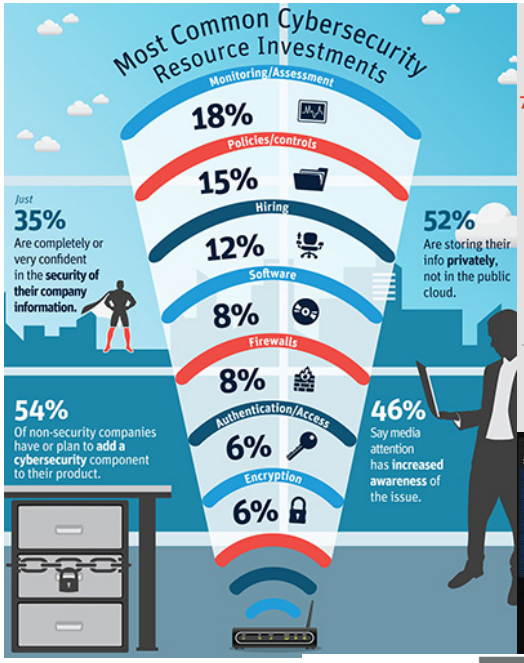
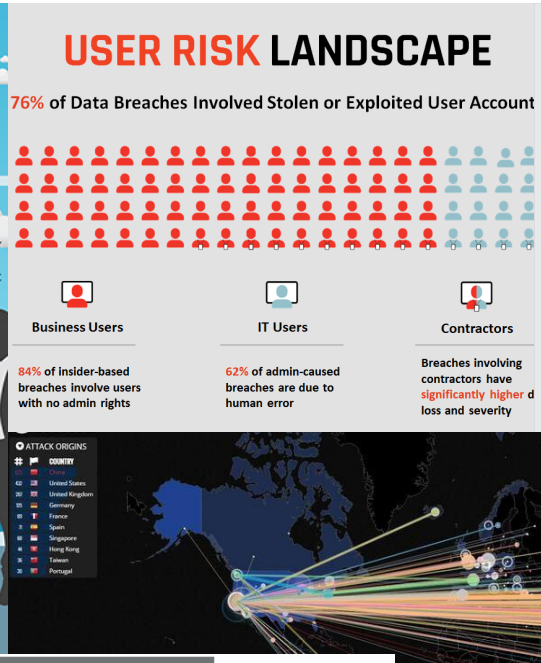
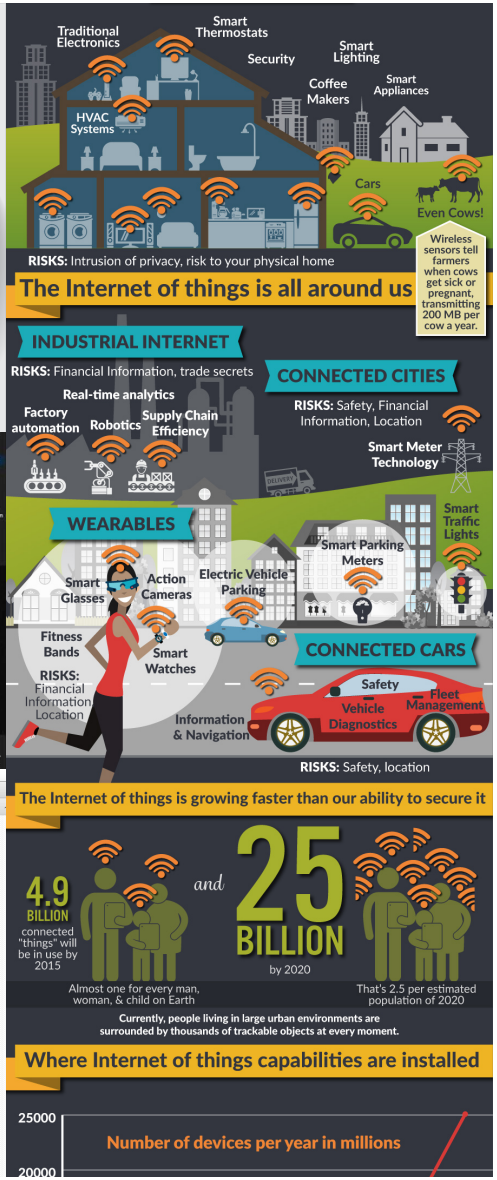
CS5333
Computer and Network Security

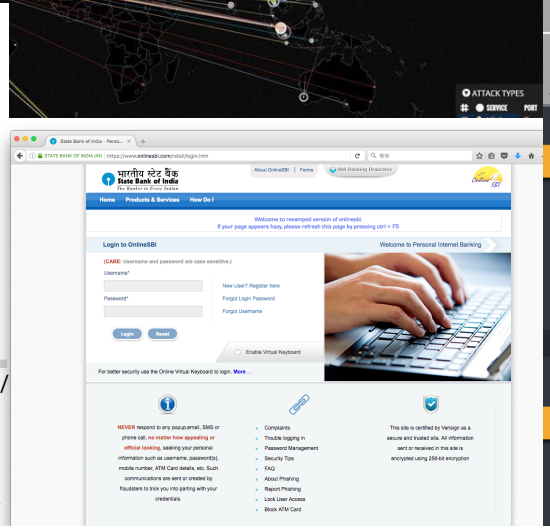
January 5th, 2018

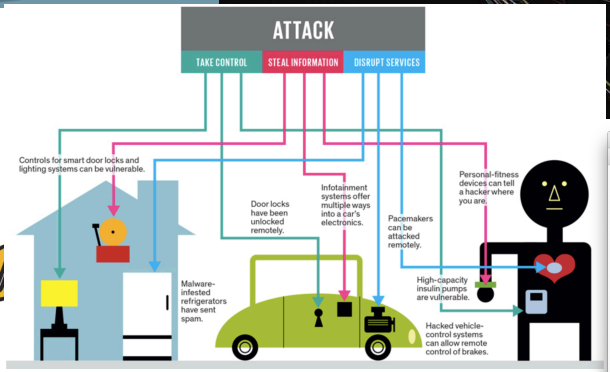
Why Security? Why NOT Security?









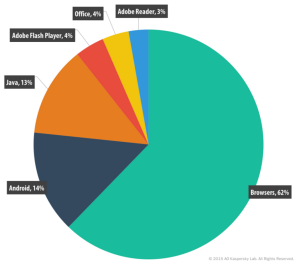


Picture Sources
https://www.pubnub.com/blog/2015-05-04-10-challenges-securing-iot-communications-iot-security/
http://www.solarwinds.com/resources/infographics/continuous-monitoring.aspx
http://www.observeit.com/blog/the-growing-risk-of-insider-threats-in-the-healthcare-industry
https://www.helpnetsecurity.com/2013/09/25/most-tech-executives-planning-for-cyber-attacks/
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

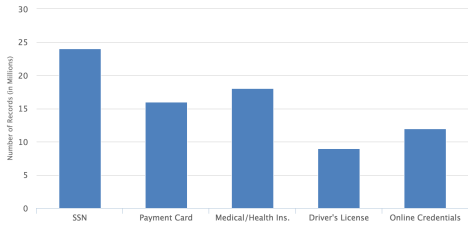
Vulnerable applications being exploited



Source: Kaspersky Security Bulletin 2015

Dan Boneh

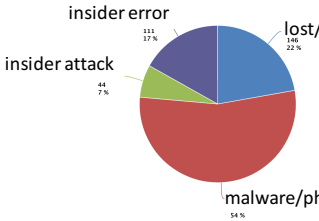
Types of data stolen (2012-2015)



Source: California breach notification report, 2015

Dan Boneh

How companies lose data



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

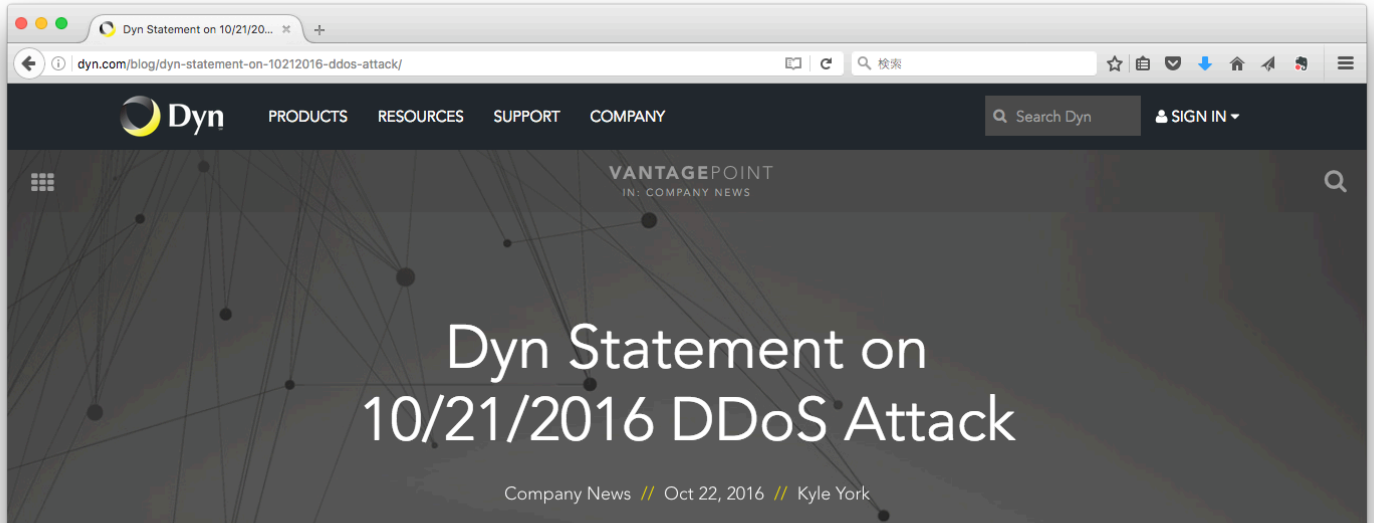
https://crypto.stanford.edu/cs155

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

Goals

- Awareness of Threats and Importance of Security
- Understanding the security mechanisms
- Motivation of Securing and Defending Things

Course Instructors and TAs

- Abhinav Kumar
- Bheemarjuna Reddy Tamma
- Kotaro Kataoka
- Sparsh Mittal
- Subrahmanyam Kalyanasundaram

- Venkatarami Reddy Ch (CS17RESCH01007)
- MRINAL AICH (CS16MTECH11009)

Course Syllabus

- Introduction/Course Plan
  - Course plan
  - Motivation/Scope of Information Security with real examples
- Principles of Cryptology
  - Brief History of Cryptology
  - Design principles of Crypto systems
  - Symmetric Cypher models & examples
  - 1-time pad
  - Recap of relevant number theory
  - Public Key Cryptography (RSA)
  - Elliptic Curve Cryptography
  - Cryptographic Hash Functions
  - Digital Signatures
  - Key Exchange Protocols
  - Public Key Infra
- Various attacks and attacking tools
  - Recap of TCP/IP
  - Different attacks
  - Attacking tools
- Hardware Security
- Internet-Security Protocols
  - SSL/TSL
  - HTTPS
  - Email Security
  - DNS Security
- Securing Wireless Access
  - Wi-Fi security
  - Cellular security
- Network Security
  - IPSec
  - Firewalls
  - VPN
- Computer System Security
  - iptables, ssh key generation, password, don't use default password, update software versions

Tentative Grading Policy

- Mid-sem Exam (25%)
- End-sem Exam (25%)
- **Hands-on Assignments** and Projects (**50%**)
  - Projects will be most probably “Pair Project”
  - Practical hands-on with clear-cut problem statement
  - Demo + presentation
- Attendance (**0%**)
- Lower Limit for Passage: 50%

Class Timings

- Mondays 12:00 PM to 1:00 PM at #317
- Tuesdays Supplemental slot
- Fridays 11:00 AM to 1:00 PM at #317

See you on Monday! Q&A?