Microsoft

Cyberspace: Enabling Trustworthy and Autonomous Agency

Brian A. LaMacchia, Ph.D.
Distinguished Engineer
Microsoft Research Security & Cryptography

Case Study: Cybersecurity in the Era of Cloud and Edge Computing

- Shift to “cloud + edge” computing model fundamentally changes how we think about securing enterprises and personal computing devices.
  - “Edge” devices can be desktops, mobile, IoT, vehicles, etc.
- Security boundaries are changing. We used to draw boundaries around a set of resources and say "inside is trusted, outside isn’t”.
  - We enforced these boundaries with various isolation techniques (e.g. firewalls, network segmentation, deep packet inspection, etc.)
- Now we must assume an edge device lives on the public network and is constantly communicating with cloud-based resources.
  - The rollout of 5G wireless will make this true for even more devices.
  - Even small, local IoT devices will be cloud-connected for analytics.

Quantifying Today's Threat Landscape

Some January 2019 numbers from Microsoft's own operations:

- **630 billion authentications** analyzed per month
- **470 billion emails analyzed** for malware and malicious sites monthly
- **1.2 billion Windows devices** updated monthly
- **$1 billion** spent on security annually
- **100 million** business and consumer accounts protected from cyberattacks daily
  - On the average day we see **30 million attempts** to log-in to Microsoft accounts by adversaries
- We analyze **6.5 trillion signals each day** for potential malicious activity in email, on desktops and laptops, and in the cloud applications that people log into for work and for personal life

Key Challenges we hear (from CISOs, SecOps,)

- **Estate Complexity:** With the transition to mobile, IoT and other Edge devices, what exactly is connected to my digital estate at any time?
- **Not enough security pros:** Today's 1+ million deficit of cybersecurity workers will worsen to 3.5 million by 2021.
  - Companies are grappling with how to recruit and train people as well as incorporate AI/ML-based solutions to enhance the speed and scale of human expertise.
- **AI/ML:** Machine learning can have has tremendous benefits for security but is not a silver bullet for all our security challenges.
  - Example: at Microsoft we use ML to help our 3,500 analysts vet those 6.5 trillion incoming security signals we get daily
  - Customers are evaluating commercial pitches closely and they realize that it takes massive sets of data to train AI well.

Challenges and Opportunities

- Economic incentives for malicious activity
  - Nation-state level actors, monetization of criminal activity (e.g. ransomware)
- Involving non-security pros in security decisions
  - Traditionally the security industry has not done a good job at communicating security policy options to “non-IT pros” and involving them in the decision-making process.
  - Opportunity to improve by developing new security models that include AI/ML assistance (if we can get the training data)
- Usable security is still an unsolved problem with lots of active research
  - 20 years after Whitten and Tygar’s “Why Johnny can’t encrypt” and we’ve made little progress.
- The coming transition to post-quantum cryptography
  - We are creating more legacy problems with every non-crypto-agile device we