Defending Cyberspace: Are We Ready?

- The current environment
- Why should we care?
- What keeps me up at night?
- The time has come
Current State

- What is the magnitude of the problem?
  - Consumers embracing mobile solutions
  - Increased reliance on the internet

- Cyber Intrusions on the Rise
  - Targeted companies among the best at security
  - Lost of intellectual property
  - Different strokes for different folks
Why is the Threat Growing?

- Hard truth: the more technology we use, the more we need to protect

- Simple Equation:
  - Growing reliance on the Internet = increased investment by malicious actors
Defining Emerging Threats

- What is an emerging threat?
- Why should we study them?
- Who are the stakeholders?
- What is at risk?
Emerging Threat Types

- Threats fall into one and/or two categories:
  - **Technological** – threats driven by new or evolving technology, standards, devices, protocols, etc.
  - **Behavioral** – threats driven by changes in attacker or target behavior, practices, operational norms, regulatory regimes, etc.
Technological Threat: Malware

- **Threat**
  - Customized malware and attacks make simple blacklisting and signature detection less effective
  - Expect to see much more on-the-fly custom generation

- **Response**
  - Reputation services provide some help, will need to get more sophisticated over time
  - Whitelisting (federated whitelisting services)
  - Trust foundations can help for the longer term
Technological Threat: 'Internet of Things'

- **Threat**
  - Increasing gadgets & gizmos on networks
  - Easy avenues for network attacks
  - Little incentive for 'thing' makers to secure them

- **Response**
  - Incentivize security with certification and liability vehicles
  - Standardize simplified protocols for 'things' to use; reduce vulnerabilities due to complexity
  - Standardize quantitative measures
Technological Threat: Mobility

**Threat:**
- More malware and attacks from mobile platforms
- Use of mobile platforms as attack surface for enterprise networks (driven by 'consumerization of IT')

**Response:**
- Addition of core security functionality to enterprise mobile platforms:
  - Data-at-rest protection, particularly for keys & credentials
  - Mobile Device Management
  - Secure communications based on standards
  - Sophisticated policy enforcement and monitoring for mobile users
Behavioral Threat: Faster Pace

**Threat:**
- All parts of attacker operation cycle accelerating
- No innate obstacles to 10-50x speed-up
- Malicious activity coordination getting tighter

**Response:**
- Automate! Drive all defensive actions at net speed
- Use hardened/layered architectures to slow attack cycles
- Standardize defensive info exchange to gain speed
Behavioral Threat: Lifecycle Scope

**Threat:**
- Attackers backing into earlier stages of security lifecycle to improve scale and utility
- Supply-chain attacks

**Response:**
- Very difficult: hardening supply chains is a very hard problem
- Software: greater use of signed software should help
- Hardware: still in research stage. Some benefit from anti-counterfeiting efforts
- Layered security
Behavior Threat: Application Focus

**Threat:**
- Initial attacks increasingly focused on applications
- Expect to see increase in breadth of apps targeted
- App developers may not have resources to harden their products

**Response:**
- Make it easier for developers to write secure apps
- Make it harder for compromised app to inflict harm across entire platform
Behavioral Threat: Counter-attack Culture

**Threat:**
- Assertions from some 'advocates' that victims can and should counter-attack
- Opens huge can of worms for mis-direction, lawlessness, etc

**Response:**
- Education about difficulties of attribution and liability issues
- Clearer laws and international norms
- Partnerships across sectors and segments
Behavioral Threat: Nation-State Actors

**Threat:**
- Nation-state level actors exploiting very broad spectrum of non-traditional targets
- Assymetry of national resources focused on commercial, academic, even NGO targets

**Response:**
- Unity of effort and visibility toward common defense
- Sharing of actionable intrusion information across sectors (eventually, at machine speed)
- Establishment of deterrents and international norms
Future of Cyber Defense

- Shift towards “stronger” commercial solutions
- Public and Private Partnerships in action
- Sharing information in real time
- Laws, policies, standards and norms
- Building the cyber workforce

Today
2014
Conclusions

- Broad spectrum of new and growing threats
- Effective response strategies must target both attacker and defender motivations
- Most effective responses cross lines between government, industry, infrastructure, etc.
- Unity of effort will be essential to success
Forward. Thinking.
Technological Threat: IPv6

- **Threat**
  - New attack, exploitation, stealth, and exfiltration techniques based on IPv6 features
  - Lack of IPv6 experience in defensive workforce

- **Response**
  - Training for defenders and IT operators
  - Coverage of IPv6 in colleges and competitions
  - Selective and measured introduction of IPv6 into enterprise operations

Welcome to IPv6 Training
- IPv6 Programming
- IPv6 in the Internet
- IPv6 Exploitation and Defense
Technological Threat: IPv6

What is IPv6 and why should we care?

- Next generation protocol for the Internet
- Defines how data is sent from one computer to another
- Contains addressing and control information to route packets
- Why a future move to IPv6?:
  - The last IPv4 blocks have been distributed
  - Increased address space
  - More efficient routing
  - Better mobility support
What about the Cloud?

- **Threats:**
  - Concentration of vulnerability/risk at cloud providers
  - Attackers co-opting cloud resources
  - Attackers purchasing cloud resources

- **Response:**
  - Standards and best practices for continuous monitoring and defense in cloud environments
  - Extension of trust foundations into cloud platforms
  - More consistent legal regimes and international norms
  - Means for extending reputation into cloud-based services
Security in the Cloud

- Separate accreditation of cloud infrastructure and cloud-borne mission applications
- Flexible accreditation for cloud infrastructure
- Accreditation based on continuous monitoring
- Cloud Security Services