20/12/2017

Mais uma vez bem sucedido ao quebrar a segurança da urna eletrônica, o professor de Computação Diego Aranha e a equipe que coordenou durante os testes promovidos pelo Tribunal Superior Eleitoral explicam que conseguiram inserir um ‘código intruso’ e modificar dados, sendo capazes de alterar a apresentação e número de um suposto candidato.

“O principal sucesso da equipe foi detectar e utilizar uma sequência de vulnerabilidades para injetar código de nossa autoria nos programas da urna eletrônica antes do processo de carga, quando o software é instalado. Fizemos o equivalente a um ‘jailbreak’ de um telefone celular moderno, só que na urna eletrônica”, explicou o professor da Unicamp sobre a segunda investida sobre o equipamento.

Assim como em 2012, quando liderou a equipe que quebrou o sigilo da urna pela primeira vez, o ataque levou o TSE a fazer alterações no sistema. Os detalhes dos ataques à urna, no entanto, só puderam ser divulgados depois da abertura do relatório final dos testes e do fim do período de sigilo exigido pela Justiça Eleitoral. Além do professor Diego, o time foi composto por Pedro Barbosa (UFCG), Thiago Carneiro (Hekima), Caio Lüders **(UFPE)** e Paulo Matias (UFSCar).

Como explicam, durante a semana de testes de segurança foi possível manipular o registro cronológico de eventos gerado pela urna, executar um programa que lia comandos do teclado e imprimia na tela e executar outro programa que zerava a chave criptográfica que protegia o Registro Digital do Voto e mesmo injetar código para alterar uma mensagem na tela de seleção do candidato, além de impedir o armazenamento dos votos na memória da urna.

O Registro Digital do Voto, ou simplesmente RDV, já tinha sido manipulado quando da primeira quebra de segurança, em 2012, quando a equipe do professor Diego teve sucesso em desembaralhar os votos e recuperar a ordem dos eleitores de uma eleição simulada, provando ser possível quebrar o sigilo do voto.

“Conseguimos zerar a chave criptográfica, efetivamente usando uma chave de nossa escolha. Isso permitiu decifrar o RDV entre votos consecutivos, de forma que a diferença entre os arquivos quebra o sigilo de um voto sensível depositado por um eleitor importante. Esse ataque é um tanto difícil de executar na prática porque é necessário adulterar o flash de carga e contar com um mesário malicioso para interromper a votação e fazer cópias dos arquivos intermediários, mas serviu para mostrar o impacto no sigilo de se executar código arbitrário no equipamento”, explica o professor.

Ao modificar o software da urna, a experiência abriu caminho para alterar qualquer posição na memória do equipamento e eventualmente até interferir com a contagem correta dos votos. “Para mudar qualquer coisa, era apenas uma questão de tempo até descobrir o endereço certo a ser alterado e o que inserir em seu lugar”, afirma. Para demonstrar o feito, o grupo mudou a tela de um candidato, seu vice e número por outro – no caso, pela chapa 99, de Darth Vader.

Segundo o grupo, combinado com os resultados do grupo de peritos da Polícia Federal que conseguiu extrair a chave de cifração durante a inicialização do sistema, o ataque poderia ser montado de posse apenas de um cartão de carga, vazado por um funcionário malicioso para realizar as adulterações antes de instalar software nas urnas.

Link da Matéria