Wilfredo Pacheco: Certificação digital brasileira é vulnerável

Pesquisadores conseguiram obter dados encriptados por dispositivos de segurança de informação que utilizam a especificação PKCS #1 v1.5, utilizada em dispositivos como o RSA SecurID 800 e, também, na encriptação de certificação digital da Estrutura de Chaves Públicas Brasileira (é possível consultar a especificação [aqui](#)).

A vulnerabilidade foi desenvolvida por um grupo de cientistas da computação que se intitulam Team Prosecco, e apresentarão sua tese na conferência Crypto 2012, a acontecer em agosto.

A característica mais notável dessa solução é sua capacidade de extrair informações em aproximadamente 10 minutos, ao invés de adotar um procedimento de tentativa-e-erro que, geralmente, duram horas.

Romain Bardou, Riccardo Focardi, Yusuke Kawamoto, Lorenzo Simionato, Graham Steel e Joe-Kai disseram que o ataque funciona contra uma vasta variedade de dispositivos que protegem o acesso a redes de computadores ou que encriptam emails, incluindo cartões de identificação eletrônica, tokens USB e smartcards, tecnologias que são utilizadas pelo governo de muitos países.

Descobrimos, também, que a forma de encriptação vulnerável, a PKCS #1 v1.5, também *é adotada pela Estrutura de Chaves Públicas Brasileiras*, conforme se confere no manual fornecido pela ICP Brasil ([clique aqui para ler](#)).

O ataque se baseia na exploração de função de importação de chaves encriptadas de uma variedade de dispositivos criptográficos. O texto cifrado é submetido a centenas de modificações para gradualmente produzir pistas da informação legível, em uma técnica apelidada de "*padding oracle attack*". Esta técnica é um refinamento de outra vulnerabilidade conhecida como Bleichenbacher.

Esta última vulnerabilidade foi desenvolvida originalmente pelo criptógrafo suíço Ph.D. Daniel Bleichenbacher, ao tempo em que era pesquisador da Bell Laboratories, que fez, em 1998, uma demonstração prática de ataque à encriptação RSA (empresa que desenvolveu o padrão de encriptação comprometido), utilizando-se da função de encriptação PKCS# v1.

O mesmo pesquisador, na Conferência Internacional de Criptologia (Crypto) de 2006, demonstrou com êxito alguns ataques simples contra assinaturas de validação RSA, utilizando-se de técnicas básicas de criptografia. Descobriu-se, a partir dessa demonstração, que a implementação de encriptação OpenSSL, presente em vários navegadores, era vulnerável ao ataque à época.

Em resposta, a RSA Security Inc., empresa de segurança de informação que desenvolveu os padrões PKCS#1 e PKCS#11, relata que esta vulnerabilidade não expõe a chave privada contida no *token* afetado, e que já não está presente no padrão PKCS#1 v2.0.

Em que pese não sejam comprometidas as chaves privadas, é possível obter, através da vulnerabilidade, as informações criptografadas através da chave privada, desde que se tenha acesso à referida função.

Ainda, é importante debater esta vulnerabilidade no âmbito da Estrutura de Chaves Públicas Brasileira (ICP-Brasil) para que esta modifique os requisitos do manual de condutas técnicas para homologação de softwares criptográficos.

Basta que o padrão exigido seja modificado para PKCS#1 v2.0, e a presente vulnerabilidade não afetará as informações cifradas pelos certificados digitais brasileiros.

A pesquisa realizada pelo Team Prosecco poderá ser consultada, em inglês, no endereço <http://hal.inria.fr/docs/00/70/47/90/PDF/RR-7944.pdf>.

Date Created

13/07/2012