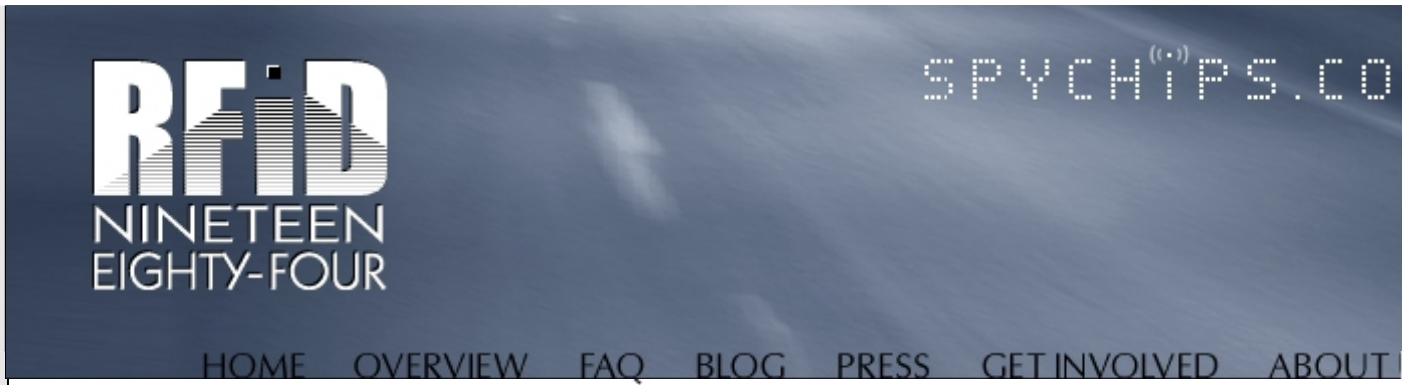

FOR IMMEDIATE RELEASE
March 15, 2006

RFID VULNERABLE TO VIRUS ATTACKS COULD WREAK HAVOC

Wake up and Put a Hold on Reckless Deployment, Say Privacy Activists

Privacy and civil liberties advocates have long been opposed to the use of RFID technology on consumer items and government documents because it can be used to track people without their knowledge or consent. But now security researchers are warning RFID systems are vulnerable to virus that could wreak havoc on databases around the world and potentially facilitate a terrorist attack. Melanie Rieback, a Ph.D. student at the Vrije Universiteit in Amsterdam, gave a live demonstration of how a hacker could deploy a single rogue RFID tag and infect associated databases at the Fourth Annu IEEE Conference on Pervasive Computing and Communications held in Pisa, Italy, March 15.

"Let's hope this puts the breaks on the irrational exuberance of Wal-Mart, Procter & Gamble, the Department of Homeland Security, and everyone else hell bent on tracking everything and everyone with this technology," say privacy advocates Katherine Albrecht and Liz McIntyre, co-authors of "Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID."

Radio Frequency IDentification (RFID) is a controversial technology that uses tiny microchips to trac items from a distance. These RFID microchips have earned the nickname "spychips" because each contains a unique identification number, like a Social Security number for things, that can be read silently and invisibly by radio waves. Security experts have theorized that RFID would be targeted by hackers, but until now, most considered the limited memory on the tags insufficient to deliver such attacks.

Rieback backs up her demonstration with details about exactly how a virus could propagate in RFID systems in a paper aptly titled "Is Your Cat Infected with a Computer Virus?" The paper opens with a scenario in which a vet's database seems to be erasing data from pet tags and finally freezes, displayin the message "All your pet are belong to us." (This is a nod to the Internet joke "All your base are belo to us.")

This damage could start with one attacker writing malicious code onto his cat's microchip and exposir it to the vet's system, she claims. But that's just the start. Her university's press release about the discovery points out how such malicious code could infect retail databases and even RFID-based airpo baggage systems, leading to more serious consequences, like a terrorist debilitating a baggage databas in order to slip in a lethal suitcase:

> "A malicious individual could put an infected RFID tag on his suitcase (or someone else's suitcase). The bag will be scanned when approaching a Y-junction, to determine which direction it should go. However the mere act of scanning could infect the airport's baggage database, and as a result, all bags checked in after could receive infected baggage labels. As these bags move to other airports, they would be rescanned -- and within 24 hours, hundreds of airports could be infected worldwide. A smuggler or terrorist using this technique could hide baggage from airline and government officials."

The university researchers recommend that developers incorporate countermeasures to "help reduce th threat of RFID viruses." They point out that these measures "take time, people, and money to implement" and urge RFID developers to take action before their software is widely deployed.

"We've long contended that RFID will put all of us at risk," says McIntyre."This is a wake-up call to RFID proponents who are recklessly rushing the technology into the marketplace before the serious societal consequences of tracking everyday objects and people with this technology can be fully explored."

==========

ABOUT THE BOOKS

"Spychips: How Major Corporations and Government Plan to Track your Every Move with RFID" (Nelson Current) was released in October 2005. Already in its fifth printing, "Spychips" is the winner of the Lysander Spooner Award for Advancing the Literature of Liberty and has received wide critical acclaim. Authored by Harvard doctoral researcher Katherine Albrecht and former bank examir

Liz McIntyre, the book is meticulously researched, drawing on patent documents, corporate source materials, conference proceedings, and firsthand interviews to paint a convincing -- and frightening -- picture of the threat posed by RFID.

Despite its hundreds of footnotes and academic-level accuracy, the book remains lively and readable according to critics, who have called it a "techno-thriller" and "a masterpiece of technocriticism."

Read the foreword by Wired technology commentator and best-selling author Bruce Sterling.

"The Spychips Threat: Why Christians Should Resist RFID and Electronic Surveillance" (Nelson Current, January 31, 2006) is a paperback version of the original book that addresses Christian concer associated with the technology.