

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: GRC-T10

THE SUPPLY CHAIN THREAT



#RSAC

Dickie George

Senior Advisor for Cyber Security
Johns Hopkins University Applied Physics Laboratory

Threat Adversary Model



- Resources
- Capabilities
- Intent
- Motivation
- Risk Aversion
- Access

The Past



- US Government drove technology
- Moore's Law
- Example: VINSON
- Cold War: Espionage and Technology (space & bombs)



Examples from the Past



- Gunman; cables; embassies, walker; chair rail; great seal, hotel in Moscow—copying machine
- We played by the rules
- On the order of one or two a decade
- Expensive
- Targeted
- Narrow



Newer



- Open source randomizer
- Security product at NSA
- Commercial product-domestic/export code
- Firewall
- Companies don't support; don't want to be liable

- International
- All countries spy
- Access—makes supply chain easy
- Broad, wide, everyone can be a target
- No risk aversion

- New intent/motivation
- One a month rather than one a decade



Apply



- Be careful of trust
- “Made in USA” doesn’t mean made in USA
- All based on trust
- Be wary!
- Check reputation!
- Report problems!
- Watch for malicious activity

