Auditoria dos Programas do TSE

Condições

- Ambiente Windows
- IDE Eclipse
- Sem anotações
- Impossibilidade de independência (Lei 9.504)
- Termo de sigilo

Resultados

- Código não facilmente compreensível
- Modificações até o último instante
- Chaves criptográficas expostas
- Inserator
- Outros (gerador ADH, internet, indireção no acesso ao código)

Chaves Criptográficas

- Chaves expostas em código
- Ataque de Princeton
- Vulnerabilidade já relatada (testes 2012)

O Inserator – o que é

- Programa do projeto SIS
- Independente (apresenta entrada por 'main')
- Faz uso da classe MiniCA.cpp
- Gera script SQL para inserção de chaves em BD
- Usado até 2004 para certificação

O Inserator – como funciona

- Chaves via linha de comando
- Cifra chaves com senha da MiniCA.cpp
- Insere chaves em script SQL
- Salva script

O Inserator – por que vulnerabiliza

- Senha da MiniCA.cpp: fixa e visível em código
- Dispersão das chaves
- Ainda na base sem propósito claro
- Indistinguível de *backdoor*

Conclusões

- Pontos de vulnerabilidade no código
- Alguns alertas ignorados
- Código legado mantido sem cuidado e sem propósito claro
- Respostas da STI não compreensíveis