UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

AUDITORIA DE SISTEMAS DE VOTAÇÃO ELECTRÓNICA: UMA PROPOSTA DE ARQUITECTURA E PROTÓTIPO DE SIMULAÇÃO

Filipe José Ferreira Simões

MESTRADO EM INFORMÁTICA

Dissertação orientada pelo
Professor Doutor Pedro Alexandre Antunes

2006

AGRADECIMENTOS

À Carla e à Filipa pela força e incentivo que me deram; aos meus pais e irmã por terem sempre acreditado em mim; ao meu orientador, Professor Doutor Pedro Antunes, pelo apoio que sempre me prestou.

ÍNDICE

ÍNDICE DE FIGURAS

RESUMO

Com a evolução do mundo tecnológico em que vivemos, o processo de votação electrónica emergiu como mais um dos desafios colocados à nossa sociedade. Um Sistema de Votação Electrónico (SVE) supõe um processo envolvendo tecnologia e pessoas que deve permitir ao eleitor exercer o seu direito de voto com a garantia das propriedades fundamentais do processo eleitoral, nas três fases essenciais que o compõem: recenseamento, votação e contagem/divulgação de resultados.
De entre essas propriedades, o processo de votação electrónica terá que transmitir confiança aos eleitores. Esta propriedade só poderá ser atingida com a auditoria do processo. Só assim a mudança para esta forma de exercer o direito de voto se tornará de vez ubíqua.

Com este trabalho pretende-se contribuir com um estudo técnico de análise de sistemas, concepção e prototipagem que permita suportar o processo de auditoria de um sistema de votação electrónica, alertando a comunidade para a necessidade de auditar os riscos do sistema. A base conceptual deste trabalho entende a auditoria como um processo que não se esgota antes do processo eleitoral, mas que corre em paralelo com o processo de votação.

O protótipo de simulação de auditoria de sistemas de votação electrónica construído neste trabalho permite:
- identificar casos de falha técnica, erro humano ou sabotagem do sistema;
- relacionar esses casos com a arquitectura do sistema;
- exercitar opções de desenho do SVE.

Este trabalho é também uma contribuição para a validação de novas propostas de arquitectura que venham a surgir, constituindo ainda uma base para a definição de regras e procedimentos de avaliação.

PALAVRAS-CHAVE: votação electrónica, análise de risco, auditoria.

ABSTRACT

With technological evolution of the world we live in, electronic voting emerged as one more of the challenges placed to our world. An electronic voting system (EVS) can be assumed as a process involving technology and people that must allow the voter to vote guarantying electoral process basic properties in its three essential phases: census, voting and counting/spreading of results. From all the basic properties, electronic voting process must transmit confidence to the voters. This property will only be reached auditing all the process. Only by this approach, electronic voting will be considered as a ubiquous way of voting.

This work intends to contribute with a technical report of system analysis, design and prototype that allows supporting the audit process of an electronic voting system, alerting the community for the need of system's risk audit. This work's conceptual base understands audit as a process that does not deplete before the electoral process, but it runs in parallel with the voting process.

The simulation prototype of electronic voting system audit proposed in this work allows:
- to identify misuse case, human error or sabotage of the system;
- to relate these cases with the architecture of the system;
- to exercise options of EVS design.

This work is also a contribution for the validation of new architecture proposals that come to appear, constituting still a base for the definition of rules and procedures of evaluation.

KEY-WORDS : e-voting, risk analysis, audit.

1 - INTRODUÇÃO

Com a evolução do mundo tecnológico em que vivemos, o processo de votação electrónica emergiu como mais um dos desafios colocados à nossa sociedade [1]. Um sistema de votação desta natureza supõe um processo envolvendo tecnologia e pessoas que deve permitir ao eleitor exercer o seu direito de voto com a garantia das propriedades fundamentais do processo eleitoral, nas três fases essenciais que o compõem: recenseamento, votação e contagem/divulgação de resultados. De entre essas propriedades, o processo de votação electrónica terá que transmitir confiança aos eleitores. Esta propriedade só poderá ser atingida com a auditoria do processo. Só assim a mudança para esta "nova" forma de exercer o direito de voto se tornará de vez ubíqua.

Convém referir que a base do trabalho aqui desenvolvido e apresentado, resulta da participação na equipa de auditoria da Faculdade de Ciências da Universidade de Lisboa que teve lugar no decorrer da experiência de voto electrónico incluído no processo eleitoral para o Parlamento Europeu em 2004, na qual eu o orientador deste trabalho estivemos envolvidos.

Com este trabalho pretende-se contribuir com um estudo técnico de análise de sistemas, concepção e prototipagem que permita suportar o processo de auditoria de um sistema de votação electrónica, alertando a comunidade para a necessidade de conhecer os cenários de mau uso e riscos de segurança que colocam em causa a credibilização de um sistema deste género.

A base conceptual deste trabalho entende a auditoria como um processo que não se esgota antes do processo eleitoral, mas que corre em paralelo com o processo de votação, tornando o sistema mais resistente à ocorrência de riscos.

Em sequência à experiência obtida durante o referida participação na equipa de auditoria em Junho de 2004 e tendo a noção que a auditoria é uma problemática muito mais extensa, iremos concentrar este estudo na vertente da inspecção e da análise do risco associado aos sistemas de votação electrónica.

A avaliação do risco será feita através da monitorização de todas as fases do processo de votação. Com a inspecção e avaliação do risco em qualquer uma das fases do processo de votação electrónica poderemos reduzir a probabilidade de ocorrência de falhas ou o seu impacte. Caso uma falha venha mesmo a acontecer, se ela for detectada atempadamente no decorrer do processo, a sua mitigação reduzirá o seu potencial impacte no funcionamento do sistema.

A previsibilidade da ocorrência de falhas baseia-se na possibilidade de testar cenários em momentos anteriores aos do processo de votação, através da simulação de situações reais.

Durante um processo de votação a capacidade de reacção do sistema em tempo real e o seu dinamismo face ao auditor servirá de apoio à mitigação dos resultados mais nefastos que a ocorrência de uma situação de risco pode provocar no funcionamento do sistema.

Este trabalho é também uma contribuição para a validação de novas propostas de arquitectura que venham a surgir. A análise do risco aqui realizada poderá ser uma primeira abordagem aos requisitos de segurança que se devem impor a sistemas desta natureza. Tal abordagem poderá constituir ainda uma base para a definição de regras e procedimentos de avaliação que ao ser seguida poderá tornar mais credível o sistema de votação electrónica, incutindo maior grau de confiança em todos os participantes no processo de votação.

1.1 - Trabalho desenvolvido

Este trabalho parte de uma enumeração exaustiva das propriedades [2] que mais directamente se relacionam com os riscos associados aos Sistemas de Votação Electrónicos (SVE), que deverão ser avaliados em qualquer instante do decorrer do processo de votação.

A revisão bibliográfica dos SVE existentes ajuda a um melhor entendimento dos trabalhos até aqui desenvolvidos, e ao se estabelecerem comparações entre eles, permitem encontrar um padrão de qualidade necessário à auditoria do sistema.

A partir da revisão bibliográfica e seu estudo, definiremos uma arquitectura de referência sobre a qual iremos basear o nosso trabalho de auditoria (análise, desenho e prototipagem).

Análise:

Os casos de uso utilizados para descrever o comportamento do sistema são uma ferramenta muito interessante no momento de análise. A utilização de "misuse cases" [3] [4] [5] [6], casos de mau uso definidos por Ian Alexander como casos de uso com intenções hostis [5], permite sistematizar casos de mau uso e falhas do SVE e identificar formas de os detectar, prevenir e mitigar.

Desenho:

Nenhum sistema informático pode ser aceite como de baixo risco, muito menos um SVE, se não estiver sujeito a uma auditoria de funcionamento. A perspectiva conceptual deste trabalho e seu respectivo desenho apresenta a auditoria como um processo que corre em paralelo com o processo de votação, adoptando a hipótese de que a capacidade de auditar o sistema em qualquer uma das suas fases irá tornar o sistema mais credível.

Prototipagem:

O protótipo construído permite simular a auditoria do SVE monitorizando o percurso dos boletins, verificando a sua integridade e completude, procurando padrões de ataque ao sistema, identificando casos de mau uso.

2 - RISCO ASSOCIADO AO SVE

O risco é um factor que determina o comportamento de um SVE. O risco a que um SVE está sujeito irá colocar em causa as propriedades que um processo de votação electrónica deve garantir. É a garantia destas propriedades que a seguir descrevemos que torna o sistema credível. Descrevendo exaustivamente estas propriedades, ficamos a conhecer qual o comportamento exigível para o normal funcionamento do SVE.

2.1 - Propriedades

Importa apresentar as propriedades [2] que mais directamente se relacionam com a questão do risco associado a um SVE e que deverão ser validadas em qualquer instante do decorrer do processo de votação.
Por questões de organização e melhor entendimento, optámos por agrupar as propriedades em três grupos:

- propriedades inerentes à democracia:
serão as propriedades a considerar sob o ponto de vista do conceito de democracia inerente a qualquer processo de votação;

- propriedades dos Sistemas de Votação Electrónica:
incluiremos neste grupo as propriedades desejáveis para garantir a credibilidade e a confiança num Sistema de Votação Electrónico;

- requisitos a cumprir pelos SVE:
são as propriedades que poderemos considerar como decorrentes de conhecimento empírico, experiência e boas práticas.

2.1.1 - Propriedades inerentes à democracia

Anonimato

A associação entre o voto e a identidade do eleitor deve ser impossível em qualquer circunstância. A separação destes dados deve garantir a impossibilidade de relacionar o votante com o respectivo voto quer durante a votação (por utilizadores privilegiados, como por exemplo os que realizam manutenção do sistema) quer após a votação (mesmo que por ordem judicial).

Autenticidade

Autenticar o indivíduo é o meio pelo qual a identificação de um votante é validada e confirmada. Apenas os eleitores autorizados devem poder votar.
Exemplos de tipos de autenticação são [7]: Presencial, PIN, Password, Certificados Digitais, Smartcard, bio-métrica.

Direito de Voto

O Direito de Voto de um eleitor é uma propriedade que obriga à verificação simultânea das propriedades de Autenticidade e Singularidade. Será sempre necessário verificar o Direito de Voto de um eleitor antes de ele poder votar.

Integridade dos Votos

Os votos não devem poder ser modificados, forjados ou eliminados, quer durante quer após o término do processo eleitoral.

Não-Coercibilidade

O sistema não deve permitir que os eleitores possam provar em quem é que votaram, o que facilitaria a venda ou coerção de votos.

Privacidade

O sistema não deve permitir que alguém tenha o poder de descobrir qual o voto de determinado eleitor, nem que o eleitor possa, mesmo querendo, tornar público o seu voto.

Singularidade

O sistema deve garantir que os eleitores não possam votar mais do que uma vez em cada processo eleitoral.

2.1.2 - Propriedades dos Sistemas de Votação Electrónica

Auditabilidade

O sistema deverá poder ser auditado quer por observadores externos – através por exemplo da análise dos registos, quer pelo próprio sistema – com a confrontação dos diversos dados.

Certificabilidade

O sistema deve poder ser testado e certificado por agentes oficiais.

Confiabilidade

O SVE deve funcionar de forma robusta, sem perda de votos, tornando-se confiável ao olhos dos diversos actores que nele participam.

Detectabilidade

O sistema deve ter a capacidade de detectar qualquer tentativa de intrusão de agentes externos e dar alertas aos diversos administradores do sistema.

Disponibilidade do Sistema

O SVE deve estar sempre disponível durante o período eleitoral, para que o processo decorra normalmente.

Integridade do Sistema

O sistema deve poder ser posto à prova, depois de validado e certificado por auditores externos.

Invulnerabilidade

A invulnerabilidade do SVE deverá ser garantida pela existência do maior número de pressupostos de prevenção e defesa às situações de risco do sistema.

Precisão

As eleições podem ser decididas por apenas um voto. O sistema não pode tolerar margens estatísticas de erro durante a sua operação. Até o erro involuntário de um eleitor, mal treinado para votar em dado equipamento, pode inverter ou modificar o resultado eleitoral.

Rastreabilidade

O sistema deve registar permanentemente qualquer transacção ou evento significativo ocorrido no próprio sistema. Deverão existir registos de entrada e saída de utilizadores, bem como registos do envio e recepção de dados, que obviamente não comprometam as restantes propriedades (Anonimato e Privacidade).

Recuperabilidade

O SVE deve permitir a retoma da operação precisamente no ponto de interrupção, sem perda de informação.

Verificabilidade

O sistema deve permitir a verificação de que os votos foram correctamente contados, no final da votação, e deve ser possível verificar a Autenticidade dos registos dos votos sem no entanto quebrar outras propriedades como o Anonimato ou a Privacidade.

2.1.3 - Requisitos a cumprir pelos SVE

Autenticação do Operador

Os utilizadores autorizados a operar o sistema devem ter mecanismos de controlo de acesso não triviais. Os operadores devem ser autenticados pelo sistema através de uma conjunção de alguns dos tipos de autenticação existentes (Smartcard + PIN + Password, ou ainda autenticação bio-métrica – impressões digitais, retina ocular, voz, etc).

Documentação

Todo o projecto e implementação do sistema, inclusive relativamente a testes e segurança do sistema deve estar documentado, devendo não conter ambiguidades e ser coerente.
Deve ser dada máxima atenção à documentação gerada ao longo de todo o processo, desde o estudo inicial dos requisitos do sistema de votação, passando pelas várias fases evolutivas de construção, até à elaboração do manual da aplicação, continuando depois pelo registo das ocorrências ao longo do "tempo" de votação propriamente dito, até á apresentação das listagens de resultados.

Cifra dos dados e Redes Privadas Virtuais

Os dados guardados nos servidores, bem como aqueles que viajam pela rede, quer seja pública quer privada, devem encontrar-se cifrados.

Fisicamente seguro

Num sistema de votação electrónico, a segurança física dos servidores é vital. Mas não só a das máquinas (consolas, pcs, servidores e respectivos periféricos – rato, teclado, impressoras, etc.), mas também a dos cabos de alimentação e comunicação.

Integridade do Pessoal

O pessoal envolvido no projecto, implementação, administração e operação do SVE deve ser incorruptível e de integridade inquestionável, inclusive os envolvidos com a distribuição e guarda de dados e equipamentos.

Política de salvaguarda e recuperação de informação

Contra uma possível perda de informação, quer seja causada por falhas de hardware, erros de software, descuidos humanos, sabotagem ou mesmo desastres naturais, o sistema de votação deve proteger-se através de uma política adequada de cópias de segurança e recuperação de dados. Devem ser estudados os requisitos de protecção e classificação de dados do sistema e em seguida enumerados os procedimentos de salvaguarda e também de recuperação caso tal venha a ser necessário.

Tolerância a Ataques

A principal característica que diferencia um SVE de outros sistemas de alto risco é que este poderá ser alvo privilegiado de ataques mal intencionados. Medidas de defesa contra fraudes, inclusive vindas dos próprios agentes que projectaram e desenvolveram o sistema, devem ser rigorosas e redundantes.

Tolerância a Faltas

É desejável a existência de métodos de detecção e tolerância a faltas nos equipamentos. A falta de um componentes do SVE não deve impedir o normal decorrer do processo de votação, que está quase sempre delimitado do ponto de vista temporal.

2.2 - Riscos dos SVE

Não será possível, de certo, acabar com os atacantes nem tão pouco eliminar os erros humanos em todos os processos electrónicos e informáticos. No entanto o SVE está sujeito a estas situações de risco. Podemos então, tentar prevê-los e evitá-los, em último caso remediá-los.

Consideremos um estudo prévio de segurança, referindo-nos aos riscos a considerar num sistema de votação electrónico. Adaptamos o modelo de Reason[8] ao contexto deste trabalho e vamos assim separar os riscos dos SVE em três grupos:
- sabotagem
- falhas do sistema
- erro humano, que por sua vez inclui os lapsos e deslizes, os enganos e as violações

Algumas das descrições dos riscos serão acompanhadas de árvores de análise de faltas [9]. Através das árvores de análise de faltas, pode ser feita uma primeira análise das causas de um risco a que está sujeito o sistema. Usando a lógica booleana, representada por portas de ”E” e de “OU”, descrevem-se combinações de falhas individuais que podem vir a causar problemas ao funcionamento normal do sistema. A leitura das árvores de faltas pode se feita “top-down” ou inversamente, dependendo por onde se queira começar, respectivamente pelos riscos inerentes ao sistema ou pelas causas que os podem originar.

A lógica booleana descrita nestas árvores de faltas é a seguinte :

 - significa “OU”

 - significa “E”

2.2.1 - Sabotagem

Como sabotagem agrupamos todos os riscos ou actos provocados por um atacante que tem como objectivo impedir o pleno e correcto funcionamento do processo de votação.

Negação de Serviço – Denial of Service (DOS) [10] [11] [12]

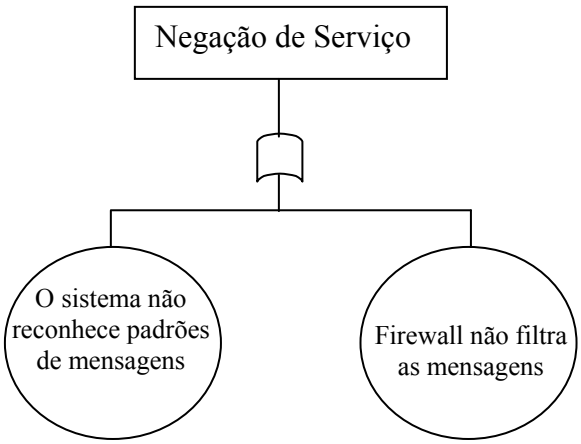

Figura 1 – Árvore de faltas do ataque de negação de serviço

- Um sniffer vigia a rede;
- O atacante tenta um ataque de DOS a componentes do sistema (em particular alguns dos mais críticos, o de votação ou o de contagem) através do envio em grande número de mensagens para os componentes do sistema;

Eveasdroping [11] [12]

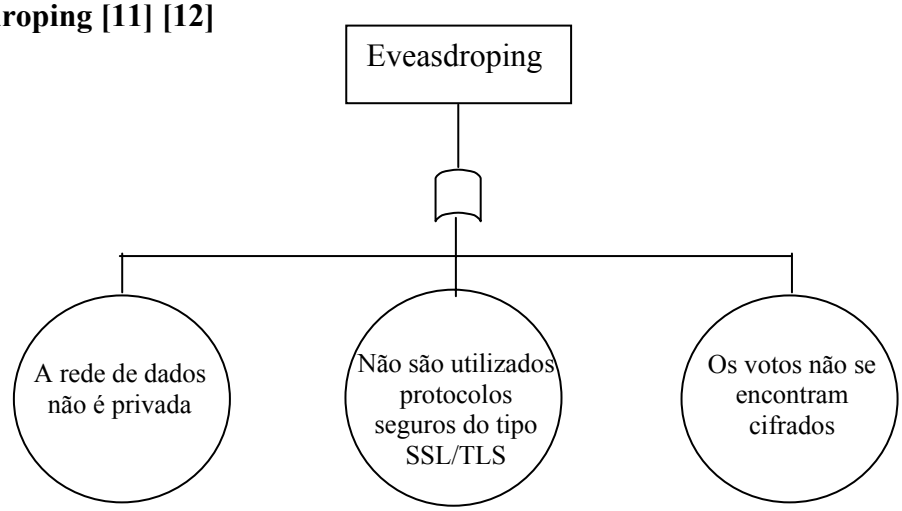

Figura 2 – Árvore de faltas do ataque "eveasdroping"

- Os votos são transmitidos através da rede, entre os vários componentes do sistema.
- O atacante tenta interceptar os votos que viajam pela rede (utilizando por exemplo um sniffer)

Spoofing/Masquerading [10] [11] [12]

- O atacante simula uma identidade oficial da organização e tenta captar informação vital (credenciais tais como códigos e palavras passe, por exemplo), por exemplo na fase de verificação do eleitor;

Replaying [12]

- O atacante tenta reenviar uma mensagem, o que se torna num ataque no caso por exemplo em que um boletim de uma eleição anterior faça sentido numa nova votação ou ainda no caso do atacante possuir uma password utilizada anteriormente e que foi "capturada" por exemplo por "eavesdropping".

Message Tampering [12]

- O atacante intercepta e altera as intenções de voto ou outra informação vital para o sistema, como saber se um votante já exerceu, ou não, e ainda que o sistema detecte alguma anormalidade no boletim pode acontecer que o voto não seja considerado, o que pode levar também à alteração de resultados.

Código malicioso [10][12]

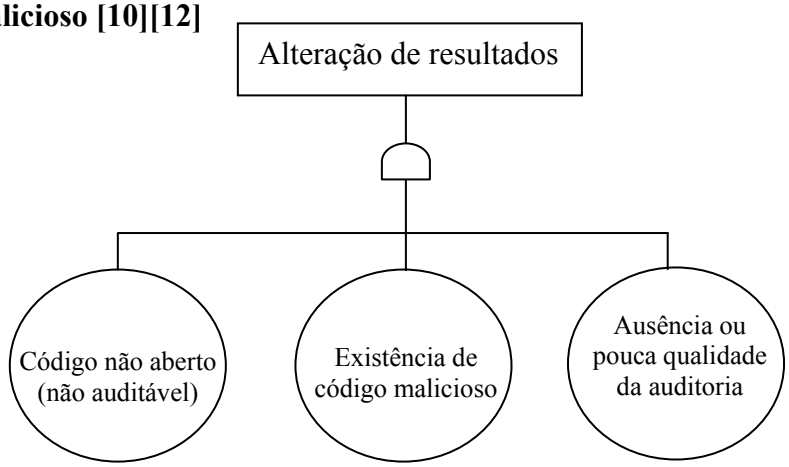

Figura 3 – Árvore de faltas do ataque de código malicioso

- Independentemente do tipo de comunicação segura e de autenticação realizadas durante o processo de votação, um pedaço de código malicioso pode ser anteriormente inserido no SVE, permitindo alterar um voto sem posteriormente se dar pelo sucedido.

Vírus e Cavalos de Tróia [10] [11] [12]

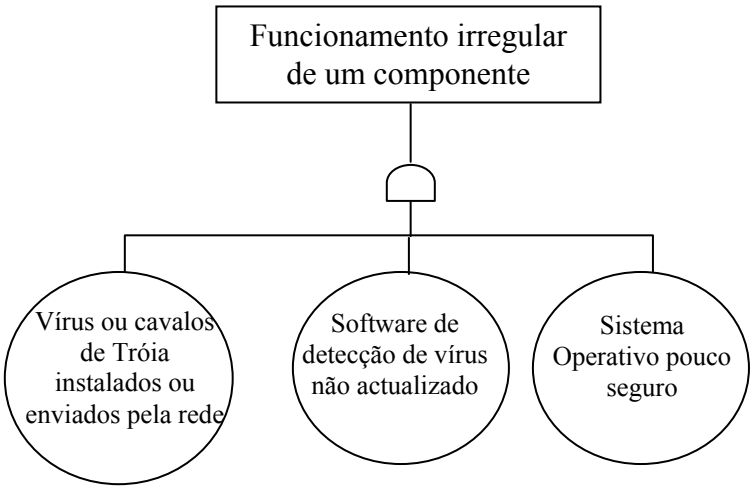

Figura 4 – Árvore de faltas do ataque de vírus e cavalos de tróia

- O atacante infecta o sistema através de um virus (software escrito para "invadir" sistemas informáticos e ficheiros desse sistema), ou então através de um cavalo de Tróia (software que reside "escondido" em outros componentes de software até alguma(s) condição(ções) o fazerem despertar, por exemplo data do sistema = dia da eleição), corrompendo o normal funcionamento de um componente.

Acessos não autorizados ao hardware [10] [12]

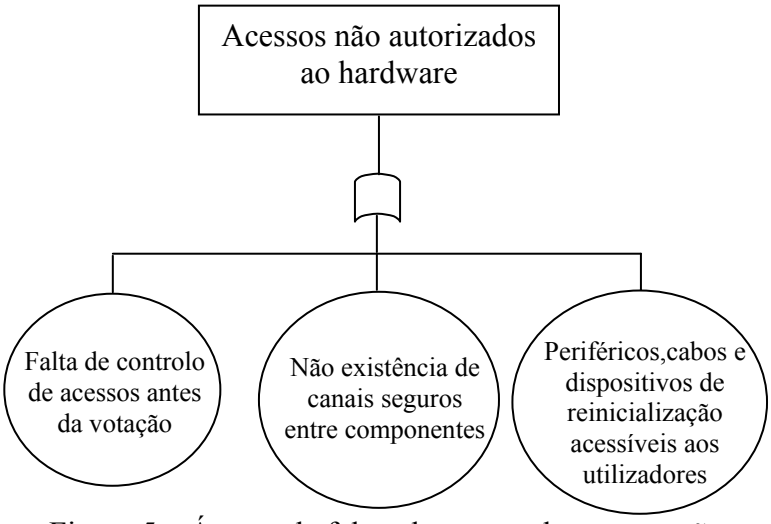

Figura 5 – Árvore de faltas do ataque de acessos não autorizados

- Acesso não autorizado a dispositivos como o ecrã, o teclado e o rato, podem permitir a um atacante captar informação confidencial como palavras passe e sentido do voto através da leitura dos movimentos do rato, da pressão das teclas ou de rápidas imagens obtidas do ecrã do dispositivo de votação

Acesso não autorizado ao software [12]

- O uso de palavras passe "fracas", facilmente sujeitas a ataques de dicionário ou de "força bruta" ou ainda caso se mantenham configurações por omissão dos componentes e propriedades da configuração da rede podem facilitar os actos de sabotagem dos atacantes.

Uso remoto de software [10] [11] [12]

- Existe no mercado software capaz de permitir a administração remota de um sistema e que pode ser usado por um atacante com intenções de sabotagem, por exemplo, PC Anywhere, LapLinks e back Orifice 200 entre outros.

Modificação (remota) de software por intrusão [10] [13] [11] [12]

- O atacante pode tentar executar os seus próprios comandos no dispositivo de votação, modificando o software de votação ou substituindo-o por outro software, explorando por exemplo erros de programação ou ainda através de ataques a palavras passe.
- O atacante pode também tentar utilizar recursos externos e dispositivos de comunicação sem fios como forma de tentar comunicar com os componentes do sistema.

Ocupação/consumo de recursos dos componentes [12]

- O atacante pode tentar servir-se dos recursos dos componentes, nomeadamente do espaço em disco, desde que lhe seja permitido escrever no dispositivo, ou dos recursos da CPU, levando o componente a executar elevado número de cálculos computacionais, provocando eventualmente demoras e atrasos no decorrer do processo.

Alterações na configuração [12]

- O atacante pode tentar alterar configurações básicas do sistema ou dos seus componentes, prejudicando o funcionamento do mesmo.

2.2.2 - Falhas do sistema

As falhas do sistema reflectem os riscos a que o SVE está sujeito quando ocorre alguma falha em algum componente específico, ou na ligação (comunicação) entre eles.

Perda de informação [11] [12]

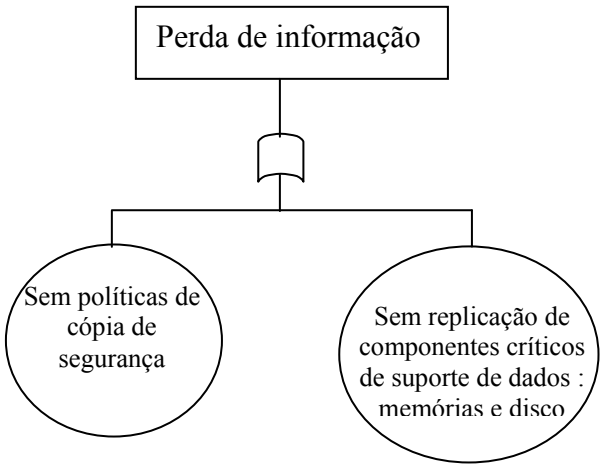

Figura 6 – Árvore de faltas do ataque de perda de informação

A perda de informação pode acontecer em vários casos:

- Em caso de acidentes (inundação, incêndio, etc.);
- Falha de um componente específico;
- Falha nos canais de comunicação;
- Quebras de energia.

Falha de um componente específico (hardware)

- A falha de um dos componentes de hardware do sistema pode vir a provocar danos e perdas de informação que dependesse directamente dele.

Falhas nos canais de comunicação

- Os componentes têm que comunicar entre si e proceder a trocas de informação. Se acontecer algum problema no momento da comunicação, a informação que deveria circular pode perder-se.

Quebras de energia

- A quebra de energia de alimentação ao sistema em procedimentos fulcrais do processo de votação (momento de salvaguarda, por exemplo) pode afectar o resultado do procedimento ou mesmo não executar esse procedimento.

2.2.3 - Erro Humano – lapsos e deslizes

O erro humano pode acontecer num processo de votação electrónica e colocar em risco o funcionamento previsto para o sistema. Uma desatenção (humana) pode ocorrer, originando um lapso, com repercussões no desenrolar do processo.

Confirmações do votante

- A confirmação de voto de um votante pode dar origem a um lapso, caso o votante se apresse a confirmar o seu voto sem realmente se assegurar da sua intenção. Ou ainda se simplesmente activar o processo de confirmação de voto não intencionalmente (carregando sem querer na tecla/no écran/etc.) de confirmação.

Operações da mesa de voto

- Ao executar algumas operações, em particular nas operações que controlam o funcionamento das máquinas de voto, a mesa de voto pode cometer um deslize. Como exemplo, autorizar quem não devia ser autorizado a votar ou ainda descarregar dos cadernos eleitorais um votante que não aquele que em determinado instante pretendesse votar.

2.2.4 - Erro Humano – enganos relacionados com procedimentos

Se algum dos procedimentos, exigidos para o normal funcionamento do sistema, não for cumprido por esquecimento, desleixo, simples incompetência ou desconhecimento, o SVE corre riscos e o seu correcto funcionamento pode ficar em causa.

Erros de programação

- Os erros de software podem ser considerados vulnerabilidades geradas por erro humano: sobrecarga de "buffers", inputs não controlados dos utilizadores (por teclado, rato, etc.), passagens de parâmetros do código de uma camada para outra, concorrência de tarefas, reserva de grandes quantidades de espaço de memória, etc. ou ainda outros relacionados com engenharia de software, como a falta de testes, má integração de módulos, etc.

Erros nos procedimentos operacionais do processo de votação

- Podem acontecer erros por exemplo na abertura das urnas, como a não inicialização das urnas de voto, não selar as urnas no final da votação, ou não imprimir os recibos de cada urna de votação.

2.2.5 - Erro Humano - violações

Para além dos riscos de sabotagem de um atacante, outros erros humanos intencionais directamente relacionado com o processo de votação podem afectar o regular funcionamento do sistema.

Fraudes internas

- As eventuais fraudes num sistema de votação electrónico podem ter origem em elementos das equipas responsáveis pelo processo de votação.

Não cumprimento de regras

- Não verificação do direito de voto de um eleitor.

Venda e delegação de votos[10]

- Um votante pode vender o seu voto, desde que consiga provar qual foi realmente a sua opção; vender a palavra passe que lhe permitiu votar (delegar o voto) [10] é bem mais fácil.

3 - ARQUITECTURAS DE SVE EXISTENTES

Neste capítulo será feita uma revisão bibliográfica sobre as mais importantes arquitecturas de sistemas de votação electrónicos existentes de forma a entender melhor o caminho que até esta altura tem sido percorrido nesta temática.

3.1 - As Arquitecturas de SVE

3.1.1 - Sistema proposto por Atsushi Fujioka, et al.

É um dos sistemas [14] para votação electrónica que serviu de base a muitos outros que se seguiram, pois apresenta um conjunto de componentes bastante completo. Na fase *Preparation*, o votante preenche o boletim de voto, compõe a mensagem digitalmente assinada, enviando-a para o *Administrator*. Por sua vez, o *Administrator*, na fase de validação, assina também a mensagem (que contém o voto "oculto") e devolve-a ao votante. Na fase seguinte, a votação, através do componente *Voting*, o votante recebe o boletim assinado e envia-o para o componente de contagem. Aí o *Counter* publica uma lista com os votos recebidos. De seguida, na fase de verificação, pelo *Opening* o votante torna o seu voto conhecido, enviando de forma anónima a sua chave de encriptação e finalmente o *Counter* conta e anuncia os resultados na fase de apresentação de resultados.

3.1.2 - O sistema FOO

É um sistema [15] também proposto por Fujioka et al., por isso reflecte um sistema que se comporta de forma muito semelhante ao anterior, onde podemos apenas referir que alguns componentes assumem outra designação: o componente que verifica a autenticidade do boletim é o *Validator* e o que conta é o T*allier*.

3.1.3 - O sistema EVOX

É um sistema [16] também baseado na arquitectura de Atsushi Fujioka et al., mas que apresenta novos componentes, quer numa fase de pré-votação mas também durante o processo de envio/recepção de mensagens, utilizando canais anónimos. Assim, nas fases anteriores ao processo de votação propriamente dito, ou seja, no pré-registo e registo dos votantes, existem, respectivamente, os componentes *Election Commission* para criação dos boletins e *Registrar* com a função de elaborar uma lista de votantes e distribuição de palavras passe. Na fase de votação, o votante preenche o boletim, assina-o e envia-o para o *Admin* que verifica a sua autenticidade e o reenvia para o votante. O votante depois de verificar a assinatura deveria enviar o boletim para o *Counter*, mas este passa ainda pelo *Anon* de forma a anonimizar o canal de envio. Na fase de contagem/apresentação de resultados, o *Counter* conta e apresenta os resultados da votação. Finalmente na fase verificação, cada votante pode confirmar o seu voto e o *Confirmation* todas as restantes assinaturas.

3.1.4 - O sistema Sensus

O sistema Sensus [17] é uma arquitectura sugerida por Lorrie Cranor e Ron Cytron que vem em sequência do trabalho realizado por Fujioka et al [18]. Inicialmente realizado para substituir a votação via correio tradicional, veio a revelar-se suficientemente flexível para permitir outros tipos de votação menos tradicionais [19].

O Sensus é um sistema que apresenta três módulos (componentes) essenciais :
O *Registrar* que é responsável pelo registo dos votantes para cada eleição; o *Validator* que tem como função verificar o registo do votante e assegura que um votante vota apenas uma vez; o *Pollster* que actua como um agente de votação, que apresenta os boletins de voto a cada votante e colecciona o voto, sendo ainda responsável pelas operações de criptografia e entrega do voto e finalmente o *Tailler* que "colecciona" e conta os votos, sendo também responsável pelas apresentação de resultados.

3.1.5 - O sistema REVS

O sistema REVS [20] proposto por Zúquete, et al. parte do princípio da existência de uma lista de eleitores já registados e preocupa-se apenas com o processo eleitoral a partir deste ponto. É um dos dois protocolos em estudo que apresenta em separado um componente responsável pela anonimização do voto. Trata-se sem dúvida de um protocolo robusto por apostar numa arquitectura baseada na replicação de componentes para minorar problemas de faltas e quebras de conexão entre os mesmos.

O REVS propõe uma arquitectura com cinco componentes, começando pelo *Ballot Distributor* que assegura a distribuição dos boletins pelos votantes e é responsável pela configuração das chaves e assinaturas envolvidas no processo; o *Administrator* assegura que só os boletins digitalmente assinados são válidos; anonimizam o voto, ocultando o endereço IP da máquina que permitiu ao votante exercer e ocultando ainda a hora em que ocorreu a votação através do *Anonymizer*; o *Voter Engine* executa o protocolo de votação em si, gere as funções de criptografia e as comunicações entre servidores; finalmente o *Counter* verifica a validade dos votos (através das assinaturas), elimina a repetição de votos e calcula os resultados.

3.1.6 - Sistema proposto por Robert Kofler, et al.

É uma arquitectura [21] que separa claramente a fase de registo da fase de votação propriamente dita (a fase em que se deposita o voto).
A fase de registo engloba o componente *Registration*, permitindo o registo de votantes durante um período anterior ao(s) dia(s) de eleições e o *Trust Center* que verifica as credenciais dos votantes e autoriza a votação.
A fase de Votação é composta pelo componente *Ballot Box* que também acumula os votos.

3.1.7 - O sistema Oasis Election

O sistema Oasis [22] propõe um componente ainda numa fase de pré-votação, o *Candidates*, sendo este responsável pela "nomeação" dos candidatos e constituição das listas; o componente *Voters* coordena o registo de votantes, a interligação entre as bases de dados e as comunicações aos votantes; o *Voting* gere os pedidos de autenticação dos votantes e respectivas respostas , o voto e "depósito do voto" e respectiva confirmação de votação; o *Results* faz a contagem dos votos e o *Audit* é o componente que pretende exercer algum tipo de verificação sobre o número de boletins entregues, inutilizados e não usados.

3.1.8 - O sistema Cybervote

Trata-se de um sistema [23] sugerido num relatório sobre requisitos para um protótipo de votação electrónica apresentado à Comissão Europeia por um conjunto de quatro organizações (EADS Systems & Defence Electronics, NOKIA Research Centre, K.U.Leuven Research & Development British e British Telecommunications)

Apresenta um componente na fase de pré-votação, o *Client repository* que contém toda a informação sobre os dispositivos que permitem os votantes vir a votar; o *Registration Server* tem como função registar os votantes; o *Vote Server* é o responsável pela recepção dos votos, após confirmação de autorização de votação de cada votante; o *Tabulation* faz a contagem, a verificação e a apresentação de resultados e finalmente sugere também um componente que se irá responsabilizar pela verificação do processo de votação e pela gestão dos registos, o *Audit and validation.*

3.2 - Quadro resumo dos SVE existentes

A partir da revisão bibliográfica efectuada sobre os sistemas de votação electrónica existentes, podemos construir um quadro resumo, conforme apresenta a tabela 1.

Sistemas / Fases	Fujioka, et al.	EVOX	Sensus	REVS	Kofler, et al.	Oasis	Cybervote
Pré-registo		election commission				candidates	client repository
Registo		registrar	registrar		registration	voters	registration server
Validação	administration	admin	validator	administrator	trust center	voting	vote server
Anonimização		anon		anonymizer			
Votação	preparation e voting	voter	pollster	voter engine	Ballot box	voting	vote server
Contagem / apresentação de resultados	counting	counter	tailler	counter		results	tabulation
Verificação	collecting e opening	confirmation				audit	audit and validation

Tabela 1 – Quadro que resume os sistemas de votação existentes, suas fases e respectivos componentes.

Os sistemas EVOX, OASIS e Cybervote incluem um componente numa fase ainda anterior ao processo de votação (anterior mesmo à fase de registo do votante), chamada de pré-registo. Nessa fase, no sistema EVOX são elaborados os boletins pelo compoennte Election Comission, no sistema OASIS faz-se a gestão de candidatos através do componente Candidates e no Cybervote a preocupação é com a gestão da informação acerca dos dispositivos que irão permitir aos votantes exercer o seu voto.

Relativamente à fase de registo dos eleitores, apenas os sistemas propostos por Fujioka et al. e por Zúquete et al. partem do princípio que a lista de eleitores já existe. Em todos os restantes se prevê o registo de votantes.

A validação do votante é tida em conta por todos os sistemas aqui apresentados, no entanto Fujioka et al., Zúquete et al. e Kofler et al. sugerem que tal validação deve ser efectuada à parte da componente de votação enquanto que os outros sistemas aglomeram as duas fases no mesmo processo. Ao separarem estas operações fundamentais para o processo, os sistemas conseguem torna-las estanques. Ou seja, a auditoria pode ser efectuada a cada uma das fases separadamente e caso ocorra algum problema numa das fases, este poderá ser isoladamente mitigado independentemente da outra.

O sistema REVS apresentado por Zúquete et al. trata da anonimização do voto com um componente em separado (Anonymizer) e com a função muito específica de encobrir a origem e data do voto. De notar que o sistema EVOX também se refere à anonimização de canais através de um componente específico, o Anon. Ainda que os outros sistemas se refiram também à anonimização, esta fase é incluída no processo de tratamento do voto durante a fase de votação.

A fase de votação é uma fase de consenso entre todos estes sistemas, enquanto que só o sistema sugerido por Kofler et al. não se refere à fase de contagem do voto.

A fase de verificação apresentada por estes sistemas pode ser considerada como a primeira abordagem deste tipo de sistemas ao processo de auditoria sem o qual não será possível tornar a votação electrónica um processo ubíquo e totalmente aceite na nossa sociedade. No entanto, os componentes apresentados pelos sistemas em estudo limitam-se a verificações após o processo ter decorrido, salvaguardando o caso da Cybervote conforme se descreve mais à frente. Mas regra geral, só já depois de ter ocorrido a votação, estes sistemas demonstram alguma preocupação com a questão do número de boletins usados ou não e inutilizados, ou com o facto de um votante ter votado e o seu voto ter sido contado. As questões e propriedades que são alvo de alguma verificação nestes sistemas responsabilizam muitas vezes apenas os próprios votantes, mesmo que de forma muito limitada, por causa da garantia de algumas propriedades, em particular a da não coercibilidade.

Sistemas como o de Fujioka et al. e o EVOX, referem-se à fase de verificação como se fossem os próprios votantes os responsáveis, permitindo algum tipo de confirmação/validação final dos votos depositados. No caso do sistema proposto por Fujioka et al. [18] é através do componente Opening, enquanto que no caso do EVOX é através do componente Confirmation que os votantes podem exercer algum tipo de verificação sobre o seu próprio voto. O sistema apresentado pela OASIS, através do componente Audit, pretende dar mais algumas garantias ao processo, desde que os membros oficiais da eleição sejam capazes de verificar que o número de boletins depositados nas urnas, mais o número de boletins inutilizado, mais os boletins não usados seja igual ao número de boletins disponibilizados para votar; sejam também capazes de fornecer um mecanismo de recontagem no caso dos resultados serem contestados e ainda permitam a observadores a "vigilância" de todo o processo. O sistema sugerido pela Cybervote já refere uma fase de verificação em três segmentos: a segurança, os registos e questionários.

Esta revisão da bibliografia sobre os sistemas de votação electrónico existentes irá contribuir para a definição de uma arquitectura mais genérica, ou de referência, a partir da qual este trabalho sobre auditoria se irá basear.

3.3 - Arquitectura de referência

A descrição das arquitecturas aqui efectuada apresenta-nos uma panorâmica sobre os componentes e suas funcionalidades num SVE. Como vimos, alguns dos sistemas apresentam arquitecturas mais completas, ou seja, incluem mais componentes para as fases consideradas comuns para sistemas de votação electrónica. A gestão do risco de um sistema deste tipo, torna-se mais completa, quando existem mais componentes pois podemos incidir e dividir a sua intervenção por um conjunto de componentes mais específicos, logo com maior granularidade. Consideramos que será benéfico poder avaliar um SVE de forma mais granular.

A partir do quadro resumo dos SVE existentes, propomos então que se construa uma arquitectura de referência baseada no sistema EVOX. Este sistema apresenta um componente para cada uma das fases que vão desde o pré-registo até à fase de verificação, o que nos parece ser consensual para sistemas deste tipo.

Ao contemplar componentes para todas as fases, a arquitectura proposta pelo sistema EVOX permite uma divisão quase estanque de cada componente e das suas funcionalidades. Assim, o EVOX torna-se uma boa proposta para ter como base, pois o estudo de comportamento deste sistema poderá ser feito em qualquer uma das suas fases, ou seja, a cada um dos seus componentes.

Propomos então uma arquitectura com as fases de pré-registo, registo, validação, votação, anonimização e contagem/apresentação de resultados e os componentes respectivos incluídos em cada uma das fases, conforme se pode visualizar na tabela 2:

As fases	**Os componentes**
Pré-registo	Gerador de listas de votantes
	Preparador de boletins
Registo	Servidor de registo de eleitores
	Servidor de credenciais
Validação	Servidor de validação de Eleitores (credenciais e direito de voto)
Votação	Disponibilizador de boletim
	Contador parcial
	Cifrador de boletim
Anonimização	Anonimizador
Contagem / apresentação de resultados	Contador final
	Divulgador de resultados

Tabela 2 – Fases e componentes da de arquitectura de referência proposta.

Na fase de pré-registo, os *Potenciais Eleitores* podem fazer uma "pré-inscrição" para a votação através do componente *Gerador de listas de votantes*. O componente *Preparador de boletins* compõe os boletins de voto de acordo com as especificações do acto eleitoral.

Na fase de registo, o componente *Servidor de Registo de Eleitores* terá como função identificar o *Potencial Eleitor* e permitir o seu registo no sistema. Após o registo do *Eleitor*, o componente *Servidor de credenciais* entrega as respectivas credenciais ao *Eleitor* para que possa vir a exercer o seu direito de voto, caso o pretenda.

Na fase de validação, é o componente *Servidor de Validação de Eleitores* que verifica as credenciais do *Eleitor* e ainda o direito de voto, para não permitir uma segunda votação por parte do mesmo indivíduo.

A fase de votação é iniciada com a apresentação do boletim de voto ao *Eleitor* pelo *Disponibilizador de boletins*. Após confirmação das opções de voto do *Eleitor*, o componente *Contador parcial* permite ao eleitor visualizar a informação que o seu voto foi contabilizado até esta fase. O *Cifrador de boletim* cifra o boletim e entrega-o para anonimização.

O componente *Anonimizador* procede à anonimização do boletim de forma a garantir que a intenção de voto não possa ser relacionada com o votante.

Na fase de contagem e divulgação de resultados, o *Contador final* procede à contagem dos votos. Finalmente, o *Divulgador de resultados* apresenta as contagens finais ao *Público em geral*.

4 - DEFINIÇÃO DO PROBLEMA E OBJECTIVOS

4.1 - Importância da auditoria do sistema

Do nosso ponto de vista, a auditoria tem como finalidade minimizar os riscos de um sistema de informação pela via preventiva, assegurando que os mecanismos de controlo de qualidade levam a um maior cuidado na análise, desenho e concepção, especificação e desenvolvimento do sistema [24]. Assim, a auditoria do Sistema de Votação Electrónico deverá, na prática, ter como finalidade:

- Reduzir a probabilidade de ocorrência de situações que coloquem em risco o funcionamento normal do sistema:
Já vimos no início deste trabalho (capitulo 1 – Riscos associados ao SVE) que, falhas no sistema como sejam um problema de carácter técnico ocorrido numa peça de hardware, ou uma falha humana, por exemplo, podem comprometer todo o funcionamento do SVE.

- Verificar a existência de mecanismos de defesa contra danos e perdas, no caso de alguma das situações de risco para o sistema se concretizar:
A não existência de componentes e processos que garantam a cópia de segurança de dados pode colocar em causa a verificação/confirmação de dados, bem como necessárias recontagens, por exemplo.

- Verificar a capacidade do sistema para manter a sua operacionalidade no caso das defesas falharem:
Por exemplo, ainda que um dos componentes do SVE entre em colapso, a existência de uma réplica ou de um processo alternativo deve estar devidamente testadas e tornar-se eficaz sempre que seja necessário.

Como vimos nos protocolos estudados inicialmente, nenhum deles faz referência explícita a um componente de auditoria ou mesmo a uma auditoria do sistema propriamente dito. Existem em alguns casos componentes de apoio à verificação do sistema.

No entanto, esses componentes não podem ser considerados como capazes de auditar o sistema, pois umas vezes são os próprios votantes a fazer essa verificação, outras vezes tal verificação é apenas efectuada por membros não oficiais. A auditoria deverá ser realizada através de uma combinação de actividades dos eleitores e entidades oficiais, devidamente credenciadas de forma a dar garantias de isenção, idoneidade e correcção no processo.

Por outro lado, os componentes de verificação dos sistemas descritos no capítulo 3, quando existentes, concentram-se numa determinada fase, normalmente no final do processo de votação. Mas não é apenas no final da votação que a auditoria deve incidir, mas sim ao longo de todo o processo. Se o problema apenas for detectado no final da votação, poderá ser demasiado tarde para recorrer a medidas de defesa e mitigação do seu impacte no resultado da votação.

Assim, poder auditar o sistema em qualquer uma das suas fases irá tornar o sistema credível perante as entidades oficiais e público em geral. Só a auditoria a cada componente do sistema e a confirmação de que ele cumpre as funções para as quais foi construído poderá dar a garantia que as propriedades (inerentes à democracia, de sistema e requisitos) já enumeradas se verificam.

A monitorização de toda a actividade ao longo do decorrer do processo poderá reduzir a ocorrência de falhas, maximizando a prevenção do risco. Em caso extremo, ao proporcionar a detecção atempada de uma falha, poderá permitir uma tomada de decisão mais eficaz, mitigando o seu impacte no funcionamento normal do processo de votação.

A auditoria ao Sistema de Votação Electrónico dá-nos ainda a oportunidade de aprender a reconhecer as situações de risco para o SVE. Conhecer e compreender os riscos para o SVE, permite, por um lado, definir recomendações e procedimentos mais robustos que evitem ou reduzam a ocorrência desses riscos. Por outro lado, permite estabelecer planos, que poderemos chamar de contingência, destinados a minimizar os impactes que os riscos poderiam ter no funcionamento do Sistema de Votação Electrónico.

4.2 – Objectivos: análise, concepção e prototipagem

Nos capítulos seguintes do trabalho, iremos proceder à análise, concepção e prototipagem da arquitectura do SVE anteriormente proposta.

De forma a melhor compreendermos o funcionamento da arquitectura de referência descrita, cada uma das fases e seus componentes ilustraremos o processo com casos de uso e de mau uso para todas as fases.

A arquitectura de referência proposta para o SVE, será a arquitectura sobre a qual o processo de auditoria irá decorrer. Assim, no capítulo de concepção e desenho do SVE iremos descrever, do ponto de vista da nossa proposta, o funcionamento da capacidade de auditabilidade do processo sobre a arquitectura descrita.

Com a elaboração e exemplificação de um protótipo poderemos demonstrar as funcionalidades previstas para uma ferramenta de auditoria desta natureza.

5 – ANÁLISE DO SVE

Neste capítulo será feita a análise do sistema de votação electrónico proposto tendo como base a arquitectura de referência apresentada no capítulo 3.

5.1 - Os actores

Os actores representam todas as entidades que interagem com o SVE. Poderá ser um utilizador no sentido restrito de termo – pessoa que utiliza o sistema (eleitor, membro oficial, etc.), um equipamento informático, como por exemplo um servidor (servidor de registo dos eleitores, por exemplo), ou ainda outro componente do sistema (o anonimizador, por exemplo).

ANONIMIZADOR

É o componente que tem como objectivo anonimizar os boletins de voto, para evitar que seja possível relacionar o eleitor com as suas opções de voto. O anonimizador contribui para a garantia das propriedades de anonimato e privacidade do votante.

AUDITOR

Elemento/equipamento/serviço/entidade que tem como objectivo auditar em cada momento (antes, durante e depois) as transacções realizadas no SVE. Cabe ao processo de auditoria do SVE registar todos os eventos pertinentes para o sistema (acessos, envio/recepção de dados, criação de novos registos, alteração de dados, etc.) para permitir a detecção de deficiências de funcionamento e/ou a presença de eventuais erros.

CIFRADOR DE BOLETIM

É o componente que cifra o boletim após a confirmação de voto do votante.

CONTADOR FINAL

É o componente que faz a contagem final do apuramento dos resultados da votação.

CONTADOR PARCIAL

É um componente que vai contando os votos chegados à fase da votação e permite a visualização ao votante desse número. Poderá ser considerado uma ajuda à confirmação do votante de que o seu voto foi contado até ao momento.

DISPONIBILIZADOR DE BOLETINS

É o componente que irá proceder à entrega do boletim ao eleitor para que ele possa exercer o seu direito de voto.

DIVULGADOR DE RESULTADOS

É o componente responsável pela divulgação e apresentação de resultados ao público em geral.

ELEITOR

Os eleitores são as pessoas previamente registadas no sistema, ou seja, qualquer pessoa com condições de participar no acto eleitoral para o qual o SVE está preparado.

GERADOR DE LISTAS DE VOTANTES

Este componente incluído na fase de pré-registo tem como função criar e gerir a lista de potenciais votantes que procederam à sua "pré-inscrição" no sistema.

MEMBRO DA MESA ELEITORAL

Elemento nomeado pelo organismo oficial a quem seja atribuída a responsabilidade do processo eleitoral, com o objectivo de verificar a autenticidade dos eleitores no processo de votação presencial em recinto controlado.

MEMBRO OFICIAL

Elemento designado pelo organismo oficial a quem seja atribuída a responsabilidade do processo eleitoral, para acompanhar o processo de contagem, publicação e divulgação dos resultados eleitorais.

POTENCIAL ELEITOR

Todo o cidadão que esteja em condições legais para participar no processo eleitoral e que pretenda registar-se como Eleitor, para posteriormente exercer o seu direito de voto.

PREPARADOR DE BOLETINS

A este componente compete a preparação e composição do boletim de acordo com as especificações determinadas para o processo eleitoral.

PÚBLICO EM GERAL

Todos os interessados (órgãos de comunicação social, partidos políticos, candidatos, população, etc.) na obtenção dos resultados parciais/finais de um processo de votação.

RECENSEADOR

Elemento, nomeado pelo organismo oficial a quem seja atribuída a responsabilidade do processo eleitoral, com o objectivo de poderem aceder ao sistema para efectuar presencialmente o registo ou recenseamento de eleitores, ou apenas para supervisionarem estas operações.

SERVIDOR DE CREDENCIAIS

É o componente responsável pela gestão e entrega das credenciais de votação que irão permitir ao eleitor a sua identificação no momento da votação.

SERVIDOR DE REGISTO DE ELEITORES

Trata-se do componente que permitirá o acesso e gestão dos dados que constituem a identificação de todos os eleitores recenseados.

SERVIDOR DE VALIDAÇÃO DE ELEITORES

É o componente que para além de permitir o acesso aos dados acerca da identificação dos eleitores recenseados, regista se o eleitor já efectuou a votação num determinado acto eleitoral, com o objectivo de não poder efectuar novamente a votação – garantia da propriedade de singularidade do voto.

5.2 - Diagrama de contexto da arquitectura proposta

O diagrama de contexto apresentado na figura 7, permite reconhecer cada uma das fases do sistema e identificar os actores que com elas se relacionam. De notar que excluímos o auditor deste diagrama pelo simples facto de não sobrecarregar o diagrama e tornar mais fácil a interpretação gráfica da figura, pois o auditor é o actor que interage em todas as fases.

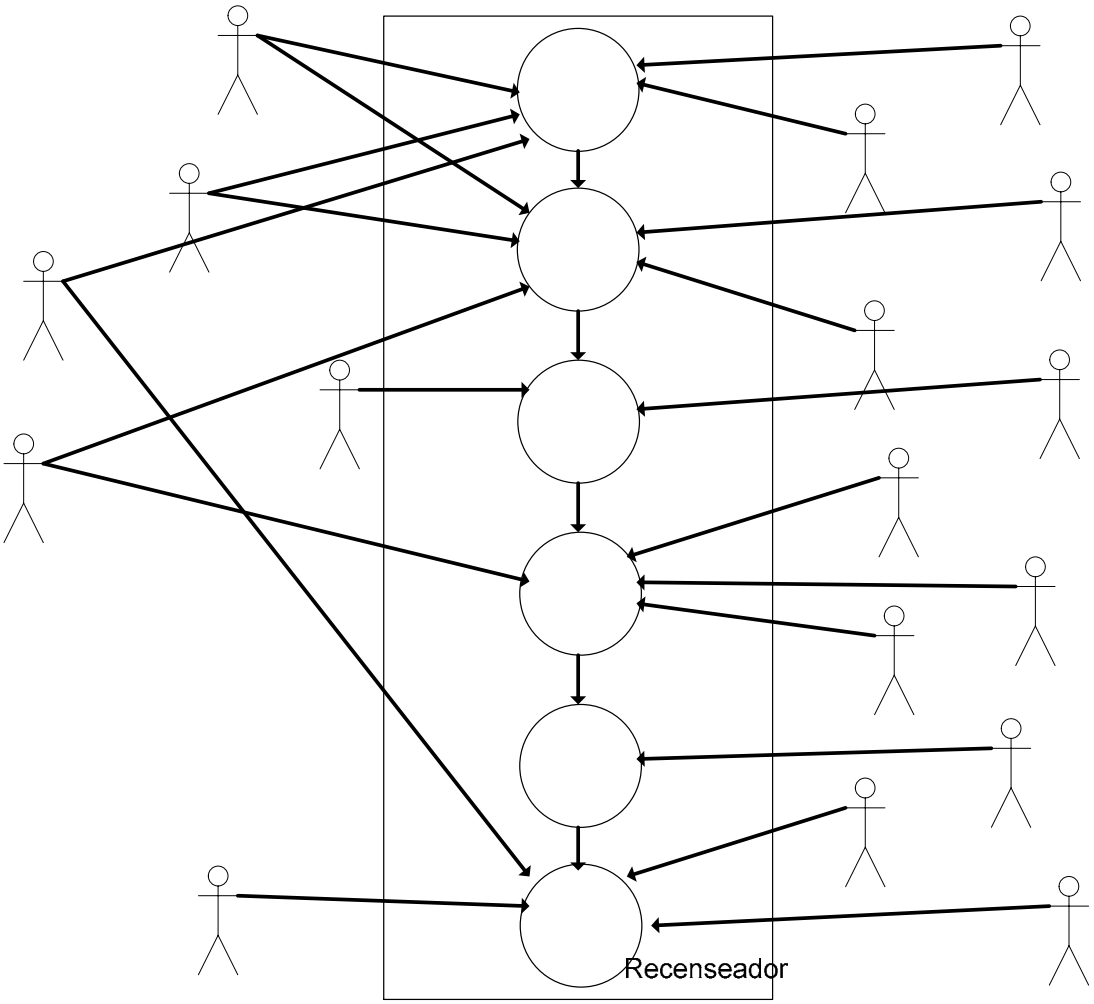

Figura 7 – Diagrama de contexto da arquitectura de referência proposta.

5.3 - Casos de uso

Os diagramas de casos de uso mostram como a utilização do sistema se encontra organizada. Os diagramas de caso de uso estão relacionados com a especificação de requisitos e discriminam o comportamento pretendido para o sistema. O estudo dos casos de uso, mais do que modelar os requisitos do sistema, destinam-se a dirigir todo o processo de desenvolvimento e avaliação do sistema [25]. Conforme já foi referido, foi adoptada uma arquitectura de referência no capítulo 3.3, pelo que passamos a apresentar os casos de uso para esta arquitectura.

5.3.1 - Casos de uso para a arquitectura de referência

Na fase de pré-registo, o *Potencial Eleitor* poderá proceder ao seu pré-registo no sistema, conforme se visualiza na figura 8. Ainda nesta fase o componente *Preparador de boletins* irá começar a compor e configurar os boletins de voto de acordo com as premissas do acto eleitoral.

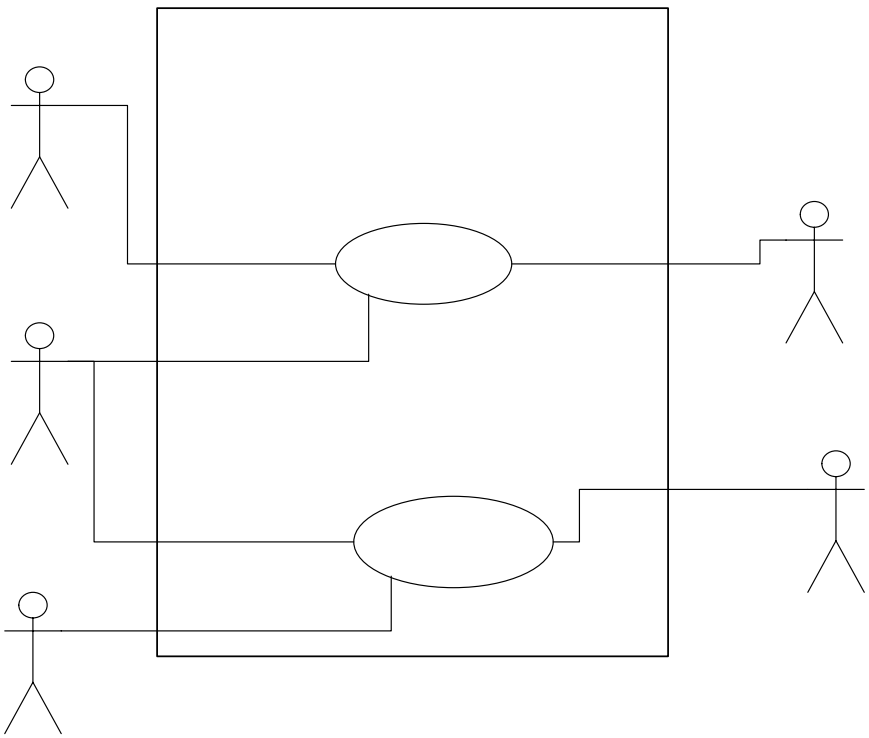

Figura 8 – Casos de uso da fase de pré-registo do votante.

Para efectuar o registo do *Potencial Eleitor*, este terá que ser identificado (presencial ou remotamente), conforme a figura 9 ilustra, por um dos dois actores (ou pelos dois) com essa função: o *Recenseador* e o *Servidor de registo de eleitores*. Após o seu registo, o eleitor recebe as credencias do *Servidor de credenciais* que irão permitir que posteriormente possa exercer o seu direito de voto. O *Eleitor* terá oportunidade, no final, de consultar os cadernos eleitorais e verificar se o seu registo realmente ocorreu.

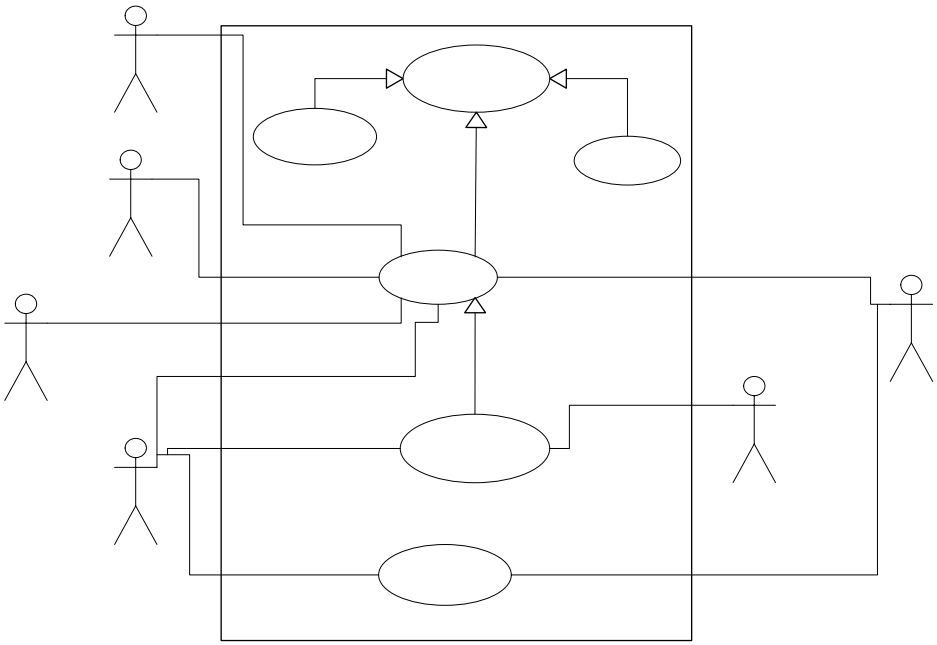

Figura 9 – Casos de uso da fase de registo do votante.

A figura 10 ilustra a fase de validação de credenciais e verificação de direito de voto do *Eleitor*. Para o votante poder votar, as suas credenciais têm que ser comprovadas e tem que se verificar se ainda não votou. Tais verificações podem ser efectuadas pelo *Membro da mesa eleitoral* e/ou pelo *Servidor de Validação de Eleitores*.

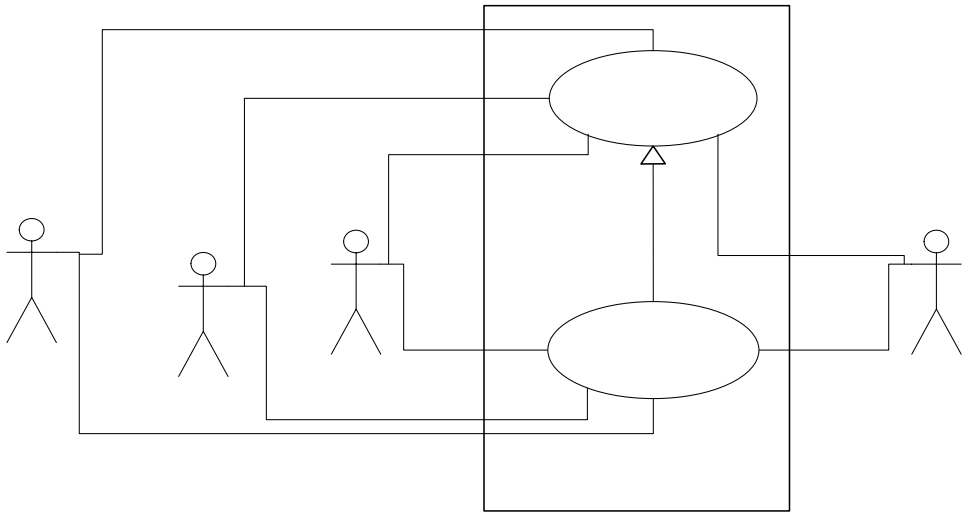

Figura 10 – Caso de uso da fase de validação e verificação do direito de voto do votante

Para votar, o boletim tem que ser disponibilizado ao *Eleitor* pelo *Disponibilizador de boletins*. O *Eleitor* preenche o boletim e confirma a(s) sua(s) escolha(s). O actor *Contador parcial* informa o eleitor da contabilização do seu voto até esta fase. O *Cifrador de boletim* cifra o boletim e procede à sua entrega para anonimização, conforme está explícito na figura 11.

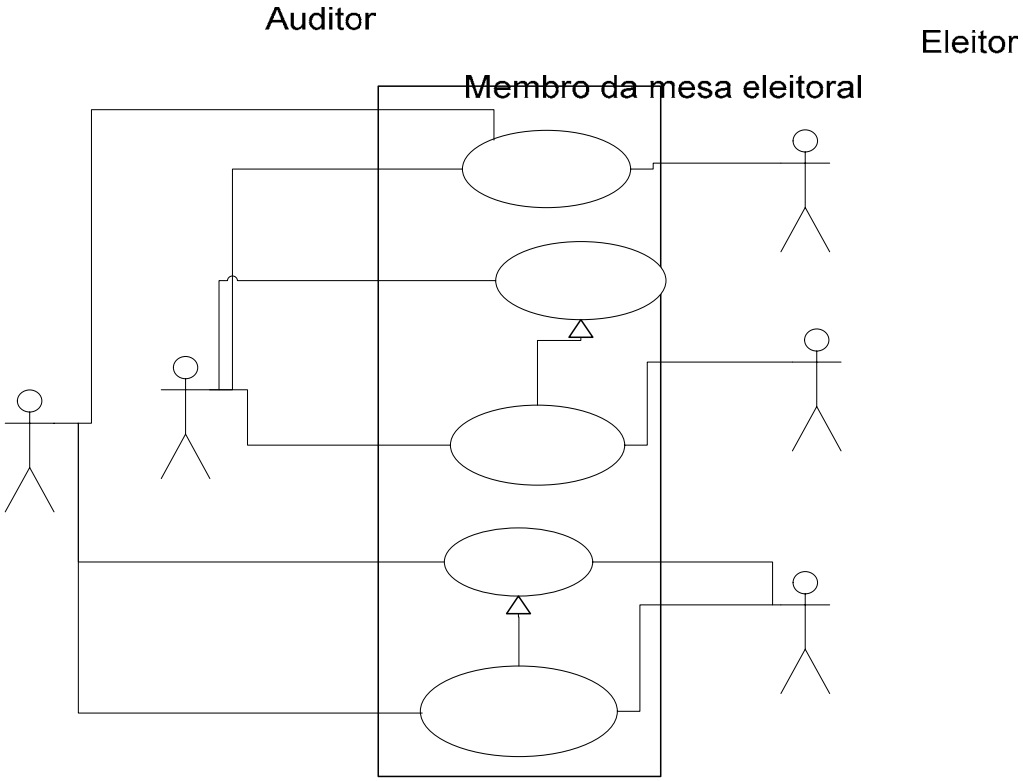

Figura 11 – Casos de uso da fase de votação

Ao *Anonimizador* compete a função anonimizar o boletim de voto e depositá-lo para contagem, conforme se visualiza na figura 12.

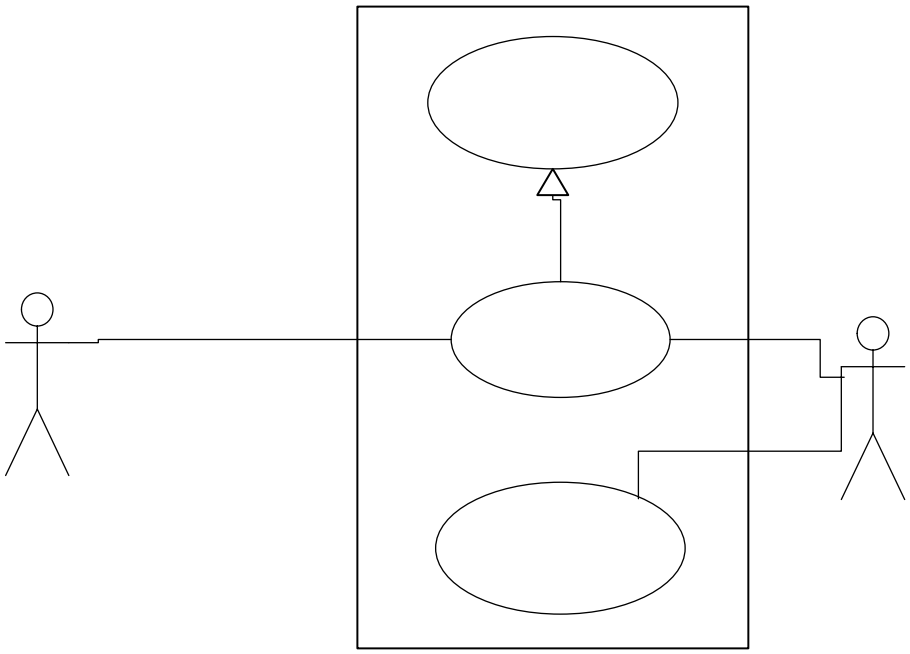

Figura 12 – Casos de uso da fase de anonimização do boletim de voto

O *Contador final* procede à contagem dos votos. O *Divulgador de resultados* disponibiliza os resultados para o *Público em geral*, tal como ilustra a figura 13.

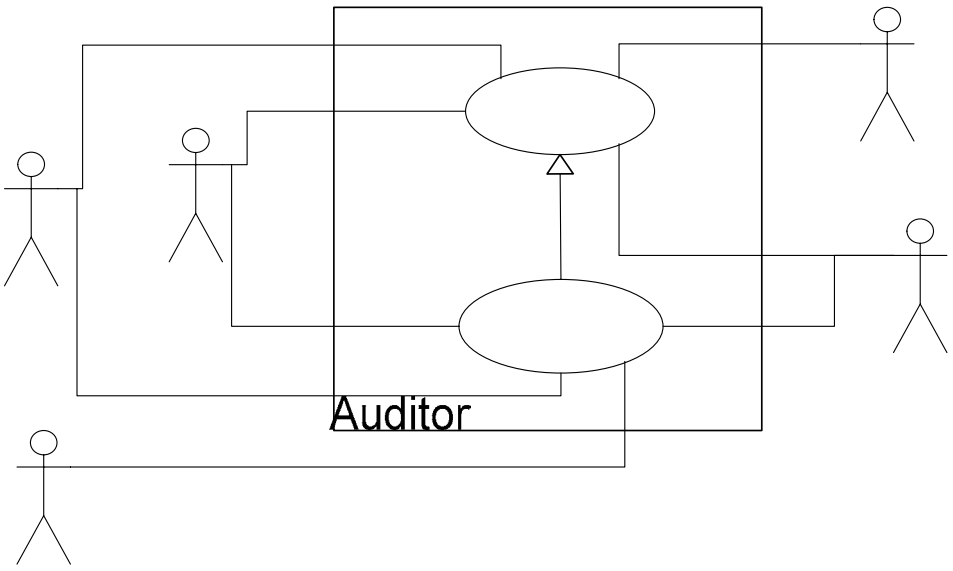

Figura 13 – Caso de uso da fase de contagem dos votos

5.4 - Casos de mau uso

Ian Alexander define casos de mau uso (misuse cases) , como casos de uso com intenções hostis [5], nos termos em que definimos lapsos e deslizes, enganos, violações e sabotagem. Como já vimos, em qualquer SVE há ameaças humanas ao seu correcto funcionamento.

Os misuse cases apresentam casos de uso relacionados com aspectos de risco do sistema, onde os actores, nesse caso "mis actors" [3], ou seja, agentes hostis ao sistema, se apresentam como alguém que intencionalmente ou acidentalmente inicia uma acção que pode representar uma ameaça ao normal funcionamento para o qual foi concebido o sistema. Os misuses case partem normalmente de casos de uso para definir cenários que fogem ao funcionamento previsto ou idealizado para o sistema.

5.4.1 - Casos de mau uso para a arquitectura de referência

Os “use cases”, descritos pelas figuras 8, 9, 10, 11, 12 e 13 podem assim ser refinados, através de misuse cases, das figuras 14, 15, 16, 17, 18 e 19.

Logo na fase de pré-registo, o sistema está sujeito a alguns dos riscos enumerados anteriormente, tal se pode visualizar na figura 14. O lapso do potencial eleitor pode ocorrer sem intenção, e dificultar alguma das tarefas seguintes no processo, nomeadamente o registo do eleitor. Um ataque de spoofing pode vir a tornar público dados privado e pessoais de um indivíduo. E a fraude interna da parte de um membro oficial é sempre um risco a ter em conta para o bom funcionamento do sistema.

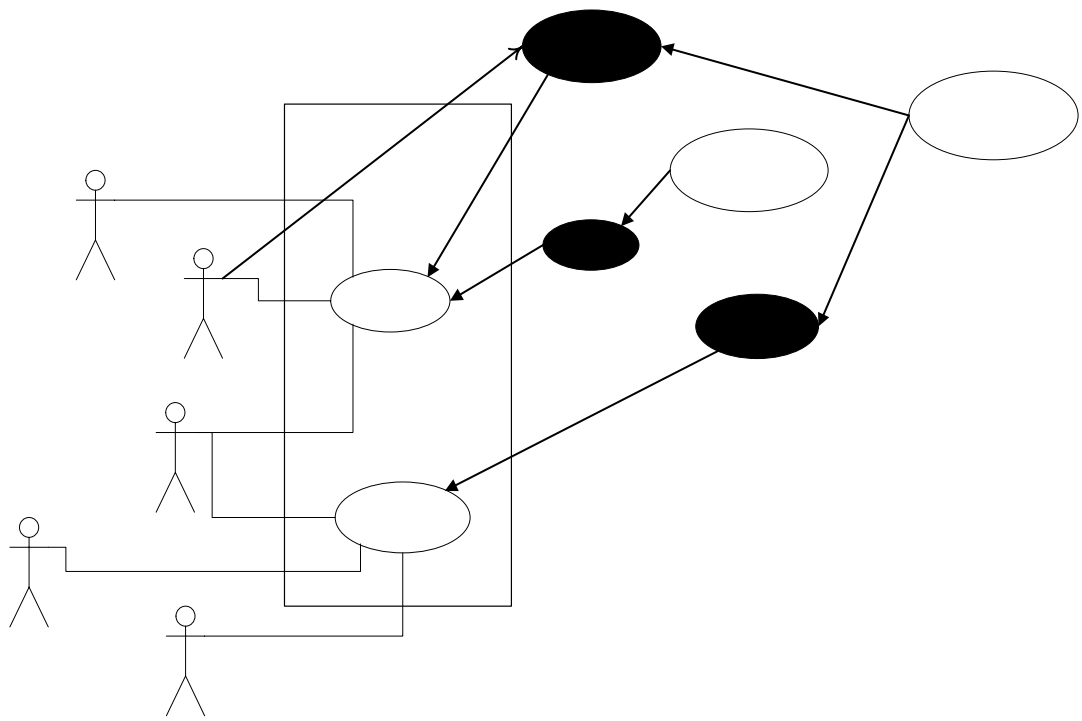

Figura 14 – Caso de mau uso para a fase de pré-registo do votante

Durante a fase de registo de votantes, o processo de votação voltar a estar em risco. Conforme ilustra a figura 15, alguns riscos, já estudados, de sabotagem, como spoofing, acesso a dispositivos e uso remoto de software poderão concretizar-se. O componente estará ainda sujeito a outros riscos de erro humano como a fraude interna ou a um lapso do *Recenseador*.

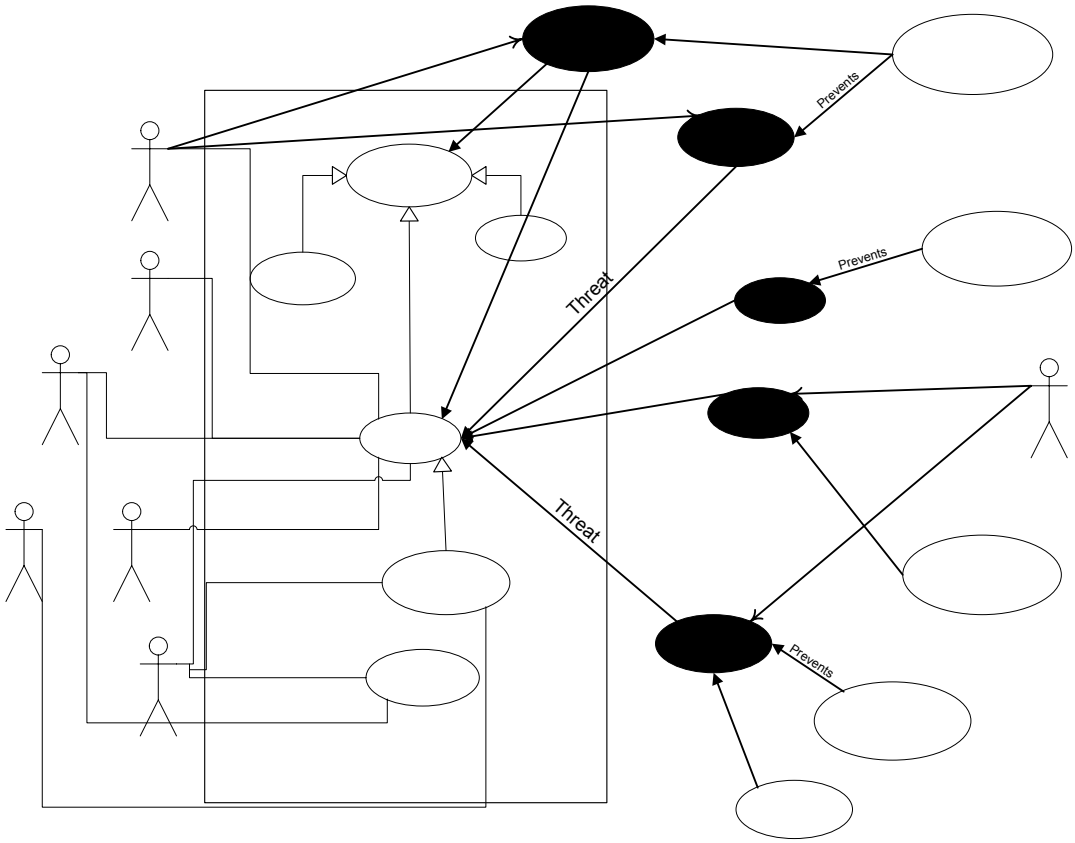

Figura 15 – Caso de mau uso para a fase de registo do votante

Na fase de validação das credenciais e verificação do direito de voto do votante do votante, os riscos de sabotagem e lapso mantêm-se, conforme se visualiza na figura 16, podendo ainda acontecer o não cumprimento de regras, como a não validação das credenciais do votante.

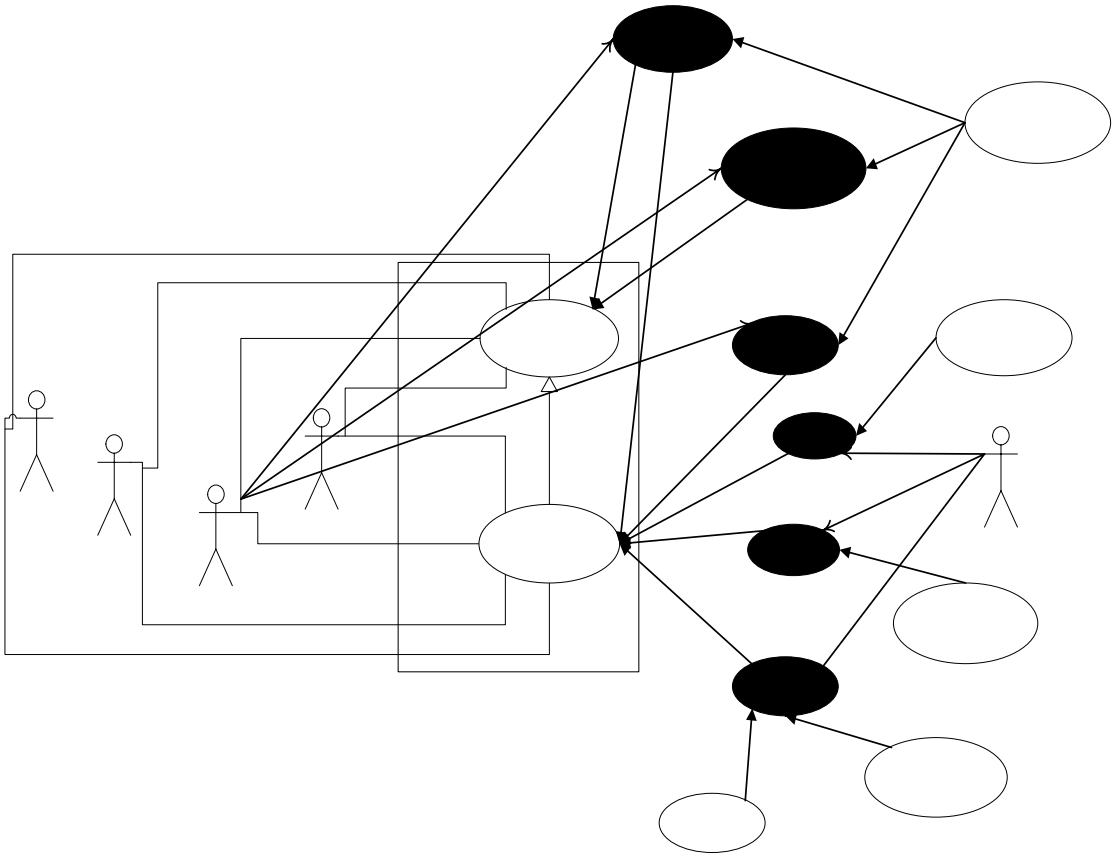

Figura 16 – Caso de mau uso para a fase de validação e verificação do direito de voto do votante.

Na figura 17, podemos observar que especialmente nesta fase – a votação, para além de alguns dos riscos já referenciados nas fases anteriores, o sistema está sujeito a ataques de negação de Serviço (DOS) e de Vírus e Cavalo de Tróia que impediriam ou dificultariam o normal decorrer do processo de votação. É nesta fase que pode ocorrer uma das violações mais difíceis de evitar/mitigar, a venda e delegação de voto.

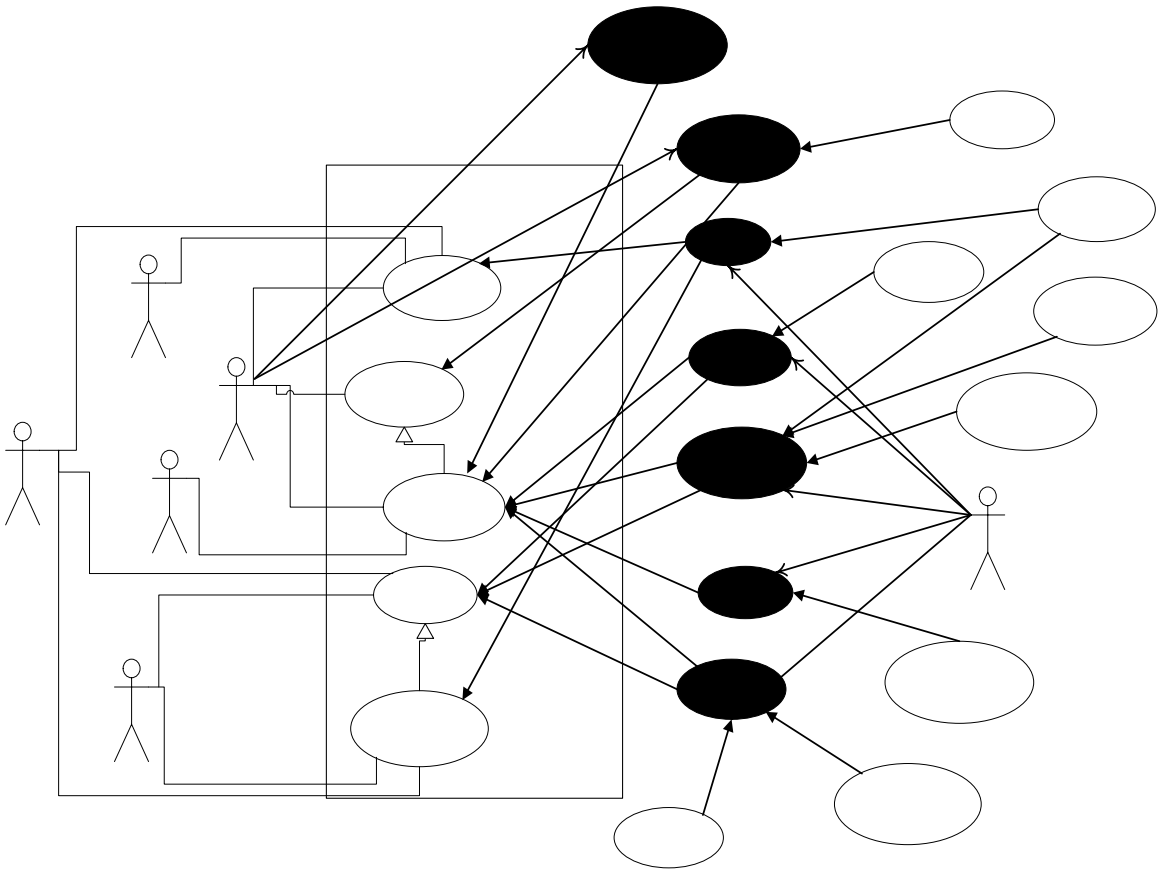

Figura 17 – Caso de mau uso para a fase de votação

Disponibilizar
boletim de votc

Disponibilizador de boletins

Preencher boletim
de votc

A fase de anonimização do boletim de voto, corre essencialmente riscos de sabotagem, conforme ilustra a figura 18. A anonimização do boletim é um processo muito "delicado" e importante num processo de votação. Sobretudo nesta fase, uma ameaça bem concretizada por um atacante pode provocar danos irreparáveis ao nível da privacidade e do anonimato - possibilidade de associação do votante com a sua intenção de voto.

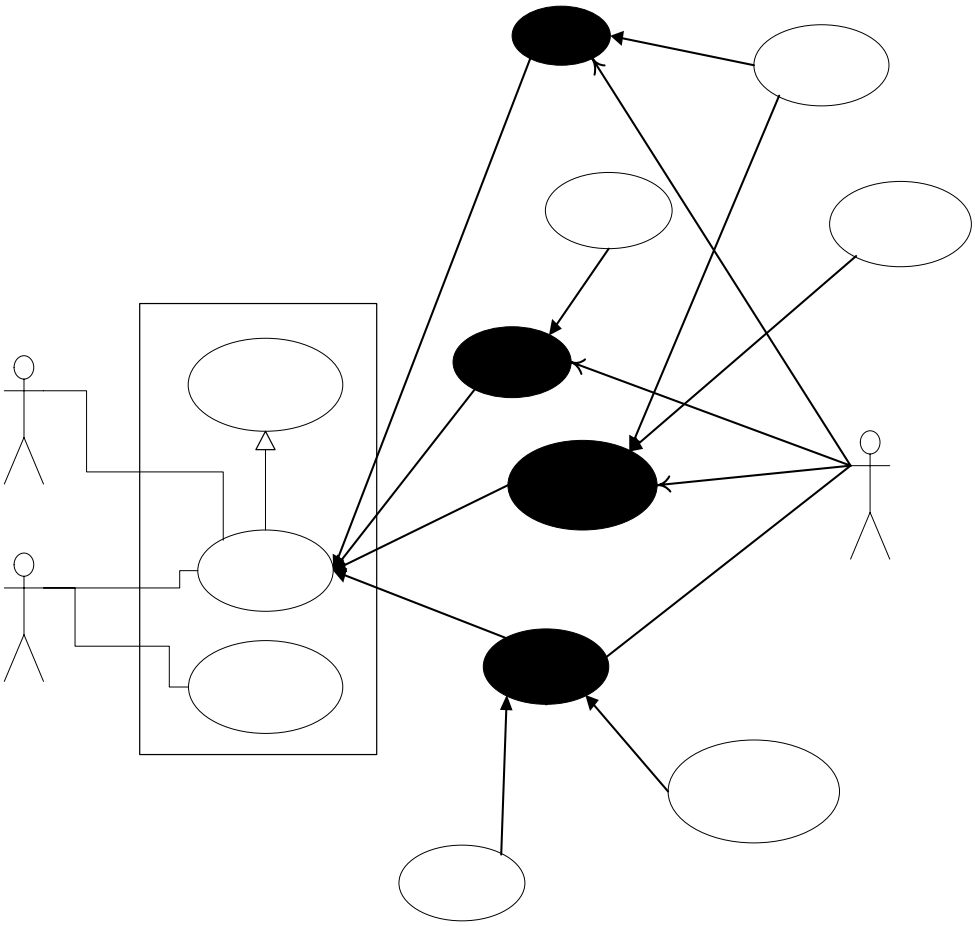

Figura 18 – Caso de mau uso para a fase de anonimização do boletim de voto.

Threat

Recolher boletim de voto

A par da fase de votação, a fase de contagem e apresentação de resultados é uma das fases cruciais do processo e por isso, vulnerável a quase todos os tipos de risco: sabotagem, erro nos procedimentos e mesmo fraude interna, tal como mostra a figura 19. Um ataque bem conduzido nesta fase pode levar a contagens enganosas ou então a "simples" erros/enganos na divulgação dos resultados.

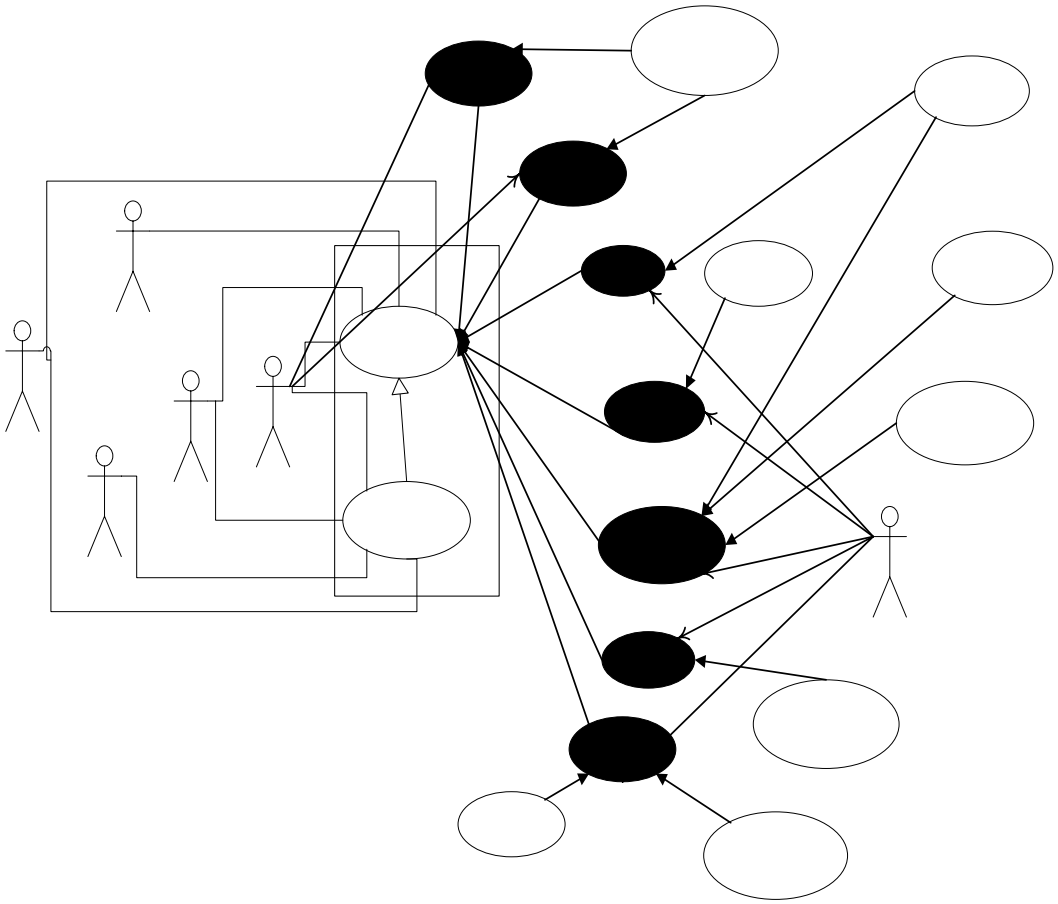

Figura 19 – Caso de mau uso para a fase de contagem/apresentação de resultados.

Threat

Thre

Contador final

Contagem dos votos

«uses»

Divulgador de resultados

Membro Oficia

Auditor

Apresentar resultados

6 – CONCEPÇÃO DO SVE

Feita a análise do sistema, estamos neste momento em condições técnicas de conceber e desenhar o SVE, conforme ilustra a figura 20 adaptada do modelo de Carroll [26].

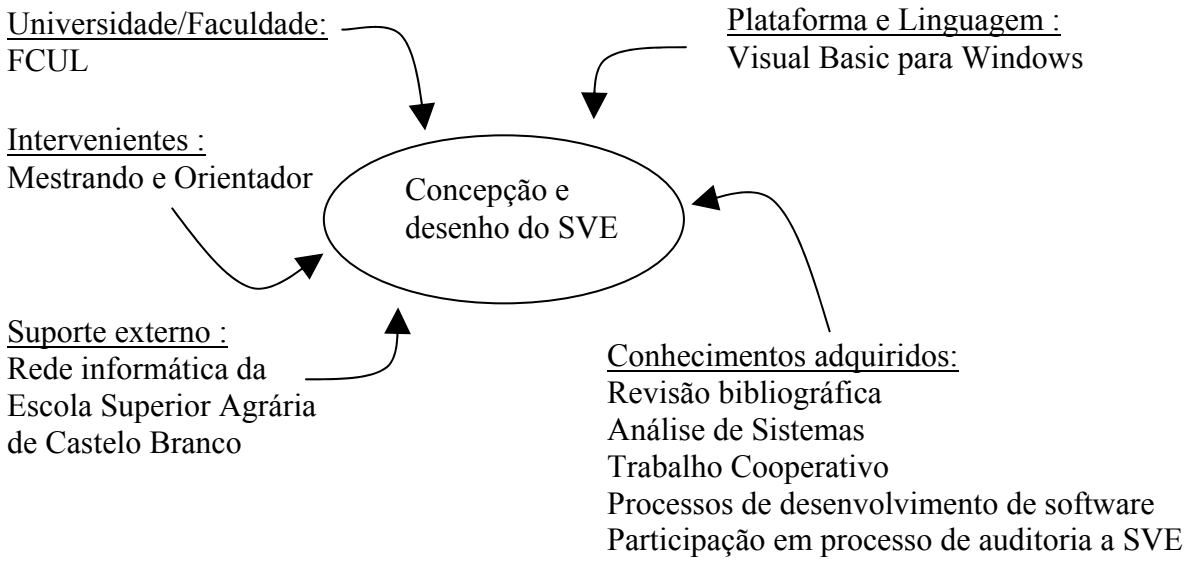

Figura 20 – Factores dinâmicos e interdependentes conducentes à concepção e desenho do SVE.

Foi na Faculdade de Ciências da Universidade de Lisboa que este trabalho foi proposto e será apresentado publicamente. Tem como intervenientes o seu autor, como mestrando e o orientador da tese de mestrado. O suporte externo ao desenvolvimento do SVE é facultado pela rede (infra-estrutura e equipamentos) existentes na Escola Superior Agrária de Castelo Branco. A plataforma utilizada para desenvolver foi a linguagem de programação orientada a objectos Visual Basic para Windows. Contribuíram de forma significativa para a concepção desta solução, a revisão bibliográfica apresentada neste trabalho, os conhecimentos adquiridos nas disciplinas de Análise de Sistemas, trabalho Cooperativo e Processos de desenvolvimento de software facultadas no plano de estudos correspondente ao 1º ano lectivo do curso de Mestrado em Informática na FCUL. Os conhecimentos e a experiência adquirida na participação na equipa de auditoria da FCUL para a experiência de voto electrónico para o Parlamento Europeu em 2004, foram também muito importantes.

6.1 – Processo de auditoria

Este trabalho apresenta a auditoria como um processo que corre em paralelo com a votação, existindo assim a necessidade de monitorizar em permanência cada componente que integra as fases do sistema de forma a garantir que ele cumpre as premissas para que foi elaborado, ou seja, para que cumpra as propriedades que lhe são inerentes.

Realça-se a prevenção das situações de risco associado ao sistema de votação, verificando dinamicamente as propriedades e casos de uso e ainda detectar os casos de mau uso relacionados. Assim, durante a monitorização do percurso do boletim, ao longo do processo de votação, deve ter-se em conta os seguintes objectivos:

- verificar a integridade e completude do percurso percorrido pelo boletim, isto é, confirmar que o boletim passou por todas as fases do processo e componentes do sistema;
- identificar casos de mau uso – as ameaças ao correcto funcionamento do sistema que se enquadrem num padrão com denominador comum ;
- procurar padrões de sabotagem, erro humano ou falha de sistema;
- garantir a qualidade do próprio processo de auditoria.

A auditoria ao longo do processo será efectuada pelas seguintes entidades:
- os auditores devidamente credenciados, e com conhecimento do funcionamento e vantagens da solução aqui apresentada;
- os votantes que vão sendo "informados" pelo sistema das operações a realizar e das opções tomadas;
- o próprio sistema, com capacidades endógenas de cruzamento e verificação de dados.

Tendo por base a arquitectura de referência anteriormente descrita, importa poder auditar os componentes em cada uma das fases do processo.

Propomo-nos então abordar a auditoria, na vertente da inspecção e análise de risco monitorizando cada fase com maior granularidade.
Se tomarmos como exemplo a fase de votação, por se tratar de uma fase crucial para o sistema, procederemos à monitorização de cada componente incluído na fase de votação (o *disponibilizador de boletins*, o *contador parcial* e o *cifrador de boletim*).

Ao refinarmos a granularidade de análise de cada fase, poderemos auditar cada uma das suas funcionalidades de forma mais rigorosa e pormenorizada. Poderemos monitorizar o que acontece passo a passo em cada fase e respectivos componentes, permitindo assim uma auditoria mais precisa e eficaz de cada etapa do percurso que deverá percorrer o boletim.

Podemos exemplificar alguns casos que demonstrem a importância de monitorizar as fases com o máximo de granularidade, ou seja, auditar as funcionalidades dos componentes incluídos em cada uma das fases:

- Se um componente não receber um boletim de voto que o outro acabou de "tratar" (disponibilizar, contar, cifrar, etc.), o boletim poderá ter-se extraviado. Se a informação de que o componente não chegou ao componente esperado for instantaneamente enviada para a interface, a propagação deste problema poderá, eventualmente, ser mitigada.

- Sob este ponto de vista da auditoria, fornecer informação de modo mais dinâmico para quem acompanha o processo, fará com que a adulteração de uma intenção de voto possa ser imediatamente detectada por exemplo através da visualização de uma informação relativa à integridade da mensagem que envolve o voto ou à alteração de um bit de controlo.

- A informação em tempo real de mau funcionamento de um componente poderá indicar problemas técnicos nesse componente, mas também poderá ser uma indicação para um ataque de negação de serviço.

- A circulação de mensagens não previstas / não autorizadas poderá por sua vez encapsular algum tipo de software maligno como um "Cavalo de Tróia". Se a solução tiver a capacidade de contabilizar e comparar o número de mensagens que deviam circular poderá fornecer a indicação correspondente e permitir ao auditor uma vigilância mais apertada no tráfego de mensagens.

- Com a capacidade de monitorizar as entradas e saídas de utilizadores, o sistema poderá reagir a uma tentativa ou mesmo entrada de um utilizador não credenciado. Podemos pelo menos ficar com o registo do momento em que as entradas de utilizadores acontecem, o que poderá ser útil no caso da entrada ter sido bem sucedida e ter dado origem ao roubo de credencias de um eleitor ou de outro actor do sistema (um membro da mesa, um membro oficial, etc.).

Medidas como a substituição de um componente por uma sua réplica poderão ser tomadas em tempo útil. Ou ainda a detecção atempada do extravio de um boletim poderá permitir tomar medidas que reponham o voto do votante ou pelos menos que evitem que outros boletins se percam.

A capacidade de recolher e guardar regularmente entradas de registos sobre os procedimentos que podemos associar ao risco, irá dar uma maior garantia de rastreabilidade de acções ainda que os atacantes tentem "limpar" as suas tentativas de ataques.

Guardar todas as estas entradas de registos importantes para monitorização e a possibilidade do auditor as rastrear e visualizar precocemente poderá evitar que o problema se prolongue ou mesmo que venha a ter alguma influência no resultado da votação, na pior das hipóteses poderá minimizar os seus efeitos.

Conforme já se referiu neste trabalho, pretende-se uma auditoria ao sistema pela via preventiva, mas pode haver algum caso em que um acontecimento de todo imprevisto possa não permitir a respectiva prevenção. Neste caso, o objectivo passa também pela mitigação do problema, ou seja, a minimização dos seus efeitos nefastos no funcionamento do sistema, caso o problema se detecte ainda durante o decorrer do processo eleitoral.

No entanto, temos ainda que acreditar que alguma situação possa não ser detectada ao longo do decorrer do processo. Neste caso os registos guardados regularmente poderão ser analisados no final do acto eleitoral para tentar reconstruir o sucedido, detectar o tipo de problema, o seu causador e contribuir para encontrar soluções futuras que o evitem ou minimizem, mas que sobretudo o possam detectar o mais atempadamente possível, evitando a repetição de tal falha.

Inicialmente, poderemos entender este processo de auditoria como uma ferramenta de análise de sistemas propostos, permitindo estudar e analisar o seu comportamento mediante um simulacro de votação. A partir desta análise poderá ser gerada uma lista de ameaças e casos de mau uso a ter em conta, ou ainda refinada a lista anteriormente descrita, bem como as respectivas medidas de intervenção para cada caso.

Desta forma, o risco que corre o SVE poderá ser minimizado, pois a experiência adquirida com as simulações realizadas a cada sistema poderão alertar para as ameaças, que apenas seriam, eventualmente, detectadas no dia da votação. As medidas de prevenção e até de solução adequadas poderão ser antecipadamente preparadas.

Com estas simulações consegue-se de certa forma o "treinar" quem constrói o sistema e também os auditores do mesmo. O treino resulta da simulação de situações reais de uma votação com a possibilidade de simular também a concretização de situações de risco para o sistema.

Assim, pensamos que esta nossa nova proposta de auditoria deverá também acompanhar o processo efectivo de votação de forma a maximizar a capacidade de responder dinamicamente à ocorrência de riscos e aplicar mecanismos de mitigação das suas consequências.

As simulações das auditorias realizadas devem servir de suporte a planos de prevenção e mitigação para o(s) dia(s) da(s) eleição(ções) propriamente dito. A experiência obtida pelo treino deverá ser uma mais valia para a monitorização do sistema no dia do acto eleitoral.

As situações ocorridas ao longo das simulações, ajudarão na preparação dos sistemas de compensação e substituição e na elaboração dos planos de resposta aos riscos e mesmo a ataques a que o SVE está sujeito.

As equipas de auditores envolvidas no processo, não deverão ser apenas constituídas por especialistas na área em causa, mas deverão também incluir pessoas da sociedade civil sem conhecimentos técnicos apurados nas ares de informática, comunicações, etc., tal como ocorre hoje em dia em Portugal com os membros da mesa eleitoral.

Entendemos que é importante para a concretização do objectivo de ubiquidade do processo electrónico de votação, que qualquer membro da sociedade possa ser envolvido na auditoria de um SVE. Neste sentido, é também objectivo deste trabalho, propor um protótipo cujas interfaces sejam de fácil interpretação e manuseamento, de forma a permitir a interoperabilidade com qualquer indivíduo ainda que não sejam considerados especialistas da área das novas tecnologias.

7 - PROTOTIPAGEM

O protótipo que aqui descrevemos deverá ser entendido na vertente de simulação. A potencialidade de usar estas funcionalidades numa situação real de votação fica para uma fase posterior, eventualmente, como trabalho futuro. Conforme já foi referido a simulação de auditoria, numa fase anterior à do acontecimento da votação propriamente dito, é também muito importante. Podemos vir a "aprender" muito com estes exercícios de simulação.

Com o estudo, ainda que em simulação, da auditoria ao comportamento de um sistema de votação, algumas das ocorrências no sistema que poderiam levar a perda ou danos de informação poderão ser previstas. Poderemos ainda acautelar situações em que, não tendo conseguido evitar uma ocorrência de risco para o sistema, poderemos tentar minimizar o seu impacte no funcionamento do sistema, pois no dia da eleição, o sistema não poderá deixar de produzir informação, ou seja, os eleitores deverão ser capazes de votar a qualquer instante. Ainda que aconteça um problema de funcionamento em algum dos componentes, eventualmente provocado por um ataque de negação de serviço, a tomada de medidas de mitigação (a substituição de um componente por outro que o substitua, por exemplo) poderá e deverá acontecer o mais depressa possível.

O protótipo será uma ferramenta de simulação da auditoria a um Sistema de Votação Electrónico que se irá basear na arquitectura de referência descrita.

7.1 – Requisitos do protótipo

O protótipo irá inspeccionar e analisar o comportamento de um sistema de votação baseado na arquitectura de referência proposta neste estudo, no capítulo 3. As fases e os componentes que este protótipo irá monitorizar são os que compõem a referida arquitectura de referência, desde o pré-registo do potencial eleitor, passando pela fase de registo, validação, votação e anonimização até à disponibilização dos resultados do escrutínio final. Em qualquer de uma destas fases o sistema estará sujeito ao risco, pelo que a auditoria terá que incidir sobre todos os componentes que compõem cada uma das fases.

Neste protótipo de simulação é o utilizador quem controla a sequência das acções, disponibilização de boletins, passagem do boletim a cada componente, cifra do boletim, etc. O que se pretende neste caso é fazer uma demonstração das capacidades de análise do comportamento do sistema, detecção de funcionamento anormal do sistema e respectiva capacidade de disponibilização de registos ao auditor para cada um dos componentes com uma ferramenta deste tipo.

O requisito principal do protótipo de auditoria ao sistema de referência é monitorizar o comportamento dos componentes e dar a conhecer ao auditor o que estará a acontecer nesse momento. O auditor deve ser informado a todo o instante do comportamento do sistema, quer o processo esteja a decorrer de forma normal, mas sobretudo se algo fora do previsto suceder. O protótipo será uma ferramenta de apoio à tomada de decisão para qualquer evento que altere o funcionamento previsto para o sistema. A tomada de decisão baseada na informação em tempo real do que está a acontecer no momento poderá ser a mais acertada e a que melhor resulta na tentativa de evitar ou mitigar os resultados negativos de uma situação de risco para o sistema.

Caso ocorra algum acontecimento fora do comportamento previsto para o sistema e para que a detecção da ocorrência de uma situação de risco para o SVE se faça o mais precocemente possível, propomos com este protótipo o registo e visualização desses mesmos registos em cada componente.

Propomos disponibilizar em tempo real as seguintes informações registados em cada componente:
- a data/hora da passagem de um boletim por cada uma das fases e dos componentes dessas fases;
- a contagem dos ataques (ou simples tentativas);
- a contagem dos boletins em cada uma das fases e respectivos componentes;
- as mensagem devolvida pelo protótipo em pontos e situações delicadas do processo, podendo dar a indicação de que algum ataque estará a acontecer;.
- a possibilidade de visualização gráfica dos casos de mau uso;

É a visualização em tempo real destes registos que irão permitir ao auditor manter um controlo o mais apertado possível do comportamento do sistema e por conseguinte uma rápida e acertada tomada de decisão.
Para além desta informação disponibilizada em tempo real, o protótipo irá registar informações sobre:
- a abertura e fecho das urnas – hora e data, identificação do individuo que procedeu a este operação;
- entradas e saídas de utilizadores do sistema (eventuais tentativas sem êxito);
- alteração de privilégios de utilizadores do sistema;
- acessos à bases de dados por utilizadores ou aplicações,
- substituição de algum componente;

Por um lado, esta informação poderá ser analisada à posteriori para simples elaboração de relatórios, documentos técnicos ou actas do processo. Por outro lado, os registos poderão ser utilizados para estudo do comportamento do sistema com vista a tentar melhorar o funcionamento do actual.

Em caso de ter ocorrido alguma situação de risco, ataque ou erro humano, sobretudo alguma violação, como o não cumprimento de regras na abertura de urnas, inicialização de contadores, etc., ou erros nos procedimentos operacionais do processo de votação, como a não verificação/confirmação de credenciais e/ou direito de voto, os registos poderão ser um contributo importante na investigação, apuramento de responsabilidades e até servir como meio de prova.

Conforme já foi referido anteriormente, este protótipo será uma ferramenta de auditoria operável e acessível por indivíduos sem preparação especial na área informática. É muito importante construir um protótipo que convença a sociedade e o público em geral, em particular os partidos políticos também, que as pessoas que hoje em dia estão "habilitadas" para integrarem a mesa de voto também podem vir a monitorizar o decorrer do processo de votação com a ajuda desta ferramenta.

Assim o protótipo é constituído por interfaces de simples interpretação, com a informação disponível para cada fase do processo e em cada uma das fases para cada componente incluído nessa fase.

Quando muito será necessário proceder a algumas sessões de formação para contextualizar os novos utilizadores e auditores acerca dos termos e função dos registos que surgem nas interfaces.

Neste protótipo, cada interface base da passagem do boletim por cada componente inclui áreas para visualização de informação – registos dos acontecimentos, dos quais poderemos destacar como mais importantes:
- área de visualização e registo do que está a acontecer ou se espera que aconteça em cada passo do percurso do boletim de votação, ou seja em cada componente de cada fase;
- uma área para registo e visualização de data e hora de chegada do boletim a cada componente;
- zona de registo, contabilização e visualização de situações de risco e ataques ao SVE;
- ainda uma área para visualização do caso de mau uso referente a um ataque ocorrido ou com indícios de ocorrência, de forma a facilitar a interpretação do risco;

Como não foi possível testar o protótipo em caso real, deixamos ao utilizador/auditor a capacidade de simular alguns ataques (extravio de boletim, alteração de voto, negação de serviço, intrusão por cavalo de Tróia e um acesso não autorizado ao sistema) de forma a tentarmos prever o comportamento do protótipo na detecção do problema e respectiva visualização da informação ao auditor.

Para melhor entendimento do funcionamento do protótipo, podemos acompanhar uma exemplificação no capítulo 7.4.

7.2 - Restrições

Seguindo a arquitectura proposta, seriam muitas as fases e respectivos componentes para exemplificação do protótipo. Sabendo que o processo de monitorização e auditoria do processo incide sobre muitos dos mesmos pontos em cada componente (comunicação entre componentes, circulação de mensagens, verificação de integridade, acessos, etc) decidimos escolher a fase da votação para exemplificação específica do protótipo.

Foi escolhida esta fase especificamente para exemplificação do funcionamento do protótipo, por se tratar de uma fase crucial para o sistema e susceptível a vários riscos e ainda por se tratar de uma fase que inclui mais que um componente : o *disponibilizador de boletins*, o *contador parcial* e o *cifrador de boletins*.

7.3 - Funcionalidades

A fase de votação considerada na arquitectura de referência, inclui três momentos fundamentais: a disponibilização do boletim, a confirmação das opções de voto do votante e a visualização da contagem do boletim pelo eleitor, e a cifra do boletim.

De forma a melhor representarmos a arquitectura do protótipo para esta fase, vamos usar um diagrama de blocos, o qual irá descrever visualmente a sequência, os componentes e o comportamento do protótipo. O diagrama apresentado na figura 21 ilustra as funcionalidades dos componentes integrados na fase de votação e a possibilidade de simular ataques a cada um deles.

As funcionalidades de disponibilização de boletins, confirmação de intenção de voto, cifragem do voto e entrega do boletim para anonimização e sua interacção com os actores do sistema já se encontram descritas no capítulo 5.3.1 - Casos de uso para a arquitectura de referência. O que acrescentamos a este diagrama é a capacidade do protótipo de simular ataques e visualizar os registos dos acontecimentos em cada um dos componentes da arquitectura de referência.

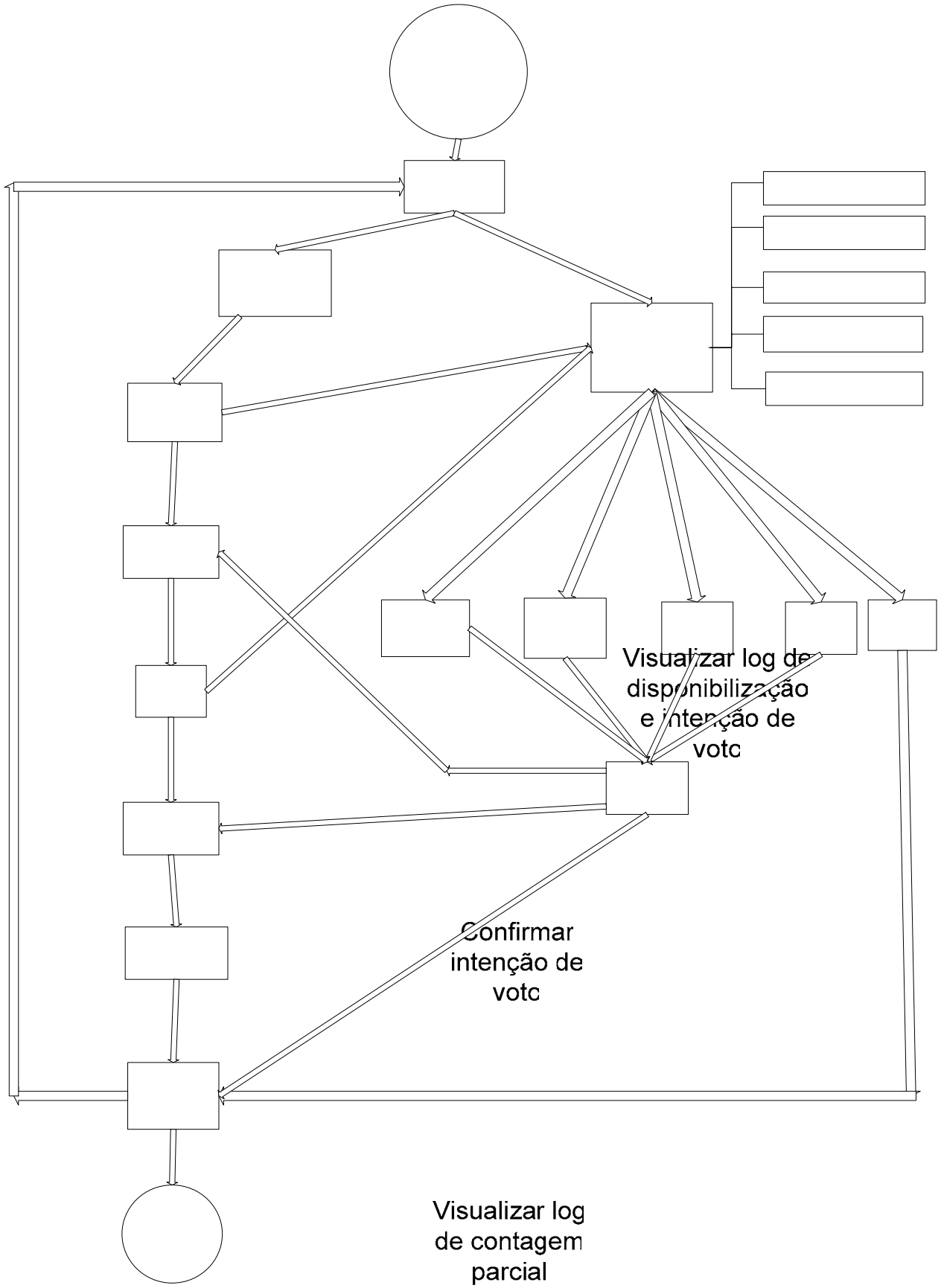

Figura 21 - Diagrama que descreve as funcionalidades do protótipo de simulação de auditoria de votação electrónica.

7.4 – Interface e diálogo com operadores

Disponibilização do boletim

Nesta fase será disponibilizado o boletim de voto ao eleitor. Já nesta fase, poderá acontecer alguma tentativa de ataque, ou então o extravio de um boletim ou alteração de intenção de voto, conforme se pode visualizar na figura 22.

Figura 22 – Interface do protótipo para disponibilização de boletim.

Caso não se verifique a concretização de nenhuma das ameaças previstas, o registo de ataques mantém-se inalterado, o boletim dado como preenchido e nos registos do componente verifica-se que tudo está a correr bem, conforme se visualiza na figura 23. Fica também registado a hora em que o boletim passou por este componente.

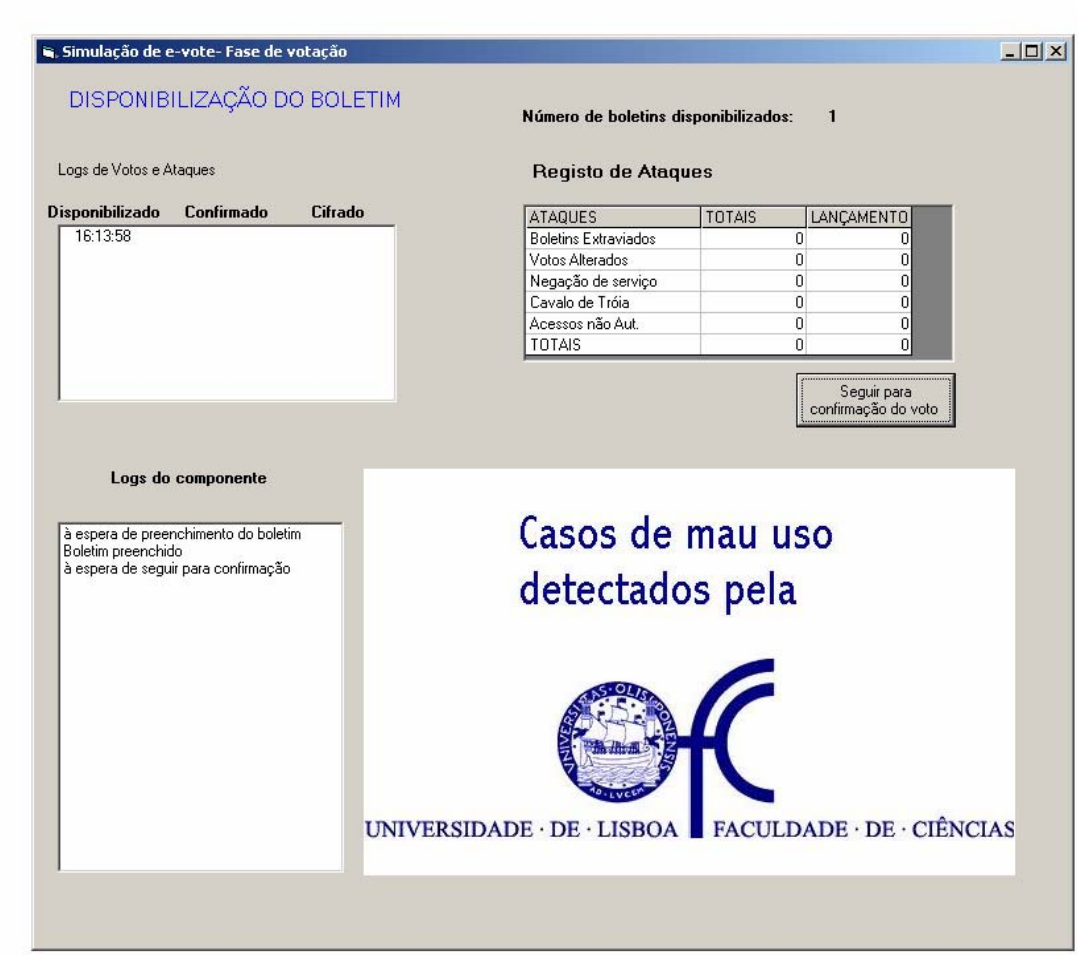

Figura 23 – Interface do protótipo após disponibilização e preenchimento de boletim.

A confirmação do voto

Após o boletim ter sido preenchido, o protótipo segue para o componente de confirmação. Este componente continua sujeito a ataques. Simulemos, por exemplo, um ataque de Negação de serviço ao componente de confirmação da intenção de voto, conforme identifica a figura 24.

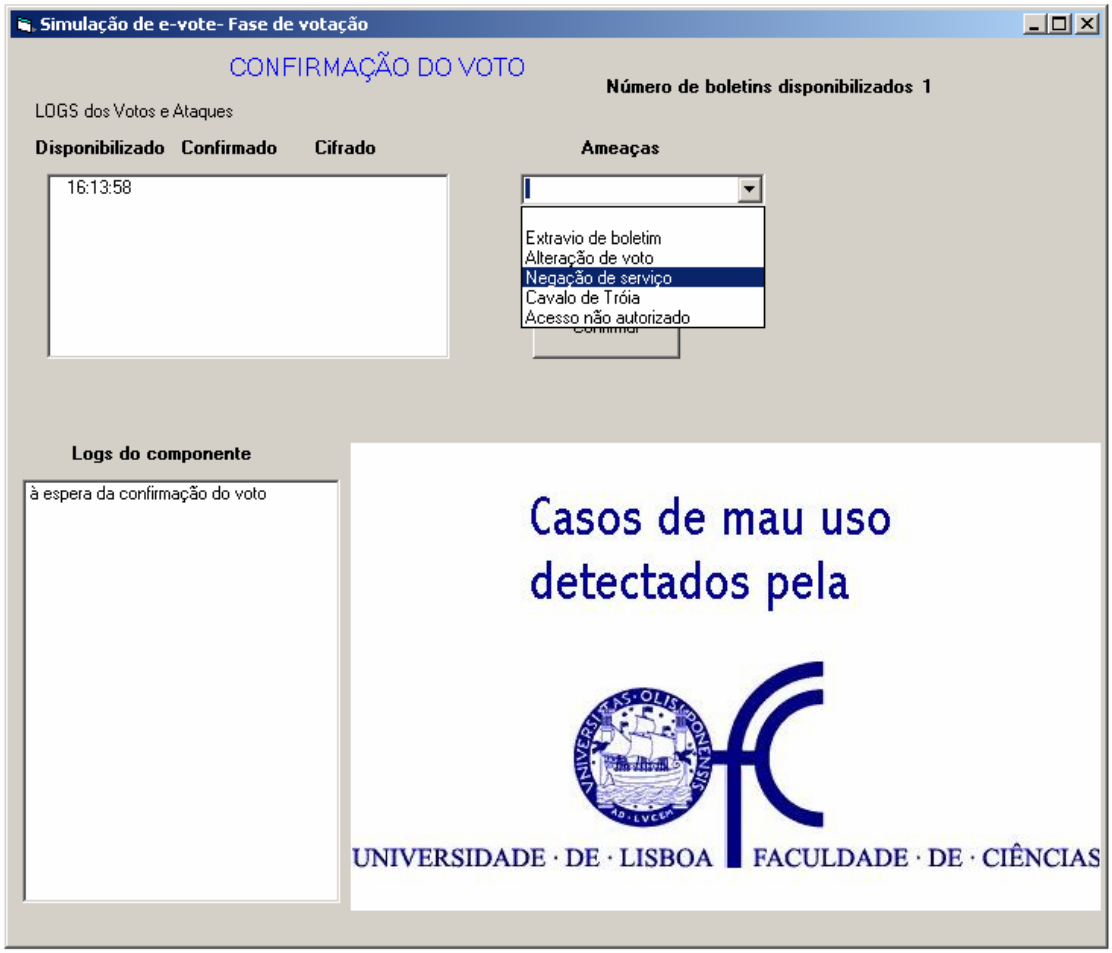

Figura 24 – Interface com intenção de ataque.

Sempre que uma ameaça se concretize, ficará registada na janela de registos do protótipo. A janela de registos do componente informa da existência de um problema, "Componente em mau funcionamento", o que dá a indicação ao auditor que o sistema está em risco e o indício leva a crer que se trata de um ataque de negação de serviço. É feita também a contabilização de um ataque de Negação de Serviço na interface de ataques (ver figura 25).

Nesta fase, como em qualquer uma das outras fases anteriores e seguintes, ao seleccionar um ataque na janela de "Registo de Ataques", surgirá uma imagem para os casos de mau uso com o respectivo "misuse case". As imagens associadas a cada caso de mau uso previsto no protótipo, facilitam o entendimento da ameaça e do tipo de medida a tomar.

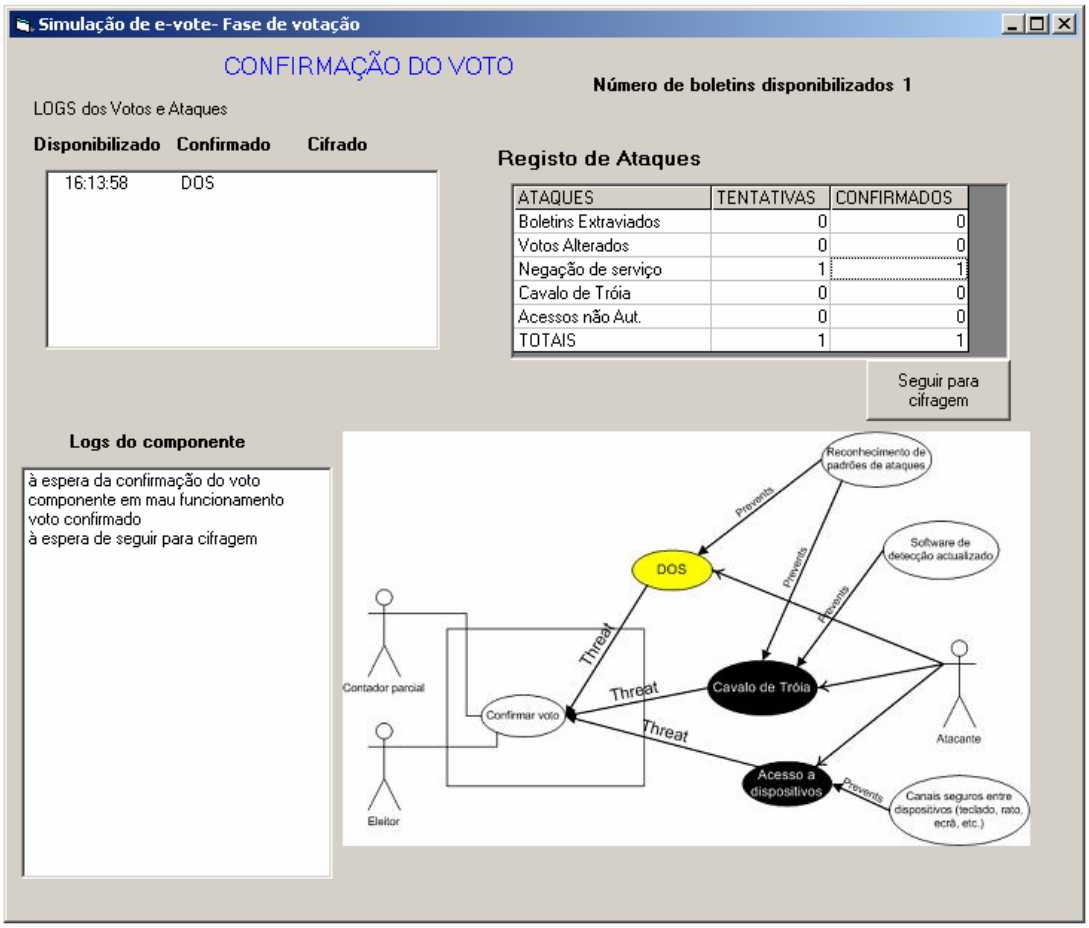

Figura 25 – Interface com simulação de ataque de Negação de Serviço (DOS) ao confirmar o voto.

A cifra do boletim

Ainda assim, caso o ataque tenha sido detectado atempadamente, o componente em falha pode ser substituído e o processo continuar em funcionamento, ou seja, seguir para a fase de cifragem do boletim, conforme figura 26.

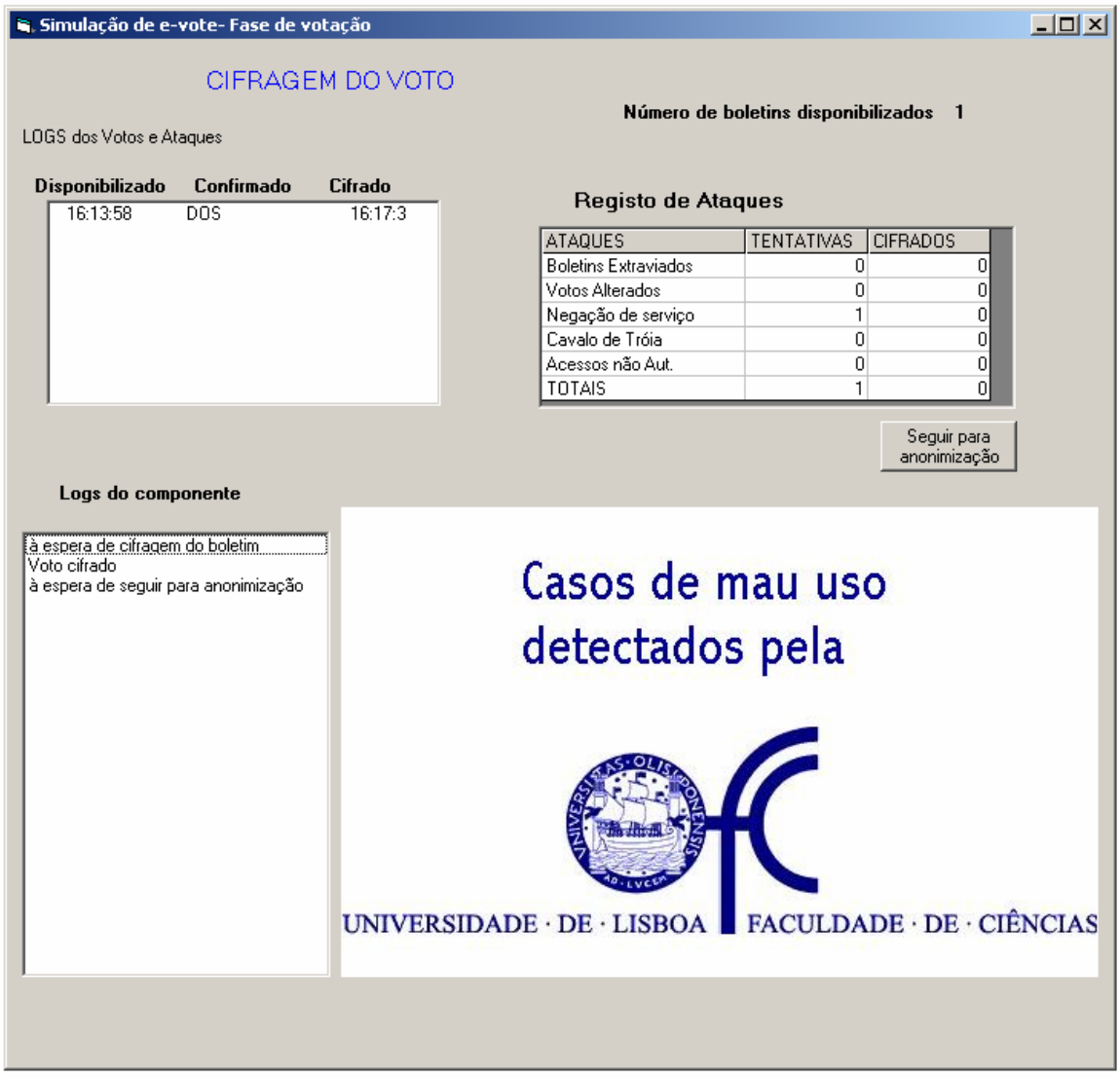

Figura 26 – Interface com os registos da simulação do sistema até à fase de cifra do boletim

Os registos finais

Na figura 27, é possível confirmar que na interface final do protótipo, se podem observar todos os registos de passagem dos boletins por cada um dos componentes, ficando inclusive registado a data/hora. Com estas indicações poderemos tentar comprovar a completude do percurso previsto para o boletim de voto.

Com a visualização do registo e contagem dos ataques ao SVE, poderemos tentar tirar algumas conclusões sobre a existência de tipos de ataques que mais aconteçam ou que se proporcionem a este tipo de sistemas. Note-se que, na figura 27 se visualiza que foram disponibilizados 5 boletins, mas apenas puderam ser contabilizados 4 pois um dos boletins extraviou-se (logo na fase de lançamento do voto).

O processo pode recomeçar do zero, ou seja reiniciando a contagem de boletins ou pode-se continuar com a disponibilização de mais boletins.

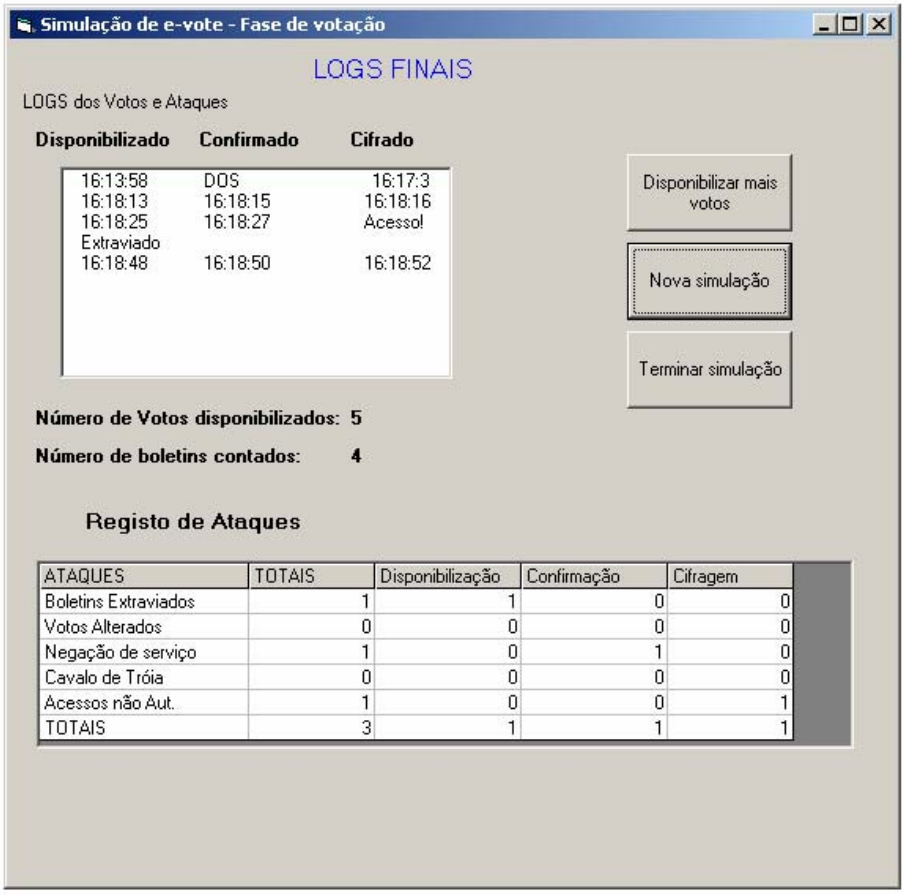

Figura 27 – Interface de registos finais da simulação.

7.5 – Cenário de uso

Conforme já foi referido, o protótipo apresentado neste trabalho poderá ser utilizado como forma de analisar e avaliar arquitecturas de sistemas propostos para Votação Electrónica. No entanto, o protótipo poderá também acompanhar o desenrolar do processo de votação no(s) dia(s) em que realmente ela irá acontecer – a votação poderá alongar-se por mais que um dia. Será com certeza uma mais valia poder ir monitorizando os procedimentos e os componentes associados ao sistema, pois isso irá permitir uma tomada de decisões dinâmica face aos acontecimentos e situações de risco que possam suceder.

Logo desde a fase de pré-registo proposta na arquitectura de referência, o auditor deverá monitorizar o comportamento do componente *Gerador de listas de votantes*, confirmando o pré-registo dos potenciais eleitores. Ainda nesta fase, deverá ser garantida a execução e configuração conforme pré-determinado dos boletins de voto, através da inspecção do componente *Preparador de boletins*.

Na fase de registo do votante, o auditor será responsável, através da vigilância ao funcionamento do *Servidor de registo de eleitores,* pelo registo do potencial eleitor. O auditor deverá ainda garantir que o Servidor de credenciais procede à entrega das mesmas aos eleitores.

Na fase de validação, o auditor deverá garantir que as credenciais do votante são validadas e que é verificado o direito de voto. Esta garantia deve ser acompanhada por um lado, pela monitorização do correcto funcionamento do componente *Servidor de validação de eleitores* e pela análise dos procedimentos executados pelo *Membro da mesa eleitoral*.

Neste caso de estudo, acompanharemos, para exemplificação mais pormenorizada, a monitorização do percurso do boletim na fase de votação, conforme simulação do protótipo, desde a sua disponibilização ao eleitor, até à sua entrega para anonimização:

A partir do momento em que ao eleitor é disponibilizado o boletim, o sistema estará sujeito a um conjunto situações de risco que já foram descritas neste trabalho. Com a monitorização dos componentes, poderemos seguir o comportamento do sistema sob alguns pontos de vista que poderão ser indícios de que algo não corre como previsto no processo.

No momento de apresentação do boletim de voto, a que podemos chamar fase de disponibilização do boletim, o próprio eleitor poderá tornar-se um auditor do sistema, confirmando se o boletim apresentado está conforme o tipo de votação previsto e se todas as opções respectivas lhe estão disponíveis. Tal como já foi referido, a auditoria de um Sistema de Votação Electrónico não deverá ser da única e exclusiva responsabilidade de um auditor. Os eleitores e o próprio sistema devem contribuir para este processo.

Seguidamente, ainda neste momento, o eleitor fará e confirmará as suas escolhas, conforme use case respectivo (figura 9).

Neste momento, o protótipo procede às seguintes operações :
- regista a data/hora da apresentação do boletim ao votante, e o momento de confirmação das escolhas por parte do eleitor;
- regista e contabiliza o boletim preenchido pelo votante;
- inspecciona o sistema para saber se ele é capaz de prosseguir com o encaminhamento correcto do boletim;
- analisa a integridade do voto, por exemplo, registando e comparando valores para o bit de controlo.
- possibilita a visualização dos registos dos acontecimentos na interface proposta, permitindo ao auditor o acompanhamento do decorrer do processo de votação.

Ainda nesta fase, baseando-nos na arquitectura de referência proposta, será indicado ao votante que o seu boletim foi contabilizado no sistema, o que poderá tornar-se para o eleitor um indício de que o processo está a decorrer com normalidade, aumentando o seu grau de confiança neste tipo de sistemas.

Seguidamente o boletim será cifrado.

O auditor acompanha este momento do processo através dos registos efectuados pelo protótipo:
- momento em que o boletim chega a esta fase deverá por sua vez ficar registado, bem como o momento em que tal operação se dá por finda;
- a contabilização do boletim como tendo sido cifrado;
- um teste de integridade a partir do bit de controlo;
- monitorização das mensagens entre os vários componentes de cada fase do sistema de forma a permitir a sua contabilização e comparação com o número de mensagens previsto pelo funcionamento normal do sistema.
- a solução continuará a inquirir o comportamento do sistema de forma a garantir que o boletim segue o seu percurso previamente estabelecido.

A solução proposta, apresentará no final de cada fase um resumo dos registos obtidos (data/hora da passagem dos boletins pelos componentes, número de boletins que passaram por cada componente, riscos a que cada componente esteve sujeito, eventuais extravios de boletins).

É esta sequência de registos contendo os momentos de passagem dos boletins por cada componente, e as respectivas contagens efectuadas, que nos dá a garantia que o boletim completou o seu percurso inicialmente previsto.

Podemos entender a confirmação da passagem do boletim por cada um dos componentes como uma cadeia de elementos (neste caso os componentes da fase de votação) que se vão encadeando, dando a garantia final da completude do percurso do voto em cada fase. Se conseguirmos monitorizar a completude de cada fase, haverá maior garantia da completude do percurso do boletim em todo o processo de votação.

Após a fase de votação, o boletim será entregue para anonimização.
Cabe ao auditor seguir esta operação, considerada como uma das mais delicadas, e garantir que a partir deste ponto, caso o componente *anonimizador* tenha cumprido correctamente a sua função, não será possível associar uma intenção de voto ao seu autor.

Na fase da contagem final e da divulgação de resultados, o auditor deve acompanhar o processo de contabilização do escrutínio e confirmar que todos os procedimentos são rigorosamente seguidos pelos membros oficiais (correcta selagem e fecho das urnas, impressão de recibos das urnas, etc.) e que o componente *Contador final* cumpre a sua missão conforme previsto e conta os votos com exactidão. O auditor deve ainda confirmar que os votos são fielmente apresentados ao público em geral pelo componente *Divulgador de resultados.*

Caso o processo de votação tenha decorrido na normalidade, e o auditor tenha acompanhado cada fase e monitorizado o comportamento de cada componente e cada actor envolvido no acto eleitoral, poderá ser dada a garantia de cumprimento das propriedades inicialmente enumeradas. E assim, atingido o objectivo que pretende tornar um Sistema de Votação Electrónico um processo cada vez mais ubíquo na nossa sociedade e aceite com confiança por todos.

8 – CONCLUSÕES E TRABALHO FUTURO

Até há algum tempo atrás, a votação electrónica só podia ser considerada como um processo complementar ao sistema tradicional em papel [27], pois deviam ser garantidos os direitos mais básicos de um eleitor: todos os eleitores têm o direito de participar no processo eleitoral e todas as formas de votação e tecnologia inerentes devem estar acessíveis aos votantes. Hoje em dia, como vários casos o demonstram, nomeadamente nos Estados Unidos da América e Brasil, a votação electrónica é a forma de votação já aceite por todos e a que tem ocorrido nos últimos tempos.

Por isso, cada vez mais, o processo de votação electrónica tem que ser um processo que transmita confiança aos eleitores. Este objectivo só poderá ser atingido por via do aumento da capacidade de auditoria em todas as fases da votação.

Neste trabalho, a auditoria foi tratada especialmente na sua vertente de inspecção e análise de risco. Ainda que a auditoria de um SVE estudada essencialmente sob estes pontos de vista possa ser considerada uma limitação, a forma mais granular e dinâmica como foi proposta, garante um aumento da capacidade de auditar o processo. Outros pontos de vista da auditoria de sistemas de votação electrónica poderão ser analisados em trabalhos futuros.

Com este trabalho pretende-se informar tecnicamente o público em geral para os riscos associados a um SVE e para os cenários de mau uso que lhe são inerentes, propondo ainda uma solução inovadora, de fácil uso e manuseamento para aprender a lidar com esses riscos.

Com a utilização de um protótipo de simulação de auditoria ao Sistema de Votação Electrónica como a que descrevemos neste trabalho, podem extrair-se experiências e "aprender" com os acontecimentos registados. Ao realizarmos este tipo de simulações, poderemos ficar a conhecer melhor o comportamento de um SVE perante as inúmeras possibilidades de ameaças concretas e reconhecer os ataques mais comuns e os mais danosos. A partir da obtenção desta informação, poderão elaborar-se planos de resposta e mitigação específicos para cada ataque e assim tornar o sistema mais seguro.

Este tipo de ferramentas poderá também ser utilizado numa situação de votação real para acompanhar o processo de votação, o percurso dos boletins e monitorizar a actividade do sistema. Poderá ainda fazer a detecção de ataques em tempo útil e aconselhar medidas de mitigação de forma a minimizar o impacte. Nesta perspectiva, permitirá aumentar substancialmente a capacidade de auditar das diversas entidades envolvidas, em particular os partidos políticos, dado que o simulador proposto poderá ser utilizado por uma grande diversidade de pessoas.

Consideramos, no entanto, este protótipo como apenas o primeiro passo para fomentar a auditoria do processo em todas as suas fases e assegurar que todas as propriedades exigidas são garantidas. Esperamos que a partir deste primeiro passo, se possa, no futuro, definir regras e procedimentos de avaliação, com vista à validação e consequente credibilização das arquitecturas propostas para votação electrónico.

8.1 - Trabalho futuro

Seria de certo muito interessante e importante identificar com maior detalhe as funções e propriedades associadas a garantir em cada componente do sistema e eventualmente aumentar ainda mais a granularidade do sistema. Ou seja, conseguir agrupar as propriedades em cada uma das fases do processo e associá-las a componentes específicos, tendo a noção que haverá casos de propriedades que não serão com toda a certeza estanques a uma só fase, mas terão que ser garantidas ao longo de todo o processo. Tal classificação iria contribuir para o estudo dos impactes que cada ataque poderia provocar em cada fase do sistema e respectivas consequências no funcionamento global do processo. Ajudaria também a desenvolver formas mais eficazes de mitigação das ameaças.

Conseguir melhorar o protótipo por exemplo na questão do lançamento dos votos e na geração, aleatória ou distribuída, de forma automatizada de ataques ao longo do processo, complementado com simulações em grande escala, por forma a conseguir tentar prever melhor o comportamento do sistema num caso real.

Ainda ao nível do protótipo, procurar auditar o comportamento do sistema, considerando a existência de replicação de componentes poderia aproximar ainda mais a simulação da realidade.

Já foi referido que seria extremamente importante e útil para a evolução deste trabalho em termos futuros que viesse a ser possível concretizar a utilização de uma ferramenta, como a que se descreve neste trabalho, numa situação real de votação.

9 - REFERÊNCIAS BIBLIOGRÁFICAS

[1] Antunes, P., Monteiro, A., Soares, N., Oliveira, R., (2001), *Sistemas Electrónicos de Votação*, DI-FCUL

[2] Rocha, Pinto R., Simões, F., Antunes, P., (2004), *Estudo dos Requisitos para um Sistema de Votação Electrónico*, Relatório Técnico – TR-04-2, Departamento de Informática da Faculdade de Ciências de Lisboa.

[3] Sindre, G., Opdahl, Andreas L., (2001), *Templates for Misuses Case Description*, Dept. of Computer and Information Science, Norwegian Univ. of Science and Technology, Dept. of Information Science, Univ. of Bergen, Norway.

[4] Alexander, I., (2002), *Misuse Cases Help to Elicit Non-Functional Requirements*, Independent Consultant

[5] Alexander, I., (2002), *Misuse Cases, Use Case with Hostil Intent*, Independent Consultant, http://www.scenarioplus.org.uk

[6] Wang, H., (2003), *Refining a Secure System through Misuse Cases*, CS681 class project

[7] Casanas, A., Machado, C., (2001), *O Impacto da Implementação da Norma NBR ISSO/IEC 17799 – Código de Prática para a Gestão da Segurança da Informação nas Empresas*, Universidade Federal de Santa Catarina (UFSC); Programa de Pós-graduação em Engenharia da Produção, Centro Tecnológico - Campus - Trindade, P.O Box 476 - CEP 88040-900 - Florianópolis, SC.

[8] Reason, J. (1990), *Human Error*, Cambridge University Press.

[9] Leveson, Nancy G., (1995), *Safeware System Safety and Computers*, Addison-Wesley Publishing Company

[10] Jefferson, D., (2000) *Internet Voting*, Compac System Research Center, Technical Committee of the California Secretary of State's Task Force on Internet Voting, California Internet Voting Advisory Committee, California Voter Foundation

[11] Pratchett, L., (2002) *The Implementation of Electronic Voting in the UK*, Montfort University of Essex, May

[12] Cybervote, (2002), *Report on Review of Cryptographic Protocols and security Techniques for Electronic Voting*, Cybervote:WP2:D6/V1:2000 v1.0

[13] Rubin, A., (2002), *Security Considerations for Remote Electronic Voting Over The Internet*, AT&T-Labs Research Florham Park, NJ.

[14] Fujioka, A., Okamoto, T., Ohta, K., (1993), *A Practical Voting Scheme for Large cale Elections*, NTT Network Information Systems Laboratories, Nippon Telegraph and Telephone Corporation, 1-2356, Take, Yokosuka-shi, Kanagawa-ken, 238-03 Japan.

[15] http://www.cs.washington.edu/homes/mausam/evote/tsld008.htm , em Setembro de 2006.

[16] Prakash, A., Mausam, (1999), *Electronic Voting System*, http://theory.lcs.mit.edu/~cis/voting/protocol/index.html , em Setembro de 2006.

[17] Cranor, Lorrie F., Cytron, Ron K., (SD), *Sensus: A Security-Conscious Electronic Polling System for the Internet*, Public Policy Research, AT&T Labs Research, Department of Computer Science, Washington University in St. Louis.

[18] Fujioka, A., Okamoto, T., Otha, K., (1993), *A practical secret voting sheme for large scale elections*. In "Advances in Criptology" – AUSCRYPT 92 (Berlim 1993), J. Seberry and Y. Zheng, EDs., vol 576 of "Lecture Notes in Computer Science", Springer-Verlag, pp. 405-419.

[19] Cranor, Lorrie F., (1995), *Can declare strategy voting be an effective instrument for group decision-making?*, Tech. Rep. WUCS-95-04, Washington University Department of Computer Science, St. Louis.

[20] Zúquete, A., Joaquim, R., Ferreira, P., (2004), *REVS, A Robust Electronic Voting System*, Universidade de Aveiro/Instituto de Engenharia Electrónica e Telemática de Aveiro, Instituto Superior de Engenharia de Lisboa/Instituto de Engenharia de Sistemas e Computadores, Instituto Superior Técnico.

[21] Kofler, R., Krimmer, R., Prosser, A., (2002), *Electronic Voting: Algorithmic and Implementation Issues*, Department Production Management, Vienna University for Business Administration and Economics.

[22] Borras, J., (2002), *Overview of the work on e-voting technical standards*, Office of e-Envoy, Cabinet Office, UK Government.

[23] Cybervote, (2002), *Report on mock-ups of architectures and overall system architecture*, CYBERVOTE:WP2:D7/V2:2001 v1.0.

[24] Hayes, B., (2003), *Conducting a Security Audit: An Introductory Overview*, http://www.securityfocus.com/infocus/1697

[25] Silva, A., Videira, C., (2001), *UML, Metodologias e Ferramentas Case*, Edições Centro Atlântico.

[26] Carroll, J., (2000), *MAKING USE scenario-based design of human-computer interactions*, The MIT Press, Cambridge, Massachusetts, London, England, p. 1-17.

[27] Gritzalis, Dimitris A., (2002), *Principles and requirements for a secure e-voting system*, Computers & Security, Vol 21, Nº 6, pp 539-556, Elsevier Science Ltd.