Keyloggers in Cybersecurity Education

Christopher A. Wood
Department of Software Engineering

Rajendra K. Raj
Department of Computer Science

Rochester Institute of Technology

July 13th, 2010

Outline

- Motivation
- Design and implementation 
- Detection and prevention 
- Educational goals
- Sample keylogging projects
- Status and future work

The Big Questions

- What are keyloggers?
- Why study keyloggers?
- What makes them unique?

ZDNet UK / News and Analysis / Security / Security Management

Stealth keylogger used in bank heist

By Tom Espiner, ZDNet.co.uk, 7 February, 2006 17:40

Topics

keylogger keystroke, Viruses

Sponsored Links

NEWS A gang of Russians and Ukrainians have been arrested for allegedly stealing more than €1m (£700,000), The Guardian reported on Tuesday.

The gang is accused of stealing from French bank accounts by installing a stealth keylogging program on users' PCs. The Trojan would infect machines through email attachments or when users visited certain Web sites.

UN serves keylogger, Trojan after online attack

By Darren Pauli, Computerworld

August 29, 2007 09:20 AM ET

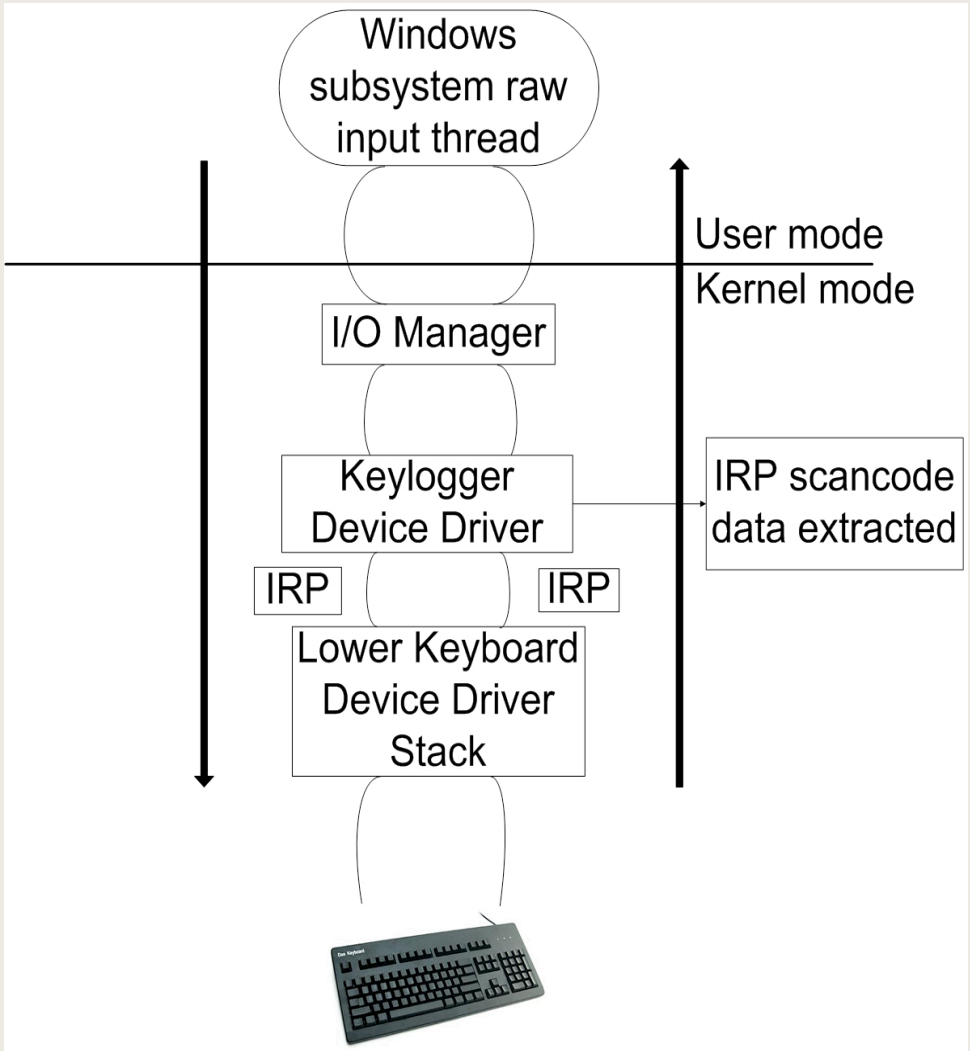
Crimeware Researchers at Exploit Prevention Labs Discover Cyber Criminals Using eCards to Deliver Malicious Rootkit And Keylogger Exploits.

Motivation

- Realistic problem in security world
- Cover wide variety of programming paradigms
- Teach fundamental security concepts

Design and Implementation

- User-mode
  - OS hooks
- Kernel-mode
  - Rootware
  - Layered drivers
- Networking
  - Client–server model
  - Covert channels

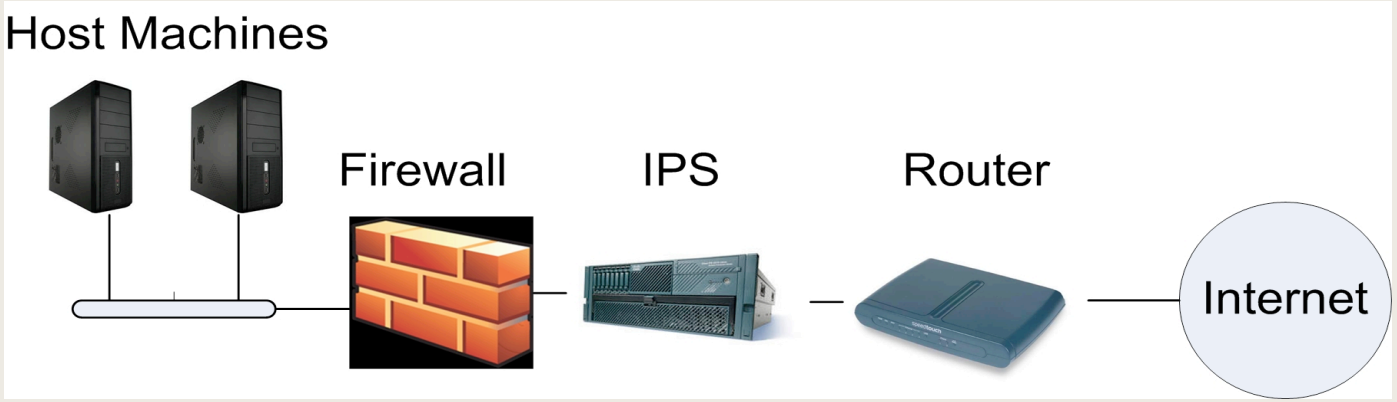


Detection

- Static detection
  - Pattern- and signature based
  - Relies on previously implemented malware with known malicious signatures (checksums)
- Dynamic detection
  - Behavioral-based using system monitoring
  - System monitored for behavior similar to that of a keylogger
  - Relevant techniques: enhanced malware categorizing and tainted data analysis

Prevention

- 5 layers
  - Application settings
  - Antivirus software
  - Firewalls
  - Intrusion prevention systems (IPS)
  - Routers



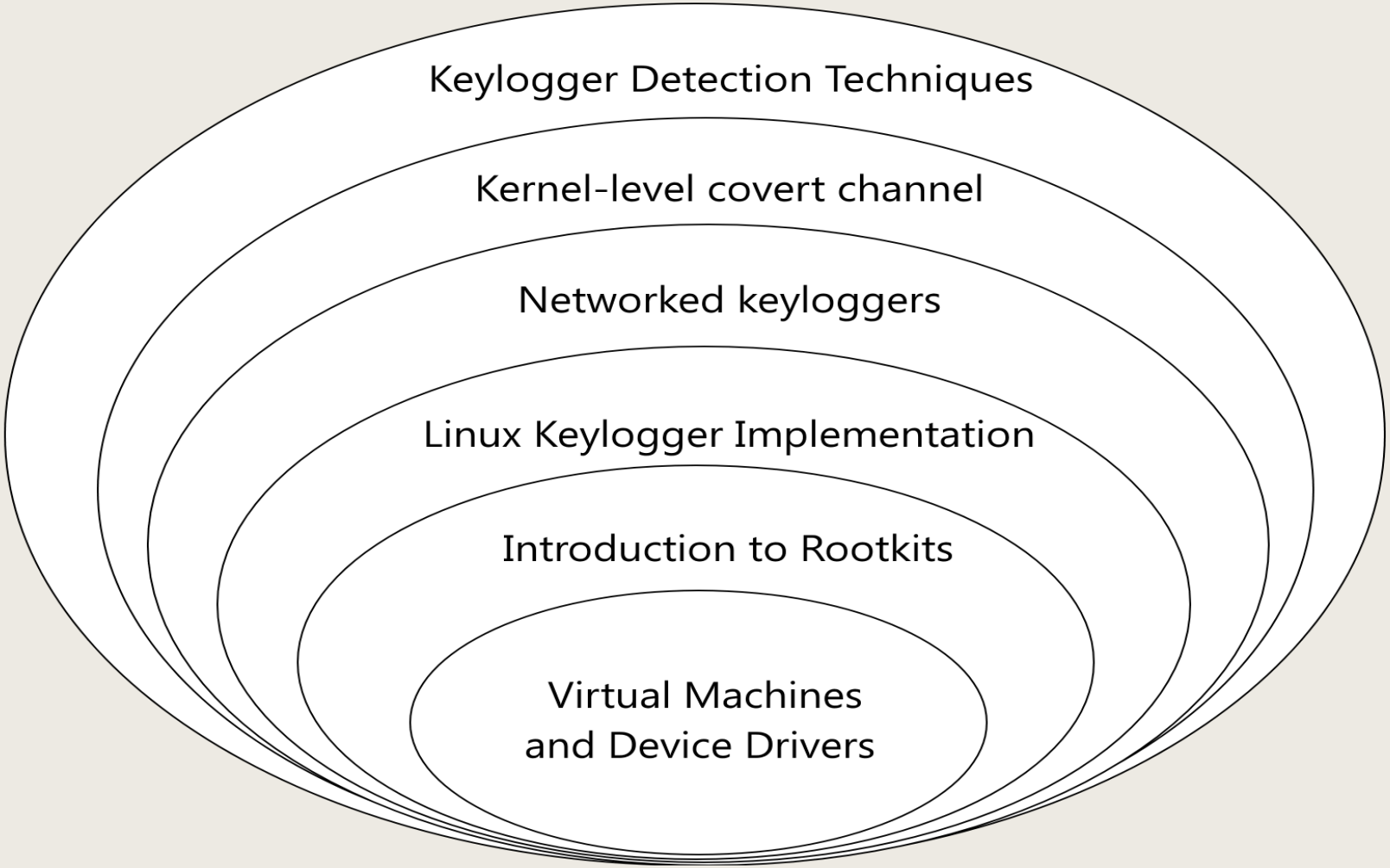
Educational Goals

- Teach students from both black- and white-hat perspective
- Introduce students to kernel development
- Broaden students' programming experience
- Encourage more student participation in research environments

Role of Keylogger Projects

- Cover legal and ethical issues
  - Crucial to make students understand them upfront
- Take the role of the black-hat hacker
  - Play around with keylogger design and implementation
  - Help create new ideas about keyloggers
- Take the role of the white-hat hacker
  - Approach malware detection by thinking like the attacker

Sample Keylogging Projects



Literature Survey Projects

- Many detection techniques are still prototypes that are not in production level
- Dive into malware detection research to stay on the bleeding edge of modern security issues
- Foster interest in future research opportunities

Status and Future Work

- Material to be adapted into a course on Secure Coding in Fall 2010
- Project exercises almost complete
- Work maintained on website hosted by the authors
  - http://www.cs.rit.edu/~rkr/keylogger2010
- Future results to be collected and presented based on student experiences and feedback

Thank You