Cyber Security Landscape and Challenges

R. Sekar
Evolution of Threats

- **Before era of modern crypto (World War II ...)**
  - Break secret messages during transmission
  - Primarily the domain of nation states
  - Modern cryptography has all but eliminated this threat

- **Modern era**
  - Focus shifts from altering messages to breaking end-systems that store and process these messages
  - Several culprits
    - Software vulnerabilities
    - Human errors
      - Carelessness or lack of awareness on the part of users
      - Operator errors
    - Emergence of cybercrime and related activities
Evolution of Modern Threats

- First generation
  - break into high-value systems (e.g., banks) through proprietary networks
  - criminal elements as well as rogue nations

- Second generation
  - Malware that spreads due to information sharing
    - Viruses and worms
  - Perpetrated by hackers as a “hobby”

- Third generation
  - Malware that spreads via the Internet
  - Email viruses and Internet worms
  - Still, no evidence of organized or criminal elements
Internet-based threats (3rd generation +)

- Initial entry: Software exploit or stealing passwords
  - Increasingly, this step needs some level of user trust
    - Spam, phishing, ...
- In some cases, esp. on servers, damage may be effected by the exploit itself
  - More common: exploit installs base for future operation
    - Bots, Trojans, spyware, ...
- Goals
  - Steal confidential information
    - Passwords, bank accounts, credit card #s, ...
  - Deface property
  - Distribute malware
4th generation: Commercialization of malware

- Hacking for profit, not just fun/fame
  - Thriving black market for exploits and other services
  - Specialization at all levels of cybercriminal enterprise
    - Exploit development, C&C software, Botnet rentals, ...
- “Bot”-centric model for cyber crime
  - Relay spam (e-mail scan, phishing)
  - Extortion (using DDoS or targeted attacks)
  - Stealing confidential data (e.g., passwords, trade secrets, IP, ...)
- Focus on stealth and obfuscation
  - Rootkits and other cloaking techniques
  - Evasion: match behavior of benign software
  - Anti-analysis techniques
    - Sophisticated packing and metamorphism
    - Detect execution within analysis environment
Current (5th?) Generation

- Major increase in targeted attacks

Source: Symantec Threat Report 2013
Current (5\textsuperscript{th}?\,) Generation

- Major increase in targeted attacks
- Advances in exploit development to overcome security improvements on recent OSes
- Sophisticated social engineering techniques
  - Gain user’s trust so that he/she may grant the level of access needed for the exploit and/or malware operation
  - Leverage social media
    - Tendency of people to share a lot of personal information
    - Tendency to trust “friends”
Spam

- Spam volumes hold steady
  - After falling from a high of 6T to about 1T/month
- Expands to social networks
  - Facebook, Twitter, Instagram, ...

Source: McAfee Threats Report: First Quarter 2013
Phishing

- New types of phishing
  - Watering hole
  - Clone phishing
  - Tabnapping

Source: Internet Security Threat Report 2013, Symantec

Source: McAfee Threats Report: First Quarter 2013
Botnets & DDOS

- Botnets now include mobile devices
  - Android botnets
    - [http://mobile.slashdot.org/story/13/01/19/0735259/android-botnet-infects-1-million-plus-phones](http://mobile.slashdot.org/story/13/01/19/0735259/android-botnet-infects-1-million-plus-phones)

- DDoS used as a diversion
Web Vulnerabilities

Scanned Websites with Vulnerabilities

- A critical vulnerability is one which, if exploited, may allow malicious code to be run without user interaction, potentially resulting in a data breach and further compromise of visitors to the affected websites.

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>77%</td>
<td>76%</td>
<td>78%</td>
</tr>
<tr>
<td></td>
<td>-1% pts</td>
<td>+2% pts</td>
<td></td>
</tr>
</tbody>
</table>

Percentage of Vulnerabilities Which Were Critical

<table>
<thead>
<tr>
<th></th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>16%</td>
<td>20%</td>
<td>15%</td>
</tr>
<tr>
<td></td>
<td>+4% pts</td>
<td>-5% pts</td>
<td></td>
</tr>
</tbody>
</table>
Zero Day Exploits ...
Ransomware ...
Data Leaks ...

- Anthem: 80,000,000
- Experian / T-mobile
- Hacking Team
- IRS
- Invest Bank
- Kromtech
- Premera
- Mozilla
- MSpy
- CarPhone Warehouse
- British Airways
- Carefirst
- AshleyMadison.com
- Adult Friend Finder
- Australian Prisons
- D&B Alimony
- Advocates Medical Group
- Kloeckner Cables
- FCA US
- Global Payments
- Florida Department of Juvenile Justice
- Medicaid
- Indiana University
- Citygroup
- Citizen Inc Whigton
- Central Region Gas & Electric
- Dropbox
- Gamigo
- Zappos: 24,000,000
- Target: 70,000,000
- Sanrio
- Slack
- IBM
- TalkTalk
- US Office of Personnel Management (2nd Breach)
- UPS
- Twitch.tv
- Ubuntu
- Uber
- Amazon
- Yahoo Japan
- HBO
- Yahoo
- Fox
- Sony Pictures
- NASA
- Leadership Council
- Verizon
- National Security Agency (NSA)
- Target
- Stealth & YourTel
- South Africa police
- NASA
- National Security Agency (NSA)
- American Heart Association
- American Red Cross
- Oracle
- E-Commerce
- Security
- Healthcare
- Technologies
- Social
- Massive American business
- UbiSoft
- "unknown"
- Mass Storage System
- Mass Surveillance
- US Office of Personnel Management
- 2/9/2009
- Latest
- 2015
- 2014
- 2013
- 2012
The Perfect Weapon: How Russian Cyberpower Invaded the U.S.

By ERIC LIPTON, DAVID E. SANGER and SCOTT SHANE  DEC. 13, 2016
Ransomware: See the 14 hospitals attacked so far in 2016

By Jessica Davis | October 05, 2016 | 12:13 PM

Ransomware attacks have been steadily increasing in the healthcare industry since the beginning of the year, and with the most recent attacks on New Jersey Spine Center, Marin Healthcare District and Urgent Care Clinic of Oxford, it doesn't look like the target placed on these providers will be shrinking anytime soon. Hospitals are recognizing the threat and are making cybersecurity a top priority. But as cybercriminals gain intelligence – and confidence – it may not be enough to make up for human error, outside vendors and other vulnerabilities.

Read the Analysis: Hollywood Presbyterian hack signals more ransomware attacks to come.
Yahoo says data stolen from 1 billion accounts

by Seth Fiegerman  @sfiegerman

December 15, 2016: 4:30 AM ET

Just when you think Yahoo’s security issues can’t get any worse, the company proves you wrong.

Yahoo (YHOO, Tech30) disclosed a new security breach on Wednesday that may have affected more than one billion accounts. The breach dates back to 2013 and is thought to be separate from a massive cybersecurity incident announced in September.

Yahoo now believes an “unauthorized third party” stole user data from more than one billion accounts in August 2013. That data may have included names, email addresses and passwords, but not financial information.