Secure Communication
(in an insecure world)

The Internet Today

Internet users worldwide:
~3 Billion
(40% of the world population)

Number of connected devices:
Over 10 Billion

eCommerce Industry:
$1.5 Trillion Globally

Online data:
Unknown, but
Google stores ~ 15 Exabytes
(15,000,000 Terabytes) of information

Approximate "weight" of the Internet
(electrons in motion)
~150g
(slightly more than a baseball)

Cybercrime

1.5 Million Cyber
Attacks every year

$781 Million in losses to
cybercrime reported to FBI in 2013

19% of U.S. Organizations
lost more than $50k to
cybercrime in 2013

7% lost more than $1 Million

47% of American Adults had
their data stolen by hackers in 2014
Poll

Which of the following do you use?

- Social media (Facebook, Twitter, etc?)
- Online banking
- Online purchases
- Cell phones
- Skype
- Online gaming
- Cloud Storage (including iCloud)

Social Media

“ Websites and applications that allow users to create and share content, or participate in social networking.”

- Facebook
- Twitter
- Snapchat
- Reddit
- YouTube
- Pinterest
- Tumblr
- LinkedIn

Social Media Risks

- Malware through links and infected ads
- Social Engineering to get private information
- Hackers obtaining sensitive information
- Foreign Intelligence elicitation via social media
- Inadvertent Release of information (OSINT)
Social Media Security

- Don’t provide information that will allow others to answer your security questions
- Restrict what personal information you share, such as job title, location, interests, family details, etc.
- Remember that you don’t control the site’s security
- Remember OPSEC
- Securely configure your social network account (http://www.cdse.edu/toolkits/cybersecurity/index.php)

Online Banking Risks

- Hacking
- Secure login
- Phishing
- Usernames/Passwords
- “Fly by Night” banks

Dimitry Belorossov, aka Rainerfox, was extradited from Spain in 2014

Online Banking Security

- Be aware of phishing attempts
- Type in the URL using https
- Change and secure passwords regularly
- Log out when done
- Be wary of online banking in public
- Install and update an antivirus and firewall
Mobile Devices

- 91% of Americans own a cell phone
- 63% of those use their phones to access the internet
- 21% only use mobile devices for internet
- 16 Million malware infections in 2014
- 25% of users have had phones lost/stolen

Zhiyun Qian (UC Riverside) demonstrated up to a 92% success rate in hacking mobile devices in a lab environment.

Mobile Device Security

- Use "https" instead of "http" whenever possible
- Use a secure password
- Enable the "find my phone" features
- Beware of fraudulent Wi-Fi networks
- Be cautious when shopping online
- Be aware of scams/ phishing
- Check privacy settings on apps
- Only install apps from trusted sources
- Delete unused apps
- Update apps/OS regularly
- Consider mobile security software

Skype

Microsoft Security Bulletin MS15-104
"Vulnerabilities in Skype for Business Server and Lync Server Could Allow Elevation of Privilege"

Public vulnerabilities in previous versions
Online Gaming Risks

• Social engineering
• Identity theft
• Account hijacking
• Malicious links
• Compromised servers/Insecure code
• Browsers risks and configuration

Online Gaming Security

• Go with reputable developers and use their official launcher
• Use anti-malware and firewall software
• Use strong passwords
• Patch software/OS
• Update browser
• Be careful about links
• Remember OPSEC
• Beware of “admin mode”

Cloud Storage

“A storage model where data is maintained, managed, and backed up remotely and made available via a network”
### 2014 iCloud Breach

2014: 500 private images of celebrities obtained via automated brute force password guessing

- Russian security researchers discussed vulnerability
- Proof of Concept script released
- Script was modified and used to compromise accounts
- Images were initially traded and sold online for bitcoin
- Later shared freely via social media

### Cloud Security

- Two-factor authentication
- Strong passwords or pass phrases
- Use a secure host (physical and personnel security controls, contractual requirements, logs, legal and regulatory requirements, etc.)
- Use encryption when possible
- Know if you’re using cloud backups

### General Security Tips

- Read up on common scams and threats
  - [http://www.ic3.gov/media/default.aspx](http://www.ic3.gov/media/default.aspx)
  - [https://www.us-cert.gov](https://www.us-cert.gov)
  - [http://www.cdse.edu](http://www.cdse.edu)
- Keep your systems and software patched and up to date
- For added security, consider encryption or a VPN
- Use strong and unique passwords for each account