Universidade Federal de Pernambuco

Graduação em Engenharia da Computação
Centro de Informática

2 0 1 0 . 1

Uma Análise da Segurança de Sistemas RFID

PROPOSTA DE TRABALHO DE GRADUAÇÃO

Aluno: Eduardo Henrique de Carvalho Franklin (ehcf@cin.ufpe.br)

Orientador: Paulo André da Silva Gonçalves (pasg@cin.ufpe.br)

Recife, 11 de março de 2010

ÍNDICE

1. Contexto

Os sistemas de comunicação por radiofreqüência, conhecidos como RFID, têm por objetivo realizar a identificação inequívoca de objetos ou pessoas de forma automática, através de consultas a etiquetas eletrônicas. Além disso, tais sistemas são capazes de armazenar e recuperar informações dos itens identificados. Nos últimos anos, a tecnologia RFID vem conquistando o mercado [4], sendo aplicada em supermercados, livrarias, automóveis, animais e diversas outras áreas.

A segurança de sistemas RFID ainda é uma questão acadêmica em aberto. O desafio consiste em conciliar a limitação do hardware das etiquetas e a confidencialidade das informações por elas armazenadas. O processo de consulta do conteúdo das etiquetas constitui um alvo potencial para diversos tipos de ataques. Outros ataques são direcionados aos chamados protocolos anti-colisão, responsáveis por ordenar a consulta de um conjunto de etiquetas, para que uma delas não interfira nas demais. Além disso, até mesmo as próprias etiquetas do sistema podem conter dados maliciosos [3], consistindo em ameaças ao sistema.

O amadurecimento da segurança de sistemas RFID é fundamental para que essa tecnologia seja aplicada de forma confiável.

2. Objetivos

O objetivo deste Trabalho de Graduação é realizar uma análise da segurança dos algoritmos RFID destinados à consulta de etiquetas, bem como daqueles que implementam protocolos anti-colisão. Além disso, será proposta uma nova modalidade de ataque capaz de explorar algoritmos anti-colisão e realizar a clonagem de uma etiqueta honesta.

3. Cronograma

O cronograma do Trabalho de Graduação é resumido pela tabela abaixo.

	Mês																				
Atividade	Dez/2009				Jan/2010				Fev/2010				Mar/2010				Abr/2010				
Levantamento Bibliográfico																					
Análise da Segurança de Algoritmos de Consulta																					
Análise da Segurança de Algoritmos Anti-Colisão																					
Elaboração de relatório																					
Elaboração de apresentação																					

4. Referências Bibliográficas

[1]Juels, A. **RFID Security and Privacy: A Research Survey**. IEEE Journal on Selected Areas in Communication, Fevereiro, 2006.

[2] Juels, A. **Minimalist Criptography for Low-Cost RFID Tags.** Proc. Fourth Int'l Conf. Computational Intelligence and Security (CIS'06), Novembro, 2006

[3] Rieback, Melanie R.; Crispo, Bruno; Tanenbaum, Andrew **Is Your Cat Infected with a Computer Virus?** Proc. Fourth Annual IEEE Int'l Conf. Pervasive Computing and Communications (PerComp'06), Março, 2006.

[4] Want, R. **The Magic of RFID**. ACM Queue, 2004

5. Assinaturas

Paulo André da Silva Gonçalves

Orientador

Eduardo Henrique de Carvalho Franklin

Aluno