Audiência Pública

Mesa: *"Viabilidade técnica da expedição de cédulas físicas no processo de votação e apuração das eleições, plebiscitos e referendos, visando à possiblidade de auditoria em casos de suspeição"*.

05 de maio de 2015

Celso Souza
Especialista em Sistemas Informatizados

Fontes especialistas

- Professor Pedro Rezende ➔ UnB.
- Professor Diego Aranha ➔ UNICAMP - liderou a equipe vencedora da 2ª edição dos *Testes Públicos de Segurança* que o TSE promoveu em 2012.
- Eng. Amílcar Bruzano ➔ moderador do *Voto Eletrônico*.
- Comitê Multidisciplinar Independente (CMind) que reúne 12 (doze) especialistas.
- Sociedade Brasileira de Computação (SBC).
- Prof Ronald Rivest ➔ MIT – referência mundial e um dos inventores da assinatura digital. Ele definiu o *Princípio da Independência do Software* para eleições (urnas) eletrônicas.
- Além de outros representantes da academia e da indústria nacional e internacional.

Gerações (ou Modelos) de Urnas Eletrônicas

- 1ª geração ➔ tipo DRE (***D**irect **R**ecording **E**lectronic*)
  - Em uso apenas no Brasil.
  - A confiabilidade do resultado é 100% dependente da integridade e qualidade do software da Urna.
  - *Testes Públicos* promovidos pelo TSE demonstraram diversas fragilidades quanto a segurança e integridade do voto.
- 2ª geração ➔ VVPAT (***V**oter-**v**erified **p**aper **a**udit **t**rail*) e 3ª geração ➔ E2E (***E**nt-to-**e**nd*)
  - Princípio da Independência do Software ➔ *"Um sistema eleitoral é independente do software se uma modificação ou erro não-detectado no seu software não pode causar uma modificação ou erro indetectável no resultado da apuração ou na inviolabilidade do voto".*

Vulnerabilidades encontradas no software da Urna (1/2)

- Registro Digital do Voto (RDV)

  Possibilidade da reprodução da ordem de votação e portanto **quebra do sigilo do voto**.

  Técnicas de *embaralhamento* inadequadas ou frágeis ➔ A descoberta desta fragilidade aconteceu na 1ª hora de análise durante os *testes públicos* promovidos pelo TSE.

  O RDV é informação redundante que é apenas mais um ponto de falha e insegurança. O RDV deve ser substituído por outro método mais simples e transparente, por exemplo o ***voto impresso***.

- Verificação da integridade do software

  - O próprio software da Urna verifica a sua integridade. O que na prática garante apenas a origem, mesmo que ela contenha falhas por desconhecimento ou fraudes.

  - A verificação de integridade deve ser independente. O que não traz qualquer tipo de risco para o sistema de votação.

Vulnerabilidades encontradas no software da Urna (2/2)

- A mesma chave criptográfica para todas as Urnas
  - Todas as Urnas produzem LOGs, RDVs e BUs após a eleição. Todas as Urnas estão protegidas pela mesma chave de criptografia, um ***"segredo"*** **compartilhado** em centenas de milhares de Urnas.
- Chave de criptografia armazenada em texto claro no próprio software
  - Isso é grave e fere todos os princípios de sigilo e segurança da informação.
- Algoritmos (funções) ultrapassados
  - Uso de funções inadequadas para uso em assinatura digital *condenadas* há anos na literatura mundial.

Pontos de atenção no software da Urna

- Tamanho do software da Urna
  - O código da Urna contém milhões de linhas de código. É muito extenso.
  - Quanto maior o software maior a probabilidade de falhas e principalmente vulnerabilidades.
  - Os *testes públicos* promovidos foram curtos e não permitiram análise detalhada.
  - As vulnerabilidades encontradas até agora podem ser uma pequena parte da realidade.
  - A segurança não deve residir no segredo do código, pelo contrário, **quanto mais conhecido melhor será a garantia de qualidade e segurança**.

Exemplos de projetos Nacionais de alta tecnologia (1/2)

- Imposto de Renda via Internet
  - Conforme já dito em outras audiências públicas, a falta de autenticação no envio da Declaração é um problema. No entanto o *contribuinte* tem um copia da Declaração e não há importante motivação para fraude durante o envio da Declaração.
- ICP-Brasil
  - Modelo e regulamentação brasileira para a Certificação Digital. O modelo é público e livre. Em uso nos órgãos do Governo e praticamente em todos os projetos de segurança no Brasil, públicos ou privados.
- Nota Fiscal Eletrônica (NFE)
  - Excelente exemplo de adoção em todo o território nacional. Apesar da obrigatoriedade, todos aceitaram e usam sem restrições.

Exemplos de projetos Nacionais de alta tecnologia (2/2)

- Sistema de Pagamentos Brasileiro (SPB)
  - Talvez o melhor exemplo de projeto que adotou as recomendações de segurança da academia e da indústria. Todas as Instituições Financeiras (públicas e privadas) no Brasil adotam o SPB.
  - Está em uso desde 2002 e não há registros nem da desconfiança e nem de falhas de segurança.
- Emissão do novo Passaporte com chip eletrônico
  - O modelo é aberto e mundial. Vários países seguem o mesmo padrão, entre eles os EUA, países Europeus e Japão.
- Saúde
  - O segmento de Saúde está se organizando para adoção em larga escala de um mesmo modelo de segurança para troca de informações digitais. O maior exemplo é o Prontuário Eletrônico do Paciente (PEP). Aqui é outro caso de participação quanto as recomendações de segurança da informação.

Referências

- http://www.cic.unb.br/~rezende/sd.php
- http://www.brunazo.eng.br/voto-e/textos/comiteTSE-1.pdf
- http://pt.wikipedia.org/wiki/Comit%C3%AA_Multidisciplinar_Independente
- http://www.kas.de/wf/doc/13775-1442-5-30.pdf
- http://www.brunazo.eng.br/voto-e/index.htm
- http://en.wikipedia.org/wiki/DRE_voting_machine
- http://en.wikipedia.org/wiki/Voter-verified_paper_audit_trail
- http://en.wikipedia.org/wiki/End-to-end_auditable_voting_systems
- http://people.csail.mit.edu/rivest/voting
- http://www.bcb.gov.br/?spb