Malware

Viruses, worms, spyware, keyloggers, botnets, embedded, defenses, oh my!

Slides by Prof. Kevin Fu with material from Prof. J. Alex Halderman

Today:

- Malware
- History
- Defenses
- Embedded malware

What is malware?

Set of instructions that
run on your computer and
do something
an attacker wants it to do.

What are the goals of malware??

Species of malware

- Trojan horses
- Viruses
- Worms
- Bots

- High risk sites for spyware [Gribble 2005]
  - Games
  - Screensavers
  - Celebrity sites

Trojan horse

Software that appears to perform a desirable function but is actually designed to perform undisclosed malicious functions

Examples??

Virus

Self-replicating software that infects other programs by modifying them to include a version of itself

Examples?

Viruses can mutate to avoid detection, changing parts of their code while keeping the algorithm intact (**"polymorphic"** or **"metamorphic"** viruses)

Worm

Self-replicating software that infects other systems by automatically spreading over the network.

Fast spreading worms an enormous threat -- fueled by software homogeneity

First worm: 1988 Morris worm
Direct descendent: 2001 Code Red worm

Remote code-injection worm
Ex: Slammer 2003 -- single UDP packet!
exploited buffer overflow
infected whole vulnerable population in 10 minutes!
took down ATMs, 911 systems, airline ticketing)

Ex: Email attachment worm (Mydoom 2004)
Ex: XSS worm (Samy 2005)
Ex: Increasing sophistication, commercialization (e.g., Conficker 2008)

Video Nostalgia Time!!

Avoiding Detection and Removal: **Rootkits**

- A component that uses stealth to maintain persistent and undetected presence on the machine
- Can be applied to any malware

Operation:

Intercept system calls for listing files, processes

Filter out malware's files and processes

Example: Magic prefix -- $sys$filename

VM Rootkit:

Install a VM below the operating system -- Blue Pill (matrix)

Bots and Botnets

- Wide scale, centrally controlled malware
- Bots infect many hosts (zombies)
- Botmaster, remote command and control

- Stacheldraht in 1999
(German for barbed wire, passwords…)

- Huge scale: 10,000s or 100,000s of bots
- Varying payloads: Instruct army of darkness to
    - Send spam
    - DDoS
    - Infect other hosts
- Financial motives
    - MaaS (Dark cloud)

- Command and control
    - Centralized
    - Distributed

Botnet Examples

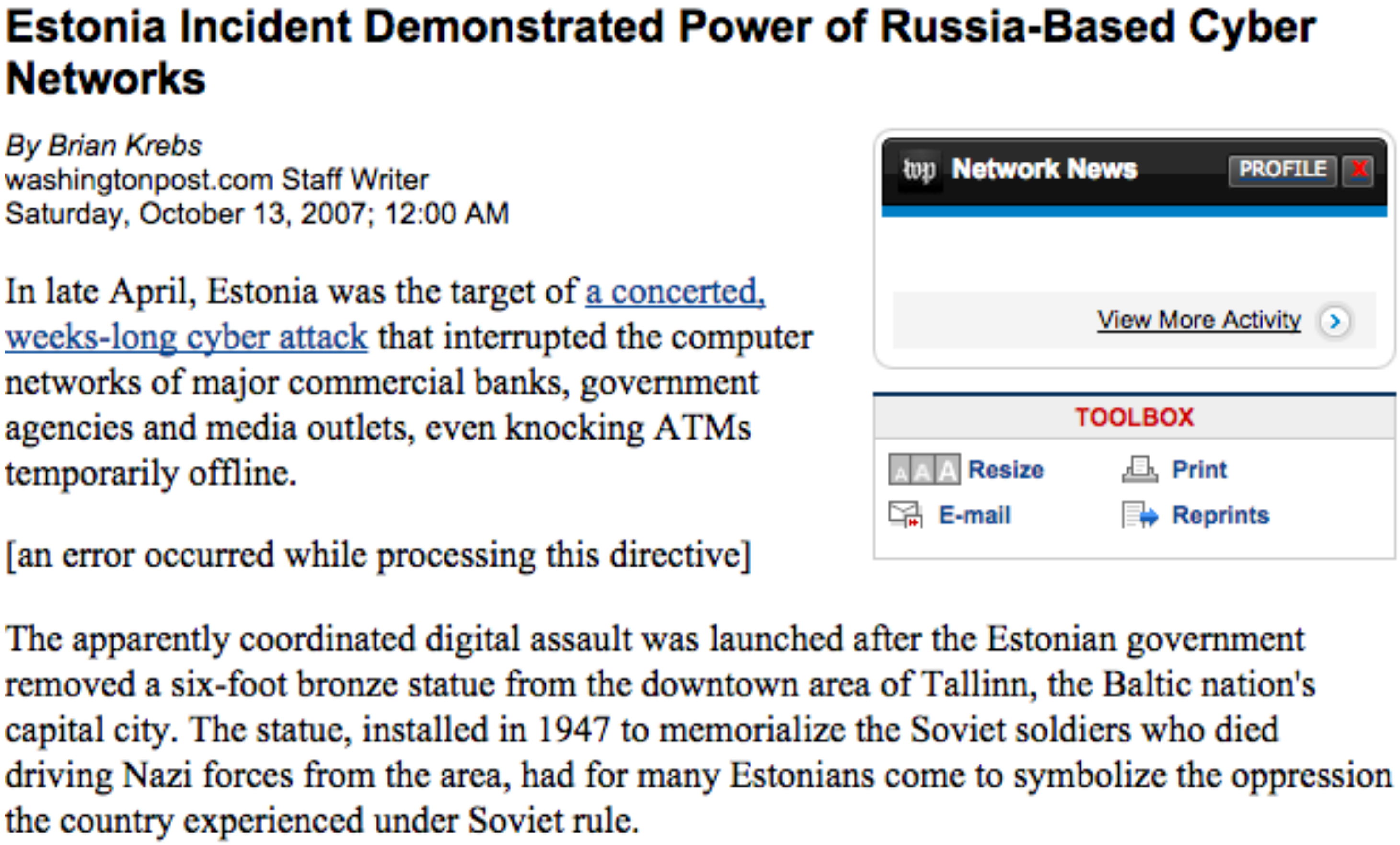
Storm

-~1M Bots, Storm email worm, 2007

- P2P, crypto (control msgs signed)
- Uses: Spam, Stock Fraud, Phishing

Estonia, 2007

Botnet Wars



Estonia Incident Demonstrated Power of Russia-Based Cyber Networks

By Brian Krebs
washingtonpost.com Staff Writer
Saturday, October 13, 2007; 12:00 AM

In late April, Estonia was the target of a concerted, weeks-long cyber attack that interrupted the computer networks of major commercial banks, government agencies and media outlets, even knocking ATMs temporarily offline.

[an error occurred while processing this directive]

The apparently coordinated digital assault was launched after the Estonian government removed a six-foot bronze statue from the downtown area of Tallinn, the Baltic nation's capital city. The statue, installed in 1947 to memorialize the Soviet soldiers who died driving Nazi forces from the area, had for many Estonians come to symbolize the oppression the country experienced under Soviet rule.

Mirai botnet DDoS of DNS

- Millions of security cameras infected with malware

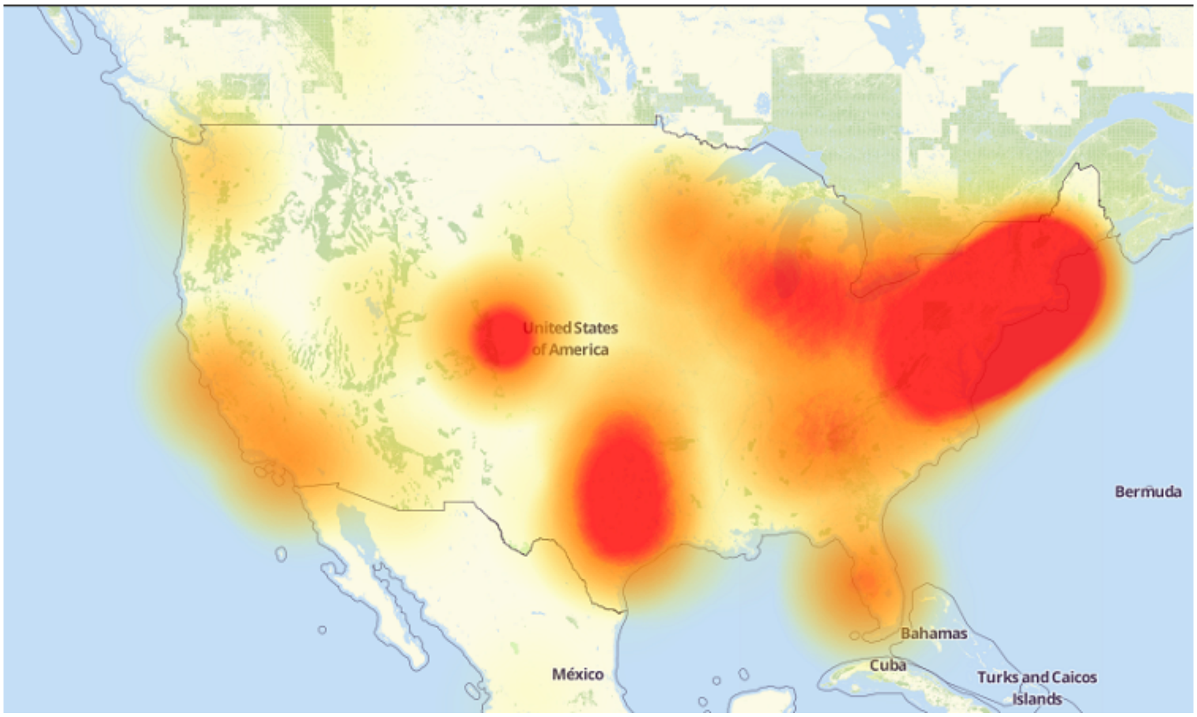
- Flooded DNS servers with traffic

- Brought down company called Dyn

- Congressional hearings

https://www.c-span.org/video/?418599-1/hearing-focuses-cyberattacks-internet-things&start=1590#

(26:28)



Defenses

- Anti-virus

Perfect virus detector is impossible!
Assume P is a perfect detector, V is a virus
V can call P:

    if P(V) = true -> halt; if P(V) = false -> spread

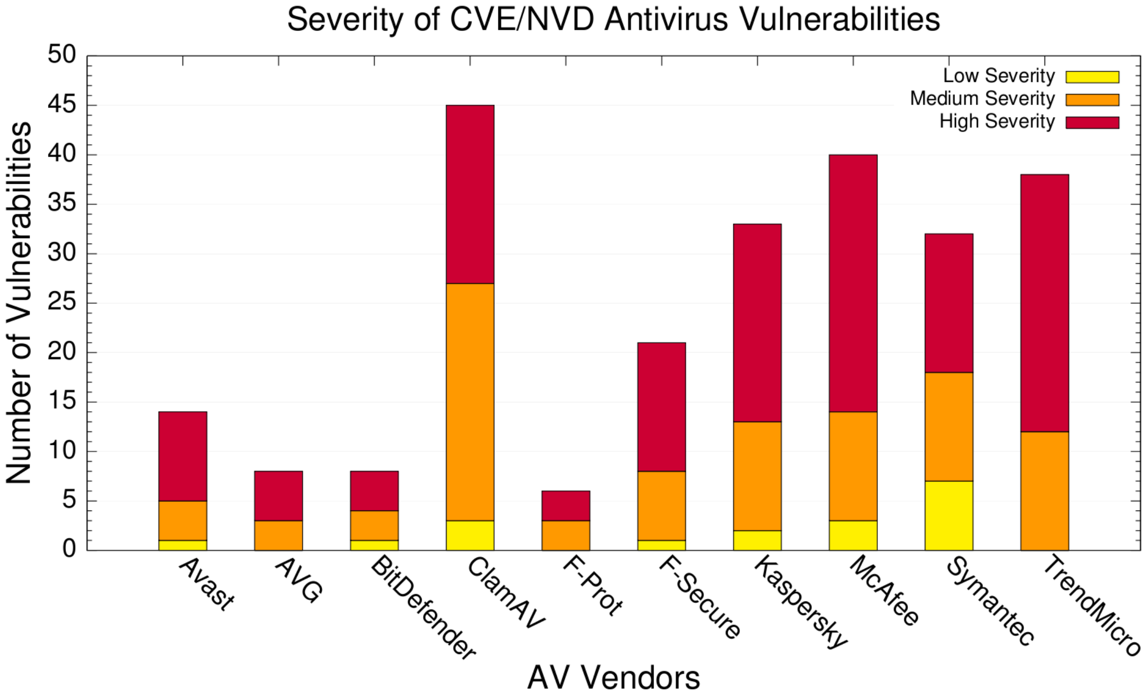
Signature detection
- Binary fingerprint
- Polymorphic virus defeats

Heuristic detection
- Analyze **program behavior** for unusual patterns
E.g., network access, file open or delete, modify boot sector

- Tripwire
- Google safe web browsing

Brand name security: Remote root exploit with rogue McAfee anti-virus update

Antivirus Vulnerabilities



Antivirus engines vulnerable to numerous local and remote exploits

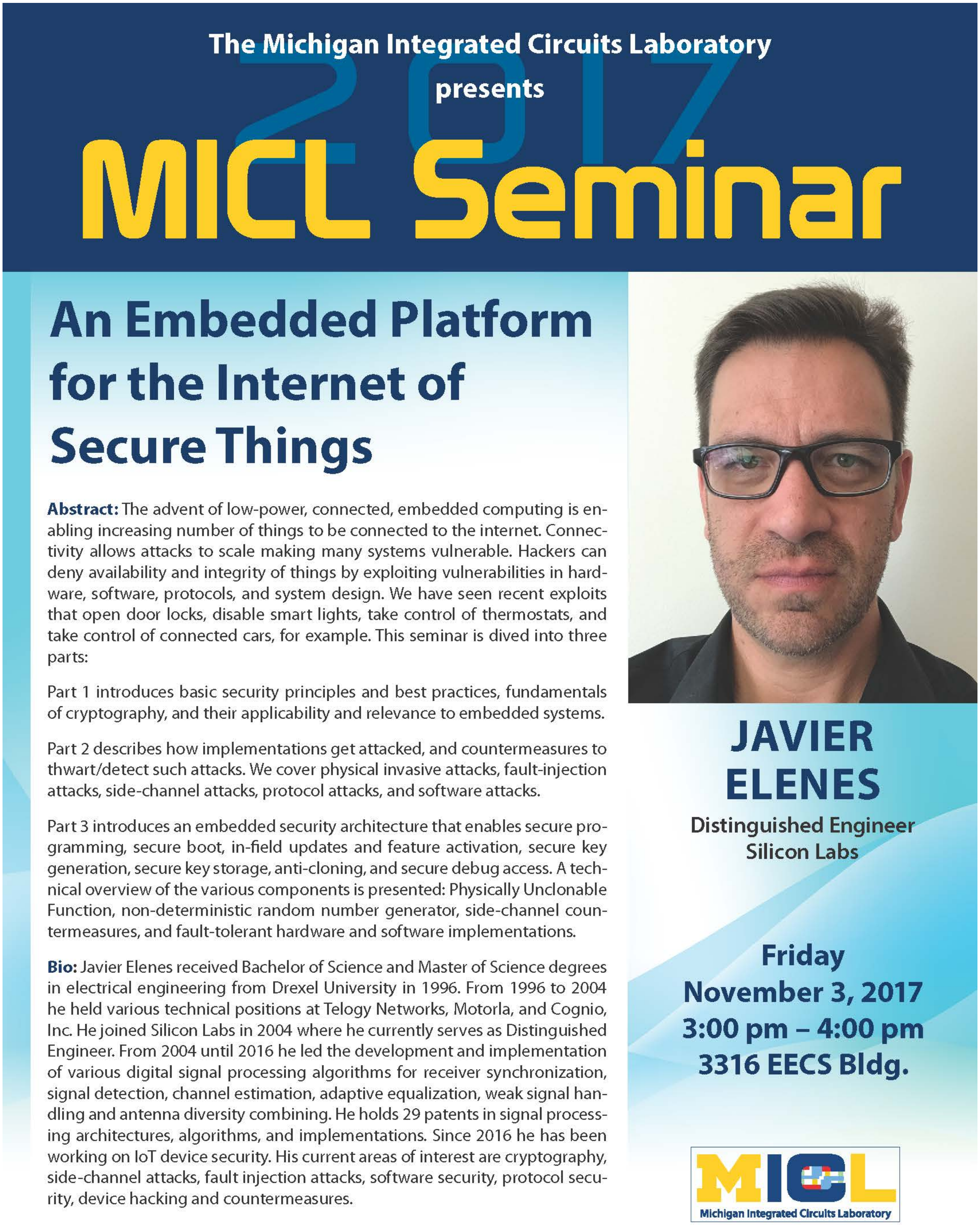
(number of vulnerabilities reported in NVD from Jan. 2005 to Nov. 2007)

Embedded Malware

- Attacks
  - Stuxnet
  - ATMs
  - POS machines
  - IoT
- Defenses
  - Shodan.io
  - Behavior analysis

Embedded Malware

Embedded Security Industry Speaker



The Michigan Integrated Circuits Laboratory
presents

2017

MICL Seminar

An Embedded Platform for the Internet of Secure Things

Abstract: The advent of low-power, connected, embedded computing is enabling increasing number of things to be connected to the internet. Connectivity allows attacks to scale making many systems vulnerable. Hackers can deny availability and integrity of things by exploiting vulnerabilities in hardware, software, protocols, and system design. We have seen recent exploits that open door locks, disable smart lights, take control of thermostats, and take control of connected cars, for example. This seminar is dived into three parts:

Part 1 introduces basic security principles and best practices, fundamentals of cryptography, and their applicability and relevance to embedded systems.

Part 2 describes how implementations get attacked, and countermeasures to thwart/detect such attacks. We cover physical invasive attacks, fault-injection attacks, side-channel attacks, protocol attacks, and software attacks.

Part 3 introduces an embedded security architecture that enables secure programming, secure boot, in-field updates and feature activation, secure key generation, secure key storage, anti-cloning, and secure debug access. A technical overview of the various components is presented: Physically Unclonable Function, non-deterministic random number generator, side-channel countermeasures, and fault-tolerant hardware and software implementations.

Bio: Javier Elenes received Bachelor of Science and Master of Science degrees in electrical engineering from Drexel University in 1996. From 1996 to 2004 he held various technical positions at Telogy Networks, Motorla, and Cognio, Inc. He joined Silicon Labs in 2004 where he currently serves as Distinguished Engineer. From 2004 until 2016 he led the development and implementation of various digital signal processing algorithms for receiver synchronization, signal detection, channel estimation, adaptive equalization, weak signal handling and antenna diversity combining. He holds 29 patents in signal processing architectures, algorithms, and implementations. Since 2016 he has been working on IoT device security. His current areas of interest are cryptography, side-channel attacks, fault injection attacks, software security, protocol security, device hacking and countermeasures.

JAVIER ELENES
Distinguished Engineer
Silicon Labs

Friday
November 3, 2017
3:00 pm – 4:00 pm
3316 EECS Bldg.

MICL
Michigan Integrated Circuits Laboratory