IEEE CQR 2009
May 11-14, 2008
Naples, FL
USA

Information and Communications Technology (ICT) Supply Chain Integrity

May 14 2009

Karl Rauscher, Bell Labs Network Reliability & Security Office, Alcatel-Lucent

Thomas la Porta

Patrick McDaniel, Computer Science Engineering

Jun Shu, Supply Chain and Information Systems, Penn State University

Agenda

- Terminologies and Background
- Problem
- Current Solutions
- Our Objectives
- Possible Directions
- What's Next?

Terminologies and Background

- What is the supply chain of information and communications technology?
  - Supply Chains in General
  - Supply Chains of ICT
  - Supply Chain of ICT in a Security Context
  - Supply Chain of ICT in a National Security Context
- What is integrity in the security context?
  - As secure as it needs to be
  - As secure as you feel comfortable with
  - As secure as public confidence in the integrity of the supply chain and its final products and services
    - Encompassing vulnerability, threat, and counter-measures

Problem Statement

- The lack of *structure* and *methods* for measuring the integrity of ICT supply chains is a chief failing of the current state of critical infrastructure protection.
  - As a result, society is exposed to quality control limitations that could result in unintentionally or intentionally catastrophic lost of critical infrastructure protection.
  - Given society's profound level of dependence on ICT infrastructure, the level of uncertainty is unacceptable to shareholders.

Current Solutions

- Project Management
- Software Engineering
  - Software Reliability
  - Software Quality Control
- Reliability Theory
- High Level Guidance at the Principle Level
  - Example: FCC NRIC Best Practice Guidance

All of which are soft, *ad hoc*, and inconsistent for aggregation and comparison purposes.

Objective

- To provide a structure and methods for measuring the integrity of ICT supply chains so that senior decision makers can have a grasp of the state of the ICT supply chains.
  - Example: a color alarm system (Green, Orange, Red, etc.)
  - The result can enhance quality control capabilities that could prevent or ameliorate the impact of otherwise catastrophic loss of ICT infrastructure functionality.
  - The result can provide guidance to senior decision makers that will enable them to improve ICT infrastructure reliability and security

Possible Directions

- The 8i (Eight Ingredient) Framework
  - Power, Environment, Software, Hardware, Network, Payload, Policy, and Human
- Threats versus Intrinsic Vulnerabilities
- Multi-level Aggregation
- Supply Chain Progress Monitoring
- Cost of Security
  - Congestion-based pricing

What's Next?

- Join our project.
- Start your own project.
- The Hawaii Workshop, Dec. 4, 2009. Come and participate in the discussion.