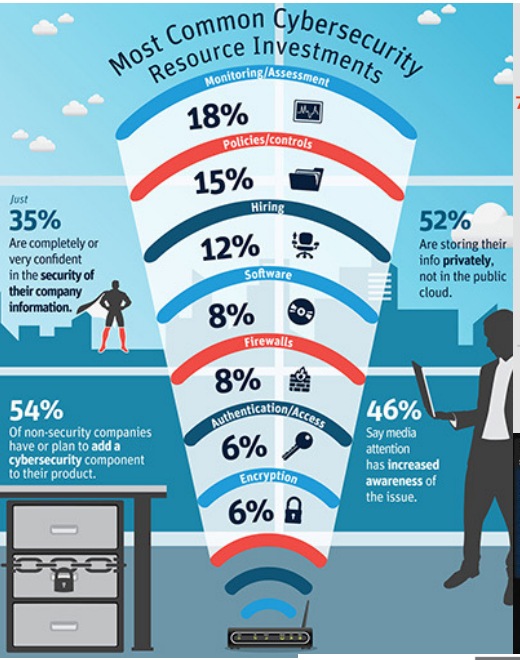
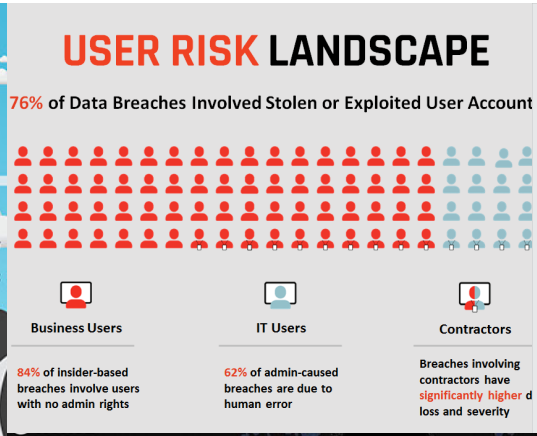
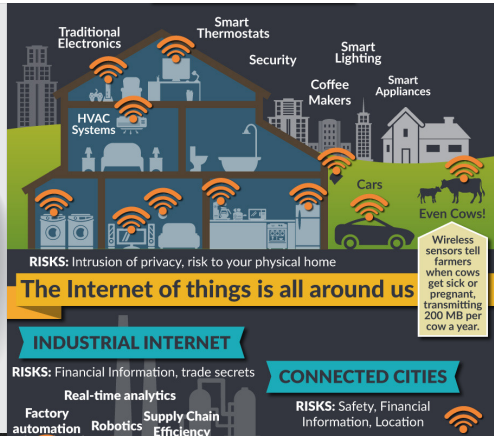
Some Parts of Network Security

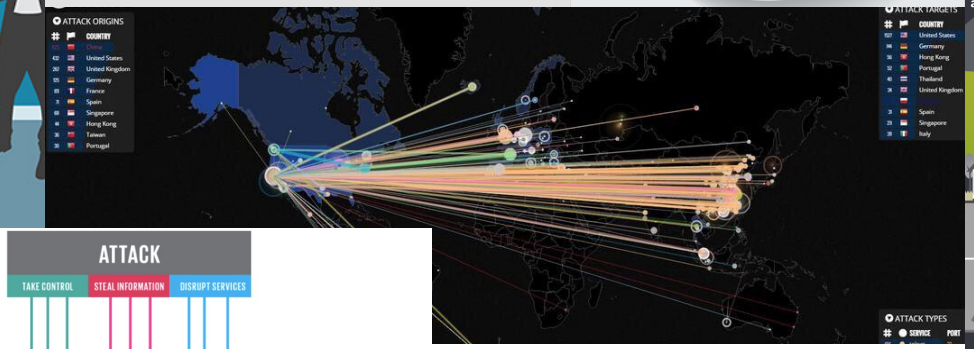
Kotaro Kataoka

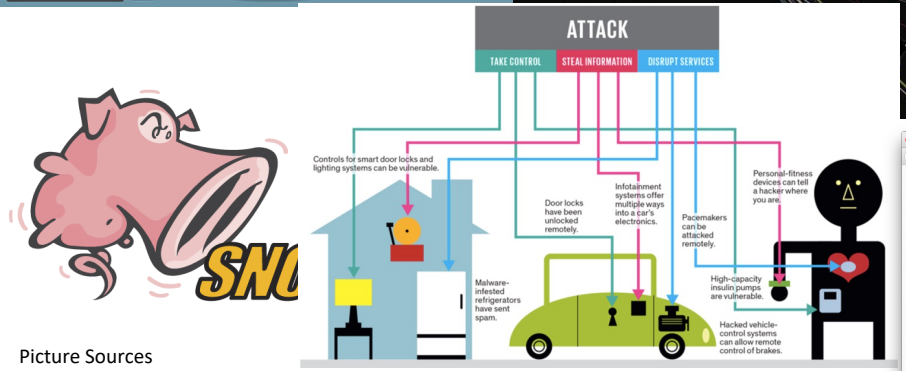
Why Security? Why NOT Security?

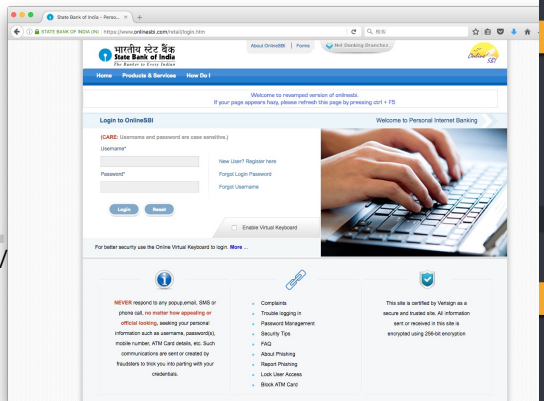












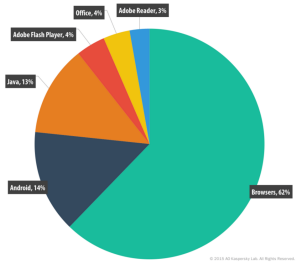
Picture Sources

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

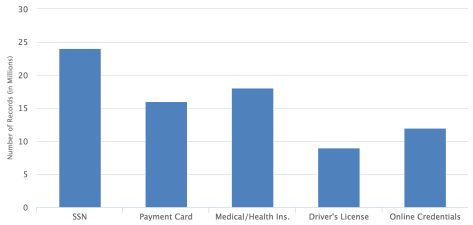
Vulnerable applications being exploited



Source: Kaspersky Security Bulletin 2015

Dan Boneh

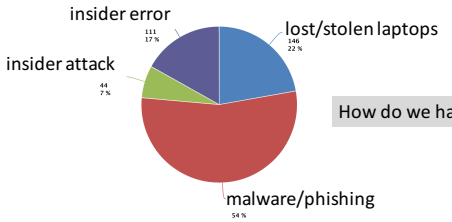
Types of data stolen (2012-2015)



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

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

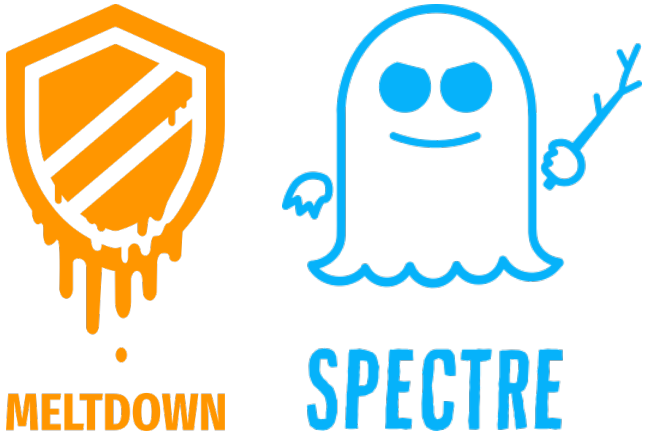
- Dyn: **DNS** Hosting Service
- Distributed Denial of Service Attack to Dyn affected the DNS service of major Internet Services in US including Amazon, Twitter, Reddit, Netflix and etc.

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 Mode** forms 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

What is Security? How do people think about it?

Security: Definition by Oxford Dictionary

- The state of **being free from danger or threat**: *'the system is designed to provide maximum security against toxic spills' 'job security'*
  - The safety of a state or organization against criminal activity such as terrorism, theft, or espionage: *'a matter of national security'*
  - Procedures followed or measures taken to ensure the security of a state or organization: *'amid tight security the presidents met in the Colombian resort'*
  - 1.3 The state of feeling safe, stable, and free from fear or anxiety: *'this man could give her the emotional security she needed'*
- A thing deposited or pledged as a guarantee of the fulfilment of an undertaking or the repayment of a loan, to be forfeited in case of default.
- often **securities** A certificate attesting credit, the ownership of stocks or bonds, or the right to ownership connected with tradable derivatives.

- **Threat**

Source: https://en.oxforddictionaries.com/definition/security

Information Security: Definition by US Government and NASA

- Federal Information Security Management Act (FISMA) defines information security as the **protection** of information and information systems from **unauthorized access**, **use**, **disclosure**, **disruption**, **modification, or destruction**.

- NASA defines information security as the **protection** of an information system's confidentiality, integrity, and availability.

NPR 2810.1A, Security of Information Technology (Revalidated with Change 1, dated May 19, 2011), May 16, 2006

National Cyber Security Policy by Government of India

- II. Mission
  To **protect** information and information infrastructure in cyberspace, build capabilities to **prevent and respond to cyber threats**, **reduce vulnerabilities** and **minimize damage from cyber incidents** through a combination of institutional structures, people, processes, technology and cooperation.

http://meity.gov.in/sites/upload_files/dit/files/National_cyber_security_policy-2013(1).pdf

Cyber Security: ITU X.1205

- 3.2.5 cybersecurity
  Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general **security objectives** comprise the following:
- **Availability**
- **Integrity, which may include authenticity and non-repudiation**
- **Confidentiality**.

X.1205, TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

Security (I) by RFC2828: Internet Security Glossary

- Measures taken to **protect** a system.
- The condition of a system that results from the **establishment and maintenance of measures to protect the system**.
- The condition of system resources **being free from unauthorized access and from unauthorized or accidental change**, **destruction**, **or loss**.

- "I" identifies a RECOMMENDED Internet definition.)

https://tools.ietf.org/html/rfc2828

$ risk (I)

- **An expectation of loss expressed as the probability** that a particular threat will exploit a particular vulnerability with a particular harmful result.

$ threat (I)

- **A potential for violation of security**, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
- (C) That is, **a threat is a possible danger that might exploit a vulnerability**. A threat can be either "**intentional**" (i.e., intelligent; e.g., an individual cracker or a criminal organization) or "**accidental**" (e.g., the possibility of a computer malfunctioning, or the possibility of an "**act of God**" such as an earthquake, a fire, or a tornado).

Why threats can't be removed?

- Systems are connected. If not connected (stand-alone), they don't make sense.
- Balancing between "the usability and implementability of security measures" and "impact of threats (must be addressed or ignorable"
- Security Assessment
  - How much do you lose if the system gets compromised? Money? Reputation?
  - Impact: Who will be affected by them
- Underestimation: You don't take necessary MINIMUM security measures!!

Security

- How to secure your host?
- How to secure our network?
  - ACL and Firewall
  - How to avoid to disturb other network?

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 + sign 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 su to root
- 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
  - use firewall
- 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

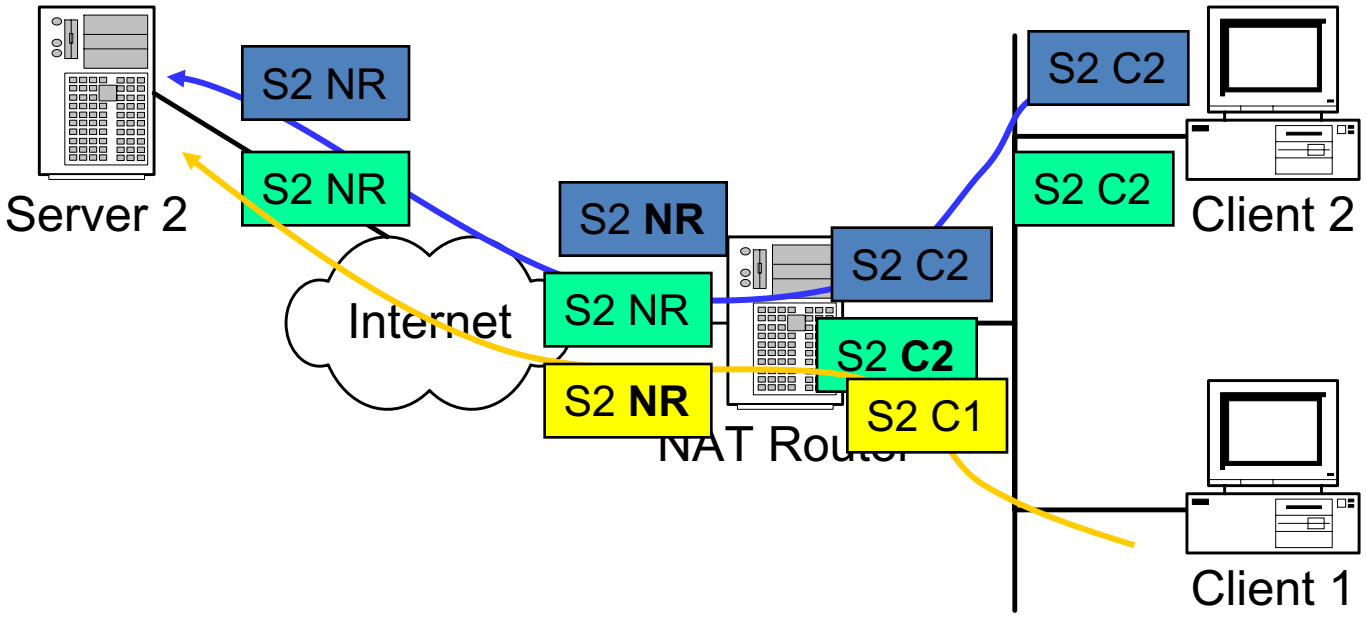
Network Servers

- 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

Network Address Translation



NAT is Dangerous

- Masquerade source address
- No log file
- If an attack is launched from behind NAT, difficult to track the culprit

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

Black List vs. White List

- Black List
  - Open access with prohibited rules
  - More freedom on network activity compared to White List
  - Malicious traffic can pass through the firewall before it gets blocked
- White List
  - Closed access with permitted rules like Intranet
  - Sometimes prohibits activity in the network unnecessarily
  - Online banking, Honey pot (experiment of petting malware-infected PCs) should go this way

Inbound Filtering and Outbound Filtering

- Inbound filtering for protecting own network from external threats
- Outbound filtering for not disturbing other networks
  - Blocking malware happening in intranet not to go out
  - Blocking, for example, open SMTP relay server (OP25B)

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

IoT Devices

- "Many" anyways
  - Now IoT Devices (LAN) < {User Devices * alpha}
  - Future **IoT Devices (Wi-Fi) >** {User Devices * beta}

- "Deploy and Forget"
  - One-time or even default (User: admin / Password: admin) configuration
  - 802.1x may not be a great help for IoT devices
  - The weakest link in the LAN security

- How can the communication legitimacy and life cycle of IoT device be maintained in the edge network?
- Deprovisioning is as important as provisioning the device
  - Device after use
  - Something is wrong (security incident)

Care about you and your things!