UNIVERSIDADE FEDERAL DE SANTA CATARINA
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA

Taciane Martimiano

ANÁLISE DE CERIMÔNIAS NO SISTEMA DE VOTAÇÃO HELIOS

Florianópolis

Taciane Martimiano

ANÁLISE DE CERIMÔNIAS NO SISTEMA DE VOTAÇÃO HELIOS

Trabalho de conclusão de curso submetido à Ciências da Computação para a obtenção do Grau de Bacharel em Ciências da Computação.
Orientador: Prof. Dr. Jean Everson Martina
Universidade Federal de Santa Catarina

Florianópolis

Catalogação na fonte elaborada pela biblioteca da
Universidade Federal de Santa Catarina

A ficha catalográfica é confeccionada pela Biblioteca Central.

Tamanho: 7cm x 12 cm

Fonte: Times New Roman 9,5

Maiores informações em:
http://www.bu.ufsc.br/design/Catalogacao.html

Taciane Martimiano

ANÁLISE DE CERIMÔNIAS NO SISTEMA DE VOTAÇÃO HELIOS

Este Trabalho de conclusão de curso foi julgado aprovado para a obtenção do Título de "Bacharel em Ciências da Computação", e aprovado em sua forma final pela Ciências da Computação.

Florianópolis, Novembro de 2014

.

Prof. Dr. Vitório Bruno Mazzola
Universidade Federal de Santa Catarina
Coordenador do Curso

Prof. Dr. Jean Everson Martina
Universidade Federal de Santa Catarina
Orientador

Banca Examinadora:

Prof. Dr.
Ricardo Felipe Custódio
Universidade Federal de Santa Catarina

Dr.
Marcelo Carlomagno Carlos
Holloway University of London

Aos meus pais, por todo amor, educação, confiança e paciência que sempre me dedicaram.

AGRADECIMENTOS

Agradeço em especial ao meu orientador Jean Martina pela oportunidade de estudo e aprendizado na área de cerimônias de segurança, a qual apresenta aspectos muito interessantes ainda inexplorados, e ajuda no desenvolvimento deste trabalho.
Agradeço à Maina Olembo pela parceria e apoio, uma vez que seu estudo sobre o voto pela Internet e melhorias no sistema de votação Helios serve de base para as análises realizadas nesse trabalho.

"Quando uma criatura humana desperta para um grande sonho e sobre ele lança toda a força de sua alma, todo o universo conspira a seu favor."

Johann Goethe

RESUMO

Cerimônias podem ser compreendidas como uma extensão da já conhecida estrutura dos protocolos, largamente utilizados no dia a dia das pessoas. Nos protocolos, as ações humanas são apenas suposições, as quais podem não ser realísticas quando implementadas, circunstância que leva à falha dos objetivos inicialmente propostos para o protocolo em questão.

As cerimônias incluem o ser humano como um nodo do sistema, portanto existem canais específicos de comunicação para relacioná-lo com os demais nodos: canal humano-dispositivo (como, por exemplo, interfaces) e canal humano-humano, para gestos e conversas entre seres humanos.

Cada um desses canais, além do canal dispositivo-dispositivo já presente nos protocolos, necessitará de análise diferenciada para detectar a quais reais ameaças estarão sujeitos em variados cenários passíveis para o sistema. Através dessa análise mais detalhada dos meios e elementos envolvidos, é possível encontrar falhas de segurança não detectáveis através apenas dos protocolos.

Neste trabalho, serão estruturadas e formalizadas as cerimônias que representam as melhorias propostas por Olembo para o sistema de votação eletrônica Helios, fazendo uso do modelo de ameaça adaptativo proposto por Carlos et al. e verificação das propriedades das cerimônias.

Palavras-chave: Análise de cerimônias de segurança, modelos de ameaça, especificação formal, Helios

ABSTRACT

Ceremonies can be understood as an extension of the already known structure of the protocols which are widely used in people's daily life. In protocols, human actions are only assumptions, which may not be realistic when implemented, such circumstance leads to failure of the objectives initially proposed for the protocol.
Ceremonies include the human being as a node of the system, so there are specific communication channels to relate it with the other peers: human-device channel, i.e. interfaces, and human-human channel, to gestures and conversations between humans.
Each of these channels, besides the device-device channel already present in protocols, requires differentiated analysis to detect the real threats they will be subject in several feasible scenarios for the system. Through this more detailed analysis of the channels and elements involved, it is possible to find security flaws not detectable in protocols. In this work, we will structure and formalize the ceremonies representing the improvements proposed by Olembo for the Helios voting system, using the adaptive threat model proposed by Carlos et al. and verification of ceremonies' properties.

Keywords: Security ceremonies analysis, threat models, formal specification, Helios

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Após a introdução da concepção de um atacante ativo no sistema por Needham e Schroeder (NEEDHAM; SCHROEDER, 1978), e seu aperfeiçoamento por Dolev e Yao (DOLEV; YAO, 1983), tem-se um modelo de ameaça largamente aceito no mundo todo e utilizado como referência para checar se um dado protocolo é seguro contra um atacante tão forte (capaz de possuir total domínio sobre o canal).

Considera-se que se um protocolo é seguro contra um dado atacante, é também seguro contra atacantes mais fracos. A mesma ideia aplica-se às cerimônias, contudo mesmo uma cerimônia provada segura contra um forte atacante pode apresentar falhas quando implementada se forem consideradas situações irreais para o seu uso.

A dificuldade de implementação de cerimônias se dá pela modelagem do nodo humano. Diferentemente de nodos 'dispositivo', não se pode programar humanos. O que se faz, nesse caso, é analisar (observar) o comportamento de um humano interagindo com o sistema (ELLISON, 2007).

Para uma implementação mais adequada das ações humanas, as cerimônias contam com dois específicos canais de comunicação: humano-humano e humano-dispositivo, canais estruturados para o envolvimento do nodo humano com a estrutura pré-existente dos protocolos.

Através do modelo adaptativo proposto por Carlos et al (CARLOS et al., 2013), é possível definir para cada um dos três canais de comunicação (canais humano-humano, humano-dispositivo e dispositivo-dispositivo) qual o modelo de ameaça mais conveniente a ser adotado dadas as reais ameaças às quais estarão sujeitos. Dessa forma, as cerimônias serão estruturadas e formalizadas de acordo com as propostas desenvolvidas para o sistema de votação online Helios (NEUMANN et al., 2014).

1.1 OBJETIVO

1.1.1 Objetivo Geral

Este trabalho visa enfatizar a importância do emprego de cerimônias na avaliação da segurança das aplicações de uso cotidiano, por meio da análise das cerimônias de um sistema real e constatação das ameaças presentes nos seus canais de comunicação.

1.1.2 Objetivos Específicos

- Estudar cerimônias de segurança de um sistema real - Helios, apresentando suas especificações formais (com base no modelo de ameaça Dolev-Yao);
- Estudar as propriedades das cerimônias a fim de fazer a análise das cerimônias para o sistema em questão;
- Distinguir os cenários de amaça realísticos e não-realísticos, fazendo uso do modelo de ameaça adaptativo e das propriedades das cerimônias.

1.2 JUSTIFICATIVA

A introdução do conceito de cerimônias (ELLISON, 2007) permitiu a descoberta de falhas de segurança antes não detectáveis. Ellison destaca que tudo o que um protocolo não consegue cobrir é incorporado pela cerimônia, uma vez que os protocolos são um subconjunto das cerimônias. Assim, o que nos protocolos eram apenas suposições (as quais quando implementadas podem comprometer a segurança do sistema e acabar por fazer o protocolo não alcançar os objetivos propostos), podem ser bem definidas no contexto das cerimônias. Adicionalmente, tem-se que estudar qual o modelo mais adequado para cada cerimônia, uma vez que não há um modelo único que se ajuste a todas. Vários cenários e circunstâncias devem ser considerados na análise e formalização das cerimônias para garantir integridade e confidencialidade ao sistema.

1.3 METODOLOGIA

Para a realização deste trabalho, foi estudado e aplicado o framework proposto por Carlos et al.(CARLOS et al., 2013). Também foram estudados outros artigos sobre análise e propriedades de cerimônias, além das melhorias propostas por Olembo (NEUMANN et al., 2014) para o sistema de votação Helios.

No que diz respeito às propostas, foram desenvolvidas especificações das cerimônias com base em diagramas do funcionamento do sistema e estudo dos possíveis cenários para tais cerimônias. A seguir, foi estruturado o modelo de ameaça que mostra para cada canal de

comunicação qual o pior risco ao qual esse canal está sujeito e quais as situações e ações realísticas de possíveis intrusos. Para isso, o modelo de ameaça de Dolev-Yao será utilizado como base na descrição e formulação das propriedades de possíveis perfis de atacantes do sistema.

1.4 PUBLICAÇÕES

Paper STAST, em anexo no site de projetos:
Modelling User Devices in Security Ceremonies. Taciane Martimiano, Jean Everson Martina (Universidade Federal de Santa Catarina - UFSC), Maina Olembo (CASED, TU Darmstadt) and Marcelo Carlos (RHUL).

Paper SBSeg, também em anexo no site de projetos:
Análise de cerimônias no sistema de votação Helios. Taciane Martimiano, Jean Everson Martina (Universidade Federal de Santa Catarina - UFSC) e Maina Olembo (CASED, TU Darmstadt).

1.5 ESTRUTURA DO TRABALHO

O capítulo 2 aborda definições importantes para a compreensão das discussões presentes neste trabalho. Nesse capítulo encontra-se a definição do conceito de cerimônias, seus meios de comunicação, relação das cerimônias e protocolos, assim como fatores presentes na interação com o ser humano.

O capítulo 3 contém uma breve descrição do Helios original, juntamente com as suposições necessárias e consideradas no presente trabalho.

O capítulo 4 apresenta as propostas para o sistema Helios estudadas, descrevendo as mudanças sugeridas tanto para a versão web com uso de institutos de verificão quanto considerando o uso de aplicativo da eleição para smartphone.

O capítulo 5 mostra as análises feitas sobre as propostas citadas, discutindo os resultados dessas análises e ressaltando os ganhos de se analisar cerimônias.

Por fim, o capítulo 6 traz as conclusões e trabalhos futuros.

2 CERIMÔNIAS DE SEGURANÇA

Este capítulo apresenta as principais características das cerimônias de segurança, além de uma breve descrição do modelo de ameaça adaptativo empregado na análise das cerimônias presentes neste trabalho.

2.1 DEFINIÇÃO

Desde que Needham e Schroeder (NEEDHAM; SCHROEDER, 1978) introduziram os primeiros protocolos de segurança, métodos de verificação tem sido estudados e propostos visando checar e provar a corretude na execução dos protocolos.

Considerando o vasto conjunto de trabalhos desenvolvidos, pode-se citar como principais: Burrows et al (BURROWS; ABADI; NEEDHAM, 1989) pela criação da lógica de derivação de crenças para as entidades dos protocolos, Abadi pelo *spi-calculus* (ABADI; GORDON, 1997), Ryan (RYAN; SCHNEIDER, 2000), Lowe (LOWE, 1996) e Meadows (MEADOWS, 1996) pelos trabalhos em enumeração de estados, e Paulson e Bella (BELLA, 2007; BELLA; LONGO; PAULSON, 2003) pelo método indutivo.

Técnicas e ferramentas para verificação de protocolos tem sido criadas, analisando complexos protocolos. Porém, como Martina et al (MARTINA; CARLOS, 2010) ressalta, mesmo os melhores e mais testados protocolos podem se tornar vulneráveis a problemas de segurança. Isso ocorre devido a uma atitude inesperada (ainda que razoável) vinda por parte do usuário.

Protocolos são verificados computacionalmente, contudo foram desenvolvidos para atender às necessidades humanas. Nesse contexto entram as cerimônias de segurança, as quais consideram os aspectos cognitivos humanos na interação com os protocolos.

A análise de cerimônias estende a análise de protocolos devido à inclusão de nodos humanos ao sistema (ELLISON, 2007). Tal inclusão traz um aumento de complexidade à análise, contudo proporciona resultados mais precisos e completos, sendo possível inclusive detectar falhas de segurança previamente não detectáveis (CARLOS et al., 2013).

Nos protocolos, as ações humanas são meramente modeladas como suposições. Quando o protocolo é então implementado, tais suposições podem resultar em interações de usuário não realísticas (não compatíveis com situações cotidianas do mundo real). Em uma ce-

rimônia de segurança, temos o fator humano projetado como parte integrante do sistema. Assim, tem-se dois canais adicionais ao canal dispositivo-dispositivo (proveniente da estrutura dos protocolos). Esses canais são o canal humano-dispositivo e o canal humano-humano, empregados para relacionar o 'nodo' humano a outros nodos humanos e demais nodos do sistema. Portanto, as cerimônias contam com três canais de comunicação: humano-humano (HH), humano-dispositivo(HD) e dispositivo-dispositivo(DD).

Entender o correto modelo de ameaça (ao qual o usuário estará sujeito ao interagir em uma cerimônia) evita sobrecarregar tal usuário com situações hipotéticas e garante propriedades de segurança, tais como sigilo e integridade (CARLOS et al., 2013).

2.2 MODELO DE AMEAÇA ADAPTATIVO

Inicialmente, os protocolos eram desenvolvidos com o intuito de serem seguros contra atacantes passivos (capazes de escutar os canais de comunicação e fazer uso dos conteúdos trocados por tais canais) (DOLEV; YAO, 1983). O conceito de um atacante ativo foi apresentado por Needham–Schroeder (NEEDHAM; SCHROEDER, 1978).

Dolev e Yao (DOLEV; YAO, 1983) formalizaram o modelo de atacante introduzido por Needham and Schroeder (NEEDHAM; SCHROEDER, 1978), onde o atacante tem total controle da rede, sendo capaz de copiar, replicar, alterar e criar mensagens. Basicamente, o que o atacante não pode fazer é criptoanálise. As capacidades de um atacante Dolev-Yao são definidas a seguir:

- Escuta (*Eavesdrop*) – O atacante aprende os conteúdos das mensagens enviadas pelo canal de comunicação apenas por ouvir o canal;

- Iniciar (*Initiate*) – O atacante pode usar qualquer informação em seu conhecimento para iniciar uma comunicação com um agente do sistema;

- Quebra Atômica (*Atomic Break Down*) – O atacante consegue quebrar uma mensagem em seus subcomponentes, onde cada um desses subcomponentes é de seu conhecimento;

- Bloquear (*Block*) – O atacante consegue prevenir o destinatário de aprender o conteúdo de mensagens enviadas para ele;

- Criptografia (*Crypto*) – Para toda mensagem cifrada com uma chave que seja de conhecimento do atacante, ele é capaz de decifrar as mensagens e aprender seus conteúdos;
- Fabricar (*Fabricate*) – O atacante pode usar funções de conhecimento público para fabricar novas mensagens;
- Fabricação (*Spoof*) – O atacante é capaz de enviar uma mensagem utilizando a identidade de um outro agente. Essa capacidade se diferencia de Iniciar por não permitir ao atacante ser um agente interno na cerimônia;
- Reordenar (*Re-order*) – O atacante pode reordenar as mensagens enviadas a um dado agente, induzindo-o a aprender as mensagens em uma ordem diferente da original;
- Modificar (*Modifying*) – O atacante usa ambas as capacidades Bloquear e Iniciar descritas acima;
- Replicar (*Replaying*) – O atacante combina Escuta e Iniciar, descritas acima.

Esse modelo de ameaça é conhecido como Dolev-Yao, sendo o padrão utilizado na análise de protocolos (BELLA, 2007). Duas linhas de pesquisa derivaram desse modelo. A primeira considera que o modelo Dolev-Yao deve ser extendido devido à restrição de que o atacante não pode realizar criptoanálise (BELLARE; ROGAWAY, 1994). A segunda defende a ideia de que se um dado protocolo é seguro contra o modelo de ameaça Dolev-Yao, então também é seguro contra um atacante 'menos poderoso'. Através do ajuste de poderes do atacante, visando aderir às circunstâncias do mundo real, eventuais sutilezas podem ser descobertas (mesmo depois do protocolo em questão ter sido provado seguro contra o modelo Dolev-Yao) (ARSAC et al., 2009).

Seguindo a segunda linha de pesquisa, o modelo de ameaça adaptativo utilizado nesse trabalho faz uso do conjunto de capacidades do atacante Dolev-Yao apresentado acima, através da adição e remoção dinâmica de capacidades. Esse modelo de ameaça realístico e dinâmico permite a concepção de atacantes mais fortes ou mais fracos (em relação ao atacante Dolev-Yao clássico) dependendo dos cenários aos quais a cerimônia estará sujeita (CARLOS et al., 2013).

3 SISTEMA DE VOTAÇÃO HELIOS

Visando a confiança dos eleitores, sistemas criptográficos de votação online que oferecem verificabilidade e sigilo do voto tem sido propostos e continuam sendo aprimorados. Nesse contexto, Helios(ADIDA, 2008)(ADIDA et al., 2009), um sistema de votação baseado na Internet, verificável e de código aberto, tem sido usado principalmente no meio acadêmico.

No Helios, assume-se que os eleitores irão verificar seus votos várias vezes (através do uso de votos de teste), visando garantir a integridade do voto final(ADIDA, 2008). Contudo, estudos apontam que isso não é feito devido à dificuldade do processo(KARAYUMAK et al., 2011a). Por exemplo, o Helios exige que os eleitores comparem manualmente os hashes apresentados pela cabine de votação (Helios *ballot preparation system* – BPS) e pelo Helios *ballot verifier system* (BVS) em ordem a confirmar que o procedimento de verificação individual do voto foi bem sucedido.

Levando a usabilidade do sistema em consideração, melhorias foram sugeridas como tentativa de estimular o uso correto e prático do sistema. Para tanto, o eleitor pode usar as páginas web dos institutos confiáveis participantes ou baixar e instalar um aplicativo em seu smartphone. Uma análise da segurança computacional de tais propostas é desenvolvida nesse trabalho, com foco em sigilo e integridade (propriedades importantes para a votação verificável).

Para tal análise, as propostas foram modeladas como cerimônias de segurança, empregando o framework proposto por Carlos et al(CARLOS et al., 2013), o qual é baseado no conjunto de capacidades do modelo de ameaça de Dolev-Yao(DOLEV; YAO, 1983), citadas no capítulo anterior.

A seguir é apresentado o protocolo do Helios original. Adicionalmente, são apresentadas algumas suposições necessárias para o presente trabalho.

3.1 PROTOCOLO HELIOS

O eleitor recebe um e-mail com o link para a cabine de votação do Helios. Ao abrir o link, o eleitor poderá escolher o(s) candidato(s) de sua preferência. A cabine de votação cifra o voto e apresenta o hash para o eleitor. Esse hash deve ser registrado para uso posterior, caso

em que o eleitor deseja verificar seu voto. A seguir, o eleitor terá então de escolher se deseja verificar seu voto ou submetê-lo para contagem final.

No caso da verificação do voto, a cabine de votação apresenta o(s) candidato(s) votado(s) e informação randômica usada na cifragem. O eleitor entra com essas informações no sistema de verificação do Helios (BVS). O BVS então cifra essas informações, apresentando ao eleitor um segundo hash. Assim, para completar o processo, é necessário que o eleitor confira se os dois hashes são iguais de forma a garantir que o sistema cifrou corretamente o voto.

O eleitor pode repetir o processo de verificação quantas vezes quiser. Votos que foram verificados não podem mais ser submetidos para contagem final, uma vez que o eleitor tomou conhecimento da informação randômica e poderia facilmente revelar seu voto. Portanto, nova informação randômica precisa ser gerada. É nesse contexto que é recomendado testar votos diferentes do voto final(KARAYUMAK et al., 2011b), para que não sejam gerados resultados 'viciados'.

No caso em que o eleitor escolhe submeter seu voto final, é requerido que ele faça login e assim seu voto é publicado no quadro de avisos (*bulletin board*, em inglês), onde é armazenado o voto cifrado assim como o hash de tal voto. Para concluir o procedimento, o eleitor deve confirmar que seu nome, ou algum pseudônimo, aparece ao lado do hash de seu voto (ADIDA, 2008)(ADIDA et al., 2009). Feito isso, considera-se que auditores conferem periodicamente o quadro de avisos a fim de prevenir comportamentos maliciosos.

3.2 SUPOSIÇÕES

Abaixo estão listadas suposições relacionadas ao Helios original e às análises utilizadas nesse trabalho, envolvendo as entidades e as próprias cerimônias.

- As entidades presentes nas cerimônias são confiáveis no que diz respeito à integridade do processo sendo executado. Essa suposição já está presente no Helios original(ADIDA, 2008).
- O atacante está presente nos canais de comunicação, sendo essa uma suposição típica do modelo Dolev-Yao.
- A cabine de votação do Helios é confiável e, assim, o eleitor tem motivação em usar o sistema para votar e verificar seu voto. O

eleitor confia na cabine de votação quanto ao sigilo das informações.

- Os institutos participantes são confiáveis, uma vez que qualquer comportamento malicioso pode conduzir à perda de reputação.
- O eleitor é um 'nodo' honesto na cerimônia, pois não considera-se coerção (eleitor sendo o próprio atacante).

- A cerimônia é considerada como tendo um único ponto de início e um único ponto de saída. O eleitor deve seguir todos os passos previstos na cerimônia que ele está executando. Portanto, as cerimônias para voto final e verificação de voto são consideradas como uma sequência ininterrupta.

4 PROPOSTAS PARA O HELIOS

Neste capítulo serão abordadas as propostas: a) aplicação web que utiliza de institutos confiáveis e b) aplicativo para smartphone, para realização dos processos de verificação e armazenamento do voto.

4.1 APLICAÇÃO WEB VINCULADA A INSTITUTOS DE VERIFICAÇÃO

Essa seção aborda brevemente os processos que os eleitores desempenhariam utilizando verificação provida pelos institutos de confiança. Tais processos são analisados através do modelo de ameça adaptativo, cujos resultados são comparados com o modelo de atacante Dolev-Yao, para ênfase dos cenários realísticos e de como a presença humana limita as ações de possíveis atacantes do sistema.

1.	V	$\xrightarrow[HD_1]{}$	B	:	URL
2.	B	$\xrightarrow[HD_1]{}$	V	:	Instructions Page
3.	V	$\xrightarrow[HD_1]{}$	B	:	"*Proceed to ballot*"
4.	B	$\xrightarrow[HD_1]{}$	V	:	Ballot Page
5.	V	$\xrightarrow[HD_1]{}$	B	:	Vote
6.	V	$\xrightarrow[HD_1]{}$	B	:	"*Review vote*"
7.	B	$\xrightarrow[HD_1]{}$	V	:	Review Page
8.	V	$\xrightarrow[HD_1]{}$	B	:	"*Encrypt vote*"
9.	B	$\xrightarrow[HD_1]{}$	V	:	$H\{\{Vote + R\}_{Epk}\}$
10.	V	$\xrightarrow[HD_1]{}$	B	:	"*Check encrypted vote*"
11.	B	$\xrightarrow[HD_1]{}$	V	:	Verifying Options Page
12.	V	$\xrightarrow[HD_1]{}$	B	:	I
13.	B	$\xrightarrow[DD_1]{}$	I	:	Vote + R
14.	I	$\xrightarrow[HD_2]{}$	V	:	$H\{\{Vote + R\}_{Epk}\}$ + Vote

Figura 1 – Instituto: voto de teste

1.	V	$\xrightarrow[HD_1]{}$	B	:	URL
2.	B	$\xrightarrow[HD_1]{}$	V	:	Instructions Page
3.	V	$\xrightarrow[HD_1]{}$	B	:	"*Proceed to ballot*"
4.	B	$\xrightarrow[HD_1]{}$	V	:	Ballot Page
5.	V	$\xrightarrow[HD_1]{}$	B	:	Vote
6.	V	$\xrightarrow[HD_1]{}$	B	:	"*Review vote*"
7.	B	$\xrightarrow[HD_1]{}$	V	:	Review Page
8.	V	$\xrightarrow[HD_1]{}$	B	:	"*Encrypt vote*"
9.	B	$\xrightarrow[HD_1]{}$	V	:	$H\{\{Vote + R\}_{Epk}\}$
10.	V	$\xrightarrow[HD_1]{}$	B	:	"*Log in to cast vote*"
11.	B	$\xrightarrow[HD_1]{}$	V	:	Login Page
12.	V	$\xrightarrow[HD_1]{}$	B	:	VoterID + Password
13.	B	$\xrightarrow[DD_3]{}$	BB	:	$\{Vote\}_{Epk}$
14.	B	$\xrightarrow[HD_1]{}$	V	:	Vote is submitted
15.	V	$\xrightarrow[HD_1]{}$	B	:	I
16.	B	$\xrightarrow[DD_1]{}$	I	:	$H\{\{Vote + R\}_{Epk}\}$
17.	I	$\xrightarrow[HD_2]{}$	V	:	$H\{\{Vote + R\}_{Epk}\}$ + VoterID

Figura 2 – Instituto: voto final

Nessa proposta[1], o processo de votação é similar ao anterior-

[1]As cerimônias que ilustram a proposta estão nas figuras 1 e 2. As mensagens estão em inglês para fazer jus ao sistema real ao qual se referem. As entidades presentes são o eleitor (representado pela letra V, *Voter* em inglês), cabine de votação (letra B, *Booth* em inglês), instituto (letra I, *Institute* em inglês) e quadro de avisos (letras BB, *Bulletin Board* em inglês). As letras abaixo das setas representam o canal pelo qual a mensagem (apresentada ao lado direito de cada imagem) é transmitida.

mente descrito para o Helios original. As diferenças entre o Helios original e as propostas aqui abordadas surgem nos processos de verificação do voto. Para poder verificar se o voto está corretamente cifrado, o eleitor primeiramente precisa registrar o hash apresentado pela cabine de votação (mensagem 9 da figura 1). O eleitor então expressa sua intenção de verificar o voto (mensagem 10 da figura 1), observa os institutos de verificação disponíveis e seleciona um no qual confia (mensagens 11 e 12 da figura 1). O eleitor é redirecionado para a página web do instituto escolhido. A cabine de votação transmite as informações necessárias para verificação para o instituto (mensagem 13 da figura 1). O instituto, por sua vez, irá computar o hash a partir das informações recebidas da cabine e apresentará o resultado de suas computações ao eleitor, juntamente com o voto recebido (mensagem 14 da figura 1). O eleitor agora precisa checar e confirmar se os dois hashes são iguais e se o voto apresentado é de fato correspondente ao candidato escolhido.

Para o eleitor conferir se o seu voto final foi corretamente armazenado no quadro de avisos, ele registra o hash apresentado (mensagem 9 da figura 2). O eleitor, então, faz login para submeter seu voto (mensagens 10-12 da figura 2). Após autenticação bem sucedida, a cabine de votação submete o voto ao quadro de avisos (mensagem 13 da figura 2). O eleitor seleciona um instituto dos vários disponíveis, após ter submetido seu voto (mensagem 15 da figura 2). Uma nova página web abre, onde o eleitor entra com o hash registrado anteriormente e confere o resultado apresentado pelo instituto (mensagem 17 da figura 2). O instituto também precisa apresentar o ID do eleitor, para evitar problemas de colisão de hashes(KUSTERS; TRUDERUNG; VOGT, 2012). Assim, mesmo que para dois eleitores seja apresentado o mesmo hash, pelo ID (que é único para cada eleitor) tal problema pode ser identificado.

Antes de entrar na análise propriamente dita das cerimônias que representam essa proposta, algumas informações adicionais são necessárias:

Com as capacidades do atacante Dolev-Yao (DY) em mente e aplicando o framework de (CARLOS et al., 2013), as cerimônias são analisadas contra um atacante menos poderoso, contudo mais realístico que o DY. Assim, aborda-se o modelo de ameaça ao qual cada canal de comunicação está sujeito, em cada um dos cenários estudados. Para isso, o modelo de ameaça adaptativo é descrito para cada cerimônia. O modelo de ameça DY também é aplicado, para posterior comparação dos resultados de maneira a mostrar que o modelo DY pode não ser o mais adequado à cerimônia sendo analisada. Para o modelo de ameaça DY considera-se que todos os canais de comunicação estão sob um

atacante DY.

Para o modelo de ameaça adaptativo, considera-se que apenas o canal dispositivo-dispositivo (DD) está sob um atacante DY, enquanto que os canais humano-humano (HH)[2] e humano-dispositivo (HD) estão sob um atacante DY-E. DY-E significa que tal atacante possui todas as capacidades de um atacante DY, exceto a capacidade Escuta. Essa capacidade é excluída, pois consideram-se ambientes controlados onde o eleitor não precisa checar ao seu redor e assegurar-se de que não há alguém espionando-o.

A respeito do canal HD, assume-se que existe um ser humano (e não uma máquina fingindo ser um humano) lidando com um dispositivo (por exemplo, olhando para a tela e digitando algo no teclado). Assim, um atacante DY-E não é capaz de comprometer o sigilo das mensagens enviadas por canais HD. Tal suposição é justificada porque o eleitor está no domínio do dispositivo, limitando as ações do atacante. Por exemplo, uma vez que o atacante não seja capaz de aprender nenhuma informação no que diz respeito às ações do eleitor, ele só consegue aplicar suas capacidades no conhecimento que ele já possui. Ou seja, mesmo que o atacante possa fabricar mensagens ou aplicar chaves criptográficas que ele possua para cifrar ou decifrar mensagens (usando suas capacidades Fabricar e Criptografia, respectivamente), ele só poderá aplicar tais capacidades em mensagens e conhecimento que ele já possua, o que não ameaça as cerimônias estudadas.

4.2 APLICATIVO PARA SMARTPHONE

Nessa proposta[3], o eleitor verifica o voto utilizando um dispositivo diferente do usado para votar, assim não há mais a necessidade de que o eleitor confie no dispositivo que utiliza para votar. Tal dispositivo para verificação é o próprio smartphone do eleitor, que já está em seu domínio e no qual ele provavelmente já confia. Essa seção aborda brevemente os processos que os eleitores desempenhariam utilizando a verificação provida pelo aplicativo da eleição no smartphone. Tais processos são analisados através do modelo de ameça adaptativo, cujos resultados são comparados com o modelo de atacante Dolev-Yao, para

[2]Neste trabalho, nenhuma das cerimônias abordadas utiliza canal humano-humano (HH), assim apenas o canal humano-dispositivo(HD) será abordado.

[3]As cerimônias que ilustram a proposta estão nas figuras 3 e 4. As mensagens estão em inglês para fazer jus ao sistema real ao qual se referem. Além das entidades que já apareceram nas cerimônias anteriores, temos a presença da entidade aplicativo (representado pela letra A, *App* em inglês).

ênfase dos cenários realísticos.

1.	V	$\xrightarrow[HD_1]{}$	B	:	URL
2.	B	$\xrightarrow[HD_1]{}$	V	:	Instructions Page
3.	V	$\xrightarrow[HD_1]{}$	B	:	"*Proceed to ballot*"
4.	B	$\xrightarrow[HD_1]{}$	V	:	Ballot Page
5.	V	$\xrightarrow[HD_1]{}$	B	:	Vote
6.	V	$\xrightarrow[HD_1]{}$	B	:	"*Review vote*"
7.	B	$\xrightarrow[HD_1]{}$	V	:	Review Page
8.	V	$\xrightarrow[HD_1]{}$	B	:	"*Encrypt vote*"
9.	B	$\xrightarrow[HD_1]{}$	V	:	Check-code + $QRCode^*$
10.	V	$\xrightarrow[HD_3]{}$	A	:	"*Open/Scan*"
11.	B	$\xrightarrow[DD_2]{}$	A	:	QRCode
12.	V	$\xrightarrow[HD_1]{}$	B	:	"*Check encrypted vote with app*"
13.	B	$\xrightarrow[HD_1]{}$	V	:	QRCode Page
14.	V	$\xrightarrow[HD_3]{}$	A	:	"*Check that vote is correctly encrypted*"
15.	B	$\xrightarrow[DD_2]{}$	A	:	$QRCode^{**}$
16.	A	$\xrightarrow[HD_3]{}$	V	:	"*Check-codes match. Is this your vote?*" + Vote
17.	V	$\xrightarrow[HD_3]{}$	A	:	Confirm (Yes)
18.	V	$\xrightarrow[HD_3]{}$	A	:	"*Close*"

*Check-code is the hash $H\{\{Vote + R\}_{Epk}\}$. In messages 9 and 11, the QRCode has the check-code contents.

**In messages 13 and 15, the QRCode has $(Vote + R + E_{pk})$ information.

Figura 3 – Aplicativo: voto de teste

1.	V	$\xrightarrow[HD_1]{}$	B	:	URL
2.	B	$\xrightarrow[HD_1]{}$	V	:	Instructions Page
3.	V	$\xrightarrow[HD_1]{}$	B	:	"*Proceed to ballot*"
4.	B	$\xrightarrow[HD_1]{}$	V	:	Ballot Page
5.	V	$\xrightarrow[HD_1]{}$	B	:	Vote
6.	V	$\xrightarrow[HD_1]{}$	B	:	"*Review vote*"
7.	B	$\xrightarrow[HD_1]{}$	V	:	Review Page
8.	V	$\xrightarrow[HD_1]{}$	B	:	"*Encrypt vote*"
9.	B	$\xrightarrow[HD_1]{}$	V	:	Check-code + $QRCode^*$
10.	V	$\xrightarrow[HD_3]{}$	A	:	"*Open/Scan*"
11.	B	$\xrightarrow[DD_2]{}$	A	:	QRCode
12.	V	$\xrightarrow[HD_1]{}$	B	:	"*Log in to cast vote*"
13.	B	$\xrightarrow[HD_1]{}$	V	:	Login Page
14.	V	$\xrightarrow[HD_1]{}$	B	:	VoterID + Password
15.	B	$\xrightarrow[DD_3]{}$	BB	:	$\{Vote\}_{Epk}$
16.	B	$\xrightarrow[HD_1]{}$	V	:	Vote is submitted
17.	V	$\xrightarrow[HD_3]{}$	A	:	"*Check that vote is on bulletin board*"
18.	A	$\xrightarrow[DD_4]{}$	BB	:	$H\{\{Vote + R\}_{Epk}\}$
19.	BB	$\xrightarrow[DD_4]{}$	A	:	Confirmation + VoterID

*Check-code is the hash $H\{\{Vote + R\}_{Epk}\}$. In messages 9 and 11, the QRCode has the check-code contents.

Figura 4 – Aplicativo: voto final

A cabine de votação apresenta um QR code contendo o hash do voto, juntamente com o próprio hash (mensagem 9 da figura 3). O eleitor utiliza seu smartphone para escanear o QR code que contém esse hash (mensagens 10 e 11 da figura 3). Tal hash será armazenado pelo aplicativo para uso posterior no processo de verificação do voto. O eleitor expressa sua intenção de verificar o voto para a cabine de votação (mensagem 12 da figura 3). A seguir, ele escaneia um segundo QR code (mensagem 15 da figura 3) e o aplicativo computa o hash e o compara com o armazenado anteriormente. Em um caso de comparação bem sucedida, o aplicativo informa que os hashes são iguais e pede ao eleitor para confirmar que o voto apresentado na tela é o voto correto (mensagens 16 e 17 da figura 3)[4].

Para verificar que o voto foi corretamente armazenado para contagem final no quadro de avisos (cerimônia apresentada na figura 4), o eleitor escaneia o primeiro QR code que contém o hash (mensagem 10 da figura 4). O eleitor faz login (mensagens 12 a 14 da figura 4) e a cabine de votação submete seu voto após autenticação bem sucedida (mensagem 15 da figura 4). O eleitor utiliza o aplicativo para checar o

[4]Essa é uma implementação de *forcing function*(NORMAN, 2002), impedindo o usuário de prosseguir sem confirmar que o voto está correto.

quadro de avisos, procurando pelo hash do seu voto (mensagem 17 da figura 4). O aplicativo realiza essa checagem consultando o quadro de avisos pelo valor do hash (mensagem 18 da figura 4). Em caso bem sucedido, o aplicativo apresenta uma mensagem para o eleitor afirmando que o hash foi armazenado no quadro de avisos. Para prevenir problemas de colisão (KUSTERS; TRUDERUNG; VOGT, 2012), o aplicativo também retorna o ID do eleitor. Em caso mal sucedido, o aplicativo informa o eleitor de que o hash não foi encontrado no quadro de avisos. O eleitor pode usar outros aplicativos para verificação. Em caso de múltiplos hashes falharem, o eleitor pode entrar em contato com a comissão eleitoral.

Antes de entrar na análise propriamente dita das cerimônias que representam essa proposta, algumas considerações adicionais são necessárias:

Apesar de os canais DD geralmente estarem sob um atacante DY, isso não é realístico para o canal DD_2 (por exemplo, na mensagem 11 da figura 3). Esse canal é um 'canal visual', uma vez que não há bluetooth ou conexão de qualquer tipo entre os dispositivos envolvidos. Nesse específico cenário, o eleitor usa seu smartphone para escanear o QR code apresentado pelo computador (considera-se que ambos os dispositivos estão no domínio do eleitor e não sob controle do atacante).

Para o canal DD_2, tem-se situações similares aos canais HD (descritas na seção 4.1). Por exemplo, o atacante não pode bloquear os conteúdos passando por esse canal uma vez que isso implicaria no atacante bloqueando a tela do computador do eleitor e seu smartphone. Situações similares acontecem se o atacante tenta aplicar qualquer outra de suas capacidades. Assim, para um ataque ser bem sucedido, o atacante precisa estar no domínio dos dispositivos do eleitor. Tal cenário só seria factível se o eleitor deixasse os dispositivos sozinhos/abandonados no meio do processo de votação.

Portanto, considera-se que o canal DD_2 também é DY-E, assim como os canais HD. Qualquer combinação enfraquecida de capacidades do atacante DY (qualquer combinação de capacidades, não envolvendo Escuta) continuará não sendo efetiva em tais canais. Isso se deve ao fato de que Escuta é a única capacidade que pode comprometer o sigilo do voto do eleitor.

5 ANÁLISE DAS CERIMÔNIAS

Aplicando o modelo de ameaça adaptativo é possível distinguir quais cenários são realísticos e se o atacante obtém sucesso em sua tentativa de corromper o sistema. Adicionalmente, são apresentadas provas que descrevem o conhecimento que cada nodo no sistema possui através do conjunto *knows(Y)*, representando o conjunto de conhecimento que um agente Y possui na cerimônia (CARLOS et al., 2013).

5.1 APLICAÇÃO WEB

A seguir estão as análises das cerimônias envolvendo os institutos. São apresentados o modelo de ameaça adaptativo e também o cenário considerando o modelo Dolev-Yao para posterior comparação na subseção dos resultados.

5.1.1 Voto de teste corretamente cifrado

Baseado na figura 1 (Instituto – cerimônia de voto de teste):
Se as mensagens M1 até M12 e a mensagem M14 são executadas contra um atacante DY-E, enquanto que a mensagem M13 é executada contra um atacante DY, tem-se que o atacante (Att) *pode impedir o instituto I de aprender Voto + R. No lugar dessa mensagem, Att envia* $Voto_{att}$ *+ R, onde* $Voto_{att}$ *é uma informação escolhida pelo atacante.*

$$\frac{(M_{1...12} \cup DY - E) \wedge (M_{13} \cup DY) \wedge (M_{14} \cup DY - E)}{\begin{array}{c} Voto \wedge R \wedge Voto_{att} \in knows(Att) \wedge Voto \in knows(B) \wedge \\ (Voto + R) \notin knows(I) \wedge (Voto_{att} + R) \in knows(I) \end{array}}$$

Prova: Assuma que o atacante *Att* iniciou duas seções do protocolo simultâneas entre a cabine de votação B e o instituto I na mensagem 13. Att usa suas capacidades Bloquear, Quebra Atômica, Fabricar e Iniciar nessa mensagem, impedindo I de aprender o correto voto e informação randômica, isso é Voto+R, sendo forçado a aprender $Voto_{att}$ + R.

Modelo de ameaça DY: Se todas as mensagens M1 até M14

fossem executadas contra um atacante DY, tal atacante poderia impedir tanto a cabine de votação B quando o instituto I de receberem o correto voto (forçadamente aprendendo $Voto_{att}$), através da execução de seções do protocolo simultâneas entre os nodos do sistema.

5.1.2 Voto final corretamente armazenado no quadro de avisos

Baseado na figura 2 (Instituto – cerimônia de voto final):

Se as mensagens M1 até M12, M14, M15 e M17 são executadas contra um atacante DY-E e as mensagens M13 e M16 são executadas contra um atacante DY, o atacante (Att) *pode impedir o quadro de avisos BB de receber o correto* $\{Voto\}_{Epk}$. *Att também pode impedir que o instituto I aprenda* $H\{\{Voto{+}R\}_{Epk}\}$. *Att, então, envia informações alteradas* $\{Voto_{att}\}_{Epk}$ *e* $H_{att}\{\{Voto_{att} + R_{att}\}_{Epk}\}$ *para o quadro de avisos e para o instituto, respectivamente, sendo* $Voto_{att}$ *escolhido pelo atacante. O atacante usa suas capacidades Criptografia e Fabricar para gerar* $\{Voto_{att}\}_{Epk}$ *e* $H_{att}\{\{Voto_{att}\} + R_{att}\}_{Epk}\}$[1].

$$\frac{(M_{1\ldots12} \cup DY - E) \wedge (M_{13} \cup DY) \wedge (M_{14\ldots15} \cup DY - E) \wedge (M_{16} \cup DY) \wedge (M_{17} \cup DY - E)}{\begin{array}{r}\{Voto\}_{Epk} \wedge \{Voto_{att}\}_{Epk} \wedge H\{\{Voto + R\}_{Epk}\} \wedge \\ H_{att}\{\{Voto_{att} + R_{att}\}_{Epk}\} \in knows(Att) \wedge \\ Voto \in knows(B) \wedge \\ \{Voto\}_{Epk} \notin knows(BB) \wedge \{Voto_{att}\}_{Epk} \in knows(BB) \wedge \\ H\{\{Voto + R\}_{Epk}\} \notin knows(I) \wedge H_{att}\{\{Voto_{att} + R_{att}\}_{Epk}\} \in knows(I)\end{array}}$$

Prova: Assuma que o atacante Att iniciou duas seções do protocolo entre a cabine de votação B e o quadro de avisos BB mantido pelo instituto I. O atacante Att usa suas capacidades Bloquear, Fabricar e Iniciar (mensagem 13 da figura 2) e envia ao BB a informação de $\{Voto_{att}\}_{Epk}$ ao invés de $Voto_{Epk}$.

Modelo de ameaça DY: Se todas as mensagens M1 até M17 fossem executadas contra um atacante DY, tal atacante poderia im-

[1] Note que o atacante tem como saber quais os votos existentes e também pode possuir a chave pública da eleição, porém ele não conhece o valor da informação randômica R.

pedir o quadro de avisos BB de ser requisitado pelo instituto I com o correto hash. A consulta ao BB seria feita com um hash calculado pelo atacante.

5.1.3 Resultados

Considerando o modelo de ameaça DY, o atacante tem total controle de todos os canais de comunicação e é capaz de manipular o eleitor durante todo o processo. Em tais cenários, o atacante intercepta todas as mensagens trocadas entre os pares de nodos do sistema, e envia mensagens de seu próprio conhecimento no lugar das originais. Nesse caso, é possível que para o eleitor sejam apresentados dados corretos, onde o atacante se faz passar pelas entidades legítimas. Assim, o eleitor acredita que seu voto foi cifrado, submetido e armazenado apropriadamente, quando isso não é verdade. Contudo, essa situação é altamente improvável de acontecer nas cerimônias apresentadas, pois o canal HD limita as ações do atacante. É difícil para o atacante controlar esse canal e as informações sendo transmitidas devido à presença do nodo humano.

Um cenário realístico e factível é o atacante interceptar mensagens apenas no canal DD. Nesse caso, o instituto recebe informações alteradas, calculando um hash diferente do esperado pelo eleitor, o que induz o eleitor a não confiar mais no instituto. Esse resultado ressalta a necessidade de se ter vários institutos disponíveis, provendo serviços de verificação para os eleitores. Portanto, o eleitor tem total liberdade de verificar usando vários outros institutos. Se as tentativas seguintes também falharem, o eleitor pode contatar a comissão eleitoral.

Analisando as cerimônias apresentadas acima, constata-se que a mensagem 13 da cerimônia Voto de teste (figura 1) apresenta Voto + R sendo transmitido como texto plano (sem criptografia) através de um canal DD. O mesmo não acontece com a cerimônia Voto final (figura 2), onde tal mensagem contém informações cifradas com a chave pública da eleição (E_{pk}). Logo, o sigilo não está presente para a cerimônia de voto de teste, estando presente apenas na cerimônia para voto final. Tal conclusão se deve ao fato que mesmo que um atacante DY intercepte a mensagem 13 da cerimônia para voto final, não conseguirá obter informações sobre o voto ou sobre a informação randômica a partir do hash.

5.2 APLICATIVO PARA SMARTPHONE

A seguir, estão as análises das cerimônias envolvendo o uso do aplicativo. São apresentados o modelo de ameaça adaptativo e também o cenário considerando o modelo Dolev-Yao para posterior comparação na subseção dos resultados.

5.2.1 Voto de teste corretamente cifrado

Baseado na figura 3 (Aplicativo – cerimônia de voto de teste):
Se todas as mensagens M1 até M18 são executadas contra um atacante DY-E, tal atacante não é capaz de realizar nenhum ataque significativo no que diz respeito ao sigilo e integridade.

$$\frac{M_{1...18} \cup DY - E}{\emptyset}$$

Prova: Considerar o canal DD_2 (mensagens 11 e 15 da figura 3) como sendo DY-E significa que o canal é uma variação enfraquecida do modelo DY. Tem-se um computador apresentando um QR code e comunicando-se com o dispositivo móvel do eleitor. Uma vez que ao atacante não é permitido escutar os canais, todas as demais capacidades não afetarão o sigilo do voto na cerimônia. Portanto, dado que o atacante não pode tomar posse dos dispositivos do eleitor e não sabe o voto, não é capaz de realizar nenhum ataque significativo.

Modelo de ameaça DY: Se todas as mensagens M1 até M18 fossem executadas contra um atacante DY, tal atacante teria total controle sobre os canais (impedindo a cabine de votação B de receber o voto) e manipularia as informações apresentadas ao eleitor, através da execução de seções do protocolo simultâneas entre os nodos do sistema.

5.2.2 Voto final corretamente armazenado no quadro de avisos

Baseado na figura 4 (Aplicativo – cerimônia de voto final):
Considere que as mensagens M1 até M14, M16 e M17 são executadas contra um atacante DY-E e as mensagens M15, M18 e M19 são executadas contra um atacante DY. O atacante (Att) *pode impedir*

que o quadro de avisos BB aprenda os corretos valores de $\{Voto\}_{Epk}$ *e* $H\{\{Voto + R\}_{Epk}\}$.

$$\frac{(M_{1...14} \cup DY - E) \wedge (M_{15} \cup DY) \wedge (M_{16...17} \cup DY - E) \wedge (M_{18...19} \cup DY)}{\begin{array}{r}\{Voto\}_{Epk} \wedge \{Voto_{att}\}_{Epk} \wedge H\{\{Voto + R\}_{Epk}\} \wedge \\ H_{att}\{\{Voto_{att} + R_{att}\}_{Epk}\} \in knows(Att) \wedge \\ Voto \in knows(B) \wedge \\ \{Voto\}_{Epk} \wedge H\{\{Voto + R\}_{Epk}\} \notin knows(BB) \wedge \\ \{Voto_{att}\}_{Epk} \wedge H_{att}\{\{Voto_{att} + R_{att}\}_{Epk}\} \in knows(BB)\end{array}}$$

Prova: Assuma que o atacante Att iniciou duas seções do protocolo simultâneas entre a cabine de votação B e o quadro de avisos BB (mensagem 15 da figura 4) e entre o aplicativo A e o BB (mensagens 18 e 19 da figura 4). Nesse caso, DD_2 continua sendo considerado DY-E uma vez que caracteriza um canal visual. O atacante Att usa suas capacidades Bloquear, Fabricar e Iniciar nas mensagens 15, 18 e 19, onde envia para o quadro de avisos BB valores diferentes para o voto e para o hash, ao invés dos originais.

Modelo de ameaça DY: Se todas as mensagens M1 até M19 fossem executadas contra um atacante DY, o atacante poderia impedir o quadro de avisos BB de armazenar o voto correto e manipularia o eleitor (fingindo tanto ser a cabine de votação B quanto o quadro de avisos BB), através da execução de duas seções de protocolo simultâneas entre os nodos do sistema.

5.2.3 Resultados

Considerando o modelo de ameaça DY, o atacante pode manipular o eleitor através da manipulação das informações apresentadas a ele. Tal situação pode ser considerada realística para a cerimônia do voto final usando aplicativo (figura 4). Contudo, é altamente improvável de acontecer devido ao fato dos canais HD estarem seguros sob a suposição de que o eleitor confere ao seu redor se não há algum possível atacante observando suas ações. Adicionalmente, foi demonstrado ser irrealista para a cerimônia de voto de teste usando aplicativo (figura 3). Tal cerimônia é mais segura por possuir o canal visual, o qual limita as

ações do atacante ao apresentar o mesmo comportamento que os canais HD. Uma contribuição muito importante da proposta usando o aplicativo constitui-se de que ambos os votos de teste e final são secretos, quando comparados com a proposta que faz uso dos institutos (onde o voto de teste é enviado sem uso de criptografia por um canal DY). Tal contribuição significa que essa cerimônia possui a propriedade do sigilo e, como as mensagens não são interrompidas e não são modificadas, conclui-se que tal cerimônia também garante integridade.

Nas cerimônias envolvendo verificação com o aplicativo, não é viável ao atacante controlar mais de um canal DD(CARLOS et al., 2013). Portanto, ou o atacante escolhe controlar o canal entre a cabine de votação B e o quadro de avisos BB (mensagem 15 da figura 4) ou ele controla as mensagens trocadas entre o aplicativo A e o quadro de avisos BB (mensagem 18 da figura 4). Quando o atacante obtiver sucesso, o quadro de avisos não apresentará ao eleitor a confirmação esperada (mensagem 19 da figura 4). Em tal situação, o eleitor pode utilizar outro quadro de avisos suportado por qualquer dos auditores da eleição. Em caso de sucessivas falhas, o eleitor deve contatar a comissão da eleição.

6 CONCLUSÃO

Neste trabalho foi analisada a segurança das propostas feitas para o sistema de votação Helios. Para tal análise foi utilizado o framework proposto por Carlos et al(CARLOS et al., 2013), aplicando o modelo adaptativo de ameaça. Para esse fim, considerou-se os processos de votação e verificação do voto como cerimônias, integrando a interação humana na análise. O modelo de ameça Dolev-Yao foi usado para comparação com o modelo adaptativo, onde foi possível ressaltar os ganhos em se empregar um modelo que reflita as necessidades de segurança para cada específico cenário sem sobrecarregar o usuário.

Na primeira proposta para verificação, usando institutos confiáveis, os resultados mostram a possibilidade de violações de sigilo quando o eleitor verifica se seu voto está corretamente cifrado, e violações de integridade quando ele verifica se seu voto foi corretamente submetido no quadro de avisos. As violações de integridade tomam forma de 'ataques de reputação', resultando na perda de confiança no instituto por parte do eleitor (ao receber informações incorretas). Para as cerimônias envolvendo o aplicativo, o sigilo é mantido devido à presença de um canal visual e ao fato da informação ser enviada cifrada (e não em forma de texto plano). Os resultados também mostram que nenhum ataque significativo pode ocorrer quando o eleitor verifica se seu voto está cifrado de forma correta. Violações de integridade acontecem através dos 'ataques de reputação', os quais conduzem o eleitor a não confiar mais nos institutos participantes do sistema.

Com relação aos 'ataques de reputação', a estratégia de mitigação utilizada é a existência de diversos institutos, ou aplicativos mantidos por esses, disponíveis para o eleitor. Através dessa solução, a propriedade da integridade pode ser mantida em ambas as propostas abordadas. No caso do processo de verificação falhar em algum dos casos, o eleitor pode verificar fazendo uso de outras fontes.

Os resultados desse trabalho ressaltaram várias melhorias que podem ser feitas ao protocolo de votação do Helios. Esse será o foco para trabalhos futuros. Uma futura proposta envolve o eleitor entrar com uma informação única conhecida apenas por ele. Verificar a presença dessa informação em um estágio posterior do sistema garante ao eleitor a integridade do voto submetido. Propostas serão desenvolvidas com o objetivo de equilibrar os aspectos de segurança e as expectativas e habilidades dos nodos humanos na cerimônia.

REFERĘNCIAS

ABADI, M.; GORDON, A. D. Reasoning about cryptographic protocols in the spi calculus. In: *CONCUR '97: Proceedings of the 8th International Conference on Concurrency Theory*. London, UK: Springer-Verlag, 1997. p. 59–73. ISBN 3-540-63141-0.

ADIDA, B. Helios: Web-based Open-Audit Voting. In: *Proceedings of the 17th Symposium on Security*. [S.l.]: Usenix Association, 2008. p. 335 – 348.

ADIDA, B. et al. Electing A University President using Open-Audit Voting: Analysis of Real-World Use of Helios. In: *Proceedings of the 2009 Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*. [S.l.]: Usenix Association, 2009. p. 10–10.

ARSAC, W. et al. Validating security protocols under the general attacker. In: DEGANO, P.; VIGANò, L. (Ed.). *Foundations and Applications of Security Analysis*. Springer Berlin Heidelberg, 2009, (Lecture Notes in Computer Science, v. 5511). p. 34–51. ISBN 978-3-642-03458-9. <http://dx.doi.org/10.1007/978-3-642-03459-6$_3$>.

BELLA, G. *Formal Correctness of Security Protocols*. [S.l.]: Springer Verlag, 2007. 274 p. (Information Security and Cryptography, XX).

BELLA, G.; LONGO, C.; PAULSON, L. C. Is the verification problem for cryptographic protocols solved? In: CHRISTIANSON, B. et al. (Ed.). *Security Protocols Workshop*. Springer, 2003. (Lecture Notes in Computer Science, v. 3364), p. 183–189. ISBN 3-540-28389-7. <http://dx.doi.org/10.1007/11542322$_2$3>.

BELLARE, M.; ROGAWAY, P. Entity authentication and key distribution. In: STINSON, D. (Ed.). *Advances in Cryptology — CRYPTO' 93*. Springer Berlin Heidelberg, 1994, (Lecture Notes in Computer Science, v. 773). p. 232–249. ISBN 978-3-540-57766-9. <http://dx.doi.org/10.1007/3-540-48329-2$_2$1>.

BURROWS, M.; ABADI, M.; NEEDHAM, R. A logic of authentication. In: *Proc. 12th ACM Symposium on Operating Systems Principles*. Litchfield Park, Arizona: [s.n.], 1989.

CARLOS, M. C. et al. An Updated Threat Model for Security Ceremonies. In: *Proceedings of the 28th Annual ACM Symposium on*

Applied Computing. New York, NY, USA: ACM, 2013. (SAC '13), p. 1836–1843.

DOLEV, D.; YAO, A. C. On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, v. 29, n. 2, p. 198–208, 1983.

ELLISON, C. *Ceremony Design and Analysis*. 2007. Cryptology ePrint Archive, Report 2007/399. http://eprint.iacr.org/.

KARAYUMAK, F. et al. Usability Analysis of Helios - An Open Source Verifiable Remote Electronic Voting System. In: *Proceedings of the 2011 International Conference on Electronic Voting Technology/Workshop on Trustworthy Elections*. [S.l.]: USENIX Association, 2011. (EVT/WOTE'12).

KARAYUMAK, F. et al. User Study of the Improved Helios Voting System Interfaces. In: *1st Workshop on Socio-Technical Aspects in Security and Trust (STAST)*. [S.l.: s.n.], 2011. p. 37–44.

KUSTERS, R.; TRUDERUNG, T.; VOGT, A. Clash Attacks on the Verifiability of E-Voting Systems. In: *Security and Privacy (SP), 2012 IEEE Symposium on*. [S.l.: s.n.], 2012. p. 395–409.

LOWE, G. Breaking and fixing the needham-schroeder public-key protocol using fdr. In: *TACAs '96: Proceedings of the Second International Workshop on Tools and Algorithms for Construction and Analysis of Systems*. London, UK: Springer-Verlag, 1996. p. 147–166. ISBN 3-540-61042-1.

MARTINA, J. E.; CARLOS, M. C. *Why Should We Analyse Security Ceremonies?* maio 2010. First CryptoForma workshop. <http://www.cryptoforma.org.uk/paris/10.pdf>.

MEADOWS, C. Language generation and verification in the nrl protocol analyzer. In: *CSFW '96: Proceedings of the 9th IEEE workshop on Computer Security Foundations*. Washington, DC, USA: IEEE Computer Society, 1996. p. 48. ISBN 0-8186-7522-5.

NEEDHAM, R. M.; SCHROEDER, M. D. Using encryption for authentication in large networks of computers. *Commun. ACM*, ACM Press, New York, NY, USA, v. 21, n. 12, p. 993–999, 1978. ISSN 0001-0782.

NEUMANN, S. et al. Helios verification: To alleviate, or to nominate: Is that the question, or shall we have both? In: *3rd International Conference on Electronic Government and the Information Systems Perspective*. [S.l.]: Springer, 2014. To appear.

NORMAN, D. A. *The Design of Everyday Things*. New York, NY, USA: Basic Books, Inc., 2002. ISBN 9780465067107.

RYAN, P.; SCHNEIDER, S. *The modelling and analysis of security protocols: the csp approach*. [S.l.]: Addison-Wesley Professional, 2000. ISBN 0-201-67471-8.