UNIVERSIDADE FEDERAL DE PERNAMBUCO

GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

CENTRO DE INFORMÁTICA

2010.2

MECANISMOS DE AUTENTICAÇÃO EM REDES IEEE 802.11

PROPOSTA DE TRABALHO DE GRADUAÇÃO

Aluno Eduardo Ferreira de Souza efs@cin.ufpe.br
Orientador Paulo André da Silva Gonçalves pasg@cin.ufpe.br

18 de Agosto de 2010

Sumário

1. Contexto

O crescimento na utilização de tecnologias de comunicação sem fio entre dispositivos tem permitido aos usuários grande praticidade e mobilidade. Atualmente a principal tecnologia de rede sem fio utilizada para acesso à Internet e criação de redes locais é a IEEE 802.11 [IEEE Standard 802.11 1999], conhecida como *Wi-Fi*. Nas redes IEEE 802.11, o tráfego de dados precisa ser protegido através de protocolos de segurança, que têm por objetivo prover autenticação dos usuários genuínos, certificar que os dados cheguem íntegros ao receptor e garantir confidência dos dados que trafegam na rede. Os principais protocolos de segurança para tais redes são: WEP [IEEE Standard 802.11 1999], WPA [Wi-Fi Alliance 2003], IEEE 802.11i [IEEE Standard 802.11i 2004] e a emenda IEEE 802.11w [IEEE Standard 802.11w 2009].

Apesar dos objetivos de garantia de segurança aos clientes da rede, os protocolos de proteção às redes IEEE 802.11 ainda apresentam significativas vulnerabilidades. Os problemas, em geral, são derivados do meio não guiado e sem controle por onde trafegam as informações. Este tipo de propagação de informações se mostra inerentemente inseguro, visto que os dados podem ser capturados por dispositivos maliciosos. A seguir são brevemente descritos os protocolos de segurança para redes IEEE 802.11 e apresenta suas vulnerabilidades.

Protocolos de Segurança

Wired Equivalent Privacy (WEP): Primeiro padrão desenvolvido para prover segurança em redes IEEE 802.11. Este padrão possui diversas vulnerabilidades e atualmente é considerado inseguro [Tews 2007, Tews et al. 2007].

Wi-Fi Protected Access (WPA): Protocolo baseado num draft do padrão IEEE 802.11i, criado para corrigir as vulnerabilidades encontradas no WEP. O WPA possui vulnerabilidades em seus mecanismos de integridade e de autenticação [Ohigashi and Morii 2009, Fogie 2005].

IEEE 802.11i (ou WPA2): Possui significativas semelhanças com WPA, visto que o WPA foi desenvolvido com base em uma versão preliminar do IEEE 802.11i. Os principais avanços estão nos mecanismos de integridade e confidência dos dados. Apesar de significativamente seguro, este padrão possui vulnerabilidades na etapa de autenticação [Fogie 2005], assim como o WPA.

IEEE 802.11w: É uma emenda aos protocolos WPA e IEEE 802.11i e tem como objetivo corrigir as vulnerabilidades encontradas nos pacotes de gerenciamento das redes IEEE 802.11. Apesar de ser uma emenda à etapa de autenticação, tal padrão possui vulnerabilidades já exploradas para realização de ataques [Fogie 2005].

2. Objetivo

O objetivo principal deste trabalho é desenvolver uma análise aprofundada dos protocolos de **segurança de redes IEEE 802.11**. Será dado foco aos **mecanismos de autenticação** existentes em tais protocolos, analisando suas limitações, vulnerabilidades e problemas de eficiência. Com base em tais estudos, este trabalho terá por objetivo desenvolver novas técnicas de autenticação que permitam aumentar o grau de segurança e a eficiência dos mecanismos utilizados até então. A proposta do trabalho será implementada e avaliada, comparando-a com as técnicas utilizadas atualmente.

3. Cronograma

	Mês															
Atividade	Agosto				Setembro				Outubro				Novembro			
Pesquisa do Estado da Arte	X	X	X	X	X											
Testes de Segurança nos Protocolos				X	X	X	X	X								
Proposição de um Novo Mecanismo de Segurança						X	X	X	X	X						
Implementação da Proposta										X	X	X	X			
Avaliação da Proposta												X	X			
Elaboração do Relatório							X	X	X	X	X	X	X	X	X	X
Elaboração da Apresentação															X	X

4. Referências

Fogie, S. (2005). Cracking Wi-Fi Protected Access (WPA), Part 2. *http://www.fermentas.com/techinfo/nucleicacids/maplambda.htm*.

IEEE Standard 802.11 (1999). IEEE Standards for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

IEEE Standard 802.11i (2004). IEEE Standard for Information Technology – Telecommunications and Information Exchange between System – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 6: Medium Access Control (MAC) Security Enhancements Interpretation.

IEEE Standard 802.11w (2009). IEEE Standard for Information Technology – Telecommunications and Information Exchange between System – Local and Metropolitan area networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 4: Protected Management Frames.

Ohigashi, T. and Morii, M. (2009). A Practical Message Falsification Attack on WPA. *In Procedings of Joint Workshop on Information Security, Cryptography and Information Security Conference System*.

Tews, E. (2007). Attacks on the WEP Protocol. *Cryptology ePrint Archive*, Report 2007/471.

Tews, E., Weinmann, R.-P., and Pyshkin, A. (2007). Breaking 104 Bit WEP in Less Than 60 Seconds. *Lecture Notes in Computer Science - Information Security Applications*, (4867):188–202.

Wi-Fi Alliance (2003). Wi-Fi Protected Access: Strong, Standards-based, Interoperable Security for Today's Wi-Fi Networks.

5. Possíveis Avaliadores

Carlos André Guimarães Ferraz

6. Assinaturas

Paulo André da Silva Gonçalves

Orientador

Eduardo Ferreira de Souza

Aluno