
# Module 37

# Bluetooth Hacking

# Lab 37-01

Objective:

Security Overview of Bluetooth whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 37**
- Open the **Security Overview of Bluetooth.pdf** and read the content

Security Overview of Bluetooth

Dave Singelée, Bart Preneel

COSIC Internal Report

June, 2004

**Abstract**

In this paper, we give a short overview of the security architecture of Bluetooth. We will especially focus on the key exchange protocol in Bluetooth. This is the most important security critical part of the security architecture. Unfortunately, there are a lot of security flaws in the Bluetooth standard. Some are rather theoretical, but most of the problems can be exploited by an attacker. An extensive overview of the security flaws in Bluetooth will be given in this paper. Some of these security problems, e.g. the Bluesnarf attack, were only discovered very recently.

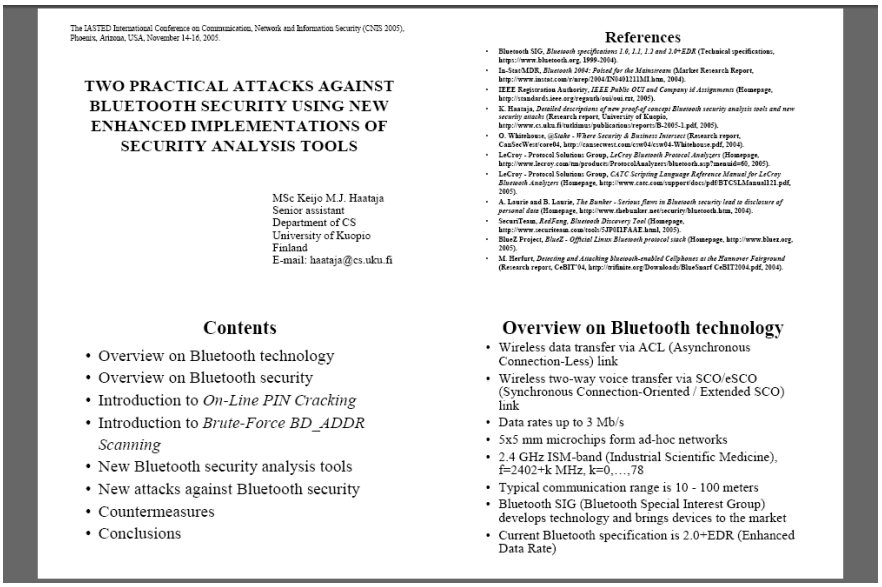
1 Introduction

# Lab 37-02

Objective:

Bluetooth Security Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 37**
- Open the **BTKeylogging attack and countermeasures.pdf** and read the content



The IASTED International Conference on Communication, Network and Information Security (CNIS 2005), Phoenix, Arizona, USA, November 14-16, 2005.

**TWO PRACTICAL ATTACKS AGAINST BLUETOOTH SECURITY USING NEW ENHANCED IMPLEMENTATIONS OF SECURITY ANALYSIS TOOLS**

MSc Keijo M.J. Haataja
Senior assistant
Department of CS
University of Kuopio
Finland
E-mail: haataja@cs.uku.fi

**References**


- Bluetooth SIG, *Bluetooth specifications 1.0, 1.1, 1.2 and 2.0+EDR* (Technical specifications, https://www.bluetooth.org, 1999-2004).
- In-StatMDR, *Bluetooth 2004: Poised for the Mainstream* (Market Research Report, http://www.instat.com/wireap/2004/IN0402113MI.htm, 2004).
- IEEE Registration Authority, *IEEE Public OUI and Company id Assignments* (Homepage, http://standards.ieee.org/regauth/oui/oui.txt, 2005).
- K. Haataja, *Detailed descriptions of new proof-of-concept Bluetooth security analysis tools and new security attacks* (Research report, University of Kuopio, http://www.cs.uku.fi/turhinen/publication/reports/B-2005-1.pdf, 2005).
- O. Whitehouse, *@Stake - Where Security & Business Intersect* (Research report, CanSecWest/core04, http://cansecwest.com/csw04/csw04-Whitehouse.pdf, 2004).
- LeCroy - Protocol Solutions Group, *LeCroy Bluetooth Protocol Analyzers* (Homepage, http://www.lecroy.com/tm/products/ProtocolAnalyzers/bluetooth.asp?menuid=95, 2005).
- LeCroy - Protocol Solutions Group, *CATC Scripting Language Reference Manual for LeCroy Bluetooth Analyzers* (Homepage, http://www.catc.com/support/docs/pdf/BTCSLManual121.pdf, 2005).
- A. Laurie and B. Laurie, *The Bunker - Serious flaws in Bluetooth security lead to disclosure of personal data* (Homepage, http://www.thebunker.net/security/bluetooth.htm, 2004).
- SecuriTeam, *RedFang, Bluetooth Discovery Tool* (Homepage, http://www.securiteam.com/tools/5JP01IFAAE.html, 2005).
- BlueZ Project, *BlueZ - Official Linux Bluetooth protocol stack* (Homepage, http://www.bluez.org, 2005).
- M. Herfurt, *Detecting and Attacking bluetooth-enabled Cellphones at the Hannover Fairground* (Research report, CeBIT'04, http://trifinite.org/Downloads/BlueSnarf CeBIT2004.pdf, 2004).


**Contents**

- Overview on Bluetooth technology
- Overview on Bluetooth security
- Introduction to *On-Line PIN Cracking*
- Introduction to *Brute-Force BD_ADDR Scanning*
- New Bluetooth security analysis tools
- New attacks against Bluetooth security
- Countermeasures
- Conclusions

**Overview on Bluetooth technology**

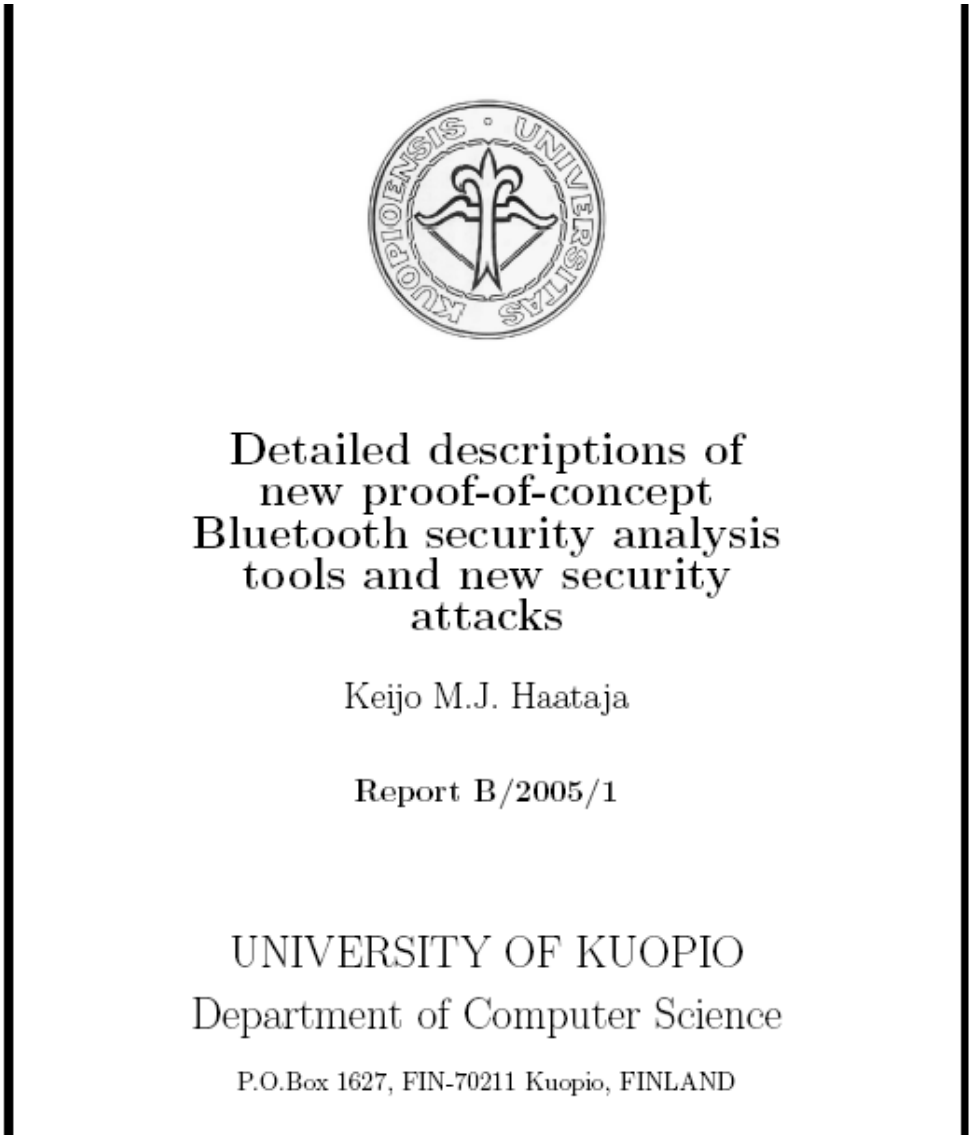
- Wireless data transfer via ACL (Asynchronous Connection-Less) link
- Wireless two-way voice transfer via SCO/eSCO (Synchronous Connection-Oriented / Extended SCO) link
- Data rates up to 3 Mb/s
- 5x5 mm microchips form ad-hoc networks
- 2.4 GHz ISM-band (Industrial Scientific Medicine), f=2402+k MHz, k=0, …,78
- Typical communication range is 10 - 100 meters
- Bluetooth SIG (Bluetooth Special Interest Group) develops technology and brings devices to the market
- Current Bluetooth specification is 2.0+EDR (Enhanced Data Rate)

## Lab 37-03

Objective:

Bluetooth Security Analysis Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 37**
- Open the **BTVoiceBugging attack.pdf** and read the content



Detailed descriptions of new proof-of-concept Bluetooth security analysis tools and new security attacks

Keijo M.J. Haataja

Report B/2005/1

UNIVERSITY OF KUOPIO

Department of Computer Science

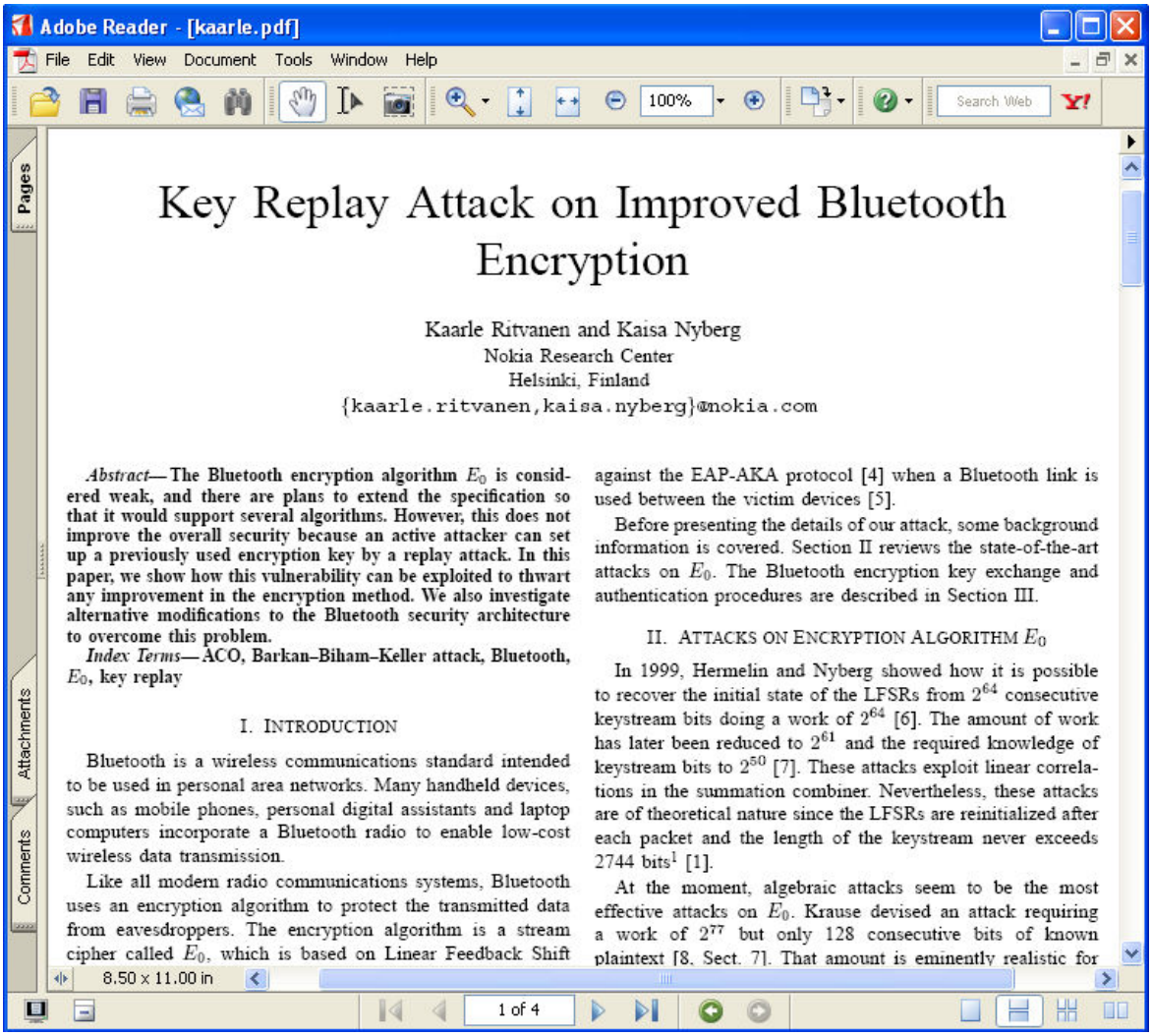
P.O.Box 1627, FIN-70211 Kuopio, FINLAND

## Lab 37-04

Objective:

Bluetooth Replay Attack Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 37**
- Open the **kaarle.pdf** and read the content




# Module 38

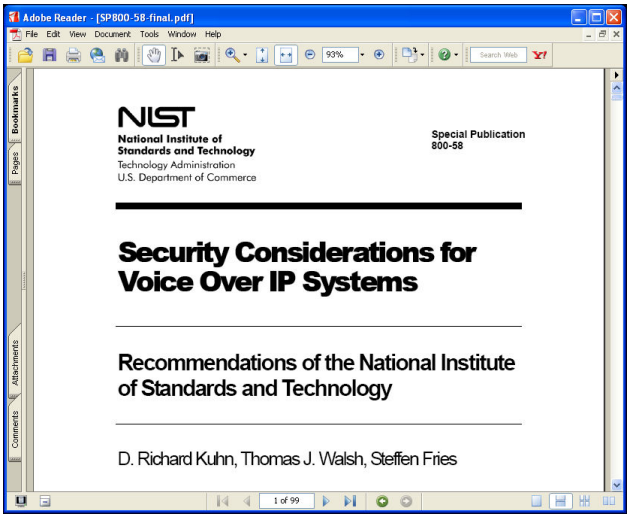
# VoIP Hacking

# Lab 38-01

Objective:

VoIP Security Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 38**
- Open the **SP800-58-final.pdf** and read the content

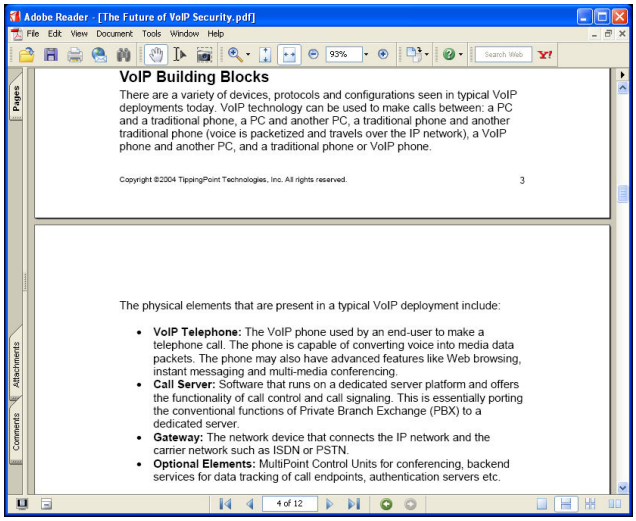


# Lab 38-02

Objective:

Future of VoIP Security Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 38**
- Open **The Future of VoIP Security.pdf** and read the content

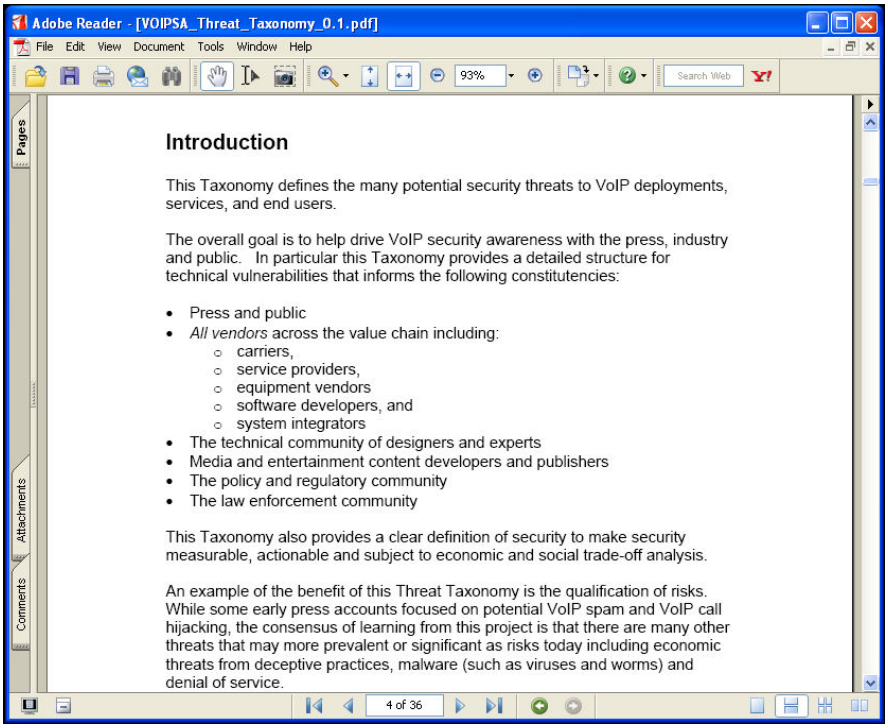


# Lab 38-03

Objective:

VoIP Threat Taxonomy Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 38**
- Open the **VOIPSA_Threat_Taxonomy_0.1.pdf** and read the content

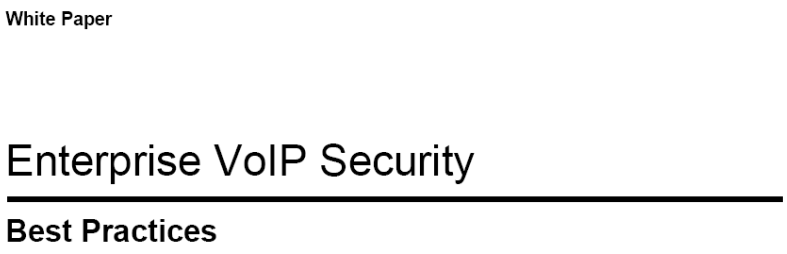


## Lab 38-04

Objective:

Enterprise VoIP Security Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 38**
- Open the **Enterprise VoIP Security.pdf** and read the content


White Paper

Enterprise VoIP Security

Best Practices


# Module 39

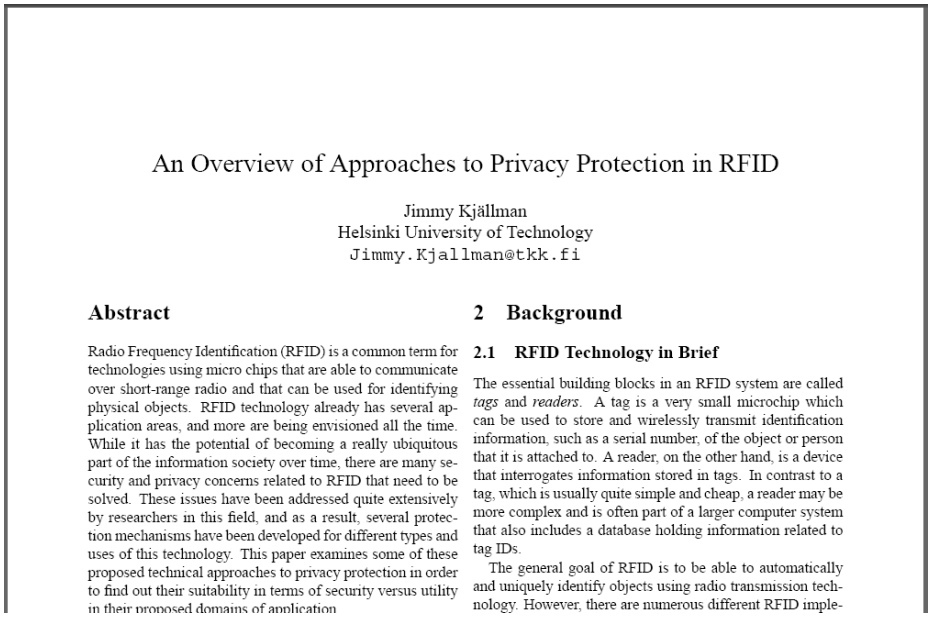
## RFID Hacking

# Lab 39-01

Objective:

Enterprise VoIP Security Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 39**
- Open the **Privacy Protection in RFID.pdf** and read the content



An Overview of Approaches to Privacy Protection in RFID

Jimmy Kjällman
Helsinki University of Technology
Jimmy.Kjallman@tkk.fi

**Abstract**

Radio Frequency Identification (RFID) is a common term for technologies using micro chips that are able to communicate over short-range radio and that can be used for identifying physical objects. RFID technology already has several application areas, and more are being envisioned all the time. While it has the potential of becoming a really ubiquitous part of the information society over time, there are many security and privacy concerns related to RFID that need to be solved. These issues have been addressed quite extensively by researchers in this field, and as a result, several protection mechanisms have been developed for different types and uses of this technology. This paper examines some of these proposed technical approaches to privacy protection in order to find out their suitability in terms of security versus utility in their proposed domains of application

**2 Background**

**2.1 RFID Technology in Brief**

The essential building blocks in an RFID system are called *tags* and *readers*. A tag is a very small microchip which can be used to store and wirelessly transmit identification information, such as a serial number, of the object or person that it is attached to. A reader, on the other hand, is a device that interrogates information stored in tags. In contrast to a tag, which is usually quite simple and cheap, a reader may be more complex and is often part of a larger computer system that also includes a database holding information related to tag IDs.

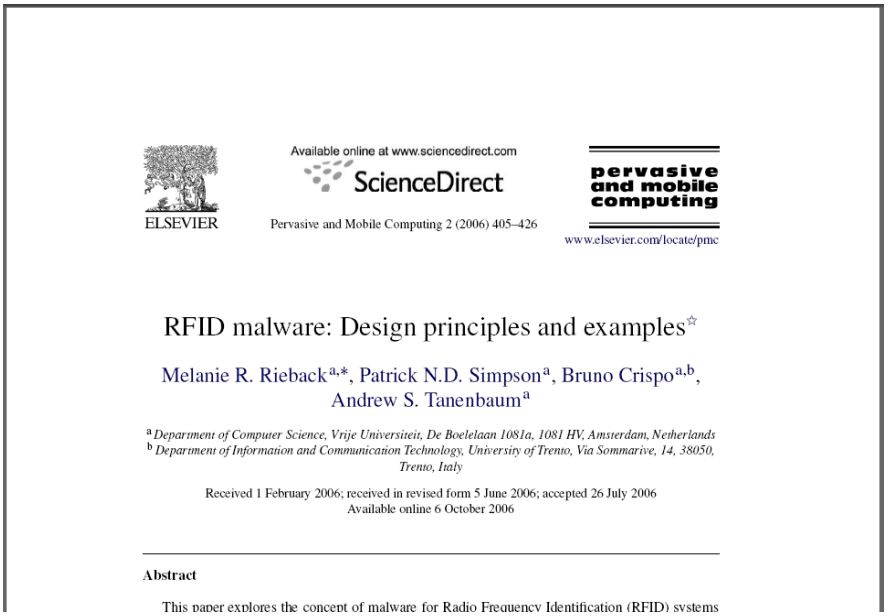
The general goal of RFID is to be able to automatically and uniquely identify objects using radio transmission technology. However, there are numerous different RFID imple-

## Lab 39-02

Objective:

RFID malware Design principles Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 39**
- Open the **RFID malware Design principles and examples.pdf** and read the content



ELSEVIER

Available online at www.sciencedirect.com
ScienceDirect
Pervasive and Mobile Computing 2 (2006) 405–426

pervasive and mobile computing
www.elsevier.com/locate/pmc

RFID malware: Design principles and examples☆

Melanie R. Rieback[a,*], Patrick N.D. Simpson[a], Bruno Crispo[a,b], Andrew S. Tanenbaum[a]

[a] *Department of Computer Science, Vrije Universiteit, De Boelelaan 1081a, 1081 HV, Amsterdam, Netherlands*
[b] *Department of Information and Communication Technology, University of Trento, Via Sommarive, 14, 38050, Trento, Italy*

Received 1 February 2006; received in revised form 5 June 2006; accepted 26 July 2006
Available online 6 October 2006

**Abstract**

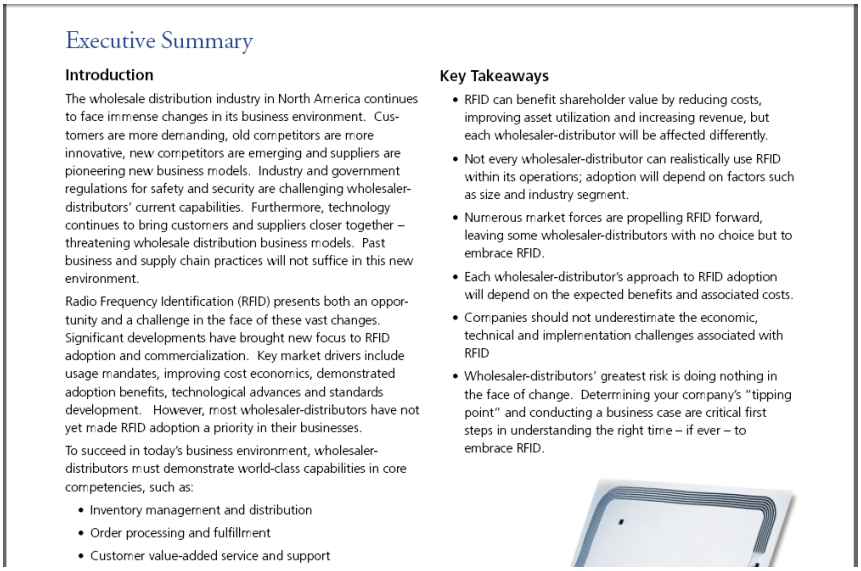
This paper explores the concept of malware for Radio Frequency Identification (RFID) systems

# Lab 39-03

Objective:

Understanding RFID Challenges and Risks Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 39**
- Open the **Understanding RFID Challenges and Risks.pdf** and read the content



## Executive Summary

**Introduction**

The wholesale distribution industry in North America continues to face immense changes in its business environment. Customers are more demanding, old competitors are more innovative, new competitors are emerging and suppliers are pioneering new business models. Industry and government regulations for safety and security are challenging wholesaler-distributors' current capabilities. Furthermore, technology continues to bring customers and suppliers closer together – threatening wholesale distribution business models. Past business and supply chain practices will not suffice in this new environment.

Radio Frequency Identification (RFID) presents both an opportunity and a challenge in the face of these vast changes. Significant developments have brought new focus to RFID adoption and commercialization. Key market drivers include usage mandates, improving cost economics, demonstrated adoption benefits, technological advances and standards development. However, most wholesaler-distributors have not yet made RFID adoption a priority in their businesses.

To succeed in today's business environment, wholesaler-distributors must demonstrate world-class capabilities in core competencies, such as:

- Inventory management and distribution
- Order processing and fulfillment
- Customer value-added service and support

**Key Takeaways**

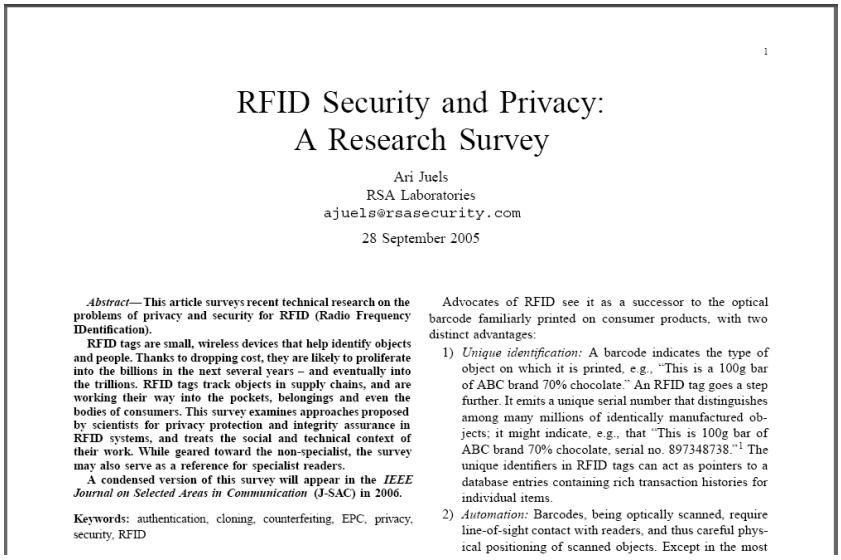
- RFID can benefit shareholder value by reducing costs, improving asset utilization and increasing revenue, but each wholesaler-distributor will be affected differently.
- Not every wholesaler-distributor can realistically use RFID within its operations; adoption will depend on factors such as size and industry segment.
- Numerous market forces are propelling RFID forward, leaving some wholesaler-distributors with no choice but to embrace RFID.
- Each wholesaler-distributor's approach to RFID adoption will depend on the expected benefits and associated costs.
- Companies should not underestimate the economic, technical and implementation challenges associated with RFID
- Wholesaler-distributors' greatest risk is doing nothing in the face of change. Determining your company's "tipping point" and conducting a business case are critical first steps in understanding the right time – if ever – to embrace RFID.

# Lab 39-04

Objective:

RFID Security and Privacy Whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 39**
- Open the **RFID Security and Privacy.pdf** and read the content



1

RFID Security and Privacy:
A Research Survey

Ari Juels
RSA Laboratories
ajuels@rsasecurity.com

28 September 2005

*Abstract*— **This article surveys recent technical research on the problems of privacy and security for RFID (Radio Frequency IDentification).**

**RFID tags are small, wireless devices that help identify objects and people. Thanks to dropping cost, they are likely to proliferate into the billions in the next several years – and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings and even the bodies of consumers. This survey examines approaches proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context of their work. While geared toward the non-specialist, the survey may also serve as a reference for specialist readers.**

**A condensed version of this survey will appear in the *IEEE Journal on Selected Areas in Communication* (J-SAC) in 2006.**

**Keywords:** authentication, cloning, counterfeiting, EPC, privacy, security, RFID

Advocates of RFID see it as a successor to the optical barcode familiarly printed on consumer products, with two distinct advantages:

1) *Unique identification:* A barcode indicates the type of object on which it is printed, e.g., "This is a 100g bar of ABC brand 70% chocolate." An RFID tag goes a step further. It emits a unique serial number that distinguishes among many millions of identically manufactured objects; it might indicate, e.g., that "This is 100g bar of ABC brand 70% chocolate, serial no. 897348738."[1] The unique identifiers in RFID tags can act as pointers to a database entries containing rich transaction histories for individual items.
2) *Automation:* Barcodes, being optically scanned, require line-of-sight contact with readers, and thus careful physical positioning of scanned objects. Except in the most


# Module 40

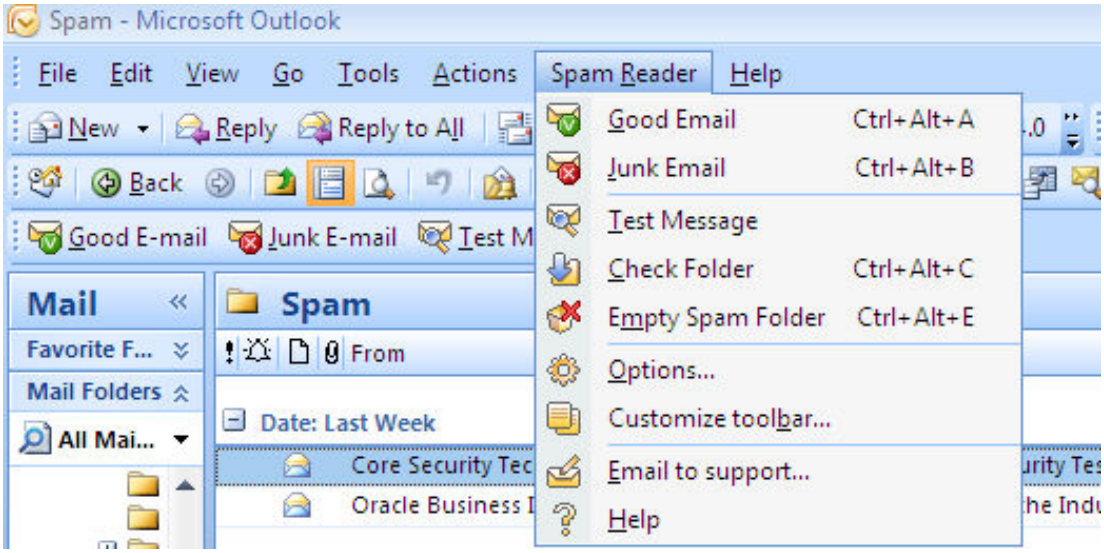
## Spamming

## Lab 40-01

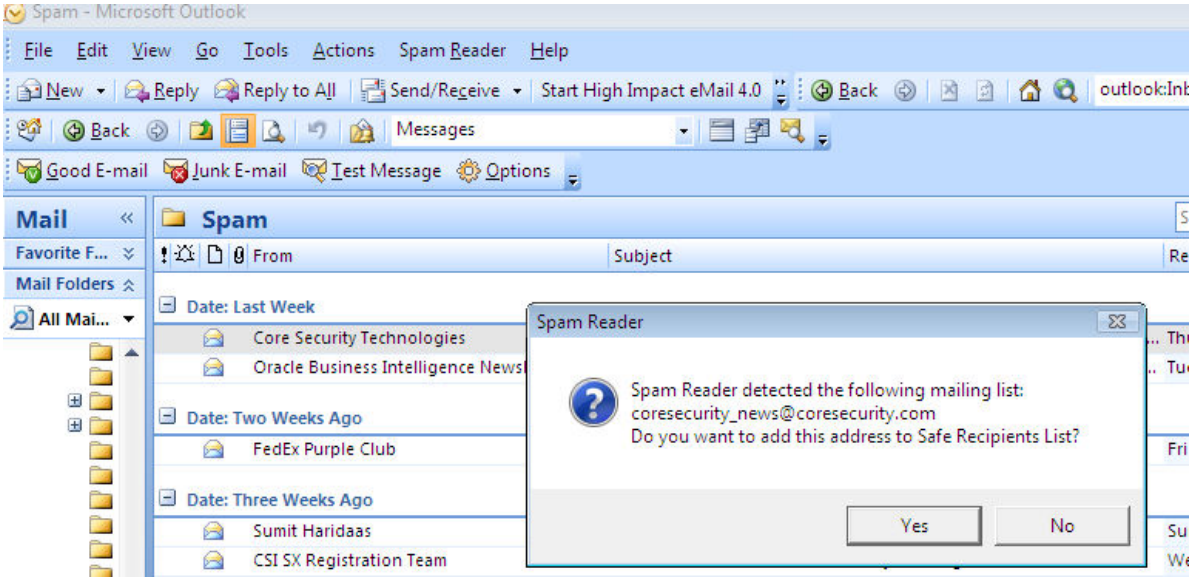
Objective:

Use **Spam Reader** to extend Outlook functionality with a Bayesian spam filter

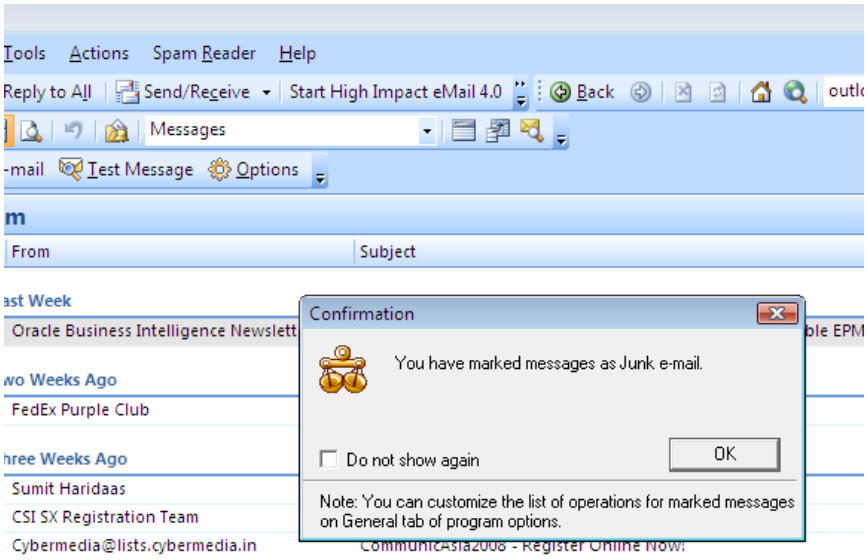
- In the **CEHv6 Labs CD-Rom,** navigate to **Module 40**
- Install and launch **Spam Reader**




- Select the email which you want to classify as **Good.** Go to Spam Reader menu and click **Good Email** to ensure the email is not caught in the Spam Box. Click **Yes** to add it to safe list



- Select the email which you want to classify as **Junk E-Mail**. Click **OK** to classify the email as Junk.



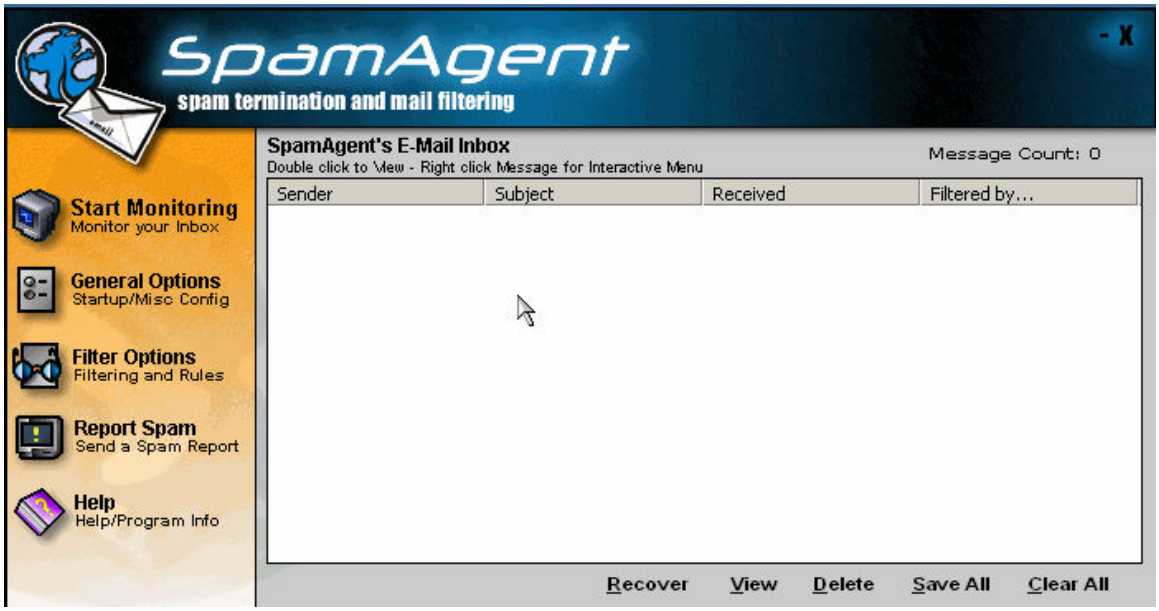

- Explore other options of the tool

## Lab 40-02

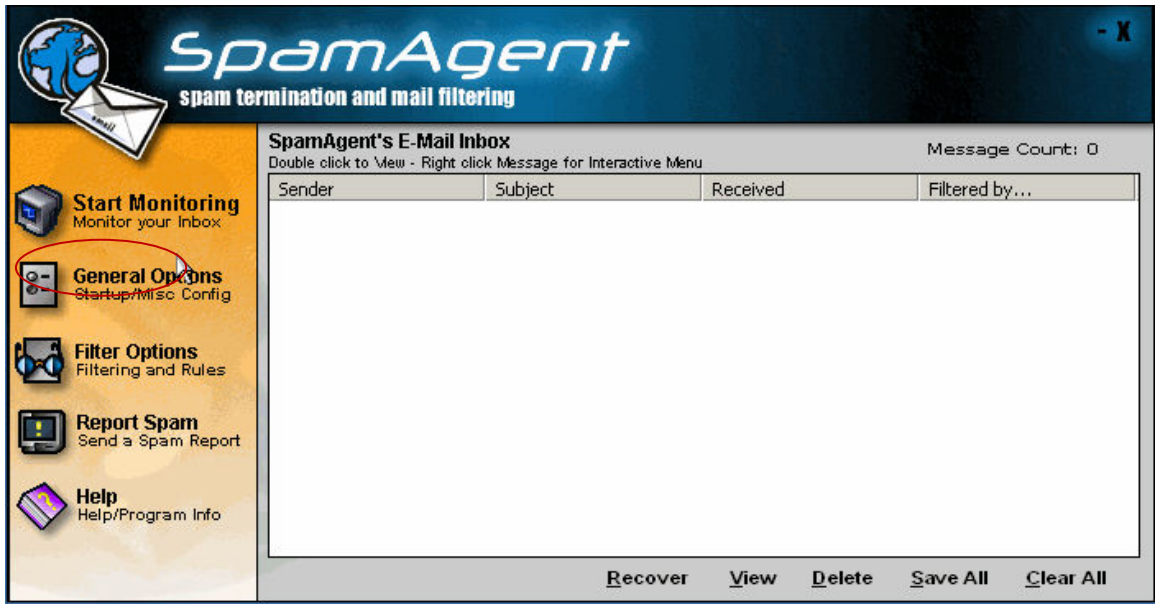
Objective:

Use **Spytech Spam Agent** to remove spam from your mailbox

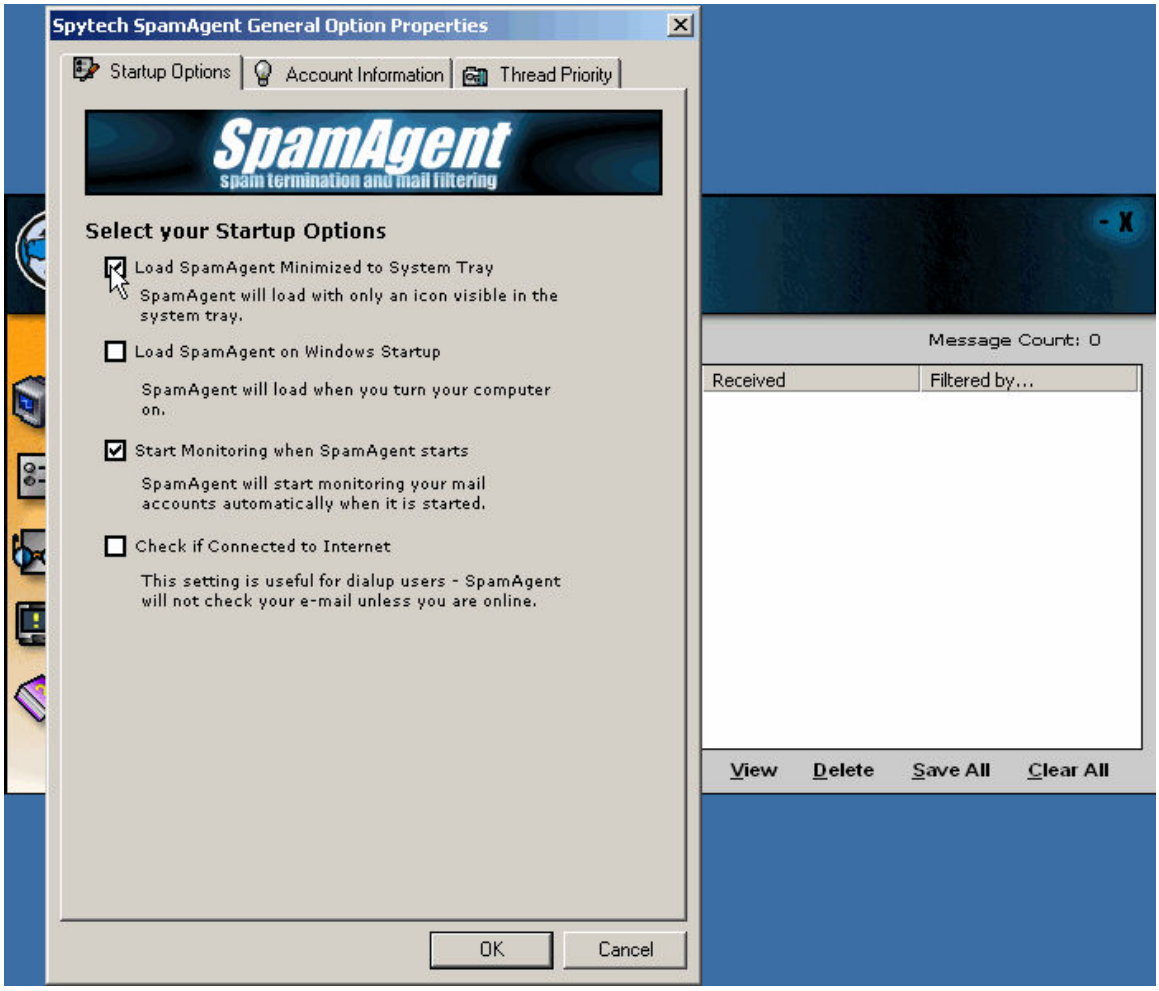
- In the **CEHv6 Labs CD-Rom,** navigate to **Module 40**
- Install and launch **Spytech Spam Agent**



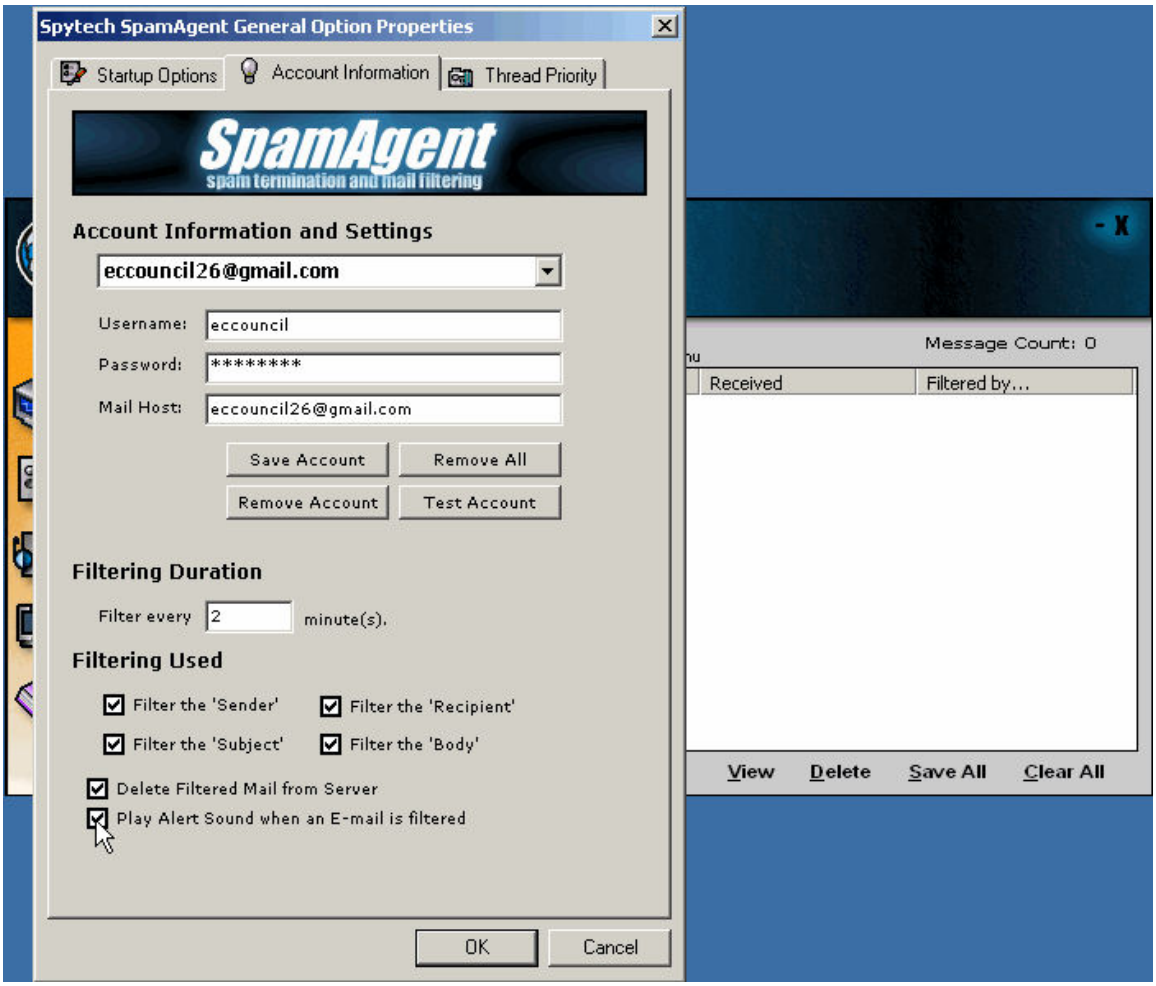

- Click on **General Options**



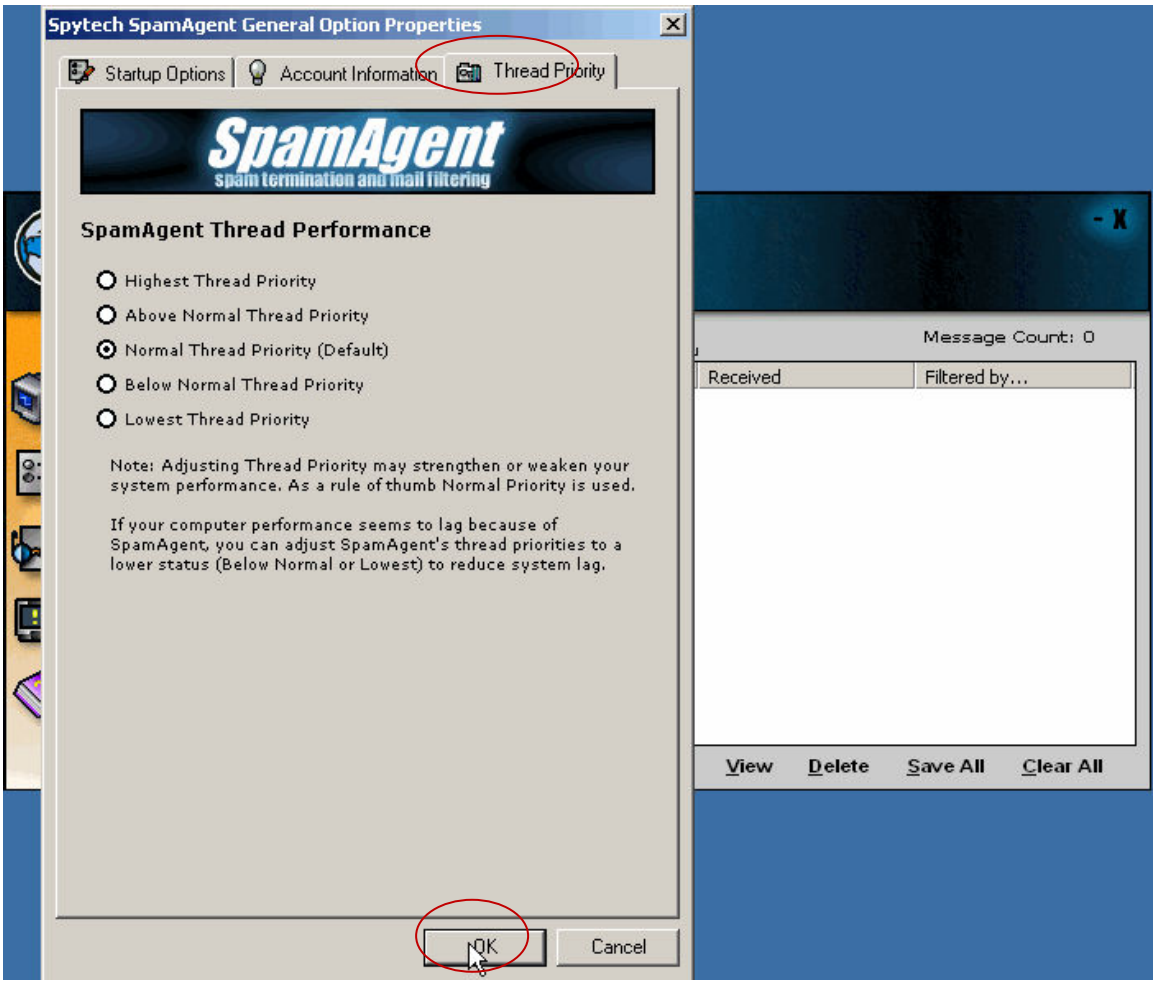

- Go to Startup Option menu and select Startup options



- Fill all the options providing the information about the Account



- Click **Thread Priority** menu and select an option to select the priority

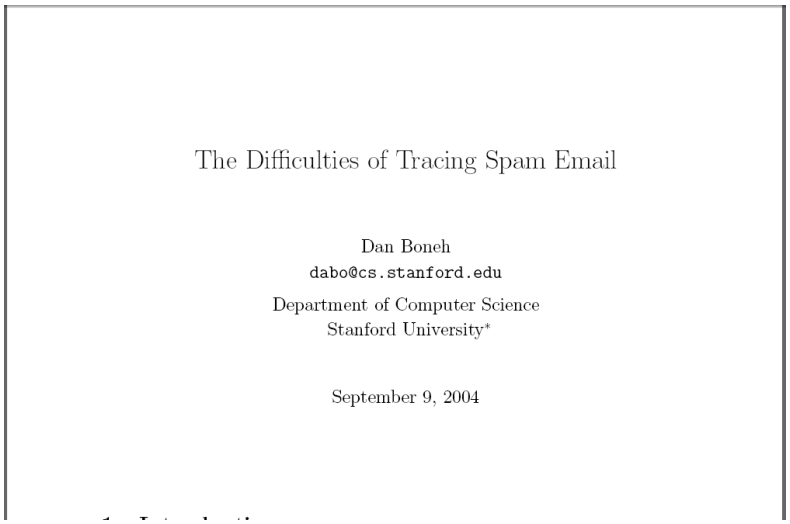


## Lab 40-03

Objective:

Difficulties of Tracing Spam Email whitepaper

- In te **CEHv6 Labs CD-ROM,** navigate to **Module 40**
- Open the **The Difficulties of Tracing Spam Email.pdf** and read the content



The Difficulties of Tracing Spam Email

Dan Boneh
dabo@cs.stanford.edu
Department of Computer Science
Stanford University*

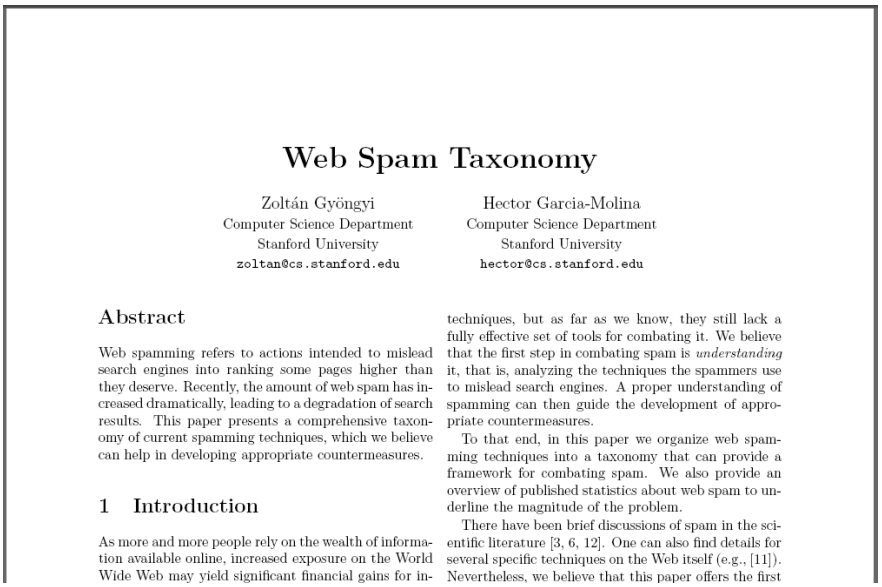
September 9, 2004

# Lab 40-04

Objective:

Web Spam Taxonomy whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 40**
- Open the **Web Spam Taxonomy.pdf** and read the content



Web Spam Taxonomy

Zoltán Gyöngyi
Computer Science Department
Stanford University
zoltan@cs.stanford.edu

Hector Garcia-Molina
Computer Science Department
Stanford University
hector@cs.stanford.edu

Abstract

Web spamming refers to actions intended to mislead search engines into ranking some pages higher than they deserve. Recently, the amount of web spam has increased dramatically, leading to a degradation of search results. This paper presents a comprehensive taxonomy of current spamming techniques, which we believe can help in developing appropriate countermeasures.

1 Introduction

As more and more people rely on the wealth of information available online, increased exposure on the World Wide Web may yield significant financial gains for individuals and companies. Consequently, many Web sites employ various techniques, but as far as we know, they still lack a fully effective set of tools for combating it. We believe that the first step in combating spam is *understanding* it, that is, analyzing the techniques the spammers use to mislead search engines. A proper understanding of spamming can then guide the development of appropriate countermeasures.

To that end, in this paper we organize web spamming techniques into a taxonomy that can provide a framework for combating spam. We also provide an overview of published statistics about web spam to underline the magnitude of the problem.

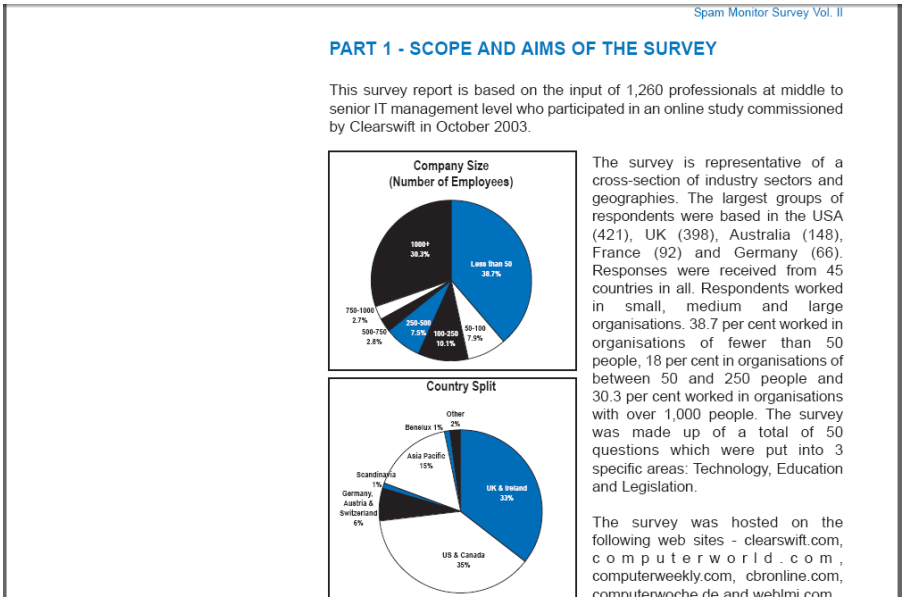
There have been brief discussions of spam in the scientific literature [3, 6, 12]. One can also find details for several specific techniques on the Web itself (e.g., [11]). Nevertheless, we believe that this paper offers the first

# Lab 40-05

Objective:

Spam Monitor Survey whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 40**
- Open the **Spam Monitor Survey.pdf** and read the content



Spam Monitor Survey Vol. II

**PART 1 - SCOPE AND AIMS OF THE SURVEY**

This survey report is based on the input of 1,260 professionals at middle to senior IT management level who participated in an online study commissioned by Clearswift in October 2003.

Company Size (Number of Employees)



Country Split



The survey is representative of a cross-section of industry sectors and geographies. The largest groups of respondents were based in the USA (421), UK (398), Australia (148), France (92) and Germany (66). Responses were received from 45 countries in all. Respondents worked in small, medium and large organisations. 38.7 per cent worked in organisations of fewer than 50 people, 18 per cent in organisations of between 50 and 250 people and 30.3 per cent worked in organisations with over 1,000 people. The survey was made up of a total of 50 questions which were put into 3 specific areas: Technology, Education and Legislation.

The survey was hosted on the following web sites - clearswift.com, computerworld.com, computerweekly.com, cbronline.com, computerwoche.de and weblmi.com

## Lab 40-06

Objective:

Spam A Security Issue whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 40**
- Open the **Spam A Security Issue.pdf** and read the content

December 2003

*Spam: A Security Issue*

*Introduction*

Spam has become a plague for email users around the world. The sheer volume of spam is annoying as users have to clean their inboxes from these unwanted messages on a daily basis. In addition, the aggressive and often sexually explicit nature of spam is offensive and frustrating to most end users. Spam is clearly a nuisance, but in this white paper, we will demonstrate how spam has evolved into a true security issue for organizations.

We begin with defining email security, followed by an analysis of spam, spam-related threats and some of the tools and methods used by spammers. Finally, we discuss next generation email threats and the requirements to protect an organization's email infrastructure appropriately.


# Module 41

# Hacking USB Devices

# Lab 41-01

Objective:

U3 USB Security whitepaper

- In the **CEHv6 Labs CD-ROM,** navigate to **Module 41**
- Open the **u3_technology_v1.0.pdf** and read the content