CS3530: Computer Networks 1

Kotaro Kataoka

Week 1-1

Today’s Topic

- Orientation
- Some security
- Hands-on

CS3530 Orientation

About Instructor

- Kotaro Kataoka
  - Mail: kotaro@cse.iith.ac.in
  - Faculty cabin: C-434

- Occupation
  - Associate Professor, IIT Hyderabad
  - Senior Researcher (Visiting), SFC Research Institute, Keio University

Tentative Grading Policy

- CS3530
  - Attendance 0%
  - Assignments & Project 40%
  - Quiz & End-sem Exam 60%
  - Contribution to the class (additional)

- This policy will be automatically final if any change is not made by December 6th, 2020

Class Timings

- Mondays 4:00 PM – 5:25 PM IST
- Thursdays 2:30 PM – 3:55 PM IST

Google Classroom as a Communication Tool

- Announcement by the instructor / TA
- Q&A about the course
- Private message (only if it’s truly needed)

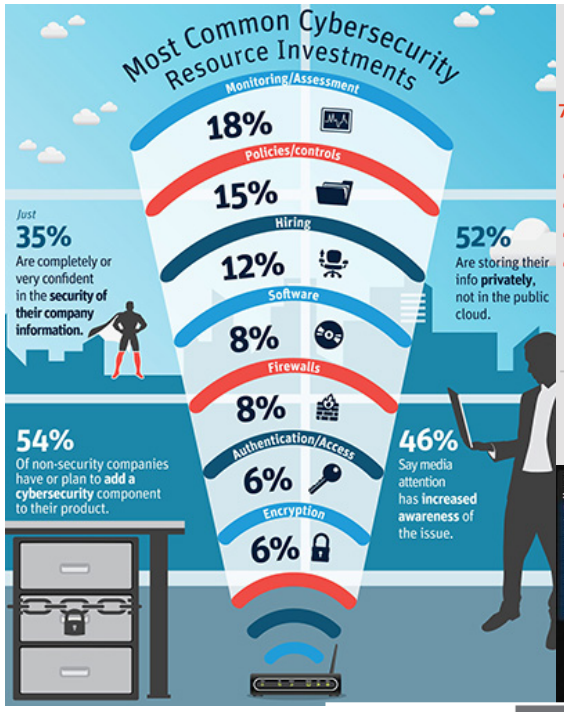
- Post your question publicly because your question may also be common or beneficial to the others.
- Avoid an email. It may not be read or replied especially when many emails are sent.

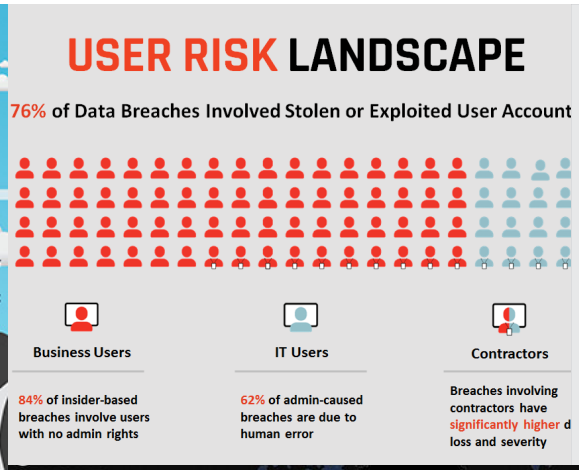
Basic Directions

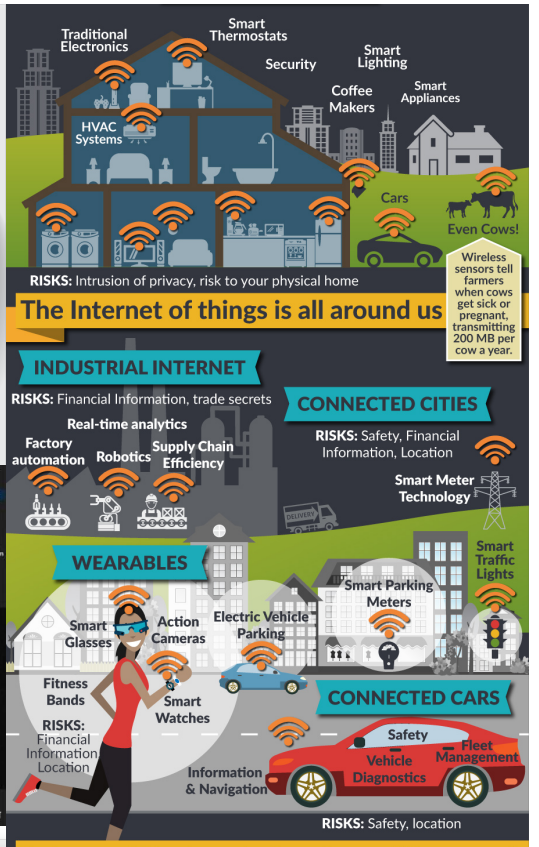
- All the classes will be video-recorded and available to the registered students
- All the course materials will be shared via the google classroom
- Assignments and Projects are group work
- Quiz/Exams will be online

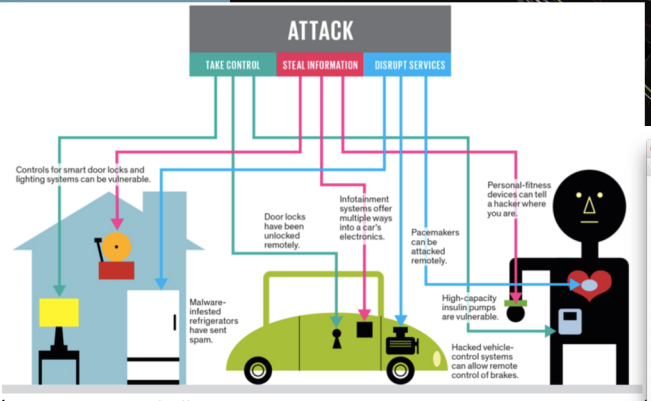
Some Part of Network Security
(Contains common slides with CS5333)

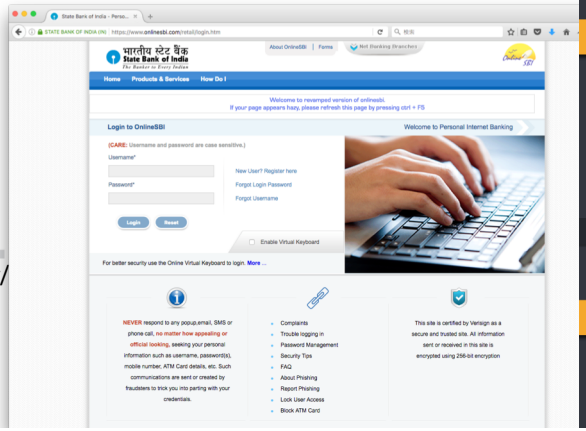
Why Security? Why NOT Security?

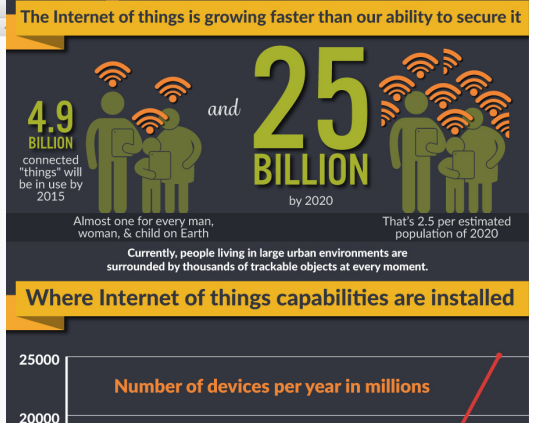










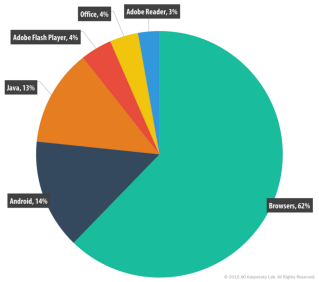


Picture Sources
https://www.pubnub.com/blog/2015-05-04-10-challenges-securing-iot-communications-iot-security/
http://www.solarwinds.com/resources/infographics/continuous-monitoring.aspx
http://www.observeit.com/blog/the-growing-risk-of-insider-threats-in-the-healthcare-industry
https://www.helpnetsecurity.com/2013/09/25/most-tech-executives-planning-for-cyber-attacks/
http://www.computersciencezone.org/security-internet-of-things/
https://www.engadget.com/2014/11/13/blizzard-confirms-world-of-warcraft-target-of-ddos-attack/

Motivations seen from Stanford's CS155 in 2015

- Awareness of the impact and motivation of attacks

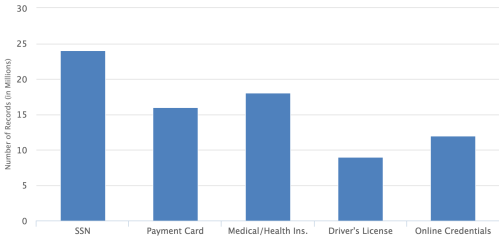
Vulnerable applications being exploited



Source: Kaspersky Security Bulletin 2015

Dan Boneh

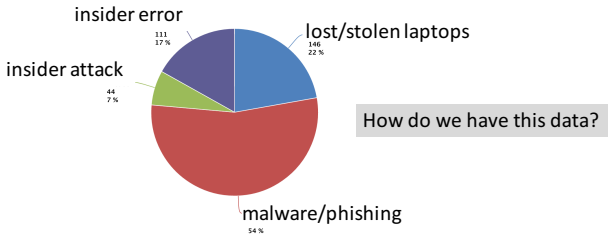
Types of data stolen (2012-2015)



Source: California breach notification report, 2015

Dan Boneh

How companies lose data



How do we have this data?

Source: California breach notification report, 2015

Dan Boneh

Marketplace for Vulnerabilities

Option 1: bug bounty programs (many)
- Google Vulnerability Reward Program: up to $20K
- Microsoft Bounty Program: up to $100K
- Mozilla Bug Bounty program: $7500
- Pwn2Own competition: $15K

Option 2:
- Zero day initiative (ZDI), iDefense: $2K – $25K

Dan Boneh

Example: Mozilla

Novel vulnerability and exploit, new form of exploitation or an exceptional vulnerability	High quality bug report with clearly exploitable critical vulnerability$_1$	High quality bug report of a critical or high vulnerability$_2$	Minimum for a high or critical vulnerability$_3$	Medium vulnerability
$10,000+	$7,500	$5,000	$3,000	$500 - $2500

Dan Boneh

Marketplace for Vulnerabilities

Option 3: black market

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Source: Andy Greenberg (Forbes, 3/23/2012)

Dan Boneh

https://crypto.stanford.edu/cs155

Attacking Systems

- Is connected to money
  - Inserting unwanted ADs
  - Stealing and selling personal / account info.
  - Controlling other's system or software to get ransom
- Disrupts important online services and life
- Damages reputation of service providers and users

DDoS Attack to Dyn in Oct. 2016 (1/2)

- Dyn: **DNS** Hosting Service
- Distributed Denial of Service Attack to Dyn affected the DNS service of major Internet Services in US including Amazon, Twitter, Reddit, Netflix and etc.

DDoS Attack to Dyn in Oct. 2016 (2/2)

- DDoS attack in a traditional mode
  - Traditional Mode forms a botnet by taking the individual computers under control through malware camouflaged as e-mail attachment, contents distributed through P2P network or websites. Then the controller sends the botnet an order to attack the target. F5, TCP SYN….
  - **IoT Nodes** formed a botnet of unsecure devices, like the estimated 100,000 Web Camera for the Dyn case. No human interaction was involved to let the devices join the botnet. Observation indicated **that their login passwords were left unsecure (most probably the weakest default)**.
- Key Findings provided by Dyn
  - The Friday October 21, 2016 attack has been analyzed as a complex & sophisticated attack, using maliciously targeted, **masked TCP and UDP traffic over port 53**.
  - Dyn confirms **Mirai botnet** as primary source of malicious attack traffic.
  - Attack generated **compounding recursive DNS retry traffic**, further exacerbating its impact.
  - Dyn is collaborating in an ongoing criminal investigation of the attack and will not speculate regarding the motivation or the identity of the attackers.

http://hub.dyn.com/dyn-blog/dyn-analysis-summary-of-friday-october-21-attack

Old and New Vulnerabilities

https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)

https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

https://www.comsoc.org/publications/magazines/ieee-internet-things-magazine

What I aim to bring into your mind (also the goals of CS5333)

- Awareness of threats and importance of security
- Understanding the security mechanisms
- Motivation of securing and defending things
- Preparedness to situations after something bad happens

Securing Your Hosts

- Account security
- Secure shell
- Network servers
- Firewall
- Keeping your system up-to-date
- Minimum requirement

Account Security

- No group and shared accounts
  - An account should correspond to only one person
- “Good” password
  - Mix alphanumeric + symbolic characters
- Password ageing
- Limit who can access to root
  - wheel group + sudo access
- Do not log on as root
  - Log on as your account, then use “**sudo**” to execute any root-privileged command
- Never leave idle console

Secure Shell

- A secure way for remote access
- Default remote access method
- More security by limiting access only from certain hosts or ranges of network
  - Using firewall or access control list
- But, sometimes a vulnerability is found
  - patch ASAP!!

SSH: Dos and Don’ts

- Use Public Key Authentication
- Use access list to limit the network that can access your server
- Don’t permit Password Authentication
- Don’t permit Root Login

- No matter where in the LAN or the Internet your SSH server is exposed, take security measures!!

Network Servers

- Disable unnecessary network servers
- Make sure that the network servers do not have vulnerabilities
  - keep up to date

Network Security

- Preventing and detecting unauthorized use of your computers and networks
- Why you have to care for network security
  - protect your data
  - prevent your network to be used as a source of attacks
- What you can do
  - secure your hosts and networks
  - keep up to date to the latest security threats

Firewall

- Block packets
- Rule based: protocol, source & destination address & port, other flags
- First match
- Example:

  0500 allow tcp from 10.0.0.0/8 to 10.1.1.1 80

  0600 deny tcp from any to 10.1.1.1 80

Securing Network with Firewall

Q: Does Firewall Provide Perfect Security?

A: No. Why?

Limitation of Firewalls

- Firewalls can be bypassed by many ways
  - Unsecure Wi-Fi APs
  - Cracked VPN connections
- Malicious traffic that matches a white listed rule can pass through the firewall
- Mobile devices get infected outside the network and come back inside

Take-away about Security

- Take a back-up of your laptop and server regularly
- Use public key authentication for remote login
- Use good password, and don’t share it
- Assume that something bad can still happen even though you are cautious, and be prepared

Preparation for the Hands-on Assignments

Should be done
by the upcoming class.