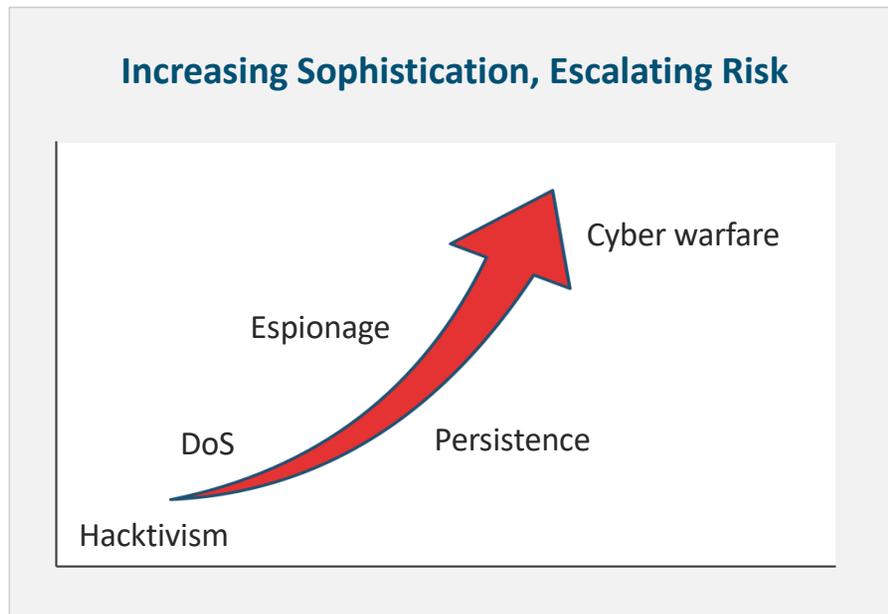




Cisco Trustworthy Systems

Chirag Shroff, Principal Engineer
Cisco Security and Trust Organization
September 10, 2019

Evolution of Cyber Threats



Cyber Trends

- Profit motive
- Nation states and crime syndicates
- Increasing attack sophistication
 - Persistence
 - Subvert the network infrastructure



Eavesdrop



Steal or
Manipulate Data



Launch Lateral
Attacks

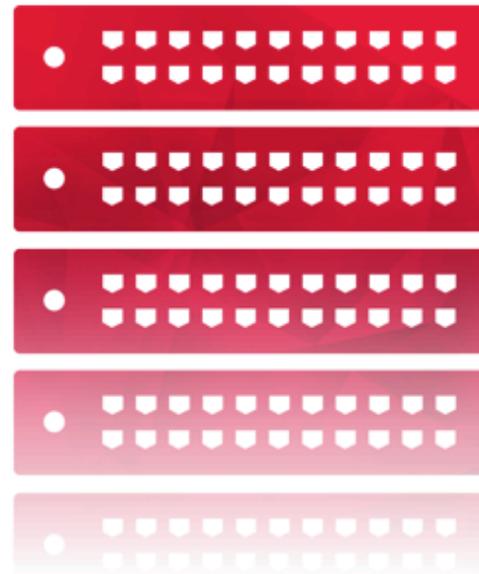
Need verification that the network is genuine, uncompromised, and operating as intended

Risks of Aging Infrastructure

92% Of devices surveyed across the Internet were running known vulnerabilities with an average of 26 each

31% Of devices surveyed across the Internet were End of Service

5% Of devices surveyed across the Internet were End of Life



- Aging, unpatched infrastructure is a leading cause of vulnerabilities and data breaches
- Counterfeit, grey market, and EOL/EOS network device pose unacceptable risks

Network Devices are Prime Targets for Cyberattack

Alert TA16-250A

The Increasing Threat to **Network Infrastructure Devices**



*“For several years now, vulnerable network devices have been the **attack-vector of choice** and one of the **most effective techniques** for sophisticated hackers...”*

US-CERT Recommendations

Harden Network Devices

- Apply software updates/patches
- Restrict physical access
- Robust password and encryption policies

Validate Integrity of Hardware and Software

- Buy from Authorized channel; **Avoid grey market**
- **Inspect** for **hardware tampering**
- **Verify** the **software** has **not** been **modified**
- Implement **Supply Chain security**

Cisco's response to
escalating threats...

Embedded Security

Trustworthy Solutions

Protection Against Today's Threats

Security Embedded in Cisco Hardware and Software by Design



Enhance Security,
Minimize Risk



Visibility into
Product Integrity



Faster Identification of
Threats

Security Embedded in Hardware

Device Identity



X.509 cert installed in hardware provides secure device identity

Root of Trust



Secure boot anchored in hardware checks device authenticity and integrity

Custom ASICs



Custom ASICs offload CPU and enable traffic inspection and analytics

Challenges

- Securing WIFI AP and IP Phones to core routers that run national infrastructure
 - Cost and availability of built in security features from component vendors all over the place
 - Adhere to principals but need to maintain flexibility in implementations
- Stand alone security posture
 - Network devices are often the first ones to come up
 - Remote deployment brings unique challenges (cant rely on physical possession to recover)
 - Can't rely solely on external entities for system integrity
- Identity of components is a huge problem
 - New standards like DICE may help in future but not there yet
 - It will take time before component vendors get this right
 - improper protection of secrets, side channel resistance, lack of crypto knowledge
 - Focus on critical components first and then expand



Cisco Trust Center: trust.cisco.com