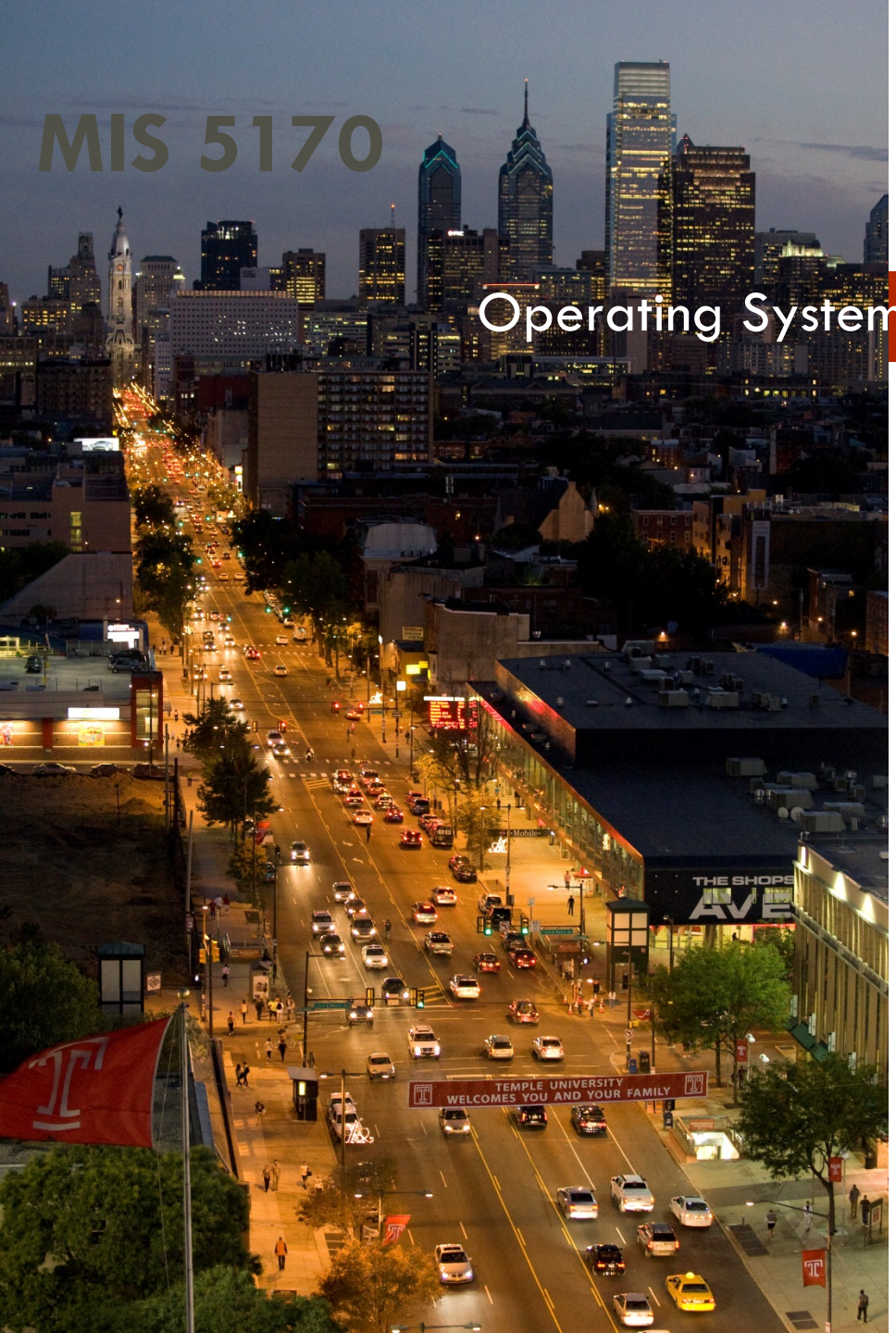


Operating System Security

Week 1

Overview

Fox School of Business
TEMPLE UNIVERSITY®

Tonight's Plan

- Introduction
- Overview of Course
- Computer Hardware Overview
- Operating System Overview
- Hypervisor Overview
- Networking Overview
- Physical Security Overview
- Operating System Security Overview
- Next Week

Introduction

- Andrew Szajlai
  - andrew.szajlai@temple.edu
  - Office hours by appointment
    - via WebEx meetings if needed
    - Setup via e-mail

Overview of Course

Operating System Security

MIS 5170 Section 001 & 701

Site: https://community.mis.temple.edu/mis5170sec001sec701sp2018/

Overview of Course (cont)

About the Course

- Our focus will be on operating system security and tools to secure operating systems. Methods of securing operating systems in theory and in hands on exercises.
  - Course has been created based on enterprise experiences
  - Tasks and assignments will focus on building two secure operating systems
  - Working with another class as an outside audit to see how well we have secured our operating system

Overview of Course (cont)

About the Course (cont)

- Additional tools and concepts we will review
  - Wireshark – not a way to secure your operating system; however used to help secure our OS with firewalls rules
  - Vulnerability scanners – used to help verify how well we have done to protect our operating system

Course Outline

Week	Topic	Assignments
1 – Jan 18th	Overview of Course, Computer Hardware Overview, Operating System Overview, Hypervisor Overview, Networking Overview, Physical Security Overview, Operating Systems Security Overview	Reading Week 1
2 – Jan 25th	Hypervisors, Network Fundamentals, TCP/IP and Network Architecture and its impact on Operating System Security, Assignment 1 Overview	Reading Week 2 Assignment 1
3 – Feb 1st	Scripting, PowerShell, Python, Appropriate permissions, Access Control, Limit services, Shares, Windows file shares / ACL	Reading Week 3 Quiz
4 – Feb 8th	Configuration management practices, System hardening, Windows Group Policies, Baselines, Enabling Logging, Baseline Standards, Intrusion detection, Host based, Network based, Intrusion prevention, Host based, Network based, Assignment 2 Overview	Reading Week 4 Assignment 2 Quiz
5 – Feb 15th	Patching, Native patching tools, Third-Party, Vulnerability scanning and remediation	Reading Week 5 Quiz
6 – Feb 22nd	Malware/Spyware, Detection tools, Native, Third-Party, Antivirus, Microsoft, Third-Party, Sniffers, NetMon, WireShark, Assignment 3 Overview	Reading Week 6 Assignment 3 Quiz
7 – Mar 1st	Firewalls, Host based, IPSec, Networkbased, Review for 1st Test	Reading Week 7 Test 1
8 – Mar 8th	Logging, Using Windows EventLog, Paid Products, Splunk, SEIM(s)	Reading Week 8 Quiz

Course Outline (cont)

Week	Topic	Assignments
9 – Mar 15th	Spring Break	Have Fun
10 – Mar 22nd	Unix/Linux basics, Scripting, bash basics, Python, Appropriate permissions, Access Control, Sudo & PAM, Limit services, Shares, NFS, Assignment 4 Overview	Reading Week 10 Assignment 4 Quiz
11 – Mar 29th	Configuration management practices, Unix/Linux System hardening, Baselines, Enabling logging, /var/log/messages or /var/log/syslog, Baseline Standards	Reading Week 11 Quiz
12 – Apr 5th	Patching, Native patching tools, Third-party, Vulnerability scanning and remediation	Reading Week 12 Quiz
13 – Apr 12th	Sniffers, Snoop/tcpdump, Firewalls, Host based, iptables, Network based	Reading Week 13 Quiz
14 – Apr 19th	Network controls, Review findings from Pen-Testing Class	
15 – Apr 26th	Review for 2nd Test, Questions	Test 2

Caution

- Some tools and techniques discussed and used in this course should only be used on systems you personally own, or have written permission to use.
- Some of the tools used have the potential to disrupt or break computer systems.

Mindset

- Successfully Securing an operating system is not keeping every bad guy out, because some will get in.
  - It is knowing if any have gotten in
  - Limiting the next steps they can take
  - Knowing what normal is
  - Protecting key aspects of an operating system will let you know something is wrong

Mindset (cont)

- Just remember the greatest tool everyone has is your past experiences and your ability to learn from your experiences. The ability to know your strengths and weaknesses.
  - This field is ever changing and the greatest take-away is how to learn and vet what you find to secure your operating system.
  - Keeping current on what is happening with an operating system you are securing
    - Protections "how to's" for keeping users and hackers out
    - Penetration testers and their tools
    - News

In The News (1 year ago)

- Dirty Cow
  - Common Vulnerabilities and Exposures site write up: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195
  - YouTube video: https://www.youtube.com/watch?v=kEsshExn7aE
- NPR: Listen to the Avi Rubin recording for 11:36 http://www.npr.org/2017/01/13/509355546/what-happens-when-hackers-hijack-our-smart-devices
  - Avi Rubin:
    - All your device can be hacked: https://embed.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked?zone=npr2
    - Hacking our watches, fridges, and more: https://www.youtube.com/watch?v=hhh3U2Swyfg
- IOT DDoS attack
  - http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/
  - https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

In The News

- Intel Spectre & Meltdown
  - Intel admits that patches for Meltdown and Spectre are causing reboots on a wider variety of systems: https://www.geekwire.com/2018/intel-admits-patches-meltdown-spectre-causing-reboots-wider-variety-systems/
  - **FireEye Notice for CVE-2017-5754, CVE-2017-5753, and CVE-2017-5715 ("Meltdown" and "Spectre" vulnerabilities:** https://www.fireeye.com/blog/products-and-services/2018/01/fireeye-notice-for-meltdown-and-spectre-vulnerabilities.html
- Some Basic Rules for Securing Your IoT Stuff
  - https://krebsonsecurity.com/2018/01/some-basic-rules-for-securing-your-iot-stuff/

Overview of the Course (cont)

- Questions?

Computer Overview

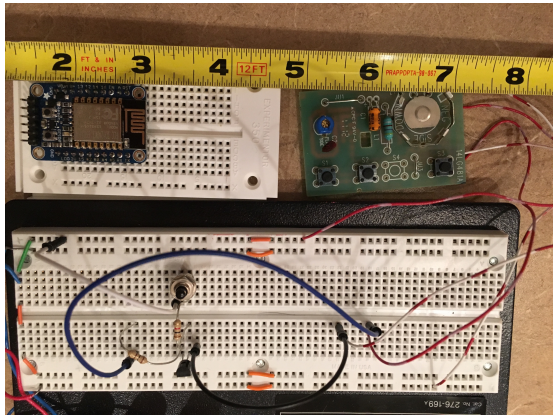
- A bit of basic review
- A bit of computer history
- What is a computer?
- What are the main parts of a computer?

A Bit of basic review

- Hardware
  - Components
  - Wire
  - Power
- Software
  - Microsoft Word
  - Chrome
  - Digital Equipment Corporation VAX/VMS - https://en.wikipedia.org/wiki/OpenVMS
  - BIOS

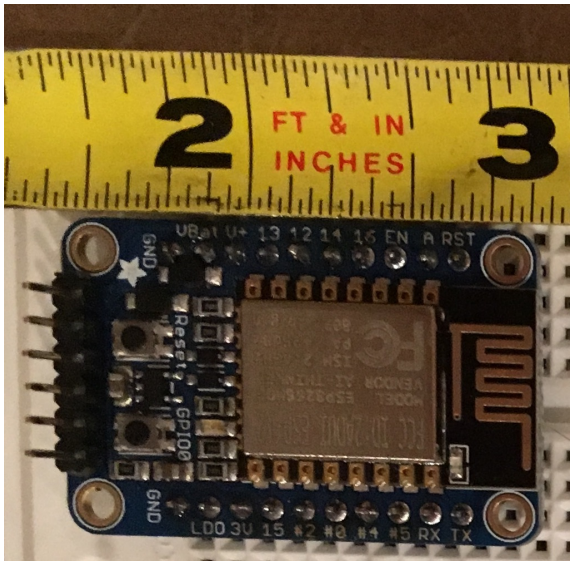
Hardware

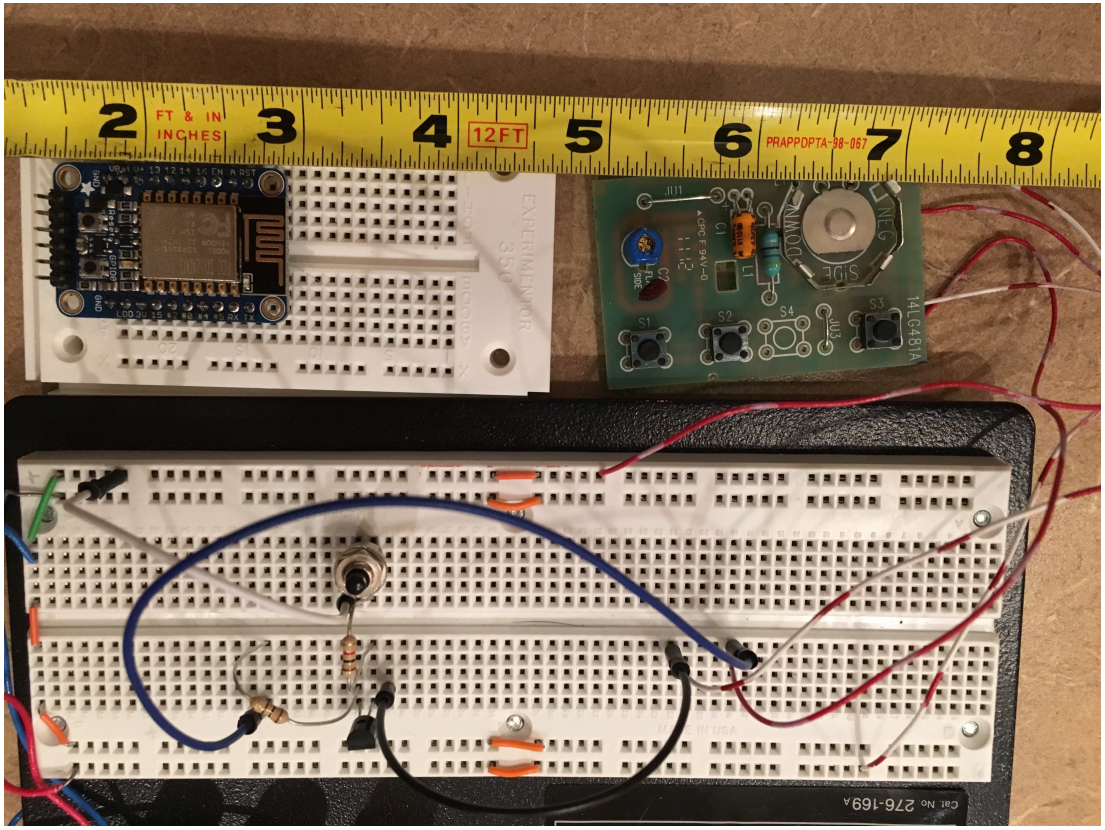
- Components
  - Transistors, CPUs, DVD – Drives, etc
- Wire
  - Circuits, Motherboards, etc
- Power
  - This one is not always so obvious, but without power your datacenter is off-line.



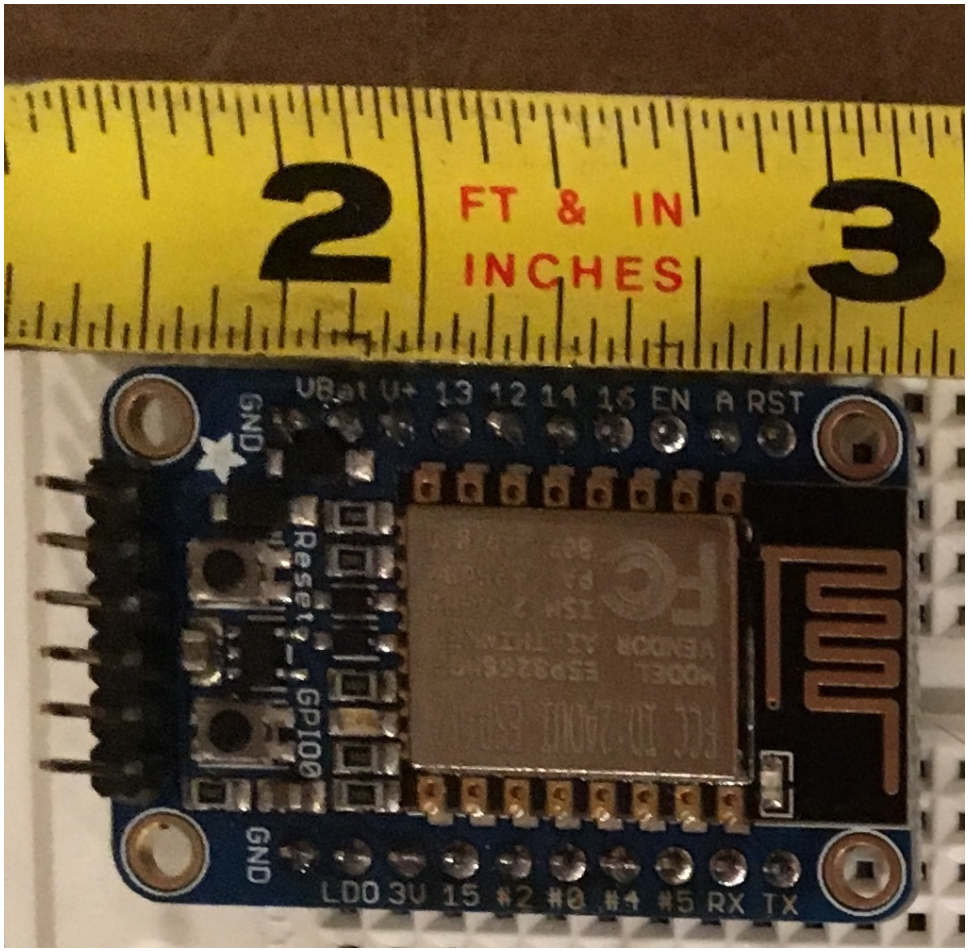
- Generally hardware is something you can touch. Sometimes touch is a relative term due to an item's physical size.

Hardware (cont)





Hardware (cont)



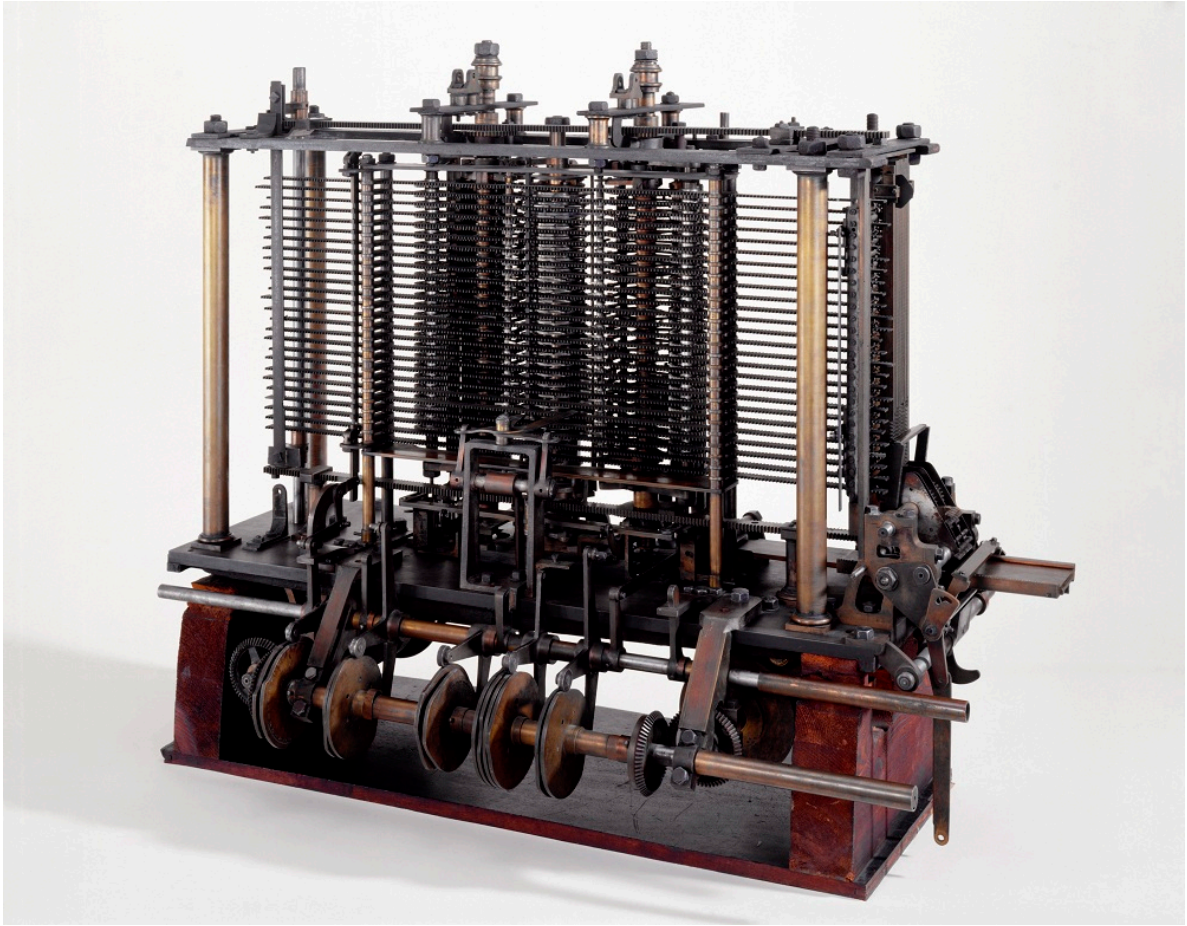
Software

- Microsoft PowerPoint
  - Presentation software that created this slide deck. Purpose built software that creates slides to present to an audience. Other examples are: Apple Keynote, OpenOffice Impress, etc.
- Chrome
  - Web-Browsing software
- Digital Equipment Corporation VAX/VMS
  - Operating system software built for general-purpose computing https://en.wikipedia.org/wiki/OpenVMS

Software (cont)

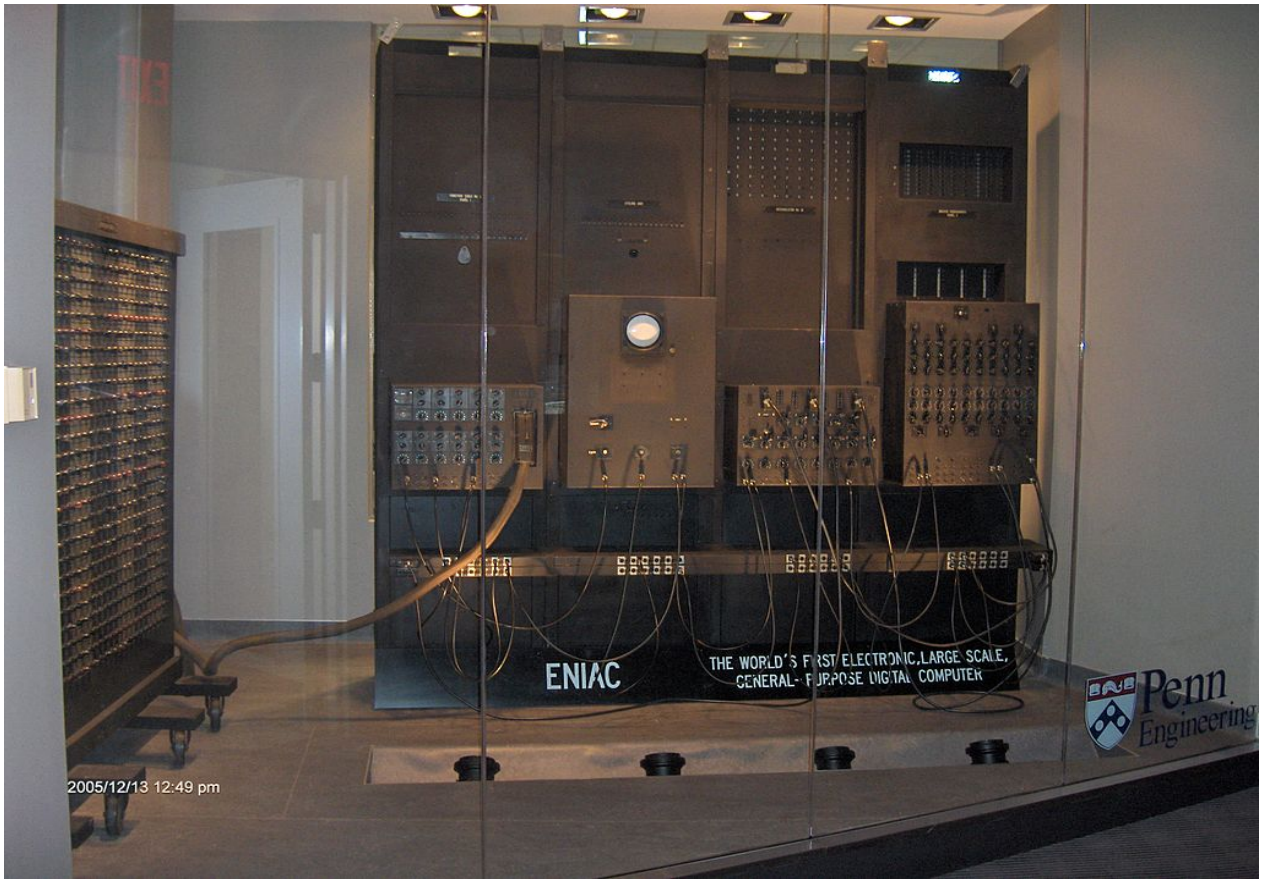
- BIOS – Basic Input Output System
  - The first software, hardware runs when powered on. The fundamental purpose of the BIOS in modern PCs is to initialize and test a system's hardware components; and to load a boot loader which allows the starting of an operating system from secondary memory. https://en.wikipedia.org/wiki/BIOS
- Generally software is something you cannot touch, lists of steps hardware uses to perform tasks. BIOS is a physical storage device once on an EEPROM chip. The storage devices has changed over the years, but it still is there to store a set of command to tell the hardware what to do.

A Bit of Computer History



http://www.livescience.com/images/i/000/032/872/original/babbage-analytical-engine-02.jpg

A Bit of Computer History (cont)



By The original uploader was TexasDex at English Wikipedia - Transferred from en.wikipedia to Commons by Andrei Stroe using CommonsHelper., CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=6557095

A Bit of Computer History (cont)

- The start of the home computer:
  - Even my sales carrier with the TRS-80 (Release date 1977)
  - Apple 2c (Release date 1984)

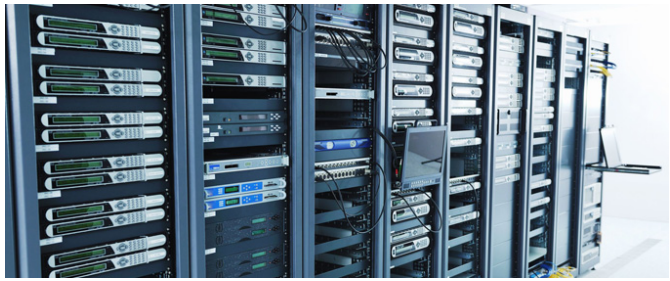
A Bit of Computer History (cont)

- OK, this one was the one I was selling; Tandy 1000 EX (Released December 1986)

By Craig Howell from San Carlos, CA, USA - Sabu with his Tandy 1000 ComputerUploaded by JohnnyMrNinja, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=16525173

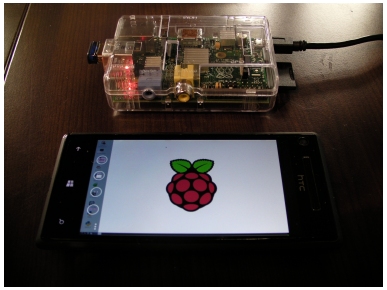
A Bit of Computer History (cont)

- Next step in computers:



A Bit of Computer History (cont)

- Modern computers:

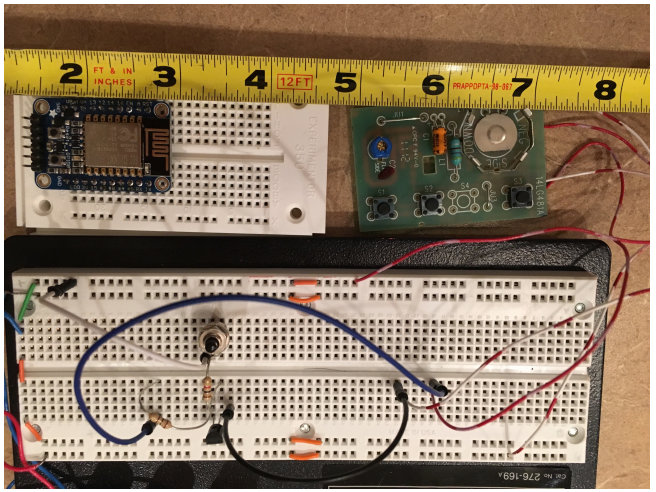


A Bit of Computer History (cont)

- Questions?

Computer Overview

- What is a computer?
  - A device that completes a task it has been programed or designed to complete based on internal or external drivers.



  - Alan Turing presents the notion of a universal machine, later called the Turing machine, capable of computing anything that is computable. The central concept of the modern computer was based on his ideas.

http://www.livescience.com/20718-computer-history.html

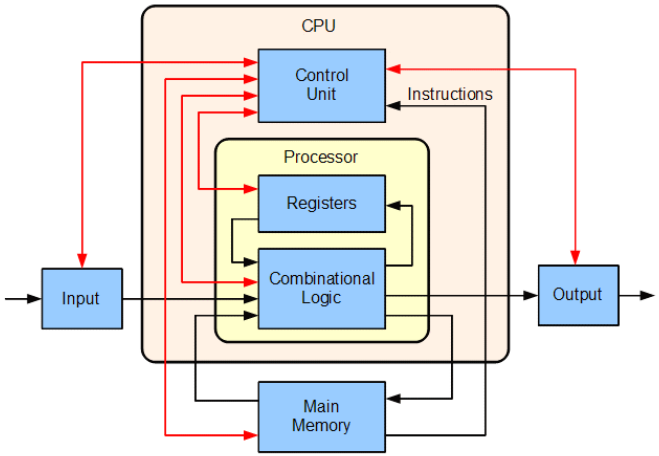
Computer Overview (cont)

- What are the main parts of a computer?
  - Motherboard – a circuit board that houses major components of a computer
    - CPU
    - RAM
    - I/O (Input/Output)
    - BIOS
  - Storage

- References
  - https://en.wikipedia.org/wiki/Computer_hardware
  - https://en.wikipedia.org/wiki/Computer

Computer Overview (cont)

- CPU – Central Processing Unit
  - A CPU is the heart of all computers. From the Dash Button to the computer we are all using
  - Attacks have been built in so if there is a vul-nerability it will be very difficult to mitigate



Computer Overview (cont)

- RAM – Random Access Memory (also known as primary storage)
  - RAM is an expensive, volatile storage device that can not maintain it's content without power. It is very fast and is the first device used by the CPU to perform tasks or store application/user data.
  - RAM is also where everything we want to secure is kept or the first way someone can get into our operating system

Computer Overview (cont)

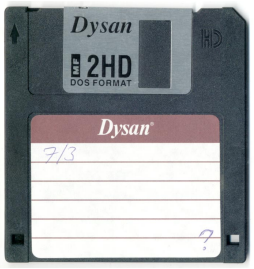
- I/O – Input/Output
  - I/O is the way a computer connects or talks to the outside world.
  - Examples are:
    - Input: Keyboard, mouse, scanner, microphone
    - Output: Printer, MIDI keyboard, speaker
  - Example of items that you don't want as an I/O device: Keyboard logger, PoisonTap

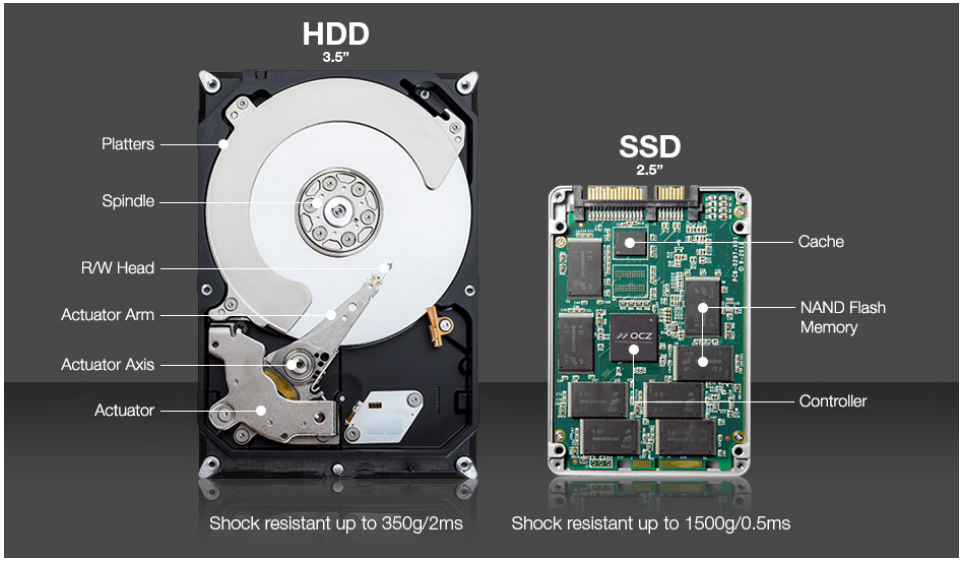
Computer Overview (cont)

- BIOS – Basic Input Output System
  - BIOS is a special type of an I/O system. Mostly read-only to allow the computer to initialize itself.
    - A number of attacks have been targeted at the ”mostly read-only” part of BIOS to infect and propagate itself to it’s neighbor via floppy drives (now general know as USB Keys)

Computer Overview (cont)

- Storage – also known as secondary storage
  - Storage is a physical device that is able to maintain computer data (application (.exe), user data (word doc), etc) if and when a computer is turned off





Computer Overview (cont)

- Questions?

Operating Systems Overview

- What is an operating system?
- What makes up an operating system?
- What are major types of operating systems?
- Examples of operating systems

Operating Systems Overview (cont)

- What is an operating system?
  - An operating system is a program (application) or set of programs that manages the physical hardware that it is running.
    - A single program is a simple representation of an OS; however the program I'm refer to might be all that there is for something like the Dash Button we talked about earlier.
    - Something like Microsoft Windows or Apple's OSx; this would be a drastic understatement. Windows 7 Pro comes on a DVD and the ISO is 3.32 GB
    - In general this main program is known as a 'kernel'; the main application/program that is the key to each operating system. Other applications help with configurations and daily tasks, but the kernel is what is being loaded by the boot loader from the BIOS of the hardware.

Operating Systems Overview (cont)

- What makes up an operating system?
  - User Space – The applications or interfaces that you see after you start the computer or log onto a computer
    - Windows you see Explorer; on a MAC you see Finder. The main application an OS presents the person interacting with the computer
  - Application Space – The program(s) installed onto an operating system
    - FireFox is a good example of an application installed on an OS to be able to browse the internet
  - Operating System – The application(s) to interface between the hardware and the user needing the hardware to complete tasks for the user
  - Hardware – The physical components CPU, Memory, Storage, Interfaces to help an OS to complete needed tasks for a user(s)

Operating Systems Overview (cont)

- What are major types of operating systems?
  - What type of OS we will focus on:
    - Single- and multi-tasking
      - Windows 3.1 – Single tasking, but faked task switch to help user better use a computer
      - Windows NT 4, on – Multi-tasking, allowing multiple applications to complete tasks without other application from starving one application's computer resources
    - Single- and multi-user
      - Windows Desktop OS, MAC OSx – Are examples of a single user OS, they can run multiple users, but in general only a single user has control of the GUI to control the computer
      - Windows Server, Unix, Mainframe, etc – Multi-user allowing one to many to be able to make effective usage of the underlying hardware to complete tasks

Operating Systems Overview (cont)

- What are major types of operating systems (cont)?
  - What type of OS we will not touch on here
    - Distributed – Computers that act as a single computer to the user; however break up tasks into small chunks given to each physical computer via a network link
    - Embedded – General examples work best here: the Dash Button, Clocks, etc
    - Real-time – A computer that can not make the user wait; best example is medical equipment

Operating Systems Overview (cont)

- Examples of operating systems
  - Microsoft Windows (2000, NT 4, Windows XP, Windows 7, Windows 2008, etc)
  - Apple OSx – a Unix based OS
  - Unix/Linux – Several different (Red-Hat, BSD, Debian, Kali a flavor of Debian)
  - IBM OS/360
  - Let's take a quick look at a couple

Operating Systems Overview (cont)

- Questions?

Hypervisor Overview

- What is a hypervisor?
- What makes up a hypervisor?
- What is the difference between a type 1 and type 2 hypervisors?

Hypervisor Overview (cont)

- What is a hypervisor?
  - A hypervisor is an application (type 2) or an OS (type 1) allowing a guest OS to be installed and executed next to another Guest OS on the same physical computer.
    - Examples:
      - Microsoft Hyper-v
      - Oracle VirtualBox
      - VMWare
        - Fusion
        - Workstation
        - Player
        - ESX/ESXi

Hypervisor Overview (cont)

- What makes up a hypervisor?
  - Hypervisor are made up of the following
    - Hardware – a computer and/or server
    - OS – not part of a type 1 hypervisor
    - VMM/Hypervisor – Virtual Machine Manager is another name for a hypervisor. This is an application or OS creating a virtual BIOS and hardware layer to the Guest OS running on top of or next to other applications
    - Guest OS – an OS running in a virtual container/environment. The guest OS mostly behaves as if it were the only OS running on the underlying hardware.

Hypervisor Overview (cont)

- What is the difference between a type 1 and type 2 hypervisor?
  - Type 1 hypervisor
    - A type 1 hypervisor is running directly on the hardware with no OS between it and the hardware it is scheduling for the Guest OS's
  - Type 2 hypervisor
    - A type 2 hypervisor is an application running on top of an OS, needing to honor all requirements of the OS it is installed. Otherwise it is very similar to a type 1 hypervisor, but resources are shared equally for applications that the user might be running next to the hypervisor.

Hypervisor Overview (cont)

- Questions?

Networking Overview

- General networking topic
- What is a Switch?
- What is a Router?
- What is a Firewall?
- What is an IDS/IPS?

Networking Overview (cont)

- General networking topics
  - DNS – Domain Name System – is a service used by computers similar to what a phone book is for our telephones. Your computer knows www.google.com, but the computer needs to talk to is via 216.58.219.206; DNS is asked for the IP address so the two computers can talk with each other.
  - DHCP – Dynamic Host Configuration Protocol – is a service to hand out IP address to a computer from a router or computer running the DHCP service. At time of access to a new network your computer request an IP address by yelling (broadcast) to the network it is trying to join. If there is a DHCP server you will get an IP address to be able to join that new network.
  - NSLookup – IP address lookup tool. Allows one to look up a name to an IP address or an IP address to a name of your default DNS server. It also allows you to point to a DNS server you have network access and ask it the same set of questions

Networking Overview (cont)

- General networking topics (cont)
  - Ipconfig/ifconfig – IP address utility to show from a command/terminal prompt the IP4 address information configured on your computer or guest OS.
  - IP Address – Internet Protocol Address is similar to what a telephone number is for our cell phones for our computers
    - Subnet Mask – Think of this as the Area Code for your Telephone Number but for your computer
    - Default Gateway – What is the phone number for the operator of my network; it allows my computer to talk to other computer networks
    - IPv4/IPv6 – There are two styles of address spaces; we will focus on IPv4 in our labs, etc.

Networking Overview (cont)

- What is a Switch?
  - A network switch is a purpose built device that allows two or more computers to talk with each other on a network. We need to look at two additional devices before we define a switch.
    - A hub is a device that links computers via a network cable and repeats what was sent to the hub and sends that same information to other computers on that network
    - A Bridge is a similar to a hub, but builds information about computers connected to it. Before it repeats network packets it looks at the information before sending it to the correct computer connected to it's ports
    - A switch is two device joined together; a hub and a bridge. This allows for less noise on the network and more directed conversations

Networking Overview (cont)

- What is a Router?
  - A network router is a device; keeping with my telephone analogy; knowing how to send phone calls (network traffic) from one area code (computer network) to another.
- What is a Firewall?
  - A network firewall is similar to a router, but has the ability to look at what conversations are being sent. Based on those conversations (ports); a user can apply rules to allow or deny those conversations to start or continue.

Networking Overview (cont)

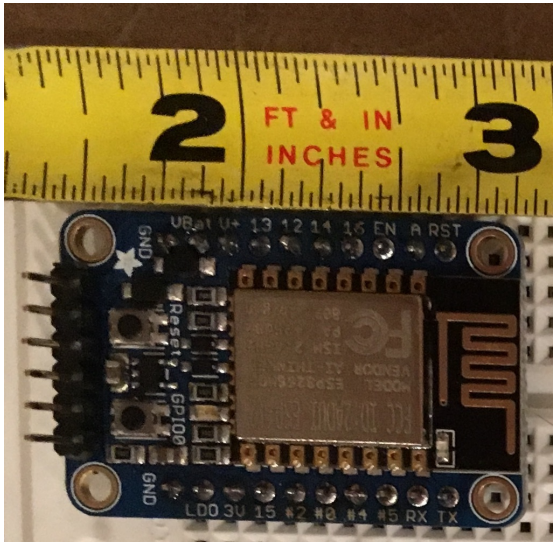
- What is an IDS/IPS?
  - A network IDS (Intrusion Detection System) is a network device that is similar to a firewall and packet capture utility, but does not change the behavior of the conversation. Based on rules it notifies companies/users via alerts that something that should not be happening
  - A network IPS (Intrusion Prevention System) is a network device similar to an IDS; however it has the ability to detect and notify, but also act upon those conversation between to devices by stopping those conversation.

Networking Overview (cont)

- Questions?

Physical Security Overview

- What is physical security?
  - Physical security is as it sounds to keep your computer(s) in control of the user or company at all times
- Why is physical security so important?
  - All computers have very simple and well documented ways to reprogram or boot to alternative devices



Physical Security Overview (cont)

- Questions?

Operating System Security Overview

- What is Operating System Security?
  - Securing an Operating System - is the process of ensuring an OS's integrity, confidentiality and availability. OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hackers intrusions.
    - Performing regular OS patching
    - Installing updated antivirus engines and software
    - Scrutinizing all incoming and outgoing network traffic via a firewall
    - Creating secure accounts and layering where accounts function
    - Baselines and/or standards

Operating System Security Overview (cont)

- Appropriate permissions
- Limit Services
- System hardening
- Baselines
- Patching
- Antivirus
- Firewalls
- Logging

Operating System Security Overview (cont)

- Appropriate Permissions
  - Think "to complete a task": The permissions to run a software installation is not the same level of access required, to view logs. Understanding of the task(s) will help drive the requirements to set appropriate permissions.
- Limit Services
  - Think "to service the clients connecting to me": A print server really only needs to authenticate users and to accept print jobs, not run every servers ever created for that OS. Note: server vendors are getting better, by turning off most services instead of starting with them on; "The easy Button" mentality. It is still something worth looking at; hackers will.

Operating System Security Overview (cont)

- System Hardening
  - Think "if I wanted to get on that computer, how would I": This can start with our last topic of "limit services", but goes into potential different ways of protections. An example is what encryptions methods will I accept on my Web-Servers, just because my computer still knows how to accepts a DES connection should I let it accept a DES connection?
- Baselines
  - Think "if I fixed this computer last week, why is it broken again": What do I care about on an OS and do I care enough to just report on it or set it back again? Remember levels of risk; preventative vs detective.

Operating System Security Overview (cont)

- Patching
  - Think “if only I wait a week; who will be getting in”: Microsoft did on really good thing for the enterprise, but a much better thing for the hacking community. What would that be?
- Antivirus
  - Think “layers; defense in-depth”: One of my favorite times is sitting at the “Genius Bar” and counting how many times I heard ”it does not need AV, we have not attack surface”. Also think of AV as a Security Yard Sign, it might only push attacks to your neighbors.

Operating System Security Overview (cont)

- Firewalls
  - Think "if I stop the connection, there is less for the next layer": This does not mean don't create the next level of protection, but it will help the next link in the chain.
- Logging
  - Think "if only I know what they did": You will never need those thousands of long entries until you don't have those logs. My home NAS was attacked and I was able to see what they were going after and how often, to re-think my choice of cleaning my NAS or do I really want to run e-mail in my house?

Operating System Security Overview (cont)

- Questions?

Next Week

- Questions from Last Week
- Hypervisors
  - Type 1 and Type 2
  - Specific Products
    - VMWare
      - Player (Windows) – Type 2
      - Workstation (Windows) – Type 2
      - Fusion (Mac) – Type 2
      - ESX/ESXi – Type 1
    - Microsoft Hyper-v – Type 1 or 2
    - Oracle VirtualBox – Type 2
  - Network Fundamentals
    - IPSecTCP/IP and Network Architecture and its impact on Operating System Security
  - Assignment 1 Overview

Citations

1. Page 9 – Wade Mackey's Advanced Penetration Testing – MIS 5212
2. Page 13 - http://www.livescience.com/images/i/000/032/872/original/babbage-analytical-engine-02.jpg
3. Page