Título

Auditoria de sistemas de votação electrónica: uma proposta de arquitectura e protótipo de simulação

Autores

Filipe **Simões**
Sector de Matemática, Estatística e Informática, Escola Superior Agrária
do Instituto Politécnico de Castelo Branco

Pedro **Antunes**
Departamento de Informática, Faculdade de Ciências de Lisboa
Campo Grande, 1700 Lisboa, Portugal

Resumo

Foram já várias as experiências de votação eleitoral electrónica realizadas em todo o mundo. Fortalecer o processo democrático foi um dos principais objectivos que levaram a todas estas experiências, principalmente nos últimos tempos em que se tem vindo a verificar um significativo desinteresse pelo "simples" direito de voto. No entanto, impera ainda a necessidade de garantir que o processo verifica as propriedades que permitam reduzir o risco inerente a um processo desta natureza. O trabalho desenvolvido enumera essas propriedades.

A revisão bibliográfica dos Sistemas de Votação Electrónicos (SVE) existentes ajuda a um melhor entendimento dos trabalhos até aqui desenvolvidos nesta temática As comparações entre esses sistemas, permitem encontrar um padrão comum de comportamento e preocupações a considerar sobre os riscos deste tipo de sistemas.

Nenhum sistema informático pode ser aceite como de baixo risco, muito menos um SVE, se não estiver sujeito a uma auditoria de funcionamento.
A auditoria do sistema de votação aplicada a cada componente e fases de funcionamento irá proporcionar a detecção de falhas no sistema. Tais falhas, eventualmente resultantes de ataques, irão ficar registadas em "logs" e a sua prematura detecção e análise poderá vir a prevenir consequências mais negativas.

Neste artigo apresentamos um protótipo de simulação da auditoria de uma votação exercitando uma das propriedades mais importantes de um SVE (verificabilidade). No entanto este é apenas o primeiro passo para garantir uma credível auditoria a um sistema de votação electrónico.

Simões, F. and P. Antunes (2006) Auditoria De Sistemas De Votação Electrónica: Uma Proposta De Arquitectura E Protótipo De Simulação. 2º Workshop sobre Voto pela Internet, Aveiro, Portugal, October.

Introdução

Com a evolução do mundo tecnológico em que vivemos, o processo de votação eleitoral electrónico 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.

O trabalho descrito neste artigo enumera as propriedades [2] que mais directamente se relacionam com os riscos associados aos SVE e que deverão ser avaliados e mitigados em qualquer instante do decorrer do processo de votação. Com a avaliação do risco em qualquer uma das fases do processo poderemos reduzir a probabilidade de ocorrência de falhas. Caso uma falha venha mesmo a acontecer, se ela for detectada atempadamente no decorrer do processo, a sua mitigação reduzirá o seu potencial impacto no funcionamento do sistema.

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

Com este trabalho pretende-se contribuir com um estudo técnico de análise de sistemas que permita realizar o processo de auditoria de um sistema de votação electrónica, alertando a comunidade para os cenários de mau uso e requisitos de segurança que podem vir a credibilizar um sistema deste género, transmitindo o nível de confiança que todos devemos exigir.

A componente prática deste trabalho pretende apresentar 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 credível.

O protótipo construído para este trabalho monitoriza o percurso dos boletins, verificando a sua integridade e completude, procurando padrões de ataque ao sistema, identificando casos de mau uso e o extravio de um boletim.

O exemplo prático aplicado ao protótipo foca uma das propriedades principais a garantir por um sistema de votação electrónico – a verificabilidade, ou seja a garantia de que todos os votos foram correctamente contados e que não aconteceu o extravio de algum.

O protótipo construído 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.

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:

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).

Auditabilidade

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

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).

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: Presencial, PIN, Password, Certificados Digitais, Smartcard, bio-métrica.

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.

Direito de Voto

O Direito de Voto será atribuído a um eleitor sempre que ele verifique simultaneamente as propriedades de Autenticidade e Singularidade. Será sempre necessário verificar o Direito de Voto de um eleitor antes de ele poder votar.

Disponibilidade do Sistema

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

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.

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.

Integridade do Sistema

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

Integridade dos Votos

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

Invulnerabilidade

A invulnerabilidade do SVE é garantida se se verificarem as condições de Autenticidade e Singularidade.

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.

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.

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.

Rastreabilidade

O sistema deve registar permanentemente qualquer transacção ou evento significativo ocorrido no próprio sistema. Deverão existir "logs" 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.

Singularidade (Não Reutilização)

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

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 de faltas no equipamento. A troca de um bit num total de um candidato pode ser a diferença entre ganhar ou perder a eleição.

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.

Arquitecturas SVE existentes

Atsushi Fujioka, Tatsuaki Okamoto e Kazuo Ohta [3]

É um dos protocolos 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.

O protocolo FOO [4]

É um protocolo cujos componentes e funcionalidade dos mesmos se baseiam, praticamente sem alterações, no protocolo descrito anteriormente (Atsushi Fujioka, Tatsuaki Okamoto e Kazuo Ohta) e por isso nos escusamos à sua descrição.

O protocolo EVOX [5]

É um protocolo também baseado no protocolo de Atsushi Fujioka, Tatsuaki Okamoto e Kazuo Ohta, 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 de pré-votação Setup e Registration, 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, através do componente Confirmation, cada votante pode confirmar o seu voto e todas as restantes assinaturas.

Sensus - Cranor e Cytron [6]

O protocolo Sensus é um protocolo sugerido por Lorrie Cranor e Ron Cytron que vem em sequência do trabalho realizado por Fujioka, Okamoto, e Otha[7]. Inicialmente realizado para substituir a votação via correio, veio a revelar-se suficientemente flexível para permitir outros tipos de votação menos tradicionais[8].

O Sensus é um protocolo que apresenta 3 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

André Zúquete, Rui Joaquim e Paulo Ferreira [9]

O protocolo apresentado por Zúquete, Joaquim e Ferreira parte do princípio da existência de uma lista de eleitores já registados e preocupa-se 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 apostarem numa arquitectura baseada na replicação de servidores para minorar problemas de faltas e quebras de conexão entre clientes e servidores do sistema.

Propõem 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.

Robert Kofler, Robert Krimmer, Alexander Prosser [10]

É uma arquitectura 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.

Oasis Election, by John Borras [11]

O protocolo 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.

Cybervote [12]

Trata-se de um protocolo 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 "logs", o Audit and validation.

Quadro resumo dos SVE Existentes e fases do processo de votação

As fases / Protocolos	Pré-registo	Registo	Validação	Anonimização	Votação	Contagem / apresentação de resultados	Verificação
Fujioka, Okamoto e Ohta			administration		preparation e voting	counting	collecting e opening
EVOX	election commission	registrar	admin	anon	voter	counter	confirmation
Sensus		registrar	validator		pollster	tailler	
Zúquete, Joaquim e Ferreira			administrator	anonymizer	voter engine	counter	
Kofler, Krimmer e Prosser		registration	trust center		Ballot box		
Oasis	candidates	voters	voting		voting	results	audit
Cybervote	client repository	registration server	vote server		vote server	tabulation	audit and validation

Identificação do problema

Importância da auditoria do sistema

A auditoria, definida no seu conceito mais comum tem como finalidade minimizar os riscos de um sistema de informação em geral.

A auditoria a um Sistema de Informações Informático [13] [14] aplicado ao caso particular de um Sistema de Votação Electrónico, terá como finalidade:
- Garantir a segurança técnica do SVE;
- Proporcionar a sua defesa, minimizando danos e perdas;
- Manter a capacidade funcionamento e de produzir informação;

Como vimos nos protocolos estudados, os componentes de verificação e auditoria, quando existentes, concentram-se numa determinada fase, normalmente no final do processo de votação.

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 que ele cumpre as funções para as quais foi construído poderá dar-nos a garantia que as propriedades 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. Deverá recorrer-se a um exame independente de todos os registos, eventos e ocorrências ao longo do funcionamento do sistema. Em caso extremo, ao proporcionar a detecção atempada de uma falha, poderá permitir uma tomada de decisão mais eficaz mitigando o seu impacto no funcionamento normal do processo.

Solução proposta

A solução proposta por este trabalho apresenta a auditoria como um processo que corre em paralelo com o processo de votação, existindo assim a necessidade de monitorizar em permanência cada componente que integra o 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.

Protótipo de Simulação e Auditoria

O protótipo pretende simular o "percurso" de um boletim de voto e sua monitorização imediatamente após o votante ter confirmado a sua escolha (**lançamento do voto**) até chegar à fase de contagem, ou seja, passando pelas fases de **anonimização**, **depósito e contagem**.

Durante a monitorização do percurso do boletim, este protótipo tem como objectivos:

- verificar a integridade e completude do percurso percorrido pelo boletim, isto é, confirmar que o boletim passou por todas as fases e componentes do processo;
- procurar padrões de ataques ao sistema, ou seja, procurar formas de ataques ao SVE que enquadrem num padrão com denominador comum ;
- identificar casos de mau uso – as ameaças ao correcto funcionamento do sistema;
- garantir a verificabilidade do processo, mais precisamente que nenhum dos votos lançado se extraviou;

Exemplificação do funcionamento do protótipo: o extravio de um voto

O sistema deve permitir a verificação de que os votos foram correctamente contados, no final da votação e que por exemplo nenhum dos votos lançados se extraviou.

A verificabilidade é uma das propriedades mais importantes a garantir num sistema de Votação electrónico e dos protocolos analisados no capítulo anterior, apenas alguns deles, nomeadamente, Fujioka, Okamoto e Ohta, EVOX, Oásis e Cybervote incluem de alguma forma, ainda que muito pouco consistente, um esquema de verificabilidade.

Protocolo	Verificabilidade
Fujioka, Okamoto Ohta	confirmação pelos próprios
EVOX	confirmação pelos próprios
Oasis	recontagem de votos (por membros não oficiais)
Cybervote	análise de logs

A ”confirmação pelos próprios” como verificação é facilmente entendida como muito fraca;
A “recontagem de votos” incluída no protocolo “Oásis” poderia eventualmente detectar no final da votação que algum voto se extraviou, mas se efectuada por membros não oficiais não acrescenta nenhuma garantia à verificação do processo;
A “análise de logs” dependendo da altura em que é feita poderá ser um elemento com alguma importância na evolução do processo de votação, mas se tal análise apenas for efectuada no final do processo, não poderá ser considerada uma mais-valia.

Vamos exemplificar o protótipo deste trabalho com a garantia desta propriedades: Verificabilidade.

Na exemplificação deste protótipo de simulação a auditoria será efectuada por um módulo que verifica de uma fase para outra o eventual extravio de um boletim e o regista em log.

O lançamento dos votos

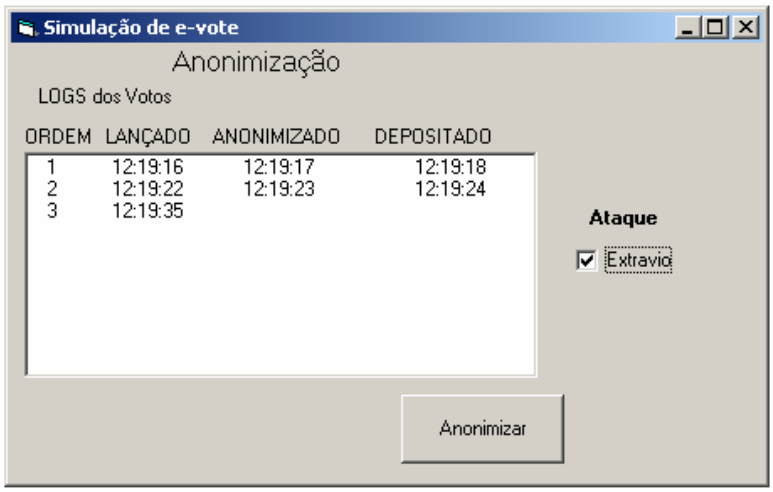
Nesta fase será feito o lançamento de um voto no processo de votação.

As fases de anonimização e depósito do voto

Nas fases de anonimização e depósito do voto será "permitido" que aconteça o extravio de um voto e sempre que tal aconteça isso ficará registado na janela de logs do protótipo. Fica também registado a hora em que cada voto foi sujeito a estas fases do processo.

O "extravio" de um voto

Permite-se o extravio de um voto em qualquer uma das fases consideradas no processo de modo a que ao passar de uma fase para outra o módulo de auditoria proceda à detecção, caso aconteça, da perda do boletim e o registe em log.



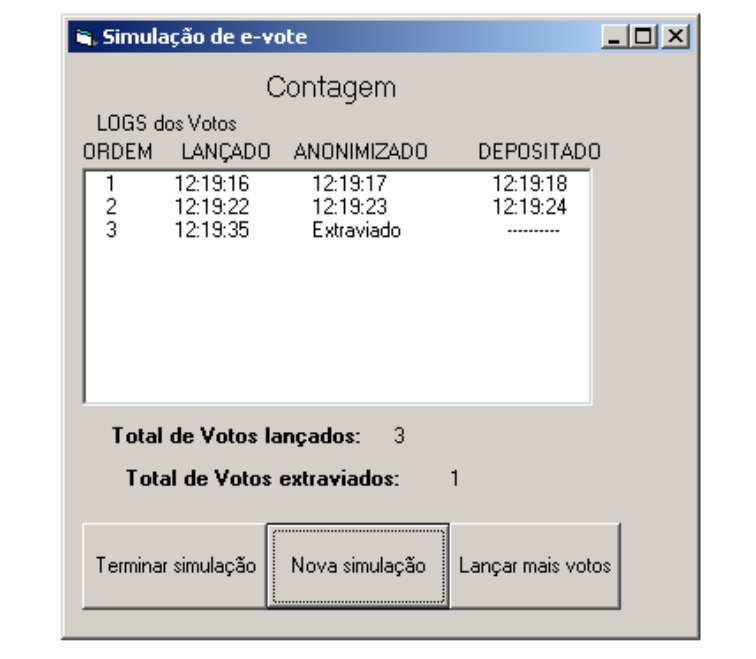
Resultados obtidos

A auditoria e logs

Neste caso optou-se por disponibilizar em tempo real os logs registados. Torna-se assim mais fácil e visual acompanhar a evolução do processo de votação e detectar qualquer extravio de boletim.

A contagem dos votos

Nesta interface, pode-se observar todos os registos de passagem dos boletins por cada uma das fases, bem como o extravio de algum dos boletins, caso tal tenha sucedido.
Para além do número de votos lançados é possível visualizar quantos votos se extraviaram.
O processo pode recomeçar do zero, ou seja sem os boletins lançados anteriormente ou pode-se continuar com o lançamento de mais votos.



Conclusões

A votação electrónica só poderá ser considerada, pelo menos por enquanto, como um processo complementar ao sistema tradicional [15], pois devem 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; como se descobre facilmente na nossa sociedade, tais condições nem sempre seriam verificadas.

No entanto, o processo de votação electrónica terá que ser um processo que transmita confiança aos eleitores. Este objectivo só poderá ser atingido com a completa auditoria a todas as fases da votação.

Com este trabalho pretende-se alertar a comunidade para os riscos associados a um SVE e para os cenários de mau uso que lhe são inerentes.

Este protótipo é apenas o primeiro passo para fomentar a auditoria do processo em todas as suas fases e assegurar que todas as propriedades exigidas são garantidas, permitindo no futuro definir regras e procedimentos de avaliação, com vista à validação e consequente credibilização das arquitecturas propostas para votação electrónico.

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", Departamento de Informática da Faculdade de Ciências de Lisboa.

[3] 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.

[4] in "http://www.cs.washington.edu/homes/mausam/evote/tsld008.htm"

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

[6] 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.

[7] 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.

[8] 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.

[9] Zúquete, A., Joaquim, R., Ferreira, P., (2004), "REVS, A Robust Electronic Voting System", UA/IEETA, ISEL/Inesc-ID, IST/Inesc-ID.

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

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

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

[13] 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.

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

[15] 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.