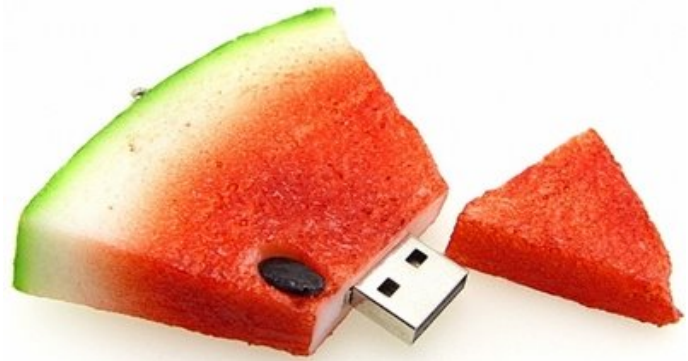
Novel Hardware-based Attacks

Jason Zheng
Aditya Joshi

Introduction

- Direct hardware hacking is as old as the trade of hacking
- Common Characteristics:
  - Physical access (at least within transmission range of EM/Accoustic signals).
  - Seemingly harmless devices
- With enough ingenuity, possibility is endless.

USB Drives



USB HID Attack

- Old-school tricks:
  - autorun.inf with auto-installed trojans
  - Only works on Windows OS
  - Easy detection: "Installing Mass-Storage Device"
  - Simple defense: disable autorun on Windows
- What is USB HID?
  - A USB Human-Interface Device is a USB device that takes input from humans, e.g. USB Keyboard/Mouse
  - The standard is well-defined as USB HID standard, and implemented by every modern OS.
  - Due to standardization, most OS are shipped with a HID device driver and will quietly install upon plugging-in.

USB HID Attack, continued

Attack Steps:

1. Prepare a special USB device that implements HID protocol.
2. Discretely plug in the device at the target computer.
3. Host computer will register the device as HID.
4. HID begins sending keystrokes and mouse clicks to host computer.

Firewire Attack

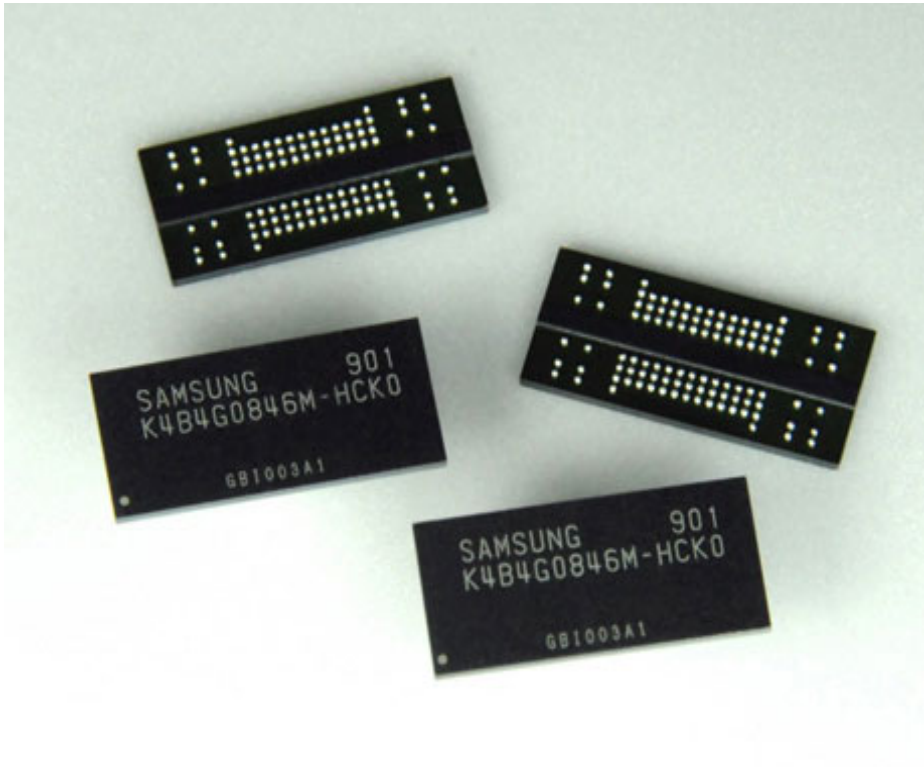
Firewire Attacks, How

- Direct Memory Access (DMA) is a way to access memory with minimal CPU involvement, common among many extension cards installed on PC.
- OHCI (Open Host Controller Interface) allows device-initiated DMA (Asynchronous Transfer). Great for performance or peer-to-peer capability.
- Unfortunately, DMA gives Firewire devices undiscriminating access to virtually every resource on the PCI bus.
- Things possible with Firewire DMA:
  - Look for encryption keys
  - Patch loaded programs or libraries in memory
  - Bypass logon screens


STAPLES
compressed gas duster
STAPLES
compressed gas duster

Cold Boot Attack

- A DRAM cell is a tiny capacitor that needs to be refreshed from time to time.
- An SRAM cell is made up of a few transistors and do not need to be refreshed.
- During a warm boot, power is not removed, only the CPU goes through reset.
- During a cold boot, power is temporarily removed and restored.



Cold Boot Attack, Continued

- A cold boot attack exploits the fact that volatile memory are not all too volatile.
- Actual data decay rate varies with the manufacturing process and temperature.
- Under normal room temperature, 50% of the data are still readable after 5-6 minutes of loss of power.
- If cooled to -50C, almost all the data are still readable after 5-6 minutes.
- Important data, such as disk encryption keys can be retrieved after cold reboot.

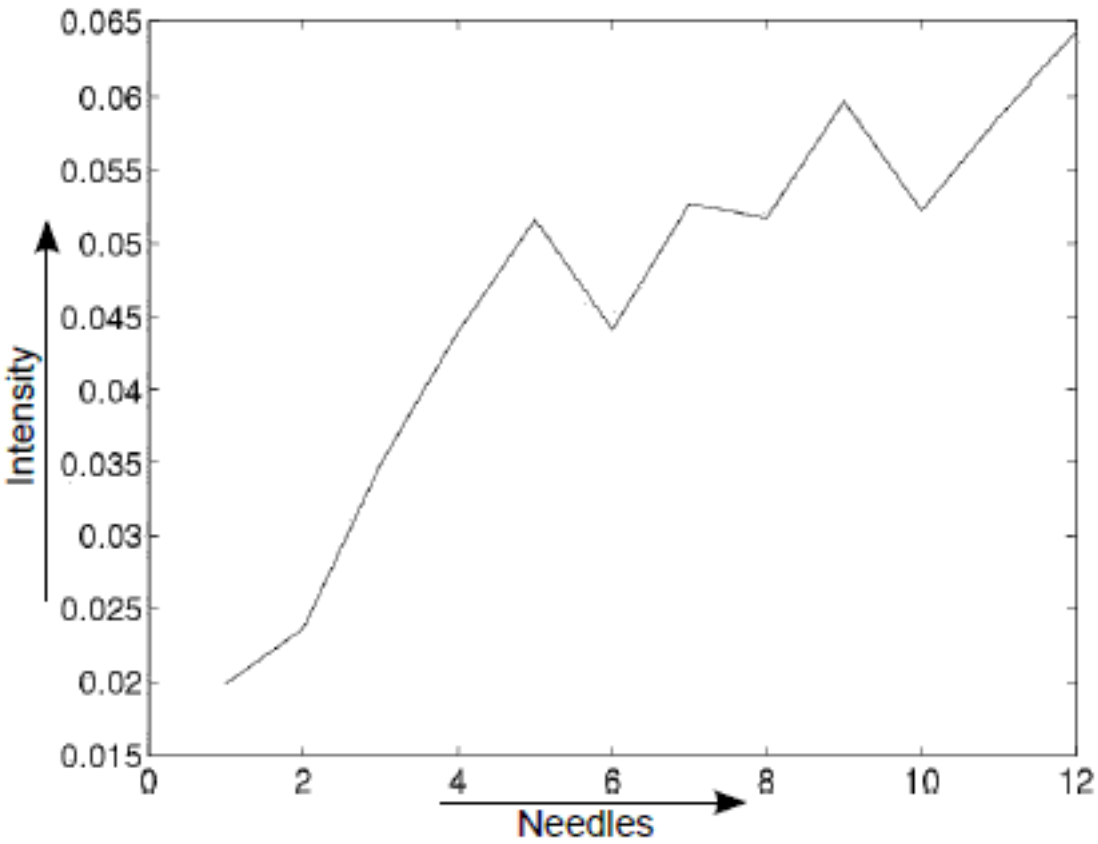
Acoustic Side Channel Attacks

Acoustic Side Channel Attacks

In general, a dot matrix printer makes a louder sound if more pins hit the paper.

The authors of the Acoustic Side Channel paper trained their system on English words from a dictionary. They would then record noise from a printer and feed it to their system which would use the statistical frequency of words in English to determine the word being printed.

70% - 95% accuracy!



Bluetooth Keyboards

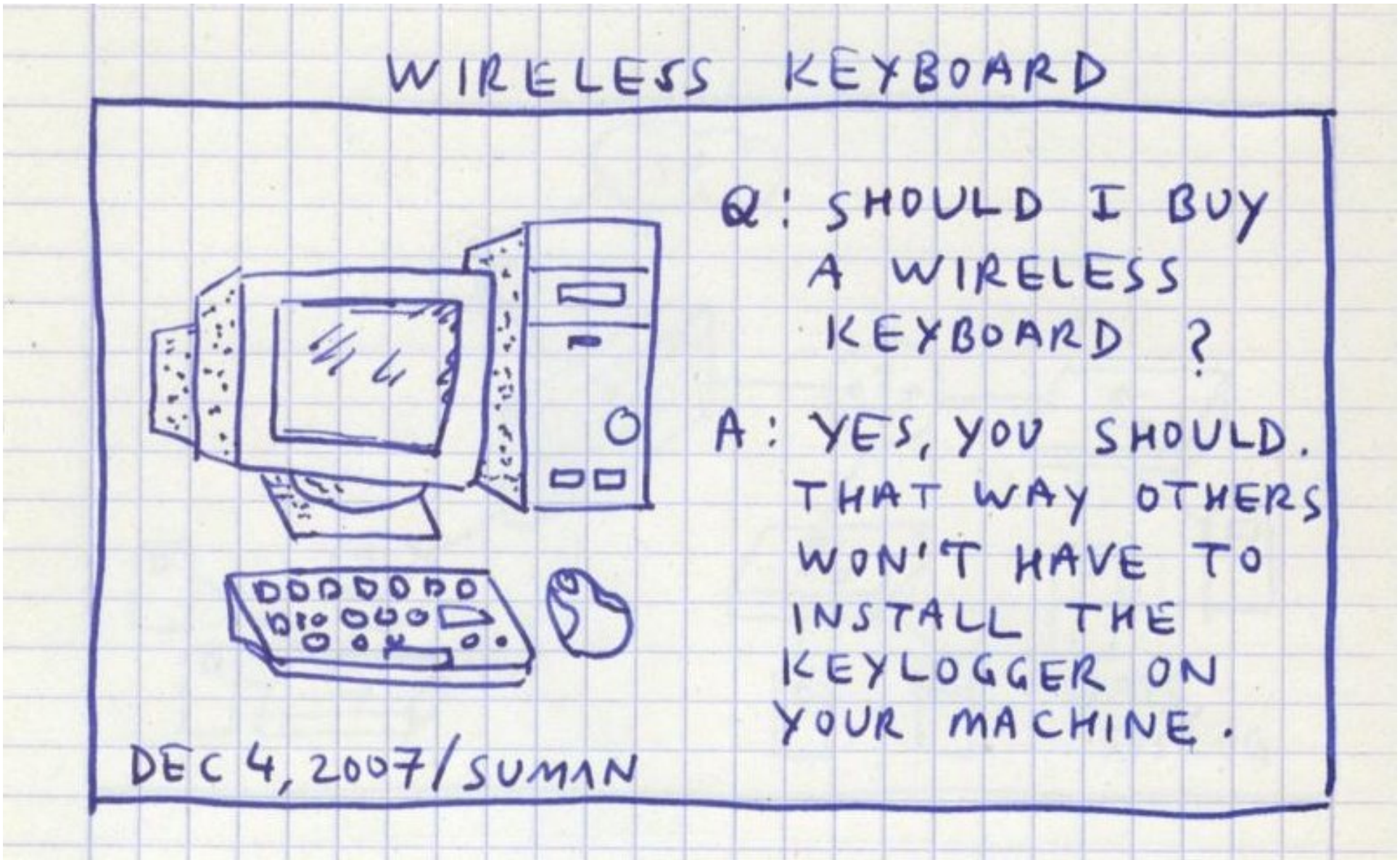
Bluetooth Keyboards

- Bluetooth keyboards need to transmit data to host machine.
- Either the keyboard or the host can attempt to discover its counterpart by broadcasting its presence.
- The host then needs to figure out the device's capabilities.
  - This is done via SDP (Service Discovery Protocol).
    - SDP specifies PSM (ports)for standard data transfer and signaling, language sets, etc.
- The control channel (which is used for signaling) needs to be established before the interrupt channel (which is used for data transfer).
  - This process is done via SDP.
  - We also need to establish a protocol for standard communication.
    - We will look at the simpler *boot protocol* which is used by Bluetooth aware BIOSs for using Bluetooth keyboards as console input

Attacking Bluetooth Keyboards

- One can fool a host into believing that our malicious device is a valid keyboard.
- First we scan for open PSMs (ports). Because of L2CAP, these ports are standardized.
  - Collin Mulliner used bt audit to do this.
  - If the security layer is not enabled, we do not need a PIN and can connect easily.
- This gives one full control over a keyboard connected to the host!
  - Note that this is not the same as full control over the host. There may be more keyboards connected.
- We can also instigate a passive attack by waiting until some computer attempts to connect to us.
  - Our device must attempt to seem like a real keyboard.
    - Discoverable, connectable, piconet slave

Bluetooth Keyboards



Wired Keyboards

Wired Keyboards

- Wired keyboards should be secure.
  - They only transmit data through a wire.
    - How could someone splice a wire in front of me without me noticing?
- Keystrokes cause keyboards to send signals to the connected computer.
  - These binary signals consist of rising and falling edges.
    - The falling edges alone can be used to determine keystrokes with about 1 bit of uncertainty.
    - Rising and falling edges together can be used to determine keystrokes with 0 bits of uncertainty!
- **Direct emanations** are a direct result of a keystroke.
- **Indirect emanations** are the result of a keystroke, but only partially so.

Wired Keyboards

- Emanations from Matrix Scan Routines can also be detected
  - Indirect Emanation
  - About 2.5 bits of uncertainty per keystroke
- Keystrokes are extracted from detected emanation by Fourier Transforms (to clean out ambient noise)
- Yields possible characters, and then exhaustive search can be applied to extract passwords, names or other data.
- Range is from 2-10 meters

Discussion Questions

Has hardware hacking gotten easier than ever?

If so, what changed in the past ten years?

What other things could be the next killer hack?

What can be done for us to trust our hardware more?


PWNED


iPad


7302
OFF
Map view
Mark
MODE
AUTO
OFF

Closing remark - http://xkcd.com/644/