Supply Chain Risk Management

Larry Wagoner
NSA SCRM SPO
Goals of a good supply chain

Build it well
Ship it well
Use it well
Goals of a good supply chain

- Build it well
  - Very little influence in a globalized COTS market
- Ship it well
  - Only some influence
- Use it well
  - Reasonably good influence
Maturing of the Science of Securing the Supply Chain

- Business Case
- Measurements
- Standards and Architectures
- Scientific Classification
- Guidance
- Common Terminology/Community Building
- Realization as a Discipline
- Initial (ad-hoc)
Our Focus

- Studies (and common sense) show that errors are most expensive to fix later rather than earlier in the software lifecycle
- Many current efforts on evaluations already
  - Very difficult, no magic bullets, unlikely to be total solution
  - Can’t evaluate ourselves out of this problem
- Concentrate on building it better
  - Additional effect is to make it easier to evaluate
ISO/IEC JTC1/SC22 Working Group on Programming Language Vulnerabilities

• Comparative guidance spanning multiple programming languages
• 53 programming types of programming language vulnerabilities
  – ex. Undefined Behavior, String Termination, Floating Point Arithmetic
• 19 application vulnerabilities
  – ex. Adherence to Least Privilege, Resource Exhaustion, Path Traversal
• Published September 2010
ISO/IEC JTC1/SC22 Working Group on Programming Language Vulnerabilities

• New version under development
• Language annexes
  – Description of vulnerability
  – Avoiding the vulnerability or mitigating its effects
OWASP Enterprise Security API (ESAPI)

• Free, open source security control library
• Quicker and easier for programmers to implement needed controls
• Security controls
  – ex. input validation, logging, authorization, output encoding, etc.
• Multiple Languages
  – Java, PHP, Python, Ruby
• www.owasp.org
Open Group Trusted Technology Provider Framework (TTPF)

- Framework that describes supply chain and risk management best practices
- Industry wide effort to identify current best practices and processes for
  - Secure and trusted development
  - Manufacture
  - Delivery
  - Product assurance
- www.opengroup.org
Digital Code Tagging/Signing

- ISO/IEC WG23 NWIP
  - Digital code signing

- ISO/IEC SC7 TagVault.org
  - Non-profit formed under IEEE ISTO structure
  - Software Identification Tag Standard
  - Software Entitlement Tag Standard
Other focus areas

• Improved tools
• Tool methodology
• Criticality analysis
Thank you!