faz pequenas mudanças na interface padrão do Gmail, utilizando metáforas e modelo de cores para apresentar e diferenciar as opções seguras (Figura 4.10). Além disso, a extensão cifra todo o conteúdo do e-mail de forma "transparente" para os usuários, não alterando o fluxo de escrita padrão do Gmail.

[13] https://scryptmail.com/
[14] https://www.streak.com/securegmail

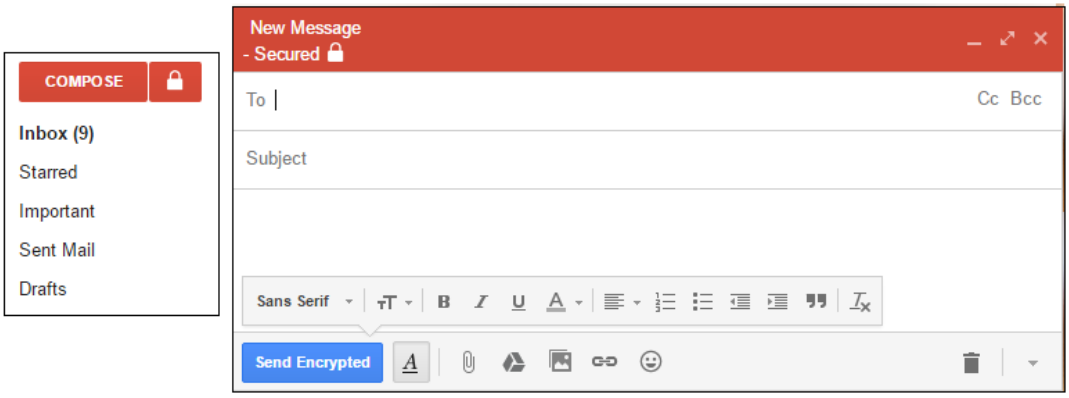


Figura 4.10: Metáforas e modelo de cores adicionados pela extensão SecureGmail na interface padrão do provedor Gmail

8- Startmail

Startmail[15] é um provedor de e-mails criptográficos proposto pelos grupos StartPage e Lxquick em 2005. Esse provedor utiliza a criptografia simétrica e, diferentemente dos provedores descritos anteriormente, para todos os e-mails seguros deve possuir uma pergunta e resposta pré-estabelecida entre os destinatários e o emissor.

Por motivos de licença, a ferramenta só pode ser testada na versão de teste. Tal versão possuiu um design mais "antigo", baseando-se em textos, botões comuns e *checkbox*. A Figura 4.11 mostra a interface do Startmail, juntamente com a inserção da pergunta e resposta.

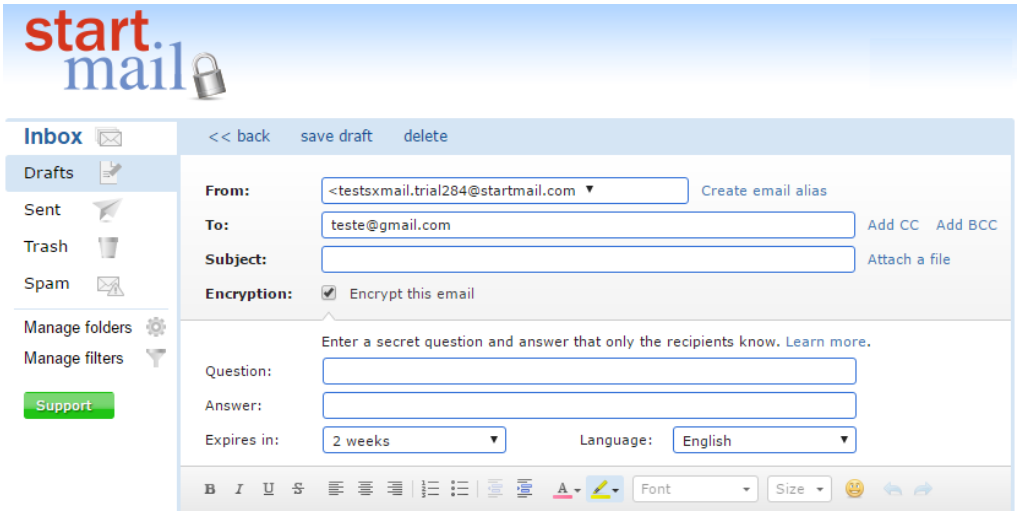


Figura 4.11: Interface e abordagem de segurança do provedor de e-mails seguros Starmail

[15] https://www.startmail.com

9- Tutanota

Tutanota[16] é um provedor de e-mail seguros criado por Matthias Pfau e Arne Möhle e lançado em 2011. Esse provedor fornece segurança e privacidade por meio da criptografia de chave pública e politicas de privacidade que asseguram a integridade de quaisquer dados dos usuários. Assim como o Protonmail, o Tutanota usa a segurança por padrão, porém nos casos de destinatários externos, o protótipo adota uma abordagem de senha previamente definida entre os interessados. O design da interface parece ser bem interativo e utiliza metáforas e *feedbacks* informativos para mostrar o status de segurança (Figura 4.12).

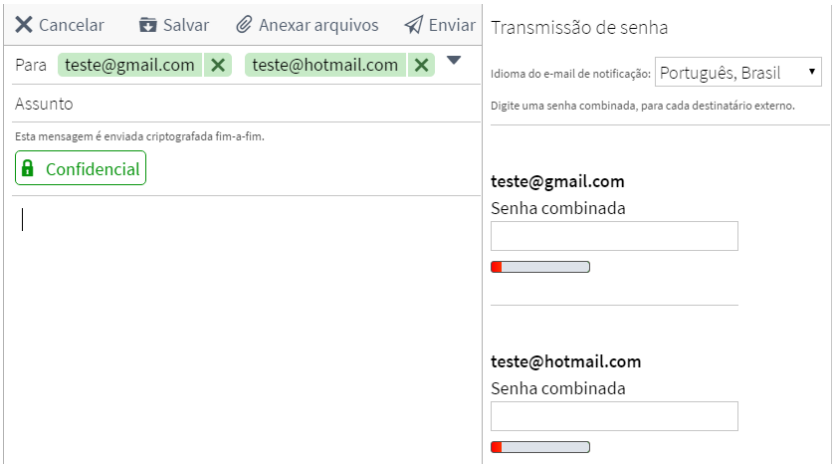


Figura 4.12: Interface e abordagem de segurança para não-clientes do provedor Tutanota

10- Virtru

Virtru[17] é uma solução de e-mail seguro criada pelos irmãos John e Will Ackerly em 2012. Esta solução oferece segurança e privacidade usando a criptografia simétrica, entretanto, o empoderamento da senha não fica com os usuários, ou seja, não precisam de um segredo previamente estabelecido, mas a percepção de segurança dos usuários pode ser duvidosa em relação à integridade dos dados.

Esta solução oferece opções de uso tanto para extensões, nos browsers Firefox e Google Chrome usando os provedores Gmail e Outlook, quanto para desktop e mobile em modo provedor. Usando o Virtru como extensão no Gmail, o design não expõe os usuários à criação de chaves ou senhas e utilizam modelos de

[16] https://tutanota.com
[17] https://www.virtru.com

cores, metáforas e *toogle switch* para indicar as opções de segurança na interface padrão do provedor Gmail (Figura 4.13).

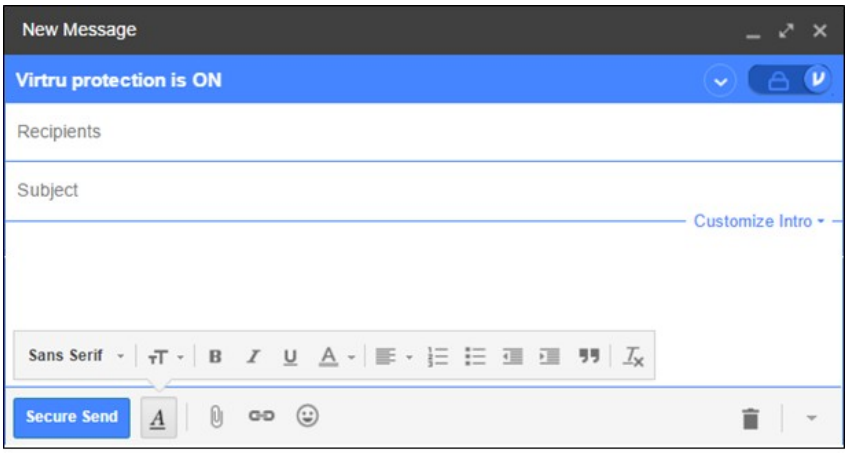


Figura 4.13: Abordagens de designs da solução Virtru inseridas na interface padrão do provedor Gmail

4.2.2.2 Categorização das Principais Características das Ferramentas Selecionadas

Após uma breve introdução de cada ferramenta e suas abordagens de design. Esta seção tem por objetivo categorizar as suas principais características, seguindo os critérios e suas descrições listados abaixo. O resultado desta categorização é apresentado na Tabela 4.2.

- **Tipo de Solução:** refere-se à técnica de implementação utilizada pela solução.
  - **Ex:** **Extensão/Plug-in**: a segurança dos dados é fornecida por meio de uma integração entre a solução e um provedor de e-mails já existente.
  - **Sç**: **Serviço privado:** a solução é um provedor de e-mail seguros totalmente desvinculado.
- **Maturidade:** referente à fase de desenvolvimento que a ferramenta se encontra:
  - **β:** **Beta:** a solução está em desenvolvimento, mas já existe uma versão disponível e pode ser avaliada.
  - **P:** **Produto:** ferramenta já consolidada, ou seja, solução pronta para uso e/ou comércio.

- **Comercialização:** como o serviço de e-mail seguro é oferecido em termos de comercialização:
    - **Tg: Totalmente gratuito.**
    - **Pg: Parcialmente gratuito:** a ferramenta pode ser utilizada de maneira gratuita, mas as funcionalidades são limitadas a versão.
    - **T: Teste:** licença gratuita somente para teste, expirando em um período determinado.
    - **Tp: Totalmente Pago.**
- **Disponibilidade do código:** disponibilidade do código fonte para acesso dos usuários:
    - **D: Disponível.**
    - **I: Indisponível.**
- **Gerenciamento da chave dos destinatários:** como a chave dos destinatários é gerenciada pela ferramenta (no nível de transparência aos usuários).
    - **A: Automático:** os usuários não precisam se preocupar em nenhum momento sobre as chaves dos destinatários.
    - **M: Manual:** os usuários precisam inserir manualmente as chaves dos destinatários.
    - **Ñ: Não se aplica:** ferramentas que usam a criptografia simétrica não precisam da gestão de chaves dos destinatários.
- **Empoderamento da criptografia:** refere-se à autonomia que as partes (aplicação e usuário) têm sobre o processo de cifragem.
    - **Fe: Ferramenta:** o processo é gerado automaticamente pela ferramenta e os usuários não possuem nenhum tipo de autonomia sobre ele.
    - **Uf: Usuário e ferramenta:** os usuários possuem “poder” no processo de criptografia, ou seja, todo o processo é baseado em uma senha/código que o usuário cria e a ferramenta não tem acesso.
- **Modelo de interação:** como a ferramenta se integra com os e-mails mais convencionais (RUOTI et al., 2016).

It: **Integrated:** ferramentas que se integram totalmente como a interface dos webmails convencionais (por exemplo, Gmail e Outlook).

Hy: **Hybrid:** ferramentas que se integram com os provedores convencionais e não necessitam de novos domínios. No entanto, realizam funções específicas fora da interface dos provedores.

Dp: **Depot-Based:** provedores de e-mail seguros totalmente desvinculados dos serviços convencionais.

Tabela 4.2: Categorização das principais características das ferramentas selecionadas

	Principais Características						
Ferramentas	Tipo de Solução	Maturidade	Comercialização	Disponibilidade do Código	Gerenciamento da chave dos destinatários	Empoderamento da criptografia	Modelo de Interação
Enlocked	Sç/Ex	P	Pg	I	A	Uf	Hy/Dp
Jumble Mail	Sç/Ex	P	Pg	I	A	Uf	Hy/Dp
Mailvelope	Ex	P	Tg	D	M	Uf	Hy
Private WebMail	Ex	β	Tg	I	A	Fe	It
ProtonMail	Sç	P	Pg	D	A	Uf	Dp
SCRYPTmail	Sç	P	T	I	A	Uf	Dp
SecureGmail	Ex	P	Tg	D	Ñ	Uf	It
Startmail	Sç	P	Pg	I	A	Uf	Dp
Tutanota	Sç	P	Pg	D	A	Uf	Dp
Virtru	Ex	P	Pg	I	A	Fe	Hy
Xmail	Ex	β	Tg	I	A	Uf	It

4.2.3 Refinamento das Ferramentas Selecionadas

A fim de identificar as ferramentas que mais se aproximam das diretivas de Segurança Usável e compreender os motivos de não adoção. Esta seção tem como objetivo refinar o conjunto de ferramentas, apoiando-se nos estudos que explicitam a ineficiência dos modelos que exigem carga extra de trabalho e/ou esforço cognitivo

excessivo dos usuários. Assim, este refinamento usa os modelo de interação e os estudos sobre gerenciamento de chaves (ver Capítulo 2). Abaixo são mostradas as ferramentas e as diretivas feridas, bem como o resultado na Tabela 4.3.

- **Mailvelope: Gerenciamento manual de chaves**

  Ferramentas que adotam o gerenciamento manual de chaves dificilmente serão usadas pela maioria dos usuários, visto que elas exigem um grande esforço cognitivo dos usuários que não possuem conhecimento de criptografia.

- **ProntonMail, SCRYPTmail, Startmail, Tutanota: Modelo de interação**

  Os usuários tendem a se interessarem por ferramentas que não quebram o fluxo normal de suas atividades rotineiras e optam por soluções de segurança de e-mails que estão integradas com seus serviços convencionais (ROUTI et al., 2016). Sendo assim, as ferramentas baseadas em *Depot-Based* também foram filtradas.

Tabela 4.3: Ferramentas selecionadas após o refinamento

Ferramentas			
1	Enlocked	4	SecureGmail
2	Jumble Mail	5	Virtru
3	Private WebMail (Pwm)	6	Xmail

4.2.4 Percepção dos Usuários Comuns e Avaliação das Ferramentas

Após o refinamento das ferramentas, viu-se a necessidade de compreender melhor suas abordagens de design e a Imagem do Sistema proposta. Sendo assim, esta seção buscou compreender a percepção dos usuários em uso de cada ferramenta, usando a Imagem do Sistema consolidada do provedor Gmail como base para a criação dos modelos de cada ferramenta. Os modelos criados para as ferramentas filtradas são apresentados, seguidos de uma avaliação analítica que verificou a conformidade delas com as *guidelines* e desafios de Segurança Usável.

4.2.4.1 Imagem do Sistema das Ferramentas Filtradas

Com o objetivo de se obter um modelo consolidado e que possa ser usado como referência e devido a todas as ferramentas serem uma extensão do provedor Gmail. Foi criado o modelo de tarefas do Gmail para as tarefas de escrita e envio de

e-mails e, em seguida, baseando-se em tal modelo foram criados os modelos de tarefas de cada ferramenta (Figura 4.14).

Vale ressaltar que os modelos criados para as ferramentas buscam entender as ações críticas providas por cada ferramenta e como tais ações impactam no design padrão do provedor Gmail. Sendo assim, como podemos observar na introdução das ferramentas e categorização, as ferramentas Enlocked, Jumble Mail, Pwm e Virtru se diferem em alguns artefatos de design, mas utilizam ações muito semelhantes para prover segurança e privacidade no envio de e-mail e, por isso, os modelos de tarefas das ferramentas foram unificados. As Figura 4.15 e Figura 4.16 mostram os modelos de tarefas de cada ferramenta, destacando as principais diferenças sobre o modelo do Gmail (para a ferramenta Xmail, o modelo já foi apresentado na Figura 3.2).

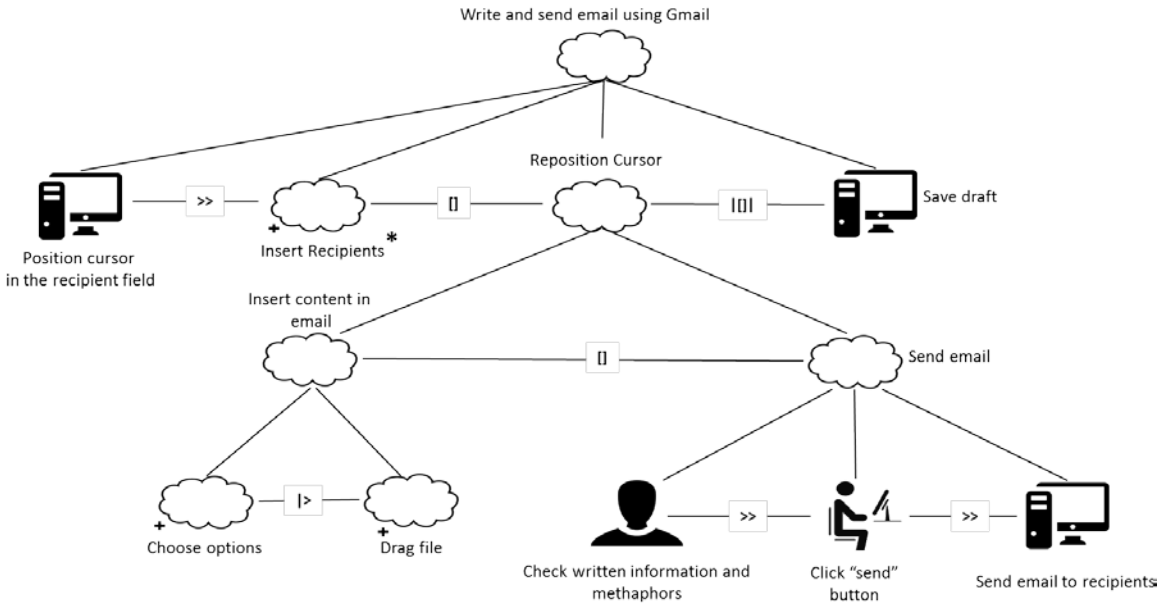


Figura 4.14: Modelo de tarefas genérico do provedor Gmail da tarefa "escrever e enviar e-mail" usando CTT.

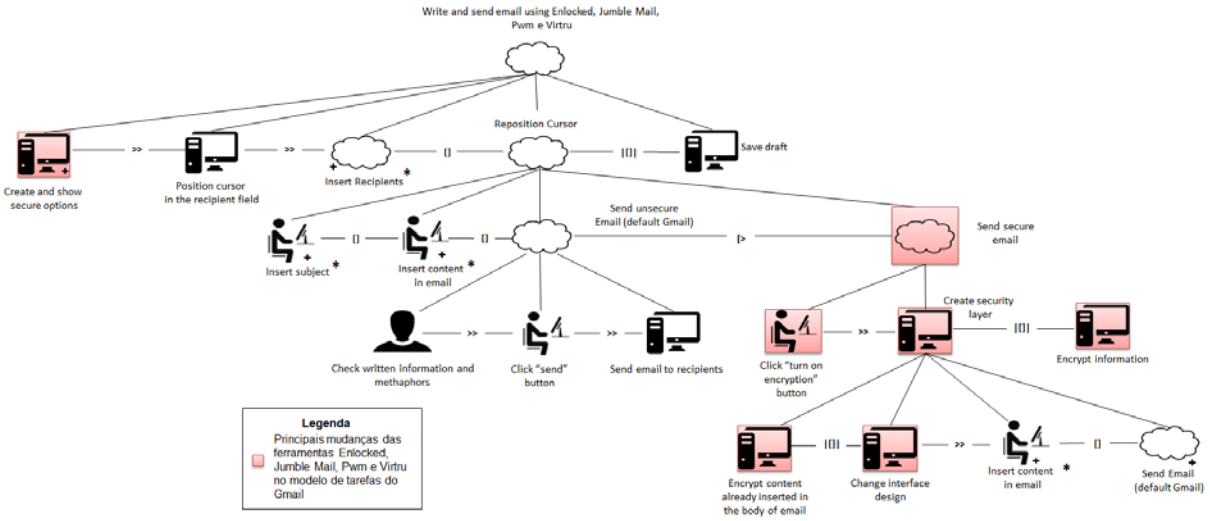


Figura 4.15: Modelo de tarefas das ferramentas Enclocked, Jumble Mail, Pwm e Virtru destacando as principais diferenças entre tais e o modelo do provedor Gmail (melhor qualidade: https://goo.gl/xGQRRw)

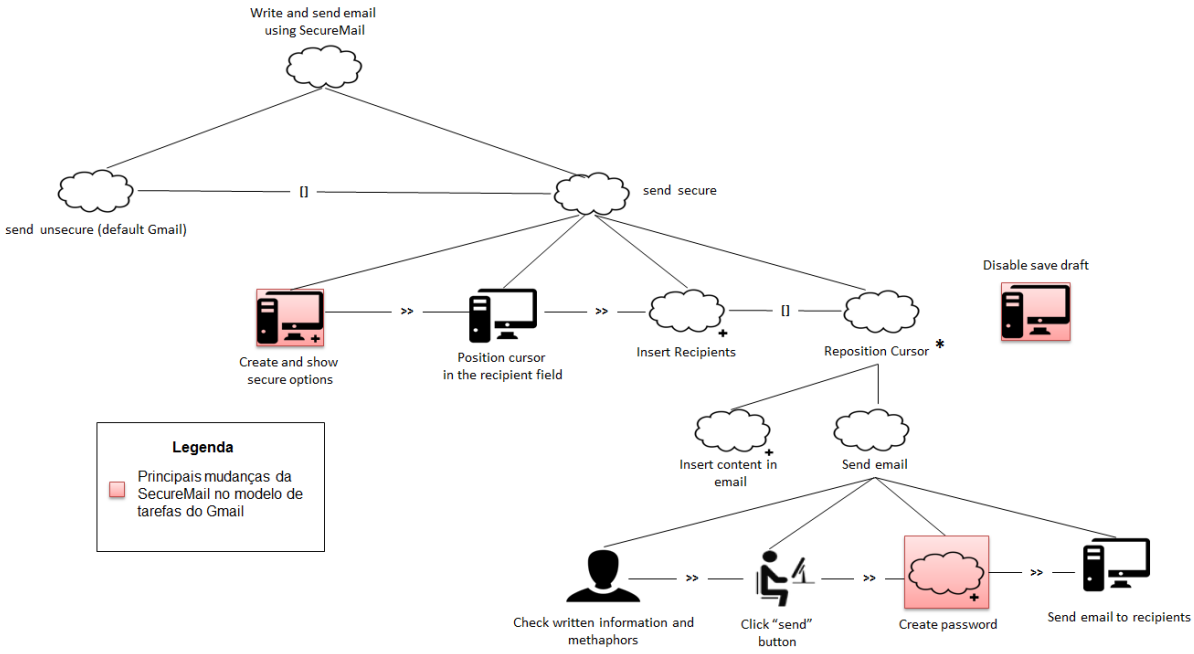


Figura 4.16: Modelo de tarefas da ferramenta SecureMail destacando as principais diferenças entre tal e o modelo do provedor Gmail (melhor qualidade: https://goo.gl/xGQRRw)

4.2.4.2 Avaliação de Usabilidade e Segurança das Ferramentas Filtradas

Segundo Whitten, um sistema interativo é seguro e usável se os seus usuários estão cientes das tarefas de segurança que precisam executar e são capazes de descobrir como executar tais tarefas com êxito (WHITTEN; TYGAR, 1999). Sendo assim, nesta seção foi feita uma avaliação analítica para cada ferramenta, usando as principais características (ver Seção 4.2.2) e modelos (ver

Seção 4.2.4.1), com intuito de verificar se tais ferramentas estão em conformidade com as *guidelines* e desafios de Segurança Usável.

Vale ressaltar que as análises feitas para cada ferramenta levaram em consideração as funcionalidade e características percebidas em seu uso e documentações disponíveis, assim detalhes técnicos (não documentados), bem como algoritmos de criptografias usados em suas concepções não foram considerados. Além disso, verificou-se que alguns desafios e *guidelines* se complementam e, por isso, foram combinados em apenas um tópico de avaliação. Os resultados da avaliação, mostrando as *guidelines* e os desafios violados pelas ferramentas são detalhados abaixo, bem como na Tabela 4.4.

Caminho de menor resistência e Usuário desmotivado

- **Enlocked, Jumble Mail, Private WebMail, Secure Gmail e Virtru**
  Observando os modelos e as interfaces das ferramentas pode-se perceber que as ferramentas criam um “caminho alternativo” na interface para envio de e-mails seguros.

Limites relevantes

- **Enlocked e Jumble Mail**
  Apesar de as ferramentas serem uma extensão do Google Chrome, todo o processo de criação de senhas é descentralizado e feito no website da ferramenta com termos técnicos e etapas confusas.

Autorização explícita

- **Private WebMail e Virtru**
  Como mostrado Tabela 4.2, as ferramentas Pwm e Virtru não explicitam como a segurança é alcançada e os usuários não tem “poder” sobre tal processo.
- **Xmail**
  Apesar de a ferramenta prover empoderamento aos seus usuários, a segurança é tratada como padrão sem uma autorização explicita dos usuários sobre este processo.

Revogabilidade

- **Secure Gmail**

  O modelo da ferramenta complementado pela sua interface (Figura 4.10) mostra que a ferramenta trata o envio de e-mails seguros e não seguros de forma totalmente distinta e, por isso, a ferramenta não permite a revogabilidade quando uma das opções é escolhida.

Falsa expectativa

- **Xmail**

  A Xmail utiliza a camada de segurança por padrão, no entanto, quando os destinatários não possuem a extensão o status da ferramenta fica “inseguro”, gerando uma falsa expectativa de segurança.
- **Secure Gmail**

  Por ser um produto já consolidado (Tabela 4.2) algumas funcionalidades do provedor Gmail estão indisponíveis para envio de e-mails seguros.

Caminho confiável

- **Private WebMail e Virtru**

  As ferramentas não empoderam os usuários no processo de segurança e não explicitam como atingem tal processo. Dito isso, não é possível “confiar” que a mensagem é *end-to-end*.

Porteira aberta

- **Enlocked, Jumble Mail, Private WebMail e Virtru**

  É possível notar nos modelos de cada ferramenta (ver Seção 4.2.4.1) que a cifragem total do conteúdo do e-mail só é garantida após a seleção da opção segura e, por isso, as ferramentas não podem garantir a integridade do e-mail nesses casos.

Identificabilidade

- **Xmail**

  A ferramenta depende muito do entendimento explícito das metáforas e feedbacks e, em alguns casos, as ineficiências de design (ícones que se escondem rapidamente) não contribuem para tal entendimento.

Elo mais fraco

- **Enlocked, Jumble Mail, Private WebMail, Secure Gmail, Virtru e Xmail**
  Quando se trata de orientação aos usuários e como seus “segredos” devem ser guardados, todas as ferramentas não possuem abordagens para este desafio.

Expressividade e Abstração

- **Private WebMail e SecureGmail**
  As ferramentas usam termos técnicos *("send encrypted" and "cryptographic password"*) que, possivelmente, estão em um nível muito abstrato para os usuários comuns.

Clareza e falta de feedback

- **Enlocked, Jumble Mail, Private WebMail e Virtru**
  O potencial risco mencionado no tópico da porteira aberta, não é explicitado aos usuários deixando-os vulneráveis a erros comprometedores.

4.3 Considerações Finais

Neste capítulo, foram apresentados estudos e acontecimentos que evidenciam a falta de privacidade dos usuários na Web. Além disso, uma revisão e avaliação das principais ferramentas e/ou protótipo que propõem segurança no envio de e-mails.

Os resultados deste capítulo apontam que as ferramentas de e-mails seguros têm melhorado significativamente a sua usabilidade, em relação às ferramentas listadas anteriormente na literatura (ver Seção 2.3.3.2), e já possuem resultados significativos em direção da segurança usável (Tabela 4.4). Entretanto, ainda tratam a segurança como algo “alternativo” e não proveem abordagem para orientar os usuários sobre os ricos potenciais. Sendo assim, os capítulos posteriores são destinados a uma avaliação de usabilidade mais profunda, usando duas das ferramentas mencionadas anteriormente. No próximo capítulo, será apresentado todo o planejamento, bem como o experimento envolvendo usuários.

Tabela 4.4: Conformidade das ferramentas com as problemáticas e *guidelines* de Segurança Usável

			Ferramentas Selecionadas					
			Enlocked	Jumble Mail	Private WebMail	Secure Gmail	Virtru	Xmail
Guidelines (Yee, 2002)	Challenges (Whitten; Tygar, 1999)	Caminho de menor resistência	✘	✘	✘	✘	✘	✓
		Usuário desmotivado						
		Limites relevantes	✘	✘	✓	✓	✓	✓
		Autorização explícita	✓	✓	✘	✘	✘	✘
		Visibilidade	✓	✓	✓	✓	✓	✓
		Revogabilidade	✓	✓	✓	✘	✓	✓
		Falsa expectativa	✓	✓	✓	✘	✓	✘
		Caminho confiável	✓	✓	✘	✓	✘	✓
		Porteira aberta	✘	✘	✘	✓	✘	✓
		Identificabilidade	✓	✓	✓	✓	✓	✘
		Elo mais fraco	✘	✘	✘	✘	✘	✘
		Expressividade	✓	✓	✘	✘	✓	✓
		Abstração						
		Clareza	✘	✘	✘	✓	✘	✓
		Falta de feedback						

Capítulo 5

AVALIAÇÃO DE USABILIDADE

Com objetivo de extrair evidências qualitativas, compreender a percepção dos usuários comuns durante o uso de ferramentas seguras e validar a proximidade dos seus modelos mentais ao modelo de tarefa proposto pela ferramenta. Este trabalho apresenta uma avaliação de usabilidade dos protótipos Xmail (LIA) e Pwm, por meio do método empírico de Teste de Usabilidade.

O Teste de Usabilidade é um método empírico que avalia a usabilidade de um sistema interativo a partir de experiências de uso dos usuários-alvo (RUBIN, 1994). A partir de objetivos e critérios de medição previamente estabelecidos, um grupo de usuários é convidado a realizar um conjunto de tarefas usando o sistema interativo em laboratórios específicos ou no ambiente real em que o software é utilizado. Durante toda a avaliação, observações são realizadas com o objetivo de coletar dados sobre o desempenho dos participantes na realização das tarefas (NIELSEN, 1993). Além do teste de usabilidade, adotou-se também a avaliação em pares de amigos, onde as tarefas são feitas exclusivamente por pessoas previamente conhecidas, tornando ambiente mais natural e descontraído (ROUTI et al., 2016).

Para a realização deste estudo, foi definido um planejamento de execução que abrange desde a escolha do local até os métodos de coleta de dados no estudo. A Seção 5.1 explica todo o planejamento desde escolha de local, aspectos éticos até cenários e tarefas. A Seção 5.2 apresenta o experimento e a coleta de dados e, por fim, as considerações finais na Seção 5.3.

5.1 Planejamento

Com objetivo de testar tanto a instalação e configuração quanto simular o uso em regime das ferramentas. Esta avaliação foi dividida em duas partes:

1) Instalação e configuração: avaliar se usabilidade e as abordagens de design (por exemplo, metáforas e feedback) das ferramentas são suficientes para os usuários concluírem a instalação, configuração e o envio do primeiro e-mail seguro sem cometer erros que comprometem a integridade da mensagem;

2) uso em regime: simular o uso rotineiro das ferramentas. Nesta parte, foram criados cenários e, a partir disso, e-mails foram trocados intercalando entre e-mails seguros e não seguros. Esta troca de e-mails serviu para identificar se o envio de e-mails seguros em rotina é viável ou não para os usuários.

5.1.1 Local de Estudo

O local escolhido para realizar o presente estudo foi o Laboratório de Interação Avançada no Departamento de Computação da UFSCar. Este local foi escolhido porque o teste demandava um ambiente controlado com equipamentos e estrutura.

5.1.2 Aspectos Éticos na Pesquisa

Atendendo ao rigor ético e científico o projeto de pesquisa foi encaminhado ao Comitê de Ética em Pesquisa em Seres Humanos da Universidade Federal de São Carlos para apreciação de acordo com as recomendações da Resolução 466/12 do Conselho Nacional de Saúde do Ministério de Saúde. O projeto foi aprovado e certificado pelo número CAAE: 68941717.5.0000.5504.

5.1.3 Coordenadores e Observadores

Para esta avaliação foi criado um grupo de 2 observadores e um coordenador geral do curso. Os observadores tiveram como principal objetivo coletar o comportamento dos usuários no uso das ferramentas enquanto o coordenador foi responsável por todo o planejamento e andamento dos testes, bem como o recrutamento, a apresentação do ambiente e o andamento do experimento.

5.1.4 Recrutamento e Critérios de Inclusão e Exclusão

Como parte do objetivo de recrutar usuários com perfis variados, a divulgação foi feita por meio de folders publicados nas listas dos departamentos da UFSCar, nos grupos do Facebook e colado em lugares estratégicos da universidade (como por exemplo, biblioteca, restaurante universitário, SIn e ATs) .

Os folders (APÊNDICE D) tinham um breve resumo da avaliação, local, tempo estimado e endereço do site de reservas de horários[18]. As opções de reservas ficaram disponíveis por duas semanas com a disponibilidade de horários durante o horário comercial (8:00 às 18:00), mas houve exceções para atender alguns participantes. Para efetuar as reservas os voluntários precisaram indicar um amigo e inserir os endereços de e-mails de ambos, bem como o nome. Vale ressaltar que tais informações foram usadas somente para o envio dos resultados e não foram consideradas na análise dos dados.

Alguns critérios de inclusão e exclusão também foram estabelecidos. Para participar do teste, além da indicação obrigatória de amigo para fazer par, os voluntários precisavam possuir contas no provedor de e-mail Gmail e consentirem com o Termo de Consentimento Livre e Esclarecido (APÊNDICE A).

5.1.5 Cenários e Tarefas

Como mencionado, a avaliação foi dividida em duas partes, sendo a primeira para testar a instalação, configuração e envio simples de e-mails e a segunda para simular o uso em regime das ferramentas. Vale ressaltar que em ambas as partes os usuários não tiveram instruções explicitas do funcionamento das ferramentas, mas

[18] https://youcanbook.me/

tiveram liberdade para explorar as informações fornecidas por tais. Esta prática foi adotada para simular uma situação real. Os cenários e tarefas de cada parte são descritos a seguir.

Parte 1 – Instalação e Configuração

- **Cenário:** "Joãozinho (Pessoa A ou emissor) precisa de ajuda para preparar seus débitos de impostos de renda deste ano e enviá-los corretamente para Receita Federal. Porém, Joãozinho não tem expertise nesta prestação e contas e decide pedir ajuda para Mariazinha (Pessoa B ou receptor), sua amiga que acabou de se formar em contabilidade e está trabalhando em um escritório contábil famoso na região. Joãozinho entra em contato com Mariazinha e a mesma pede para ele enviar, por e-mail, alguns documentos particulares, como Cadastro de Pessoa Física (CPF) e o número do recibo da última Declaração do Imposto de Renda de Pessoa Física (DIRPF). Visto que essas informações são particulares de Joãozinho, a comunicação entre os amigos deve ser segura e privada".
- **Tarefas:**
    1. Joãozinho (Pessoa A) precisa enviar um e-mail seguro com o número do recibo da última Declaração do Imposto de Renda de Pessoa Física (DIRPF) e seu Cadastro de Pessoa Física (CPF) para Mariazinha (Pessoa B).
    2. Mariazinha (Pessoa B) responde o e-mail seguro enviando o novo DIRPF para Joãozinho (Pessoa A).
    3. Joãozinho (Pessoa A) responde o e-mail seguro agradecendo e confirmando o recebimento.

Parte 2 – Uso em Regime

- **Cenário:** Foram criados no momento do teste, ou seja, o interlocutor conversava com os participantes e escolhia um cenário comum e, a partir disso, iniciava a troca de e-mail com os participantes. Em casos em que os cenários não vinham à tona, o interlocutor usava cenários previamente estabelecidos.
- **Tarefas:** Trocar, em média, 7 e-mails intercalando entre e-mails seguros e não seguros.

5.2 Experimento e Coleta de Dados

Na chegada ao laboratório de testes, o par de participantes foi apresentado ao ambiente de teste, ao coordenador do estudo, aos observadores e a uma breve descrição do projeto, bem como os objetivos da pesquisa. Depois, o par foi solicitado a ler, juntamente com o coordenador, as Instruções e o Termo de Consentimento e, caso concordassem, eram solicitados que o assinassem.

Após a assinatura do termo, o coordenador escolheu a função de cada participante na avaliação (emissor ou receptor), a ordem das ferramentas a serem testadas e solicitou aos mesmos que sentassem em seus respectivos lugares e preenchessem o pré-questionário, usando os notebooks “limpos” para o teste. Logo após o preenchimento, o coordenador introduziu a primeira parte da avaliação. Nesta etapa, o participante A (emissor ou Pessoa A) seguiu com a avaliação de instalação e configuração enquanto o participante B (receptor ou Pessoa B) esperou pelo e-mail do amigo (nesses momentos, os participantes tinham autonomia para navegar na Web). Após o participante B receber e-mail, o mesmo seguiu com o teste enquanto o participante A esperava o confirmação. Esse processo se repetiu até o termino das tarefas e durante todo este período de teste os observadores deveriam anotar os problemas de usabilidade encontrados e os comentários pertinentes dos participantes.

Com a primeira parte da avaliação concluída e com a ferramenta instalada nos computadores dos participantes, o coordenador deu início à segunda etapa do teste. Nesta etapa, o coordenador iniciou a troca de e-mails, usando o cenário previamente escolhido, onde tinha a responsabilidade de intercalar entre o envio seguro e inseguro de e-mails, manter a troca de e-mails entre os participantes (em média, doze e-mails foram trocados) e estimular os participantes na troca de e-mails. Após concluírem esta parte, o coordenador “limpava” os dados da primeira ferramenta e o processo se repetia para a segunda ferramenta.

Vale ressaltar que o tempo total de estudo foi medido a partir do momento em que o participante recebeu a autorização para iniciar a primeira etapa até o final da segunda. No entanto, o tempo de “espera pelos e-mails” foi descontado. Além disso, toda a interação do usuário com o teclado e mouse, bem como todos os comentários

feitos durante a realização do estudo, expressões e possíveis erros foram registrados pelo software Camtasia[19].

Ao término do teste, os participantes foram solicitados a responder o pós-questionário para coleta de opiniões dos usuários quanto à facilidade de uso, percepção de segurança e adoção das ferramentas. Por fim, cada participante escolheu um brinde pela sua participação e recebeu os agradecimentos de todo o grupo.

A Tabela 5.1, resume os dados coletados, juntamente com os tipos de instrumentos para a coleta.

Tabela 5.1: Dados coletados no teste de usabilidade usando as ferramentas Xmail e Pwm

Dados coletados no Teste de Usabilidade	
Tempo do teste	Observação direta
Problemas de usabilidade	
Erros comprometedores	
Expressões faciais	
Depoimentos dos usuários durante o estudo	
Perfil dos Participantes	Pré-questionário (APÊNDICE B)
• Dados demográficos	
• Conhecimentos de Privacidade	
• Conhecimentos de Segurança da Informação	
Opiniões dos Participantes	Pós-questionário (APÊNDICE C)
• Facilidade de uso	
• Percepção de segurança	
• Adoção das ferramentas	

5.3 Considerações Finais

Neste capítulo, foi apresentada a avaliação de usabilidade usando duas ferramentas de e-mails seguros, Xmail e Pwm. Além disso, todo o planejamento e o relato do teste foram descritos.

Os dados obtidos, juntamente com suas análises, resultados e discussões são apresentados e no capítulo posterior.

[19] http://discover.techsmith.com/camtasia-brand-desktop

Capítulo 6

ANÁLISE DOS DADOS, RESULTADOS E DISCUSSÃO

A fim de verificar as evidências qualitativas e compreender a percepção dos usuários em uso de ferramentas de e-mail seguros, este capítulo apresenta os dados coletados, suas análises e discussão.

A Seção 6.1 apresenta, de forma ampla, os dados que foram coletados durante os testes, entre eles dados gerais da avaliação e perfis demográficos. Na Seção 6.2, como tais dados foram analisados, seus resultados e suas discussões são apresentados e, por fim, as considerações finais se dão na Seção 6.3.

6.1 Dados Coletados

Como mencionado anteriormente, as reservas para o teste ficaram disponíveis durante duas semanas e 10 pares de voluntários participaram do teste. Neste período, foram recebidos 20 participantes, sendo 35% do gênero feminino e 65% do masculino com idade entre 18 a 29 anos e ensino médio completo. Além disso, foram gravados 20 vídeos com uma duração média de 40 minutos, totalizando 12 horas de gravação. A Figura 6.1 mostra com mais detalhes os dados demográficos dos participantes do teste de usabilidade.

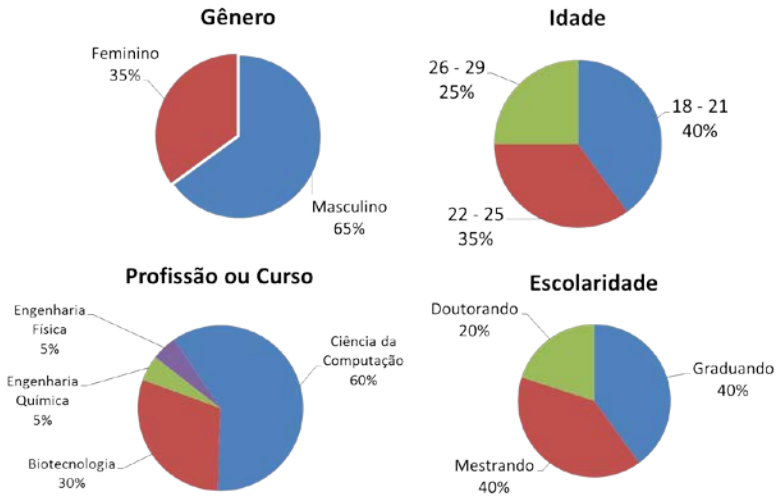


Figura 6.1: Dados demográficos dos participantes do teste de usabilidade

6.2 Análise dos Dados, Resultados e Discussão

No contexto de segurança usável, a capacidade das ferramentas em oferecer uma modelo eficiente para os usuários concluírem suas tarefas com êxito sem comprometerem a sua privacidade e segurança é algo essencial. Por isso, os dados coletados são avaliados e analisados a partir de cinco vertentes principais:

i. Ciência e consentimento de privacidade e segurança de dados;
ii. Eficiência e eficácia das ferramentas;
iii. Percepção de segurança dos usuários;
iv. Facilidade de uso das ferramentas;
v. Adoção das ferramentas.

Cada uma destas vertentes se dará por meio da análise de características específicas destes dados coletados e serão abordadas nas seções seguintes.

6.2.1 Ciência e Consentimento de privacidade e segurança de dados

Com o objetivo de avaliar o quão os participantes estão cientes de sua privacidade, segurança de seus dados e consentimento das políticas de privacidade. Foram calculados os percentuais, por meio do pré-questionário, de participantes que declararam já terem usado aplicativos e/ou sites para transações bancárias,

saberem de casos de violações de dados e/ou já terem sido vitimas de tais casos. Além disso, meios utilizados para enviar dados que consideram sigilosos, consentimento das politicas de privacidade, expertise em segurança da informação e, também, a opinião sobre a coleta de dados como “pagamento” pelo serviço prestado. Os resultados de tal análise são mostrados nas Figura 6.2 e Figura 6.3.

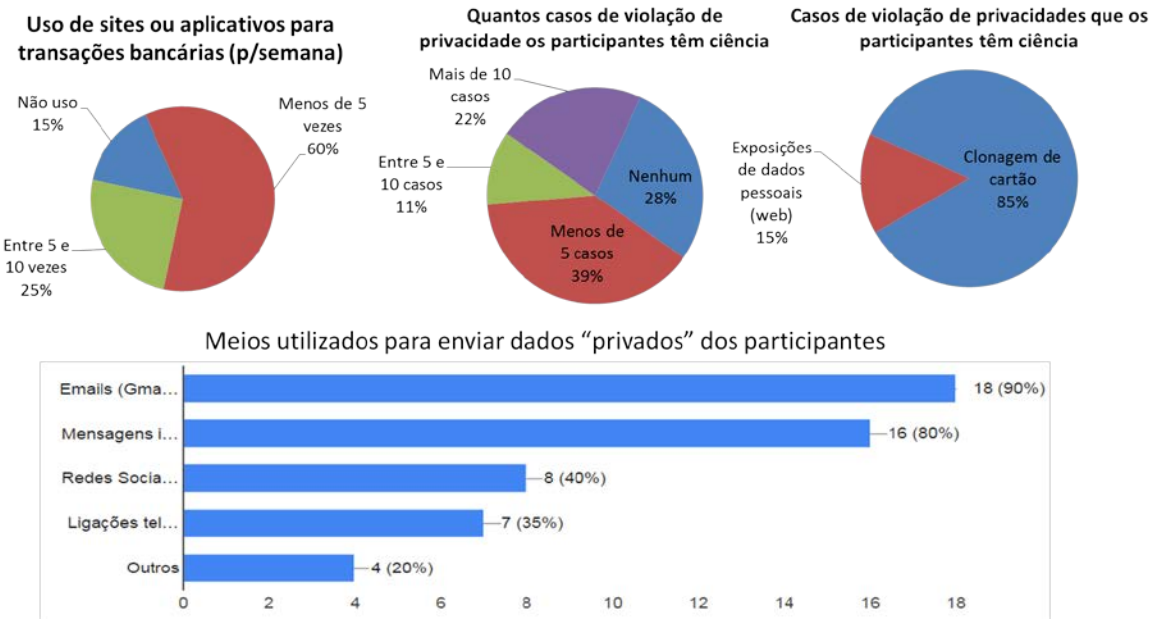


Figura 6.2: Percentual de casos de violação de privacidade e meios utilizados para envio de informações privadas

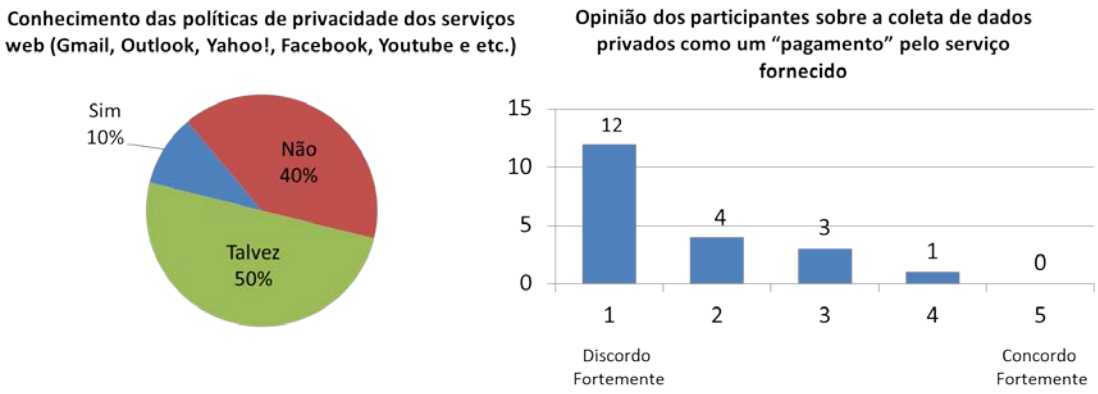


Figura 6.3: Ciência das políticas de privacidade e opinião dos participantes sobre a coleta de dados privados como um “pagamento” pelo serviço prestado

Como mostra os resultados na Figura 6.2, é possível identificar que os participantes tem ciência de casos de violações de dados. No entanto, quando tal ciência é desmembrada é possível perceber que 85% dos casos estão relacionados a dados “financeiros”, ou seja, dados que podem causar algum estrago financeiro e, somente 15% foram relacionados à exposição de dados.

Se por um lado os participantes têm ciência de casos de violação, pelo outro somente 10% têm conhecimento das politicas de privacidade dos serviços web usados e, apesar da percentagem ser baixa, a maioria não concorda com o uso de dados privados como um “pagamento” pelo serviço oferecido.

Por fim, com mostra tais resultados, é possível ter indicativos que a compreensão de privacidade na web dos participantes é algo “primitivo”, ou seja, a preocupação ainda está relacionada há estragos diretamente financeiros e, apesar de não consentirem da coleta, os participantes não tem ciência dos dados coletados.

6.2.2 Eficiência e eficácia das ferramentas

Como já mencionado, a usabilidade é dependente de fatores, como a eficiência e eficácia, que os sistemas interativos devem proporcionar aos usuários em seu uso. Quando unidos aos fatores de segurança de informação (como integridade e autenticidade), tais sistemas precisam garantir uma experiência que exige o menor esforço possível e a geração de poucos erros com integridade e autenticidade.

Esta seção busca identificar esses fatores em cada uma das ferramentas tanto na instalação e configuração quanto na simulação em regime. Para tal, foram usadas métricas de medição e comparações entre as ferramentas, às análises e os resultados são apresentados a seguir nas subseções.

6.2.2.1 Parte 1 – Instalação e Configuração

Eficiência

Com o objetivo de verificar se as ferramentas são capazes de oferecer segurança de modo eficiente na instalação, configuração e envio do primeiro e-mail seguro. Foram contados os tempos de teste de cada participante, distinguindo-os em atores (emissor e receptor) e as tarefas específicas de cada ferramenta. As descrições completas dessas tarefas e como o tempo foi contabilizado e mostrado a seguir na Tabela 6.1.

Por fim, os tempos foram agrupados entre os pares e gerado o tempo médio da instalação e configuração, usando média aritmética simples. Os resultados

individuais de cada participante, juntamente com o tempo médio para a instalação e configuração das ferramentas são mostrados na Figura 6.4 e Figura 6.5.

Tabela 6.1: Subtarefas de cada ferramenta e descrições de como o seus tempos foram contabilizados.

Xmail		
Emissor	Criação da *passphare*	Da abertura da tela de criação até o clique em botão "ok"
	Escrever e enviar e-mail	Da abertura da janela de escrita do Gmail até o clique em "enviar" ou até a ação de clicar no *"Invite recipients to use xmail"*
	Enviar convite	Da abertura da tela de convite até o clique em "enviar". **(para os usuários que falharam na primeira tentativa, o tempo foi contabilizado depois da explicação)**
	Responder e-mail	Da abertura da tela do e-mail recebido até o clique no botão "enviar".
Receptor	Criação da *passphare*	Da abertura da tela de criação ate a ação de clicar em "ok"
	Responder e-mail	Da abertura de tela do e-mail recebido até clicar no botão enviar. **(o tempo de escrita do corpo não foi considerado)**
Pwm		
Emissor	Feedbacks	Do momento em que aparece o primeiro *feedback* até o seu término **(por desistência ou conclusão)**
	Escrever e enviar e-mail	Da abertura da janela de escrita do Gmail até o clique em "enviar"
	Responder e-mail	Da abertura da tela do e-mail recebido até o clique no botão "enviar".
Receptor	Feedbacks	Do momento em que aparece o primeiro *feedback* até o seu término **(por desistência ou conclusão)**
	Responder e-mail	Da abertura de tela do e-mail recebido até clicar no botão enviar. **(o tempo de escrita do corpo não foi considerado)**

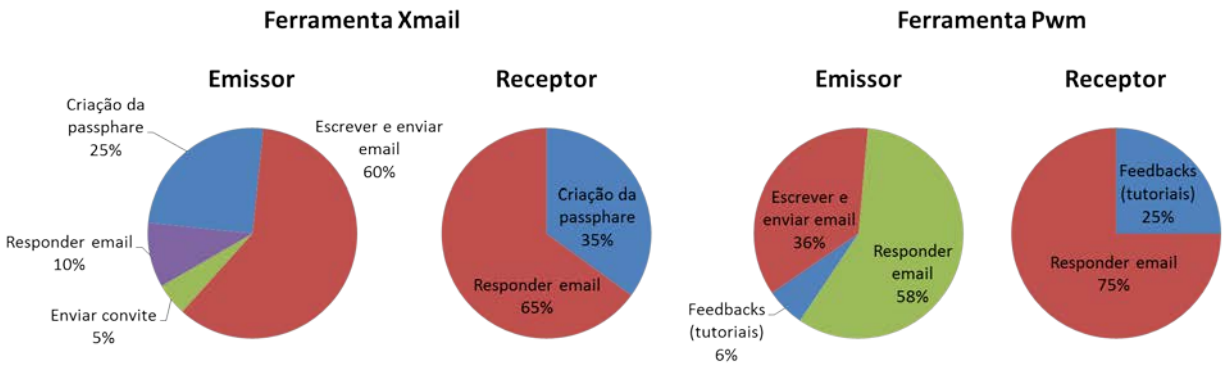
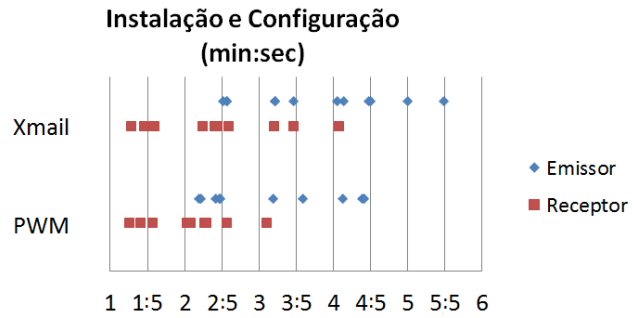


Figura 6.4: Distribuição do tempo médio total em subtarefas para ambas as ferramentas



Ferramentas	Personagem	Usuários	Média (min:sec)	Mínimo (min:sec)	Máximo (min:sec)
Xmail	Emissor	10	04:10	02:51	05:48
	Receptor	10	02:43	01:28	04:07
	Juntos	**20**	**06:53**	**04:19**	**09:55**
Pwm	Emissor	10	03:35	02:19	04:42
	Receptor	10	02:14	01:25	03:10
	Juntos	**20**	**05:49**	**03:44**	**07:52**

Figura 6.5: Tempo de cada participante e tempo médio para a instalação e configuração das ferramentas Xmail e Pwm

Se tratando de eficiência, como mostra os resultados acima, é possível perceber que a ferramenta Xmail foi menos eficiente em relação à Pwm. Em média, os emissores demoraram aproximadamente 1 minuto a mais para completar toda a tarefa usando o Xmail, mas esta diferença é diminuída, em média, para 30 segundos quando a comparação é feita usando os receptores.

Apesar desta diferença de tempo entre as ferramentas, a Tabela 6.1 e a Figura 6.4 mostram que boa parte do tempo usado pelos usuários na ferramenta Xmail foi destinado à tarefa de "Criação da *passphare*" que, em média, equivaleu 25% para os emissores e 35% para os receptores do tempo da tarefa.

Eficácia

Em segurança usável, a incapacidade de um sistema interativo em prover uma imagem do sistema próximo do modelo mental do usuário pode gerar inúmeros erros e, consequentemente, não garantir os fatores de segurança da informação. Sendo assim, esta seção tem por objetivo analisar os dados coletos, buscando identificar se as ferramentas são capazes de oferecer eficácia na instalação, configuração e envio do primeiro e-mail seguro.

Para medir se as ferramentas proveem estes fatores, os dados coletados foram analisados usando métricas de avaliações e o modelo de tarefa das ferramentas. Para as métricas de avaliação, o coordenador e os observadores

definiram um conjunto de métricas e como tais foram aplicadas para análise dos dados coletados. No caso do modelo de tarefas, buscou-se identificar em quais partes desses modelos houve uma ruptura, ou seja, em quais partes a imagem do sistema foi ineficiente quanto ao modelo mental dos participantes.

Os resultados destas análises são mostrados a seguir nas Tabela 6.2, Tabela 6.3 e Tabela 6.4 e nas Figura 6.6 e Figura 6.7. Vale ressaltar que métricas comuns às duas ferramentas foram agrupadas apenas na Tabela 6.2 e as específicas foram separadas. Além disso, a amostra considerada para esta análise foi de 20 participantes divididos em 10 pares (emissores e receptores) e alguns itens se referem somente aos participantes com os papéis de emissores.

Tabela 6.2: Métricas de avaliação e seus resultados aplicados as ferramentas Xmail e Pwm

Xmail e Pwm – Amostra 20 (10 emissores e 10 receptores)			
Métricas – Emissores e Receptores	**Como foi analisado**	**Xmail**	**Pwm**
Dificuldades de saber o que "fazer" após a instalação das ferramentas	Cliques no ícone das extensões em busca de alguma mudança na interface; dúvidas e perguntas para os observadores.	30%	35%
Leitura das páginas de traduções	Deslocamento do Gmail para as páginas auxiliares de traduções.	35%	35%
Leitura das páginas das ferramentas após se depararem com um problema	Deslocamento do Gmail para as páginas de instalação das ferramentas, buscando por informações.	20%	10%
Envio inseguro dos e-mails - **Emissor**	E-mails enviados em texto simples.	70%	20%
Envio inseguro dos e-mails - **Receptor**	E-mails enviados em texto simples.	0%	0%
Após o envio inseguro, percepção das ações inseguras.	Para os envios inseguros, repostas e comentários dos participantes após o envio.	100%	0%

Tabela 6.3: Métricas de avaliação e seus resultados aplicados a ferramenta Xmail

Xmail – Amostra 20 (10 emissores e 10 receptores)		
Métricas – Emissores e Receptores	**Como foi analisado**	**Xmail**
Dificuldades na criação da *passphare*	Uso das traduções e páginas da ferramenta; dúvidas e perguntas; fechamento imediato do *popup* de criação da *passphare.*	30%
Métricas – Emissores	**Como foi analisado**	**Taxa**
Dificuldades em o que fazer para fechar a metáfora "cadeado aberto"	Diversos cliques na metáfora do "cadeado"; tempo ocioso; expressões faciais demostrando dúvidas; releitura dos materiais de apoio.	100%
Convidar o amigo usando a interface	Ação de clicar no botão *"Invite recipients to use xmail"*; expressões de objetivo completo; dúvidas sobre o que fazer nesta etapa.	30%
Quando requisitado, o envio correto do e-mail convite.	Autossuficiência da ferramenta; dúvidas e perguntas dos participantes.	100%
Compreensão da espera pelo "aceite" do amigo para a troca de e-mails seguros	Autossuficiência da ferramenta; dúvidas e perguntas dos participantes.	10%

Tabela 6.4: Métricas de avaliação e seus resultados aplicados a ferramenta Pwm

Pwm – Amostra 20 (10 emissores e 10 receptores)		
Métricas – Emissores e Receptores	**Como foi analisado**	**Taxa**
Interrupção dos tutoriais de instruções	Contagem de participantes que interromperam as etapas do tutorial de uso da ferramenta.	55%
Escrita do corpo do e-mail antes de acionar a opção de segurança	Ação dos participantes em iniciar a escrita do corpo do e-mail antes de acionar a opção de segurança	10%

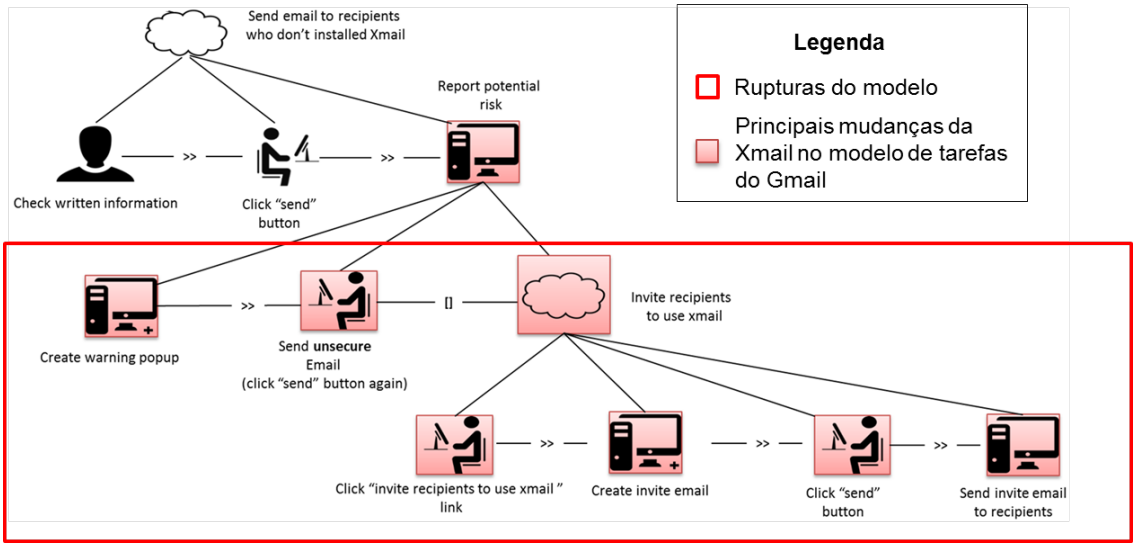


Figura 6.6: Parte do modelo de tarefas da ferramenta Xmail e a ruptura do modelo na instalação e configuração (modelo completo: https://goo.gl/xGQRRw)

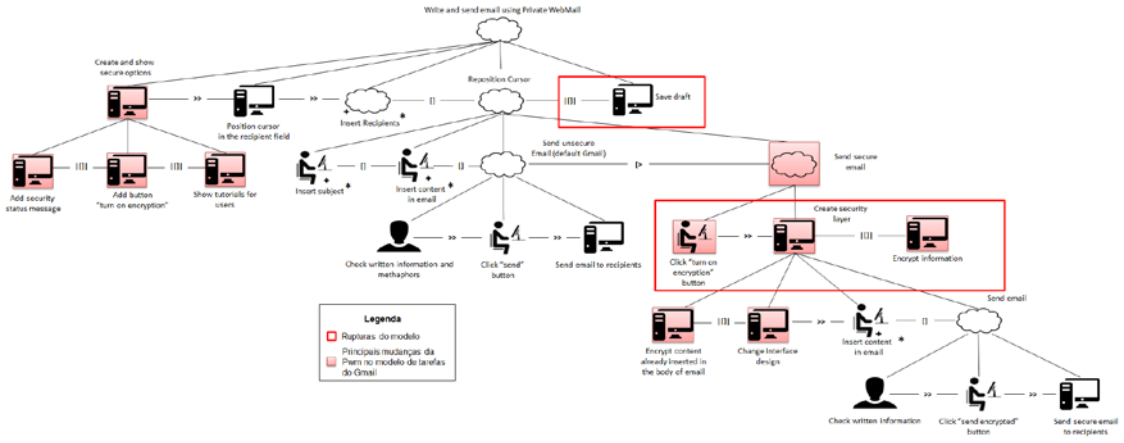


Figura 6.7: Modelo de tarefas da ferramenta Pwm e as rupturas no modelo mental dos participantes (melhor qualidade: https://goo.gl/xGQRRw)

Como mostra a Tabela 6.2, é possível identificar que ambas as ferramentas possuem ineficiências e se equipararam, tratando-se de feedbacks e abordagens que auxiliaram os participantes a "seguirem em frente" após a instalação. Junto a isto, a busca dos participantes por informações externas também foram similares

entre as ferramentas, porém, foi possível notar que na ferramenta Xmail a porcentagem de participantes buscando por soluções para possíveis problemas foi maior.

Se por um lado as ferramentas se assemelharam nas abordagens de auxílio aos participantes, a diferença é grande quando se trata de envio de e-mails não seguros. Visto que na Tabela 6.2, 70% dos participantes enviaram o e-mail em texto simples para os receptores em uso da Xmail, enquanto na Pwm a porcentagem foi de 20%.

A ineficiência da ferramenta Xmail pode ser discutida observando a Tabela 6.3 e a Figura 6.6, é possível notar que toda a abordagem de design, bem como o modelo proposto para "*Invite recipients to use xmail*" não foi compreendia e rompeu o modelo mental dos participantes com o modelo proposto e, até para os casos de sucesso, a compreensão da espera pelo "aceite" do receptor foi compreendia somente por um participante. Na ferramenta Pwm, a ruptura do modelo (Figura 6.7) foi observada nos casos em que os participantes inseriram as informações sigilosas antes de acionar a opção de segurança e, nesses casos, a ferramenta não os informou do potencial risco e o e-mail foi enviado sem segurança.

Conclui-se que apesar desta ineficiência da ferramenta Xmail, foi possível identificar que nos casos de insucesso e envio não seguro, todos os participantes tiveram ciência de tal comprometimento, enquanto na ferramenta Pwm, esta compreensão não foi adquirida, trazendo uma falsa sensação de envio seguro.

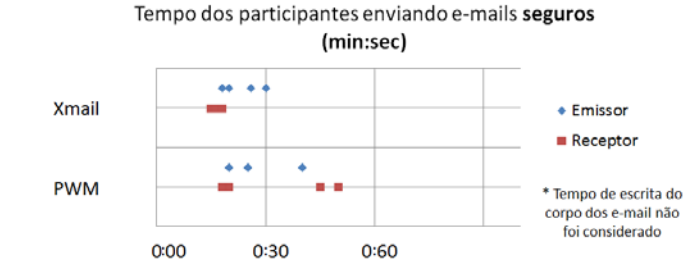
6.2.2.2 Parte 2 – Uso em Regime

Eficiência

Além de testar a instalação e configuração das ferramentas Xmail e Pwm, este trabalho buscou, também, simular o uso rotineiro dos participantes. Sendo assim, com o objetivo de verificar se tais ferramentas foram capazes de se permanecerem eficientes após a instalação e configuração, foram calculados os tempos que cada participante usou para o envio de e-mails seguros e não seguros.

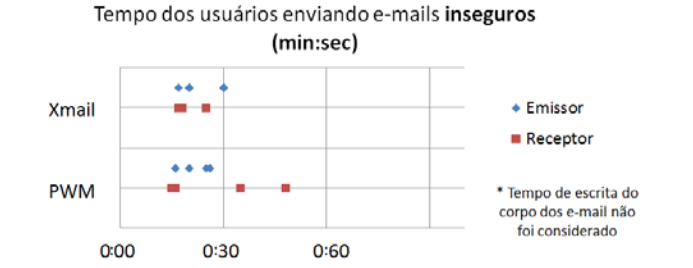
Por fim, os tempos de e-mail dos participantes foram agrupados, distinguindo-os entre envios de e-mails seguros e não seguros e, após isso, foram geradas as médias de cada participante usando média aritmética simples. Os resultados individuais de cada participante, juntamente com o tempo médio, maior e menor para

o envio de e-mails seguros e não seguros em simulação do uso rotineiro das ferramentas são mostrados na Figura 6.8 e Figura 6.9.



Ferramentas	Personagem	Usuários	Média (min:sec)	Mínimo (min:sec)	Máximo (min:sec)
Xmail	Emissor	10	00:24	00:18	00:30
	Receptor	10	00:16	00:15	00:16
	Juntos	**20**	**00:30**	**00:23**	**00:46**
Pwm	Emissor	10	00:28	00:20	00:40
	Receptor	10	00:36	00:18	00:50
	Juntos	**20**	**01:04**	**00:38**	**01:20**

Figura 6.8: Tempo médio dos participantes para de envio de e-mails seguros, simulando o uso em regime usando as ferramentas Xmail e Pwm



Ferramentas	Personagem	Usuários	Média (min:sec)	Mínimo (min:sec)	Máximo (min:sec)
Xmail	Emissor	10	00:25	00:17	00:30
	Receptor	10	00:18	00:17	00:25
	Juntos	20	00:43	00:34	00:55
Pwm	Emissor	10	00:21	00:16	00:26
	Receptor	10	00:27	00:15	00:48
	Juntos	20	00:49	00:31	01:14

Figura 6.9: Tempo médio dos participantes para de envio de e-mails não seguros, simulando o uso em regime usando as ferramentas Xmail e Pwm

Como já discutido anteriormente, a ferramenta Xmail foi menos eficiente do que a Pwm na instalação e configuração. Contudo, na simulação do uso em regime tanto para envio seguro quanto não seguro a Xmail obteve, em média, melhores tempos sendo 30 segundos para envio seguro e 6 segundos para não seguros. Além disso, o tempo máximo da Pwm foi muito superior ao da Xmail (aproximadamente 1 minuto).

Com estes resultados, é possível identificar indícios de que as abordagens *Seamless* e *Always-on* da ferramenta Xmail no uso em regime obteve resultados positivos e diminui o tempo de envio seguro e não seguro.

Eficácia

Esta seção tem por objetivo identificar se as ferramentas se permaneceram capazes, o suficiente, para oferecer eficácia no uso em regime. Para medir este fator, os dados coletados foram analisados usando métricas de avaliações e o modelo de tarefa das ferramentas. Para as métricas de avaliação, buscou-se identificar, principalmente, se a dinâmica de troca de e-mails[20] pôde ser correspondida pelos participantes sem instruções. Para o modelo de tarefas, buscou-se verificar se as rupturas da instalação e configuração persistiram e/ou surgiram novas. Os resultados destas análises são mostrados a seguir na Tabela 6.5 e nas Figura 6.7 e Figura 6.10. Vale ressaltar que os resultados da Tabela 6.5 mostram a quantidade de participantes que feriram as métricas pelo menos uma vez. Além disso, o modelo de tarefas da Pwm persistiu com as mesmas rupturas da instalação e configuração.

Tabela 6.5: Métricas e quantidades de participantes que as feriram-nas no envio de e-mails seguros e não seguros simulando o uso em regime

Xmail e Pwm – Amostra 20 (10 emissores e 10 receptores)			
Métricas	**Como foi analisado**	**Xmail**	**Pwm**
Quebra de fluxo de envio de e-mails **(não seguro para seguro)**	Resposta dos e-mails não seguros usando a opção de segurança.	6	2
Quebra de fluxo de envio de e-mails **(seguro para não seguro)**	Resposta dos e-mails seguros usando a opção de não segurança.	0	2
Em casos de erros, a percepção dos participantes identificando tais erros.	Comentários dos participantes, pedidos de desculpas, cliques nas metáforas após o envio.	5	4

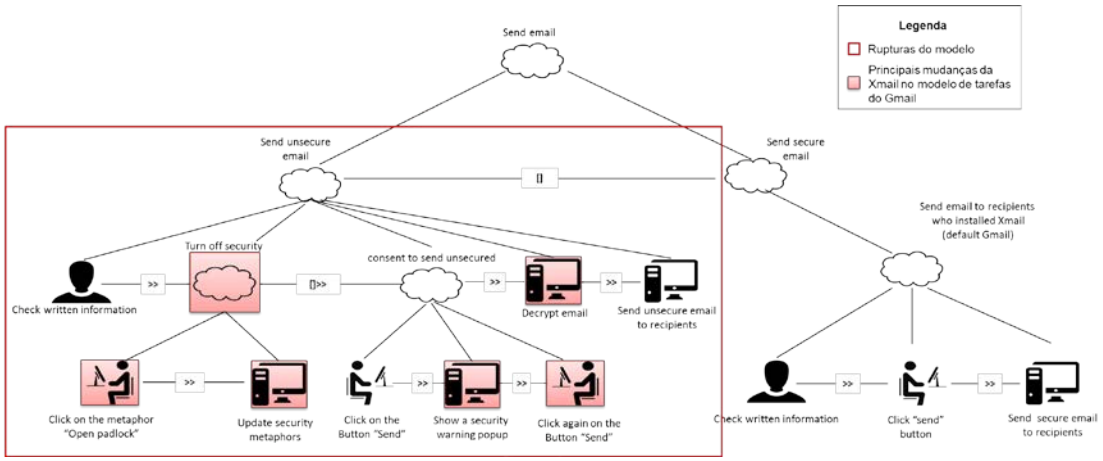


Figura 6.10: Parte do modelo de tarefas da ferramenta Xmail e a ruptura do modelo no uso em regime pelos participantes (modelo completo: https://goo.gl/xGQRRw)

[20] Os participantes deveriam seguir o fluxo seguro ou não seguro, ou seja, quando recebessem um e-mail seguro a resposta deveria ser segura e vice-versa.

Os resultados acima mostram que na simulação do uso em regime também houve rupturas no modelo dos usuários. Na ferramenta Xmail, as rupturas ocorreram no envio de e-mails não seguros, observando a Figura 6.10 é possível perceber que o esforço exigido para o envio de tais e-mails não foi compreendido, juntamente com as metáforas indicando o status não seguro no corpo do e-mail recebido (Figura 3.5) e, consequentemente, 6 participantes (pelo menos uma vez) não fizeram a troca de status exigida na tarefa e os e-mails foram enviados seguros quando a resposta esperada era e-mails não seguros.

Na Pwm, assim como na instalação e configuração, o fluxo de segurança esperado (acionamento da segurança antes da escrita do e-mail) não foi compreendido por 2 participantes pelo menos uma vez e, nesses casos, a integridade do e-mail não pôde ser garantida.

A partir de tais resultados, conclui-se que a ferramenta Xmail possui ineficiência em expressar o status não seguro, no entanto, tal ineficiência não comprometeu a integridade dos e-mails, visto que tais foram enviados com segurança. Por outro lado, a segurança da Pwm depende de um fluxo de ações específicas dos usuários e, casos tais ações não sejam as esperadas, a ferramenta não pode garantir a integridade dos e-mails.

6.2.3 Percepção de segurança dos usuários

Como definido por Whitten e Tygar, um sistema interativo é seguro e usável se os seus usuários estão cientes das tarefas de segurança que precisam executar e são capazes de descobrir como executar tais tarefas com êxito (WHITTEN; TYGAR, 1999). Dessa forma, buscou-se identificar se as ferramentas Xmail e Pwm são capazes, o suficiente, de prover abordagens de design que possam ser percebidas pelos usuários, apoiando-os em seu uso.

Para medir estes fatores, foram criados critérios de avaliação que listou os artefatos de design de cada ferramenta e buscou-se identificar, nas anotações e nos vídeos gravados, evidências que comprovam a percepção dos participantes sobre tais artefatos. A Tabela 6.6 os critérios de avaliação, como foram extraídos e a quantidade de participantes que percebeu o artefato.

Além dos critérios, buscou-se identificar qual metáfora e ferramenta passou mais segurança para os participantes. A Figura 6.11 e Figura 6.12 mostram os resultados desta análise, bem como o agrupamento dos relatos dos participantes.

Tabela 6.6: Métricas e abordagem de design percebidas pelos participantes em uso das ferramentas Xmail e Pwm

Xmail e Pwm – Amostra 20 (10 emissores e 10 receptores)		
Xmail		
Métricas	**Como foi analisado**	**Qtd**
Exploraram a metáfora “cadeado aberto” assim que abriram o pop-up do Gmail	Clicou e/ou parou o cursor na metáfora logo após a abertura do pop-up Gmail.	10
Exploraram a metáfora “cadeado aberto” após a escrita do corpo do e-mail	Clicou e/ou parou o cursor na metáfora somente depois da escrita do corpo do e-mail.	10
Exploraram a metáfora no campo dos destinatários	Após inserir um destinatário, clicou e/ou parou o cursor em cima da metáfora.	4
Exploraram as metáforas no corpo do e-mail recebido (certificado e assegurado)	Após receberem um e-mail, clicou ou parou o cursor para ler a mensagem nos ícones.	20
Compreenderam a camada *Always-on* (mesmo com o cadeado aberto o conteúdo estava seguro)	Perguntas e comentários dos participantes	0
“Sensação de certeza” após fechar a metáfora do cadeado	Expressões faciais indicando “passo concluído” e comentários dos participantes	20
Pwm		
Exploraram o botão “turn on encryption” assim que abriram o pop-up do Gmail	Clicou e/ou parou o cursor no botão logo após a abertura do pop-up Gmail	18
Exploraram a opção de ”help” após o tutorial inicial	Clicou e/ou parou o cursor no botão de ajuda	0
Nos casos de acionamento tardio, compreenderam o risco potencial	Perguntas e comentários dos participantes	0
“Sensação de certeza” após a mudança de cores	Expressões faciais indicando “passo concluído” e comentários dos participantes	20

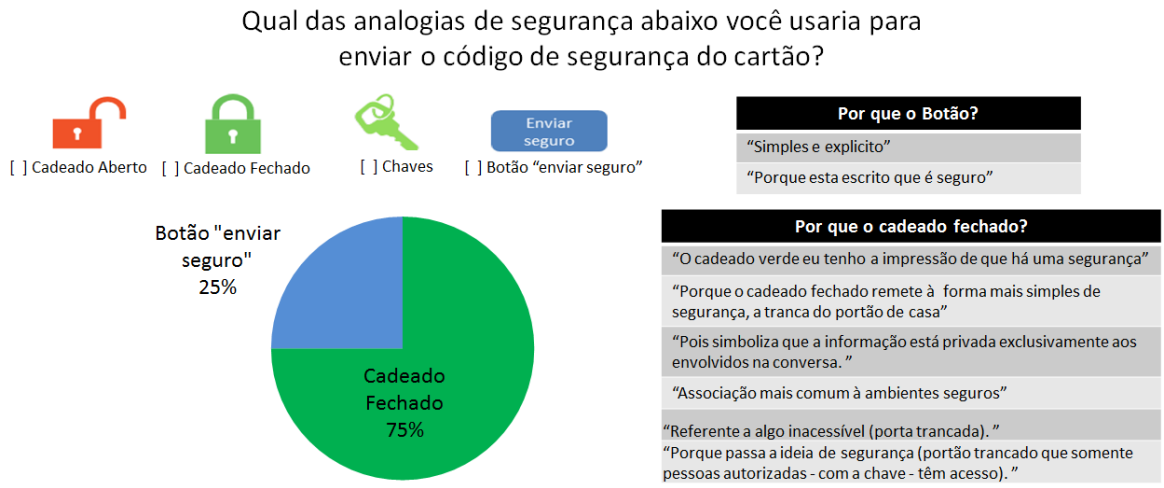


Figura 6.11: Analogias preferidas dos participantes para envio de conteúdo privado e agrupamento das suas opiniões

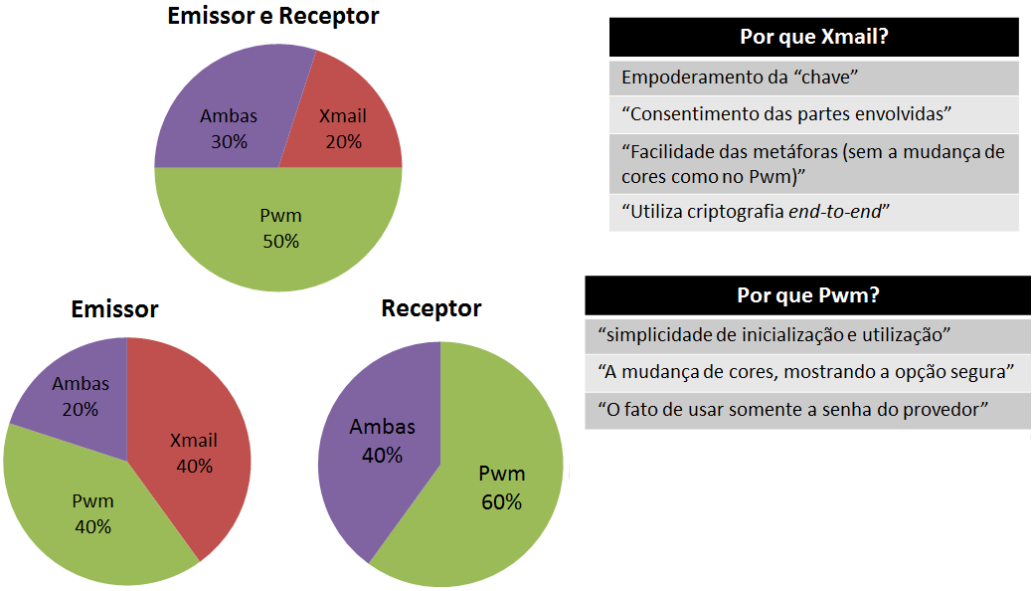


Figura 6.12: Ferramenta mais segura e agrupamento dos principais comentários feitos pelos participantes

Como mostra os resultados na Tabela 6.6, a percepção da metáfora de "acionamento" de segurança na ferramenta Xmal foi percebida por todos os participantes, porém, 10 participantes perceberam tal metáfora logo após a abertura da janela do Gmail e os outros participantes somente após a escrita do corpo do e-mail. Na ferramenta Pwm, todos os participantes também exploram a interface e perceberam a metáfora, portanto, 2 participantes acionou" a segurança após a escrita do e-mail. Além disso, as abordagens de design utilizadas para expressar o status de segurança também foram percebidas por todos os usuários em ambas as ferramentas. Entretanto, os resultados também mostram ineficiências em ambas às ferramentas, tanto na Xmail, com as metáforas inseridas no campo dos destinatários (Figura 3.5) e a camada *Always-on,* quanto na Pwm com as opções de ajuda.

Outro ponto abordado na avaliação foi às metáforas para representarem segurança e, como mostra a Figura 6.11, a metáfora do cadeado aberto foi a mais escolhida, obtendo 75% de escolha contra 25% do botão "enviar seguro".

Por fim, por meio do pós-questionário, buscou-se identificar qual ferramenta foi mais segura para os participantes e, como mostra a Figura 6.12, a Pwm teve 50% de escolha enquanto a Xmail teve 20%. Entretanto, apesar desta diferença considerável, 30% dos participantes escolheram ambas as ferramentas e, além disso, quando os participantes são divididos em receptores e emissores a proporção se iguala para receptores e aumenta para emissores. Cabe ressaltar ainda que o agrupamento dos comentários dos participantes apontou as abordagens de design

para a escolha da ferramenta mais segura, tratando-se da Xmail os comentários foram mais referentes à segurança enquanto na Pwm, os comentários foram mais relacionados à simplicidade e facilidade.

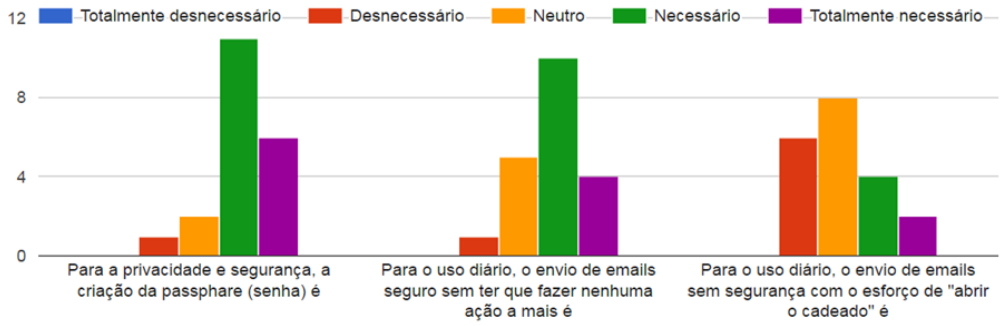
Com os resultados, conclui-se que, apesar das rupturas de modelo das ferramentas (ver 6.2.2), as abordagens de design utilizadas para indicar o acionamento e o status geral de segurança foram percebidas. Além disso, os resultados mostraram indícios de que metáforas visuais foram mais eficientes do que o texto simples para representar segurança, visto que tais metáforas foram análogas a objetos reais. Por fim, apesar de a Pwm ter sido considerada a ferramenta mais segura, há indícios de que as rupturas de modelo da Xmail na instalação e configuração, mais especificamente na tarefa *"invite recipients"*, pode ter impactado em tais resultados, visto que os comentários feitos na escolha da Pwm estão relacionados à facilidade e a porcentagem se iguala para os receptores.

6.2.4 Facilidade de uso

Como já citado, privacidade e segurança de dados na Web é um objetivo secundário da maioria dos usuários e qualquer esforço cognitivo e/ou trabalho adicional pode dificultar o uso e adoção de ferramentas que proveem tais funcionalidades. Sendo assim, buscou-se identificar se as ferramentas satisfizeram os participantes e propuseram uma experiência positiva.

Para testar a facilidade de uso das ferramentas Xmail e Pwm e identificar seus principais problemas de design. Foram calculadas as opiniões dos participantes quando a importância das abordagens de design propostas e as dificuldades enfrentadas no uso de cada ferramenta e, também, foram feitas comparações entre as ferramentas buscando identificar qual proporcional mais facilidade para o envio de e-mails seguros e não seguros.

Nas Figura 6.13 e Figura 6.14, os gráficos apresentam as abordagens utilizadas pelas ferramentas e seus respectivos resultados, seguidos das dificuldades enfrentadas pelos participantes. A Figura 6.15 mostra as opiniões dos usuários quanto à facilidade de envio de e-mails.



Dificuldades dos participantes em usar a ferramenta XMAIL

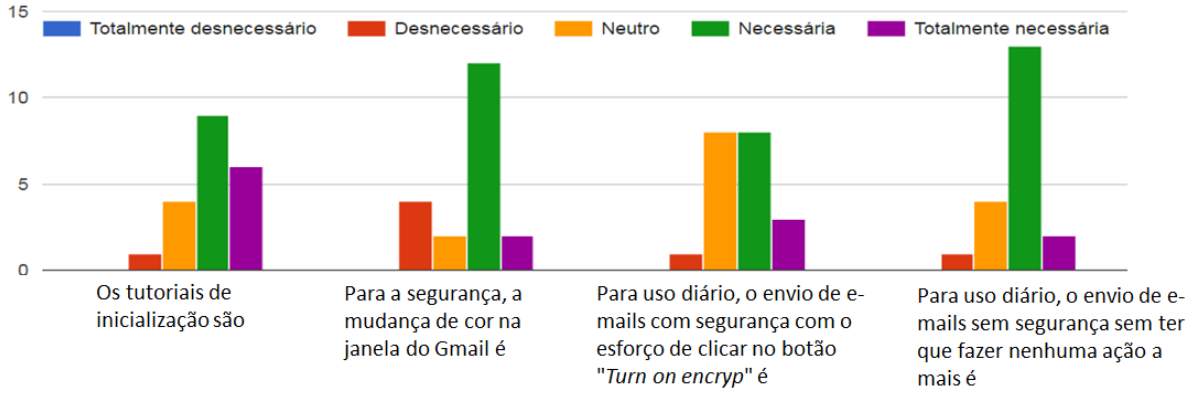
Emissores – Amostra: 10 participantes

Subtarefas	Qtd Participantes
Criar *passphare* (senha)	1
O envio do convite para o amigo	10
O envio do e-mail seguro	1
O envio do e-mail sem segurança	0
Não tive dificuldades	0

Receptor – Amostra: 10 participantes

Subtarefas	Qtd Participantes
Criar *passphare* (senha)	1
O envio do e-mail seguro	0
O envio do e-mail sem segurança	2
Não tive dificuldades	8

Figura 6.13: Opiniões dos participantes quanto as abordagens de design e dificuldades enfrentadas na ferramenta Xmail



Dificuldades dos participantes em usar a ferramenta Pwm

Emissores – Amostra: 10 participantes

Subtarefas	Qtd Participantes
Entender os tutoriais	0
O envio do e-mail seguro	0
O envio do e-mail sem segurança	0
Não tive dificuldades	10

Receptor – Amostra: 10 participantes

Subtarefas	Qtd Participantes
Entender os tutoriais	1
O envio do e-mail seguro	1
O envio do e-mail sem segurança	0
Não tive dificuldades	8

Figura 6.14: Opiniões dos participantes quanto as abordagens de design e dificuldades enfrentadas na ferramenta Pwm

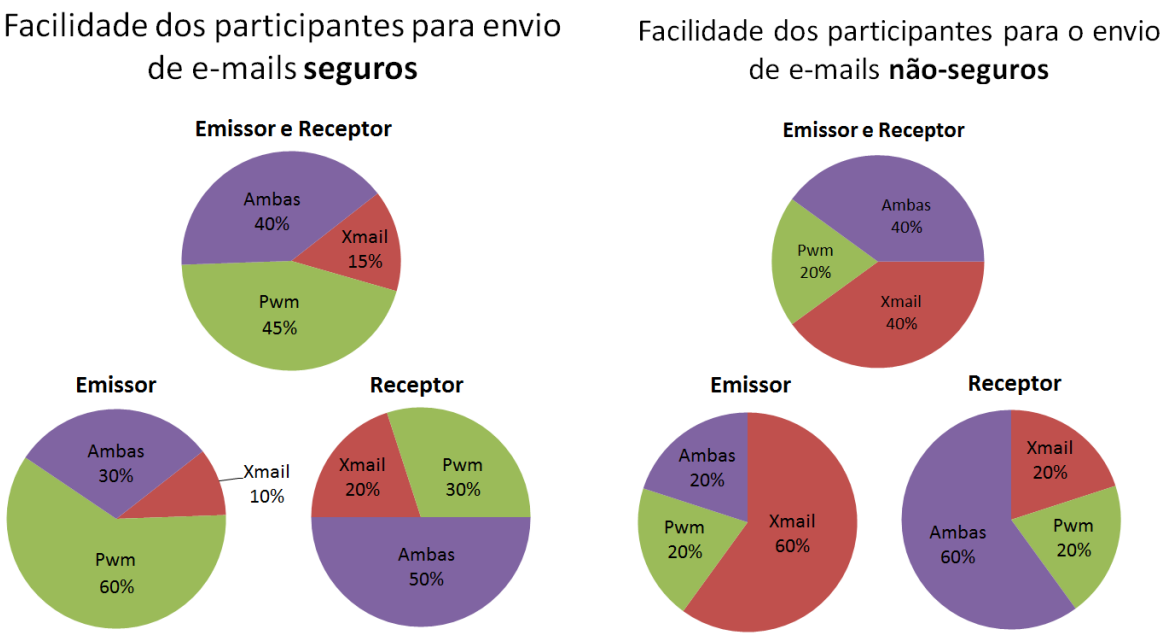


Figura 6.15: Opiniões dos participantes sobre a facilidade de envio de e-mails seguro e não seguros.

Baseando-se nos resultados da ferramenta Xmail (Figura 6.13), é possível identificar que o empoderamento da "chave" e o envio de e-mails seguros sem esforço extra, foram considerados necessários ou totalmente necessários para a maioria dos participantes. Porém, o esforço exigido para o envio de e-mails não seguro obteve mais opiniões neutras e desnecessárias. Junto a isto, e complementando aos resultados anteriores, tais resultados explicitam novamente a ruptura do modelo da ferramenta Xmail na subtarefa *"invite recipientes to use xmail"*, visto que 100% dos receptores classificaram-na com uma dificuldade para o uso da ferramenta. Além disso, para 2 participantes a "criação da *passphare*" também foi uma dificuldade, bem como o esforço para o envio de e-mails sem segurança.

Na ferramenta Pwm, os resultados (Figura 6.14) mostram que os tutoriais, a mudança de cor (para indicar o status de segurança) e o envio de e-mails não seguros sem esforço extra foram classificados, pela maioria dos participantes, como necessário ou totalmente necessários. Entretanto, o esforço extra para o envio de e-mails seguros teve uma pequena diferença entre a neutralidade e a necessidade. Os resultados indicam também que os participantes não tiverem dificuldades para usar a ferramenta e, somente 2 participantes receptores, tiveram dificuldades em entender os tutoriais e enviar o e-mail seguro.

Além dos resultados individuais, a Figura 6.15 mostra que a ferramenta Pwm foi considerada a mais fácil para o envio de e-mails seguros, obtendo 45% de escolha contra 15% da Xmail, mas é possível observar que esta diferença concentrou-se para os emissores, visto que a diferença para os receptores é de 10%. Por outro lado, a ferramenta Xmail foi a mais escolhida para o envio de e-mails não seguros, obtendo 40% contra 20% de escolha, no entanto, esta porcentagem retém-se para os emissores, dado que a porcentagem é igual para os receptores.

Em virtude dos resultados, conclui-se que o empoderamento dos participantes sobre a ferramenta, bem como tutoriais e abordagens que expressam o status de segurança foram considerados necessários às ferramentas. Além disso, tais resultados evidenciaram que o esforço extra nas abordagens pode comprometer sua importância.

6.2.5 Adoção das ferramentas

Além da facilidade de uso, testou-se também, a possibilidade do uso das ferramentas testadas ser estendido para o cotidiano dos participantes. Para isto, foram calculadas as opiniões dos participantes em uma escala de pouco provável até muito provável. Além disso, os comentários feitos sobre a adoção também foram analisados e agrupados em: i) não vejo necessidade; ii) já uso uma ferramenta segura; iii) usaria somente em casos específicos e iv) usaria no dia-a-dia. Vale ressaltar que o agrupamento foi baseado na interpretação dos comentários feitos, assim, diferentes interpretações podem ser feitas. As Figura 6.16 e Figura 6.17 mostram os resultados desta analise.

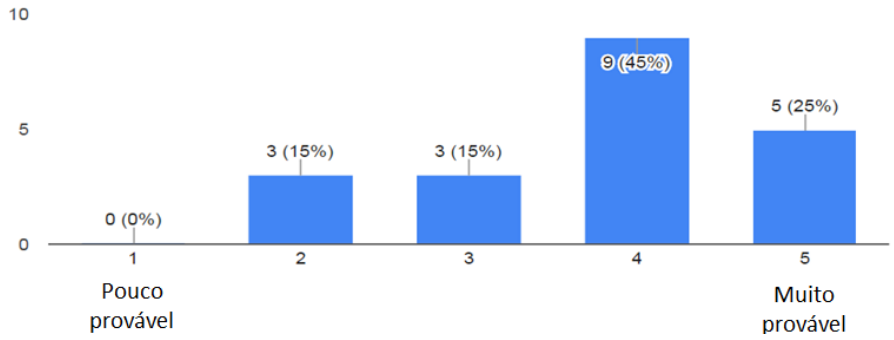


Figura 6.16: Opiniões dos participantes sobre a adoção das ferramentas no uso cotidiano

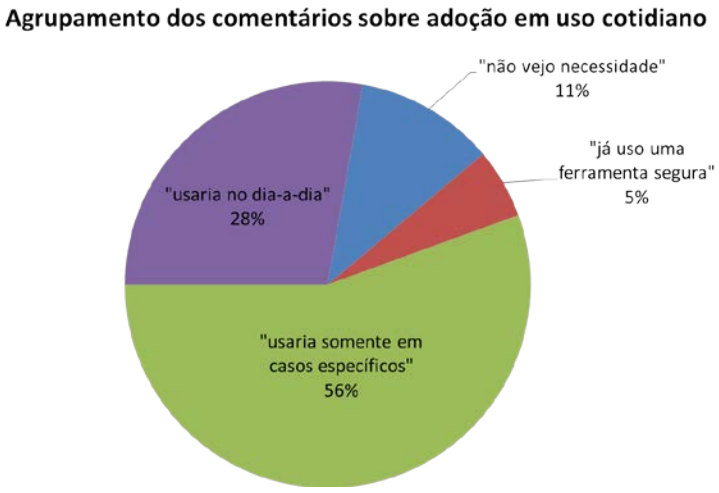


Figura 6.17: Agrupamento dos comentários feitos pelos participantes sobre a adoção das ferramentas em uso cotidiano

As opiniões dos participantes quanto ao possível uso das ferramentas em seus cotidianos apontam que 65% dos participantes adotariam tais ferramentas (Figura 6.16). Entretanto, as compilações das suas respostas mostram uma divisão entre participantes que usariam no dia-a-dia e os que usariam somente em casos específicos (Figura 6.17). Sendo assim, conclui-se que a maioria dos participantes quer ter a possibilidade de proteger seus dados privados, mas apenas 28% querem adotar tais soluções no uso diário.

6.3 Considerações Finais

Neste capítulo, foi descrita a compilação de todos os dados coletados pelo teste usabilidade usando as ferramentas Xmail e Pwm. Tais dados também foram analisados e seus resultados foram discutidos, visando identificar as principais falhas de design e rupturas de modelos propostos pelas ferramentas.

Os resultados analisados e discutidos neste capítulo apontam indícios de que o uso de camadas de segurança podem a prevenir erros comprometedores. Além disso, apontam as abordagens que foram eficientes, eficazes e que ajudaram os participantes a concluírem suas tarefas.

Tomando como base a discussão dos resultados apresentados neste capítulo, o capítulo seguinte apresenta as contribuições deste trabalho, os trabalhos publicados bem como os trabalhos futuros.

Capítulo 7

CONCLUSÃO

A adoção da tecnologia de informação e comunicação em ambientes pessoais, sociais e corporativos é cada vez mais evidente e traz complexidade, interdisciplinaridade e diversidade ao estudo sobre segurança da informação. À medida que esse fenômeno se torna cada vez mais comum, juntamente com a vigilância global e o marketing eletrônico (baseado na coleta de informações pessoais), atingiu-se uma situação onde a coleta de dados permeia os espaços pessoais, sociais e de trabalho e está, muitas vezes, acima dos consentimentos e direitos das pessoas.

Por isso, as preocupações têm se intensificado em relação à segurança, sigilo, privacidade e governança da informação e, por consequência, novas ferramentas que provem tais medidas seguras também ganharam mais evidência e novas concepções tem surgido. No entanto, eventos e estudos têm mostrado a dificuldade de uso e adoção dessas soluções seguras, mesmo à possibilidade técnica de se obter privacidade e segurança com o ferramental tecnológico na maioria das vezes já ser eficiente, há evidências da necessidade de modelos mais eficazes de segurança e privacidade na Web, de maneira que possam ser mais compreensíveis para os usuários não especialistas.

Sendo assim, neste trabalho buscou-se identificar os principais motivos dessa não adoção e, consequentemente, estabelecer novas estratégias de design para dar poder e autonomia ao usuário final em relação à segurança de seus dados na adoção efetiva dos serviços de e-mail seguros.

Para o desenvolvimento deste trabalho foi realizada uma revisão dos conceitos de usabilidade, segurança da informação e modelos mentais, bem como

uma revisão e análise contínua dos trabalhos científicos e ferramentas relacionados no contexto de segurança e usabilidade. Além disso, foram feitos testes de usabilidade, usando o protótipo Xmail (desenvolvido pelo LIA) e a ferramenta Private WebMail (Pwm), a fim de extrair evidências qualitativas.

Este capítulo está organizado da seguinte forma: a Seção 7.1 destaca as contribuições deste trabalho, discutindo os principais resultados obtidos. As limitações referentes ao trabalho desenvolvido são identificadas e apresentadas na Seção 7.2. Por fim, na Seção 7.3, são apresentadas algumas possibilidades de trabalhos futuros do trabalho desenvolvido.

7.1 Contribuições

Durante todo o trabalho foi mencionado à dificuldade de encontrar trabalhos consolidados e concretos sobre a área de HCI-Sec. Sendo assim, uma das contribuições deste trabalho é a compilação de estudos encontrados na literatura e a junção de tais. No Capítulo 2, as principais diretivas e desafios da área são destacados, juntamente com um panorama geral dos trabalhos que instanciam o estudo de e-mails seguros e usáveis.

Outra contribuição deste trabalho foi à metodologia e os resultados alcançados na revisão e avaliação das principais ferramentas de segurança em e-mails descrita no Capítulo 4. Em tal revisão, cada etapa, como a identificação, categorização, refinamento e avaliação foi descrita e detalhada possibilitando a replicação da metodologia para além das ferramentas de e-mails seguros. Além disso, o uso dos modelos de tarefas para cada ferramenta possibilitou uma compreensão mais precisa sobre o modelo mental dos usuários. Por fim, os resultados mostram um panorama geral das ferramentas e suas conformidades com as diretivas da área, podendo concluir que houve indícios de melhoria na usabilidade, mas a maioria ainda trata segurança como algo adicional para os usuários.

O trabalho desenvolvido também apresentou os resultados de uma análise quantitativa a partir da realização de um experimento para avaliar a utilização das ferramentas Xmail e Pwm. Foram coletados dados sobre os perfis dos participantes,

o tempo gasto e erros comprometedores na realização das tarefas, e suas as opiniões sobre o uso de tais ferramentas como parte dos seus ferramentais diários.

A partir dos dados coletados e todas as observações feitas durante a realização do experimento, teve-se como resultados os benefícios e falhas de design de cada ferramenta, juntamente com a compreensão do modelo do sistema das ferramentas. As conclusões extraídas a partir de tais resultados (ver Capítulo 6) são destacadas abaixo:

- **Ciência e consentimento de privacidade e segurança de dados:** Como a literatura destaca, privacidade e segurança é um objetivo secundário dos usuários em uso de uma solução Web. Porém, baseando-se nos resultados é possível ter indícios de que este objetivo secundário pode ser recorrência dos termos e políticas de privacidade não eficientes das ferramentas, visto que ao explicitar os termos aos participantes a privacidade se tornou mais necessárias aos participantes.

- **Percepção de segurança dos usuários:** Os resultados evidenciam a eficiência de metáforas visuais e analogias que tem representações no mundo físico. Sendo assim, é possível concluir que tais metáforas têm um papel essencial no design e ajudam na compreensão das tarefas, aproximando o modelo do sistema com o modelo mental dos usuários. Em complemento a isto, o poder dos participantes sobre o processo de criptografia também se mostrou essencial e, mesmo diminuindo o desempenho no processo de instalação, garante uma “sensação” de segurança mais efetiva para os usuários.

- **Modelo mental dos usuários:** Como destacado nos resultados, os participantes possuem um modelo mental para escrita e envio de e-mails e propor alterações não é uma tarefa trivial e podem gerar rupturas e, consequentemente, a não compreensão das tarefas. Sendo assim, é possível concluir que a compreensão do modelo mental dos usuários, bem como as possíveis sequências do fluxo das tarefas tem um papel essencial na usabilidade e na redução de erros comprometedores.

- **Segurança como padrão:** Os resultados mostram que o fluxo de execução de tarefas na escrita de e-mails pode variar de usuário para usuário e a dependência de tarefas especifica não pode garantir a integridade dos e-mails em todos os casos. Desta forma, é possível concluir que a segurança como padrão tem um papel fundamental em tais ferramentas.

- **Adoção das ferramentas de segurança:** Neste trabalho, é possível ter indicativos de que a adoção efetiva das ferramentas tem ganhado mais espaço (em relação à literatura), mas ainda não seriam adotadas pela maioria dos participantes. Por outro lado, a melhoria na usabilidade e aproximação do modelo da ferramenta com o dos usuários tem contribuído para o uso efetivo.

No geral, esta pesquisa reforça o papel essencial da usabilidade em ferramentas de e-mails seguros, avaliando as principais abordagens de design das ferramentas existentes e propondo estratégias de design para dar poder e autonomia ao usuário final em relação à segurança de seus dados na adoção efetiva dos serviços de e-mail seguros. Além disso, com os resultados apresentados é possível ter indícios de que um design centrado no modelo mental de segurança dos usuários ajuda na utilização e/ou adoção de ferramentas de e-mails seguros.

7.2 Limitações

Uma vez tendo concluído o desenvolvimento do trabalho proposto, algumas limitações foram identificados por meio de uma análise crítica.

Na revisão das ferramentas descrita no Capítulo 4, algumas limitações identificadas referem-se ao processo de busca, categorização e avaliação das ferramentas. No processo de busca, não foram feitas buscas exaustivas e, mesmo identificando as principais ferramentas, a revisão não traz um panorama total. Além disso, limitações como a licença e a disponibilidade do material técnico, fizeram com que a categorização e a avaliação fossem feitas somente com as informações

disponibilizadas e a compreensão obtida nas interações com tais, assim, tal revisão não descarta novas perspectivas.

Outra limitação existente no trabalho desenvolvido está relacionada aos resultados obtidos a partir da avaliação de usabilidade no Capítulo 5. Embora os resultados do estudo tenham evidenciado rupturas, abordagens não eficientes e indícios de adoção, é necessário considerar que esses resultados estão limitados ao escopo de estudantes universitários e ambiente controlado. Considerando questões de validade, para estender e generalizar os resultados obtidos para um contexto mais amplo torna-se necessária a reaplicação da avaliação em ambientes não controlados, com participantes de outros perfis e, preferencialmente, um estudo longitudinal.

7.3 Trabalhos Futuros

Espera-se que este trabalho possa inspirar novos trabalhos a alcançar objetivos a partir dos alcançados e contribuir ainda mais para a concepção de soluções seguras e usáveis. Alguns pontos para futuros projetos são:

- Evoluir o protótipo Xmail, de modo que possa aproximar sua imagem do sistema ao modelo mental dos usuários comuns, juntamente com refinamentos no design.
- Realizar um estudo longitudinal, com mais tempo de coleta de dados e observações, com o objetivo obter mais evidências sobre a extensão do uso para a adoção.
- Realizar uma pesquisa semelhante ou mesmo reproduzi-la para novos perfis de participantes, a fim de verificar se tais mudanças impactam nos resultados.
- Estender os conceitos *Always-on security*, *seamless* e os resultados obtidos neste estudo para além da ferramenta Xmail, ou seja, para além da instância de ferramentas de e-mails seguros.

PUBLICAÇÕES

Durante todo o desenvolvimento da pesquisa apresentada nesta dissertação, os seguintes artigos científicos foram publicados em colaboração com diferentes pesquisadores:

- Relacionado ao tema desta pesquisa
    - FERREIRA Lucas, ANACLETO Junia. Usability in Solutions of Secure Email – A Tools Review. In: Tryfonas T. **Human Aspects of Information Security, Privacy and Trust**. HAS 2017. Lecture Notes in Computer Science, vol 10292. Springer, Cham, 2017;

- Relacionado aos temas desta pesquisa do LIA:
    - BUENO, Andre, FERREIRA, Lucas, FERREIRA, Vinicius, ANACLETO, Junia. Tendências de Pesquisa em IHC no Brasil: Uma Análise em Relação ao GranDIHC-Br. **In the 15th Brazilian Symposium on Human Factors in Computing Systems**, São Paulo, Brazil, 2016;

- Relacionado a outros temas de pesquisa:
    - TSHAM MPINDA, Steve Ataky; FERREIRA, Lucas Cesar; RIBEIRO, Marcela Xavier; PRADO SANTOS, Marilde Terezinha. Evaluation of Graph Databases Performance through Indexing Techniques. **International Journal of Artificial Intelligence & Applications (IJAIA)**, v. 6, p. 87-98, 2015

REFERÊNCIAS

BARBOSA, S. D. J.; SILVA, B. S. da. Interação humano-computador. [S.l.]: **Elsevier**, 2010.

BBC. Brazil's president Rousseff attacks US over spy claims. **BBC**. 2013. Acesso em: 05 de Julho 2016. Disponível em: <http://www.bbc.com/news/world-latin-america-24230069>.

BØDKER, S. When second wave hci meets third wave challenges. In: **Proceedings of the 4th Nordic Conference on Human-computer Interaction: Changing Roles.** New York, NY, USA: ACM, 2006. (NordiCHI '06), p. 1–8. Disponível em: <http://doi.acm.org/10.1145/1182475.1182476>.

COOK, T. A Message to Our Customers. **Apple Inc.** 2016. Acesso em: 06 de Julho 2016. Disponível em: <http://www.apple.com/customer-letter>.

CRAIK, K. J. W. The nature of explanation. [S.l.]: **CUP Archive**, 1967.

DESURVIRE, H. W. Faster, cheaper!! Are usability inspection methods as effective as empirical testing? In **Nielsen, J., and Mack, R. L. (Eds.), Usability Inspection Methods, John Wiley & Sons**, New York, 173–202, 1994.

DIAPER, D.; STANTON, N. The handbook of task analysis for human-computer interaction. [S.l.]: **CRC Press**, 2003.

DIX, A. Designing for appropriation. In: **Proceedings of the 21st British HCI Group Annual Conference on People and Computers: HCI...But Not As We Know It - Volume 2.** Swinton, UK, UK: British Computer Society, 2007. (BCS-HCI '07), p. 27–30. Disponível em: <http://dl.acm.org/citation.cfm?id=1531407.1531415>.

DOURISH, P. et al. Security in the Wild: User Strategies for Managing Security As an Everyday, Practical Problem. **Personal Ubiquitous Comput.** ,London, UK, UK , v. 8, n. 6, p. 391--401 , 2004.

DOYLE, J. K.; FORD, D. N. Mental models concepts for system dynamics research. **System dynamics review**, v. 14, n. 1, p. 3–29, 1998.

GARFINKEL, S. PGP: pretty good privacy. [S.l.]: **O'Reilly Media**, Inc., 1995.

GARFINKEL, S. L. et al. How to Make Secure Email Easier to Use.
Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. New York, NY, USA : ACM. 2005. p. 701--710.

GAYLE, D. The Edward Snowden guide to encryption: Fugitive's 12-minute homemade video ahead of leaks explaining how to avoid NSA from tracking emails.

Mail Online. 2014. Acesso em: 15 de Julho 2016. Disponível em: <http://www.dailymail.co.uk/news/article-2628082/The-Edward-Snowden-guide-encryption-Fugitives-12-minute-homemade-video-ahead-leaks-explaining-avoid-NSA-tracking-emails.html>.

GENTNER, D.; STEVENS, A. L. Mental models. [S.l.]: **Psychology Press**, 1983.

GLOBO.COM. WhatsApp deve ser bloqueado por 72 horas, ordena Justiça. **Grupo Globo**. 2016. Acesso em: 07 de Julho 2016. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/05/justica-do-sergipe-manda-operadoras-bloquearem-whatsapp.html>.

GREENWALD, G.; MACASKILL, E. NSA Prism program taps in to user data of Apple, Google and others. **The Guardian**. 2013. Acesso em: 05 de Julho 2016. Disponível em: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>.

HARPER, E. R. et al. Human-computer interaction in the year 2020. **Citeseer**, 2008.

HECHT, P.; FELS, S.; ANACLETO, J. Seamless and always-on security in a bring-your-own-application world. In: **Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems**. New York, NY, USA: ACM, 2015. (CHI EA '15), p. 2019–2024. Disponível em: <http://doi.acm.org/10.1145/2702613.2732880>.

ISO 9241-11. Ergonomic requirements for office work with visual display terminals (VDTs) Part 11: Guidance on Usability. **International Organization for Standardization**. 1998.

ISO/IEC 27000. Information technology—Security techniques—Informaiton security management systems. **International Organization for Standardization**. 2012.

ISO/IEC 9126. International Standard ISO/IEC9126 Information Technology – Software product evaluation – Quality Characteristics and Guidelines for their use. **International Organization for Standardization.** 1991.

JOHNSON-LAIRD, P. N. Mental models: Towards a cognitive science of language, inference, and consciousness. [S.l.]: **Harvard University Press**, 1983.

JOHNSON-LAIRD, P. N. 8 the history of mental models. Psychology of reasoning: Theoretical and historical perspectives, **Psychology Press**, p. 179, 2004.

JUNIOR, S. T. Obama defende acesso a informações criptografadas em evento. **Revista Exame**. 2016. Acesso em: 06 de Julho 2016. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/nao-podemos-ter-visao-absolutista-sobre-criptografia-diz>.

KAINDA, R.; FLECHAIS, I.; ROSCOE, A. Security and usability: Analysis and evaluation. In: **IEEE. Availability, Reliability, and Security**, 2010. ARES'10 International Conference on. [S.l.], 2010. p. 275–282.

LEWIS, C.; WHARTON, C. Cognitive walkthroughs. In M. Helander, T.K. Landauer, P. Prabhu (Eds.) **Handbook of human-computer interaction**, 2nd ed. Elsevier Science. Pp. 717-732, 1997

LIMBOURG, Q.; VANDERDONCKT, J. et al. Comparing task models for user interface design. **The handbook of task analysis for human-computer interaction**, Lawrence Erlbaum Assoc, v. 6, p. 135–154, 2004.

LUHN, A. Russia passes 'Big Brother' anti-terror laws. **The Guardian**. 2016. Acesso em: 07 de Julho 2016. Disponível em: <https://www.theguardian.com/world/2016/jun/26/russia-passes-big-brother- anti-terror-laws>.

MACK, R. L.; NIELSEN, J. Usability inspection methods. [S.l.]: **Wiley & Sons New York**, NY, 1994.

MATHIASEN, N. R.; BøDKER, S. Threats or Threads: From Usable Security to Secure Experience? **Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges**. New York, NY, USA : ACM. 2008. p. 283-289.

MCKENDRICK, J. Public Cloud Computing Growing Almost 50 Percent Annually. **Forbes**. 2016. Acesso em: 06 de Julho 2016. Disponível em: <http://www.forbes.com/sites/joemckendrick/2016/05/31/public-cloud-computing-growing-almost-50-percent-annually-cisco-says/#142396b22273>

MORI, G.; PATERNO, F.; SANTORO, C. Ctte: support for developing and analyzing task models for interactive system design. **IEEE Transactions on Software Engineering**, v. 28, n. 8, p. 797–813, Aug 2002. ISSN 0098-5589.

NIELSEN, J. Usability Engineering. [S.l.]: **Elsevier**, 1993.

NORMAN, D. A. The design of everyday things: Revised and expanded edition. [S.l.]: **Basic books**, 2013.

NOVAK, J. D.; CANAS, A. J. Theoretical origins of concept maps, how to construct them, and uses in education. **Reflecting Education**, v. 3, n. 1, p. 29–42, 2007.

PAGLIERY, J. Edward Snowden defends Apple in fight against FBI. **CNN**. 2016. Acesso em: 06 de Julho 2016. Disponível em: <http://money.cnn.com/2016/02/17/technology/apple-fbi-phone-unlock-edward-snowden>.

PATERNO, F. Model-Based Design and Evaluation of Interactive Applications. 1st. ed. London, UK, **UK: Springer-Verlag**, 1999.

POLSON P., LEWIS, C., RIEMAN, J. e WHARTON, C. Cognitive Walkthroughs: A method for theory-based evaluation of user interface. **International Journal of Man-Machine Studies**, n. 36. Pages. 741-773, 1992.

RAMSDELL, B. S/mime version 3 message specification. **RFC Editor**. 1999.

ROCHA, H. V.; Baranauskas, M. C.C. Design e Avaliação de interfaces humano-computador. 242p. **IME-USP**, São Paulo, 2000.

RUBIN, J. Handbook of Usability Testing: How to Plan, Design and Conduct Effective Tests. **John Wiley & Sons**. New York. 330 p, 1994.

RUOTI, S. et al. Confused johnny: When automatic encryption leads to confusion and mistakes. In: **Proceedings of the Ninth Symposium on Usable Privacy and Security**. New York, NY, USA: ACM, 2013. (SOUPS '13), p. 5:1–5:12. Disponível em: <http://doi.acm.org/10.1145/2501604.2501609>.

RUOTI, S. et al. Why johnny still, still can't encrypt: Evaluating the usability of a modern pgp client. **arXiv preprint arXiv:1510.08555**, 2015.

RUOTI, S. et al. "we're on the same page": A usability study of secure email using pairs of novice users. In: **Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems**. New York, NY, USA: ACM, 2016. (CHI '16), p. 4298–4308. Disponível em: <http://doi.acm.org/10.1145/2858036.2858400>.

SALTZER, J. H.; SCHROEDER, M. D. The protection of information in computer systems. **Proceedings of the IEEE**, IEEE, v. 63, n. 9, p. 1278–1308, 1975.

SHAMIR, A. Identity-based cryptosystems and signature schemes. In: **Advances in Cryptology: Proceedings of CRYPTO 84**. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985. p. 47–53. Disponível em: <http://dx.doi.org/10.1007/3-540-39568-7_5>.

SHENG, S. et al. Why johnny still can't encrypt: evaluating the usability of email encryption software. In: **Symposium On Usable Privacy and Security**. [S.l.: s.n.], 2006. p. 3–4.

SNOWDEN, E. Russia's new Big Brother law is an unworkable, unjustifiable violation of rights that should never be signed. **Twitter**. 2016. Acesso em: 07 de Julho 2016. Disponível em: <https://twitter.com/Snowden/status/746671700247457792>.

THE GUARDIAN. Mark Zuckerberg 'sympathetic' with Apple over FBI but 'we'll help government'. **The Guardian**. 2016. Acesso em: 06 de Julho 2016. Disponível em: <https://www.theguardian.com/technology/2016/feb/22/mark-zuckerberg-sympathetic-apple-fbi-encryption-battle>.

THIELMAN, S. Apple v the FBI: what's the beef, how did we get here and what's at stake? **The Guardian.** 2016. Acesso em: 06 de Julho 2016. Disponível em:

<https://www.theguardian.com/technology/2016/feb/20/apple-fbi-iphone-explainer-san-bernardino>.

THOMSEN, S. Extramarital affair website Ashley Madison has been hacked and attackers are threatening to leak data online. **Business Insider Australia**. 2015. Acesso em: 05 de Julho 2016. Disponível em: <http://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7>.

TZU, S. Arte Da Guerra. [S.l.]: **Editora Pensamento**, 1988.

WESTIN, A. Privacy and Freedom. **Bodley Head**, 1970. ISBN 9780370013251. Disponível em: <https://books.google.com.br/books?id=rapOSAAACAAJ>.

WHITTEN, A.; TYGAR, J. D. Why johnny can't encrypt: A usability evaluation of pgp 5.0. In: **Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8**. Berkeley, CA, USA: USENIX Association, 1999. (SSYM'99), p. 14–14. Disponível em: <http://dl.acm.org/citation.cfm?id=1251421.1251435>.

WINCKLER, M. A.; PIMENTA, M. S. Análise e modelagem de tarefas. In: **Congresso Brasileiro de Fatores Humanos em Sistemas Computacionais.** [S.l.: s.n.], 2004. p. 3.

WINTER, B. Insight: How U.S. spying cost Boeing multibillion-dollar jet contract. **Reuters**. 2013. Acesso em: 05 de Julho 2016. Disponível em: <http://www.reuters.com/article/us-boeing-brazil-insight-idUSBRE9BJ10P20131220>.

YEE, K.-P. User interaction design for secure systems. In: SPRINGER. **International Conference on Information and Communications Security.** [S.l.], 2002. p. 278–290.

YUHAS, A. Hillary Clinton campaign blames leaked DNC emails about Sanders on Russia. **The Guardian**. 2016. Acesso em: 07 de Agosto 2016. Disponível em: <https://www.theguardian.com/us-news/2016/jul/24/clinton-campaign-blames-russia-wikileaks-sanders-dnc-emails>

ZURKO, M. E.; SIMON, R. T. User-centered security. In: **ACM. Proceedings of the 1996 workshop on New security paradigms.** [S.l.], 1996. p. 27–33.

APÊNDICE A - TERMO DE CONSENTIMENTO

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

1. Você está sendo convidado para participar da pesquisa “Usabilidade nas Soluções de E-mail Seguro: O Modelo Mental de Segurança do Usuário”.
2. Esta pesquisa tem como objetivo avaliar a percepção dos usuários em uso das ferramentas de e-mail seguro Xmail e Private WebMail (Pwm), verificando a proximidade do modelo mental dos usuários com o modelo conceitual implementado pelas ferramentas. Para a coleta de informações serão utilizados questionários digitais, câmeras de vídeo, captura de telas e uma entrevista pós-estudo.
3. Sua participação é voluntária e não é obrigatória.
4. Você será convidado a responder um questionário e/ou uma entrevista sobre a sua opinião em relação ao uso, à privacidade, segurança da informação e a sua experiência com as ferramentas de segurança.
5. Faremos o possível para minimizar e evitar possíveis constrangimentos ou desconfortos. No entanto, caso ocorra alguma inconveniência, você pode se recusar a responder ou mesmo interromper a sua participação a qualquer momento, sem qualquer prejuízo. Além disso, caso venha a sofrer qualquer tipo de dano resultante desta participação, asseguramos o direito à indenização.
6. Antes e durante a sua participação na pesquisa, você receberá esclarecimentos a respeito dos procedimentos que serão feitos durante a pesquisa.
7. A qualquer momento você pode solicitar mais esclarecimentos e/ou se recusar a participar ou retirar seu consentimento, sem prejuízo algum.
8. As informações obtidas através dessa pesquisa, por meio dos questionários e pelo sistema computacional serão confidenciais e asseguramos o sigilo sobre esses dados.
9. Vale ressaltar que, as ferramentas da avaliação ainda são protótipos e problemas técnicos podem acontecer durante o teste. Além disso, os e-mails enviados para o teste deverão ser apagados no final do teste, bem como todos os registros das ferramentas usadas.
10. Ao participar deste estudo, você autoriza a captação de sua imagem e voz pelo grupo de pesquisadores, a serem utilizadas em obras audiovisuais a serem produzidas para fins didáticos e/ou científicos, sejam essas destinadas à divulgação ao público em geral e/ou apenas para uso interno do grupo de pesquisadores.
    a. A presente autorização, concedida a título gratuito, confere à Universidade Federal de São Carlos – UFSCar, através do Laboratório de Interação Avançada – LIA do Departamento de Computação, o direito de utilizar as mensagens, imagens e voz, que farão parte de um “banco de imagens”, nas obras para veiculação interna na

UFSCar, bem como em eventos externos, no Brasil e no exterior, por mídia escrita, eletrônica ou digital, tais como atividades de caráter científico, trabalhos científicos, Revistas, folders, programas de Rádio e TV, entre outros, a critério exclusivo do LIA, desde que não haja desvirtuamento da sua finalidade.

b. Para minimizar os riscos envolvendo a sua privacidade, todos os dados coletados, as mensagens, imagens e voz não estarão expostos na internet durante o experimento e somente a equipe de pesquisa terá acesso aos dados para análise posterior. Todos os cuidados serão tomados com os dados a serem publicados para assegurar o anonimato.

11. Os resultados obtidos através dessa pesquisa serão utilizados para investigar melhorias no design das ferramentas para promover uma experiência de uso cada vez melhor.
12. Além de colaborar com o presente estudo, você pode se sentir beneficiado por ter acesso às ferramentas Xmail e Private WebMail, as quais fornecem uma maneira de preservar sua privacidade e garantir a integridade de seus dados, por meio da comunicação de e-mails utilizando o navegador Google Chrome e o webmail Gmail.
13. Você receberá uma cópia deste termo onde consta o telefone e o endereço do pesquisador principal, podendo tirar suas dúvidas sobre o projeto e sua participação, agora ou a qualquer momento:

Lucas Cesar Ferreira
Celular: (14) 99660-3812
Email: lucascesarf@gmail.com
Laboratório de Interação Avançada – LIA
Departamento de Computação - DC
Universidade Federal de São Carlos - UFSCar
São Carlos/SP
Tel.: (16) 3351-8615/8233

Declaro que entendi os objetivos, riscos e benefícios de minha participação na pesquisa e concordo em participar.

Nome: _____ Assinatura: _____

Data: ___ /___/_____ Local: _____

APÊNDICE B - PRÉ-QUESTIONÁRIO

Você está sendo convidado para participar de uma pesquisa sobre segurança e privacidade, realizada pela Universidade Federal de São Carlos - UFSCar.

Leia cuidadosamente e indique sua opinião sobre cada afirmação. A sua opinião é muito importante.

Lembre-se que não há respostas "certas" ou respostas "erradas". Todas as respostas são anônimas.

SEÇÃO 1 – PERFIL E DADOS DEMOGRÁFICOS

Perguntas relacionadas ao seu perfil.

1. O seu gênero:

[ ] Masculino

[ ] Feminino

[ ] Outro

[ ] Prefiro não responder

2. A sua idade: _____

3. Qual o seu grau de escolaridade?

[ ] Nenhuma escolaridade

[ ] Ensino fundamental completo

[ ] Ensino médio completo

[ ] Ensino superior

[ ] Pós-graduado

[ ] Prefiro não responder

4. Qual é sua profissão ou curso? _____

5. Você já tem mais de um ano de curso ou experiência?

[ ] Sim [ ] Não [ ] Talvez

6. Quantas pessoas próximas a você possuem algum certificado ou diploma relacionado à área de computação?

[ ] Nenhuma

[ ] Menos de 5 pessoas

[ ] Entre 5 e 10 pessoas

[ ] Mais de 10 pessoas

7. Qual(is) do(s) dispositivo(s) você usa para enviar e-mails?

[ ] Computador/Notebook

[ ] Tablet

[ ] Smartphone

[ ] Outros

8. Com qual frequência, em média, você envia e-mails (p/dia)?

[ ] Menos de 5 vezes

[ ] Entre 5 e 10 vezes

[ ] Entre 10 e 20 vezes

[ ] Mais de 20 vezes

9. Além do Gmail, você atualmente usa outros serviços webmail?

[ ] Outlook/Hotmail

[ ] Yahoo!

[ ] Outros

[ ] Não uso outros serviços

SEÇÃO 2 – PRIVACIDADE E SEGURANÇA

Estamos interessados em saber como sua opinião sobre privacidade e segurança da informação. Lembre-se que todas as informações dadas são anônimas.

10. Qual a frequência, em média, que você utiliza aplicativos ou sites para transações bancárias (p/semana)?
    [ ] Não uso
    [ ] Menos de 5 vezes
    [ ] Entre 5 e 10 vezes
    [ ] Mais de 10 vezes

11. Qual(is) meio(s) você envia seus dados que considera “privados” ?
    [ ] E-mails (Gmail, Outlook e etc.)
    [ ] Mensagens instantâneas (Whatapps, Telegram e etc.
    [ ] Redes Sociais (Facebook, Twitter e etc.)
    [ ] Ligações Telefônicas
    [ ] Outros

12. Quantos casos, em média, de violação de privacidade você conhece (clonagem de cartão, exposição de dados pessoais e etc.)?
    [ ] Nenhum
    [ ] Menos de 5 vezes
    [ ] Entre 5 e 10 vezes
    [ ] Mais de 10 vezes

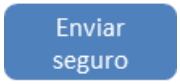
13. Caso conheça algum, fale sobre (nome, lugar, principal prejudicado e etc.):

    _____

14. Algum desses casos com pessoas/empresas próximas a você?
    [ ] Sim [ ] Não [ ] Talvez

15. Suponhamos que você está no WhatApp e precisa enviar o código de segurança do seu cartão para um amigo. Qual das analogias de segurança abaixo você usaria para enviar o código de segurança do cartão?



[ ] Cadeado Aberto [ ] Cadeado Fechado [ ] Chaves [ ] Botão “enviar seguro”

16. Por que acredita ser a melhor analogia?

_____

17. Você conhece as políticas de privacidade dos serviços web (Gmail, Outlook, Yahoo!, Facebook, Youtube e etc.)?

[ ] Sim [ ] Não [ ] Talvez

18. Suponhamos que esses serviços web, como Gmail, Facebook e WhatsApp, coletam e vendem seus dados privados como um "pagamento" ao serviço oferecido. Qual sua opinião sobre isso?

	1	2	3	4	5	
Discordo	[ ]	[ ]	[ ]	[ ]	[ ]	Concordo

19. Por que concorda ou discorda? Comente:

_____

20. Marque abaixo o seu nível de conhecimento geral:

	Nenhum	Iniciante	Intermediário	Avançado
Qual seu nível de expertise em computação?	[ ]	[ ]	[ ]	[ ]
Qual seu nível de conhecimento geral sobre Privacidade e Segurança da Informação?	[ ]	[ ]	[ ]	[ ]

APÊNDICE C - PÓS-QUESTIONÁRIO

Você está sendo convidado para participar de uma pesquisa sobre segurança e privacidade, realizada pela Universidade Federal de São Carlos - UFSCar.

Leia cuidadosamente e indique sua opinião sobre cada afirmação. A sua opinião é muito importante.

Lembre-se que não há respostas "certas" ou respostas "erradas". Todas as respostas são anônimas.

SEÇÃO 1 – PERCEPÇÃO EM USO DAS FERRAMENTAS

1. Qual foi seu personagem na avaliação?

[ ] Pessoa A (emissor)

[ ] Pessoa B (receptor)

2. Marque abaixo a sua opinião sobre a ferramenta Xmail

	Totalmente Desnecessário	Desnecessário	Neutro	Necessário	Totalmente Necessário
Para a privacidade e segurança, a criação da passphare (senha) foi	[ ]	[ ]	[ ]	[ ]	[ ]
Para o uso diário, o envio de e-mails seguro sem ter que fazer nenhuma ação a mais foi	[ ]	[ ]	[ ]	[ ]	[ ]
Para o uso diário, o envio de emails sem segurança com o esforço de "abrir o cadeado" foi	[ ]	[ ]	[ ]	[ ]	[ ]

3. Qual(is) foi(ram) sua(s) maior(es) dificuldade(s) para o envio de e-mails?

[ ] Criar a passphare (senha)

[ ] O envio do convite para o seu amigo

[ ] O envio do email seguro

[ ] O envio do email sem segurança

[ ] Não tive dificuldades

4. Caso teve outras dificuldades, comente:

_____

5. Marque abaixo a sua opinião sobre a ferramenta Xmail

	Totalmente Desnecessário	Desnecessário	Neutro	Necessário	Totalmente Necessário
Os tutoriais de inicialização foram	[ ]	[ ]	[ ]	[ ]	[ ]
Para a segurança, a mudança de cor na janela do gmail foi	[ ]	[ ]	[ ]	[ ]	[ ]
Para uso diário, o envio de e-mails com segurança com o esforço de clicar no botão "Turn on encryp" foi	[ ]	[ ]	[ ]	[ ]	[ ]
Para uso diário, o envio de e-mails sem segurança sem ter que fazer nenhuma ação a mais foi	[ ]	[ ]	[ ]	[ ]	[ ]

6. Na ferramenta Private WebMail (Pwm), Qual foi sua maior dificuldade para o envio de e-mails?

[ ] Entender os tutoriais

[ ] O envio do e-mail seguro

[ ] O envio do e-mail sem segurança

[ ] Não tive dificuldades

7. Caso teve outras dificuldades, comente:

_____

8. Qual ferramenta você se sentiu mais seguro(a)?

[ ] Nenhuma

[ ] Xmail

[ ] Private WebMail (Pwm)

[ ] Ambas

9. Caso teve outras dificuldades, comente:

_____

10. Após a instalação e configuração, qual ferramenta você achou mais fácil de enviar e-mails SEGUROS?

[ ] Nenhuma

[ ] Xmail

[ ] Private WebMail (Pwm)

[ ] Ambas

11. Por que achou essa ferramenta mais fácil de enviar e-mails seguros?

_____

12. Após a instalação e configuração, qual ferramenta você achou mais fácil de enviar e-mails SEM SEGURANÇA

[ ] Nenhuma

[ ] Xmail

[ ] Private WebMail (Pwm)

[ ] Ambas

13. Por que achou essa ferramenta mais fácil de enviar e-mails sem segurança?

_____

14. Os Feedbacks (uso de cores e ícones de cadeados, e-mails de convite/confirmação, pop-ups de tutoriais) das ferramentas te ajudaram na conclusão das tarefas?

[ ] Nem percebi

[ ] Sim

[ ] Não

[ ] Talvez

15. Caso sim como te ajudou?

_____

SEÇÃO 2 – ADOÇÃO DAS FERRAMENTAS

Estamos interessados em saber a sua opinião sobre a adoção das ferramentas.

Lembre-se que todas as informações dadas são anônimas.

16. Qual foi sua ferramenta favorita?

[ ] Nenhuma

[ ] Xmail

[ ] Private WebMail (Pwm)

[ ] Ambas

17. Por que escolheu esta ferramenta?

_____

18. Por que escolheu esta ferramenta?

	1	2	3	4	5	
Pouco Provável	[ ]	[ ]	[ ]	[ ]	[ ]	Muito Provável

19. Comente a resposta acima

_____

APÊNDICE D - FOLDER DE APRESENTAÇÃO

Estudo com o Gmail

Estamos conduzindo um estudo para saber o que você acha da segurança de seus dados quando manda e-mails.
Venha participar e traga um amigo pois precisamos de duplas que possam nos ajudar a entender o que podemos fazer para melhorar o design dessas ferramentas.

- O estudo vai demorar no máximo 35 minutos
- Precisamos que venha junto com alguém
- Você não será remunerado, mas receberá um pequeno brinde em agradecimento por sua participação.
- Marque um horário conosco por:
  - Site: lia-ufscar.youcanbook.me
  - Whatsapp: (14) 99660-3812
  - Email: lucas.ferreira@gmail.com

LABORATÓRIO DE INTERAÇÃO AVANÇADA
UFSCAR

Mais Informações
Lucas Cesar Ferreira (pesquisador responsável)
Celular: (14) 99660-3812
Email: lucas.ferreira@gmail.com
DC - UFSCar

lia-ufscar.youcanbook.me Teste segurança no Gmail