Towards A Comprehensive Study of Supply Chain Integrity

Matt Broda	Microsoft
Sławomir Górniak	ENISA
Christian W. Probst	TU Denmark
Claire Vishik	Intel

TIPS 2009, Honolulu, 4th December 2009

European Network Information and Security Agency

- Centre of excellence on information security issues
- At the disposal of MSs and EU bodies
- Has the mandate to express its technical opinion in international forums
- Working on the basis of Multiannual Thematic Programmes

Resilience

The ability of a system
to provide & maintain an
acceptable level of service
in face of faults
(unintentional, intentional, or naturally caused)
affecting normal operation

PROCENT

- Priorities of research on current and emerging network trends
- Assessment of the impact of new technologies
- Identification of need for research
- Areas of biggest interest
  - Cloud Computing
  - Real-Time Detection and Diagnosis Systems
  - Future Wireless Networks
  - Sensor Networks
  - Integrity of Supply Chain

Integrity of supply chain

- ICT products today
- Integrity
  - Consistency of actions, values, methods,..
  - Ability of a system to achieve its goals
  - Notion related to security and trust
- EU approach – ARECI study

  Need for *"focused program to promote the integrity of supply chains used to build network systems, and promote the implementation of innovative trust concepts to support the operation of these systems"*

Current situation

- Outsourcing in communication networks
- Convergence of services
- Highly interfaced, complex networks
- Multiple vendors – difficult recovery
- Current business model
- Surface of attacks

Challenges

- Complex nature of supply chain
- Lack of common guidelines
- Absence of tools, processes, and controls
- Ineffective methods for end users
- Detection of counterfeiting hardly possible
- Lack of coordinated approaches
- Absence of common business model

Understanding the risks

- SCI checks in the “early days” and today
- “Supply chain attacks”
  - Insertion of malicious code
  - Creation of counterfeited elements
- Questionable practices
  - Purchasing from unknown/known(!) sources
  - Purchasing with focus only on costs
  - Inappropriate disposal of used elements
  - Lack of controls beyond the life cycle
  - Intermixing elements without traceability

Managing the risks

- Clear definition of requirements
- Methodologies for evaluation
- Ability to assess provenance
- Measures to protect integrity

Evaluation framework – Common Criteria

- CC Recognition Agreement
- Theory: coverage of the whole life cycle
- Constraints
  - Complexity
  - Product-orientation, revalidation needed after every change
  - “Open” standard
- Necessary adaptations:
  - Developing verification approaches
  - Adapting generic methodologies
  - Develop methodologies for end user

Opportunities for research

- Improved and innovative trust models
- Evaluation and integrity checking techniques
- Study of good practices
- Solutions to detect and prevent counterfeiting / overproduction
- New approaches to security assurance
- Inventory/configuration control and maintenance
- Approaches for assessing policy needs on the global scale

Conclusions

- Integrity of the supply chain is crucial for trust and confidence in the infrastructure
- Area is ready for new research challenges
- Subject should be treated on international level

Thank You!

Matt Broda	matt.broda@microsoft.com
Sławomir Górniak	slawomir.gorniak@enisa.europa.eu
Christian W. Probst	probst@imm.dtu.dk
Claire Vishik	claire.vishik@intel.com

- References
  - http://www.enisa.europa.eu/sta
  - http://www.youtube.com/user/enisasta