Implementation and Management of Systems Security

158.738

A/Prof. Julian Jang-Jaccard
Massey University

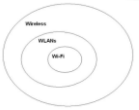
MOBILE SECURITY

Ubiquitous computing

- Wireless data networks and the mobile devices are “ever-present” or “found everywhere”
- 58% user on mobile devices vs 42% users on desktop (In 2008, > 80% on desktop)
- 4 out 5 web searches today are performed first on mobile and wireless devices
- *Nomophobia* is the fear of being without your mobile phone
- Attacks have increased significantly in this area

Wireless Technology

- The term “wireless” is generally used to describe equipment and technologies operating in the radio frequency (RF) spectrum between 3Hz and 300 GHz.
  - E.g., Baby Monitoring, Keyless entry systems, Smartphones, GPS devices, Remote controls, Garage-door openers, Walkie-talkie, Bluetooth devices
- Wi-fi (wireless fidelity) is a wireless network technology that provides high-speed data connections
- Wi-Fi grown in popularity
  - Eliminates cabling
  - Facilitates for mobile workers (as in a hospital)
  - Used in 90 percent of companies
  - Facilitates network access from a variety of locations

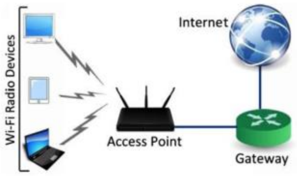


Components of Wireless

- Wireless network interface cards (WNICs): transmits and receive wireless signals
- Access Points: Bridge between wired and wireless networks
- Wireless networking protocols: defines rules for wireless communication and authenticates the users to the wireless network
- A portion of the RF spectrum which replaces wire as the connection medium

Association with an AP

- Scanning- searching for available APs
- NIC transmits probe frame on all active channels
- AP responds with info to associate with it



(Source: http://computer-trickster.blogspot.com/2015/05/wireless-hacking.html)

WLAN Security

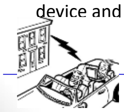
- Service Set Identifier (SSID)
  - Required by all clients to include this in every packet
  - Included as plain text →Easy to break
- Wired Equivalent Privacy (WEP)
  - Requires that user enter a key manually (to NIC and AP)
  - Communications encrypted using this key
  - Short key (40-128 bits) → Easy to break by "brute force"
- Extensible Authentication Protocol (EAP)
  - One time WEP keys created dynamically after login
  - Requires a login (with password) to a server

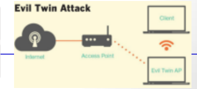
Recent WLAN Security

- Wi-Fi Protected Access (WPA)
  - new standard
  - longer key, changed for every packet
  - Have data integrity check
- 802.11i (WPA2)
  - EAP login used to get session key
  - uses AES encryption
- MAC address filtering
  - Allows computers to connect to AP only if their MAC address is entered in the "accepted" list

Wi-Fi attacks

- Wi-Fi communication is vulnerable from attack because the signal can be received anybody within the range
  - War Driving: searching for wireless signals from an automobile or on foot using a portable hacking device
  - WarFlying: use drones to find insecure WLAN
  - Warchalking: writing symbols on walls to indicate presence of an unsecure WLAN
  - Evil twin: setting up an AP to mimic an authorized Wi-Fi device and directs all traffic to the fake AP





Bluetooth

- A short-range wireless technology for quick "pairing" or interconnecting of two or more devices
  - A Tablet with a bluetooth speaker
  - A laptop computer with a bluetooth mouse
- Covers range of about 10 meters with transmission rate of 1Mbps.

Bluetooth®

Bluetooth Attacks

- Exploit others' Bluetooth connections without their knowledge.
  - Bluejacking : sending unsolicited messages/video/audio to bluetooth-enabled devices
  - Bluesnarfing: accesses unauthorized information from a wireless device through a bluetooth connection (e.g., calendars, contact lists, emails and text messages)

DIGITAL FORENSICS

Digital Forensics

- Digital forensics is a branch of forensics science.
- Forensics science is the application of science to criminal and civil laws.
- Recovery and investigation of material found in digital devices.
- Often related to cyber crime but could be for other purposes such as incident response.

Digital Forensics

- Relates to any criminal or civil law issue involving:
  - Internet
  - computer
  - any electronic device
- Encompasses wide range of devices:
  - PCs
  - Mobile devices
  - CCTV cameras
  - Fitness trackers
  - Cloud services
  - …

Forms of Crime

- Some crime is specific to computers but also:
  - Fraud
  - Harassment
  - Copyright breaches
  - Making, possessing or distributing objectionable material such as child pornography.
- Some relevant New Zealand legislation:
  - Unsolicited Electronic Messages Act 2007
  - Copyright (Infringing File Sharing) Amendment Act 2011
  - Harmful Digital Communications Act 2015

Digital Forensics Process

- Investigators follow a process so that they avoid tainting the evidence and make unusable in court.
- A well-known process was defined by the Digitial Forensics Research Workshop (DFRWS)Digital Investigation Process
  - Identification
  - Preservation
  - Collection
  - Examination
  - Presentation

Identification

- We first need to identify our evidence, this is usually not the event but related to the event.

"When two objects come into contact, they leave a trace on each other" - Locard's exchange principle

- Consider someone entering a house with carpeting.
  - What are some examples of potential traces?
- Consider someone browsing a website?
  - What are some examples of potential traces?

Preservation

- Safeguard from:
  - Deletion
  - Modification
- Isolate the system from the network (logical or physical).
- Snapshot virtual machines.
- Do not allow users access to suspect system.
- Use of encryption or digital signatures to ensure that any tampering is noticed.

Collection

- Process of acquiring digital evidence.
- Volatile evidence = evidence lost when switch off the system.
- Most volatile to least volatile (see RFC 3227):
  - Registers, cache
  - Routing Table, ARP Cache, process table, kernel statistics, Memory (RAM)
  - Temporary filesystems
  - Disk
  - Remote logging and monitoring data
  - Physical configuration, network topology
  - Archival media

Examination

- Use tools.
- Standard tools that have been approved within legal jurisdictions exist (for example, enCase).
- Might be tools to extract from:
  - Memory
  - Network traces
  - Log files on servers
  - Mobile phones
- Again need to prevent damage to the evidence when examining it.

Analysis

- Examination phase extracted potentially relevant pieces of data.
- Analyse data in light of other relevant data.
- Example:
  - Host as open connection to external IP address
  - Examine a packet capture
  - Use IP address as starting point and isolate that traffic
  - Perhaps determine if host is contacting a Control and Command server.
  - This might lead to an understanding of the type of attack.

Presentation

- Present the findings:
  - Clear
  - Concise
  - Capture every action taken and reports on critical data.
  - Without opinion or bias.
  - Aids in determining the root cause
- Might have to appear in court and state the facts.
- Might have to be an expert witness who is allowed to give an opinion.

Forensics Lab

- Requires special tools, techniques and knowledge.
- Use a separate location from rest of organisation.
- Aim is to avoid damage to the evidence.
- Also privacy.

Physical Security

- Access to lab must be controlled for chain of custody purposes.
- Remove chance of tampering or destruction of evidence.
- Locked always with access via access cards etc.
- Keep a log of entry and exit.
- Evidence lockers as well.
- Ideally keep evidence related to different incidents separate.
- Climate controlled environment.

Tools

- Literally have hand tools.
- Boxes for securing evidence.
- Faraday bags for smart phones or tablets to isolate them from network.

Hardware

- Forensic workstations with plenty of storage.
- Workstation is not connected to Internet for protection against corruption of evidence.
- Internet connected machine in same room.
- Physical write blocker:
  - Connects hard drive and forensic imaging machines.
  - Prevents writing of data to a drive.

Hardware

- Going offsite with hardware
- Durable case to transport necessary hardware.
- Support offsite examination.
- Should be capable of being checked in on a plane and arriving undamaged.

Software

- Forensic applications
  - Carry out variety of tasks
  - Documentation as well as collection etc.
- Three most common:
  - EnCase –works with hard drive and storage media.
  - FTK Forensic Tool Kit –similar to EnCase.
  - X-Ways –low cost Linux based.
- Platforms for RAM captures and network evidence:
  - SANS SIFT –imaging, memory analyses, timeline creation etc. (free)
  - CAISE Computer Aided Investigative Environment -multiple tools

Jump Kit

- Equipment for forensics analysis on the move,
- Suggested components:
  - Forensic laptop.
  - Networking cables.
  - Physical write blocker.
  - External USB hard drives and USB devices.
  - Bootable USB or CD/DVD
  - Evidence bags or boxes
  - Anti-static bags.
  - Chain of custody forms.
  - Tool kit
  - Notepad and writing instrument

END