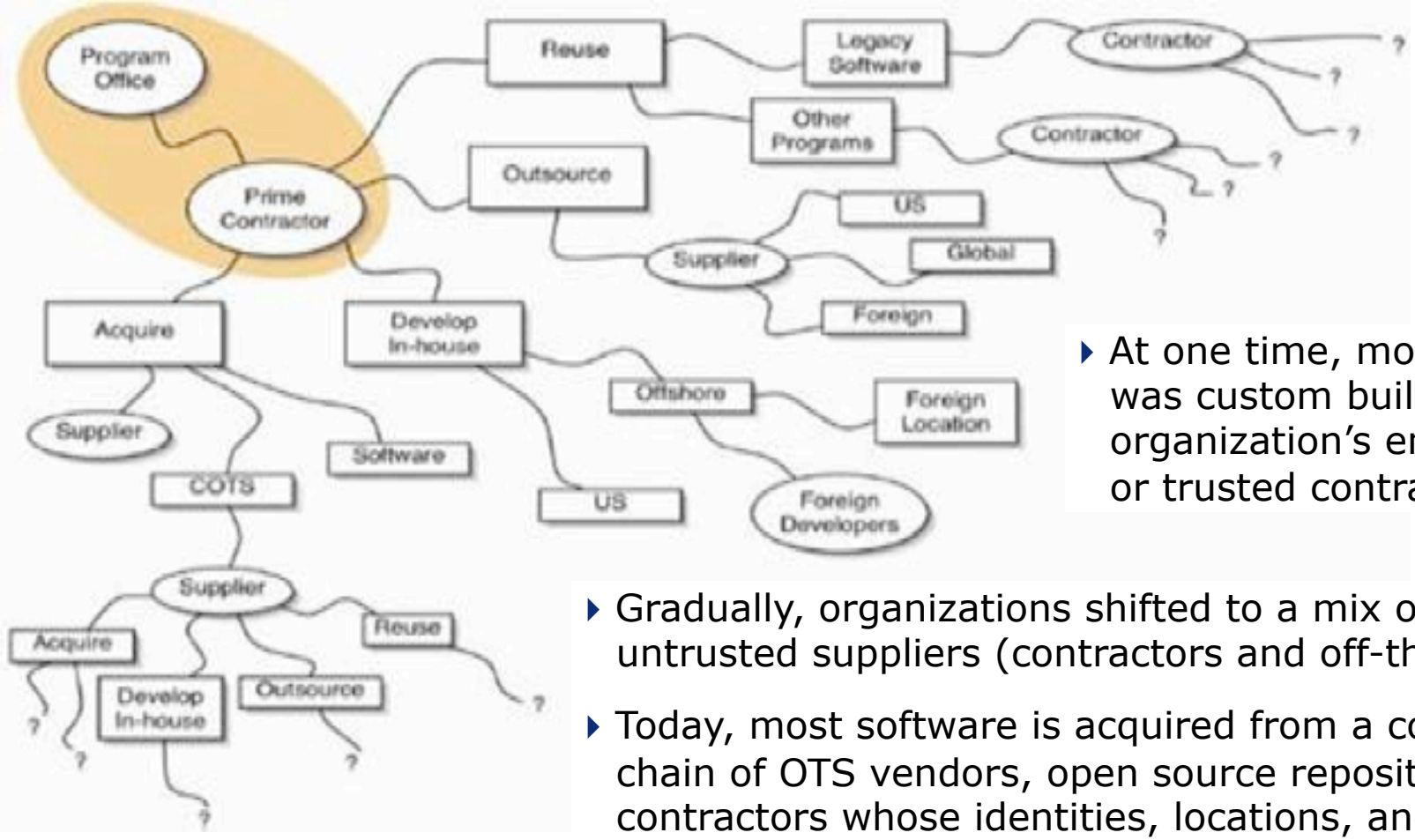
Supply Chain Risk Management and the Software Supply Chain

Karen Mercedes Goertzel, CISSP
Lead Associate
Booz Allen Hamilton
OWASP AppSec DC 2010

What constitutes a supply chain?

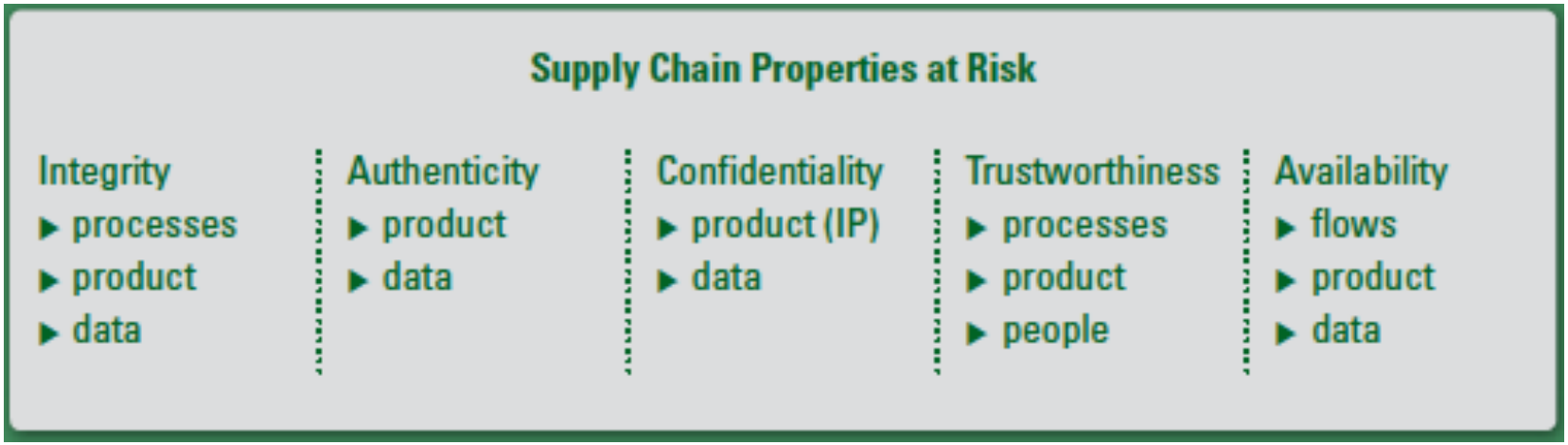
- Processes
- Products (including their innate intellectual property)
- Product flows
- Data (e.g., supply chain management data, product data and metadata)
- Data flows
- Participants (people)

Evolution of the Problem

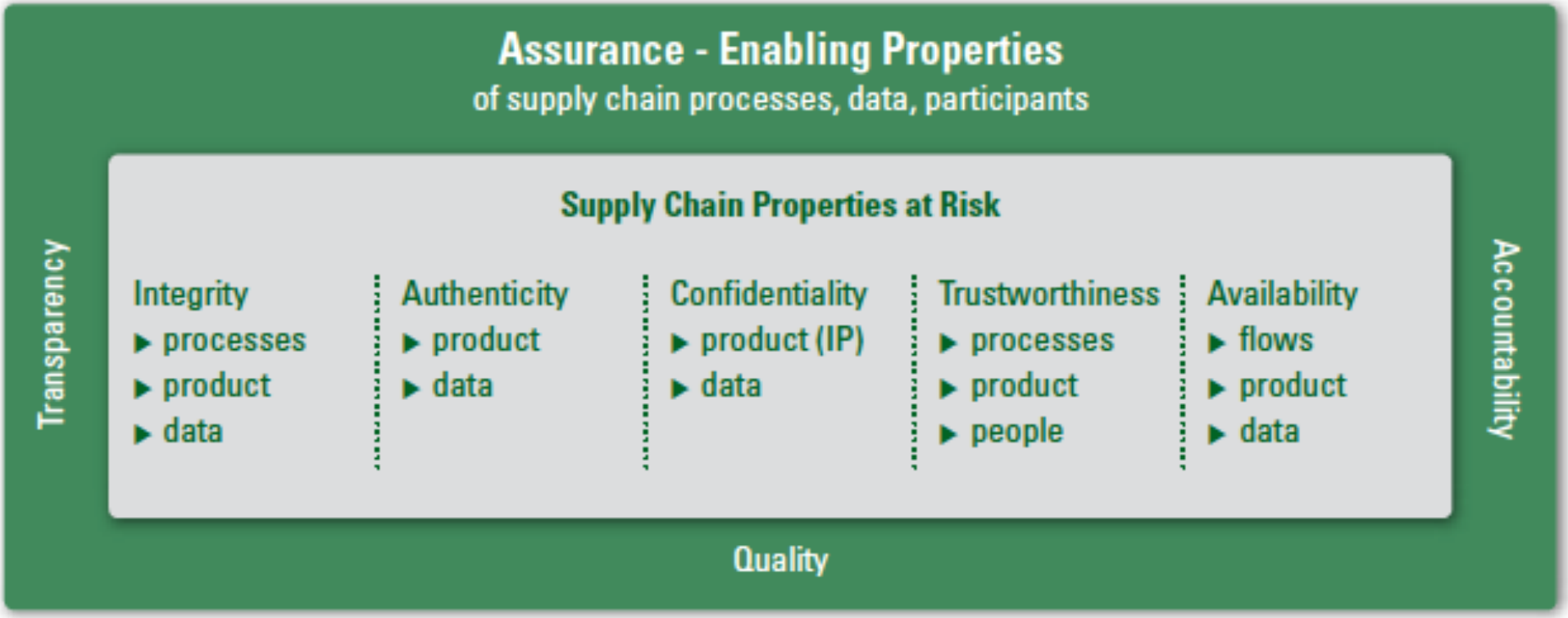


- At one time, most software was custom built by an organization's employees or trusted contractors.
- Gradually, organizations shifted to a mix of trusted and untrusted suppliers (contractors and off-the-shelf).
- Today, most software is acquired from a complex supply chain of OTS vendors, open source repositories, and contractors whose identities, locations, and trustworthiness are often unclear or unknown (possibly unknowable).

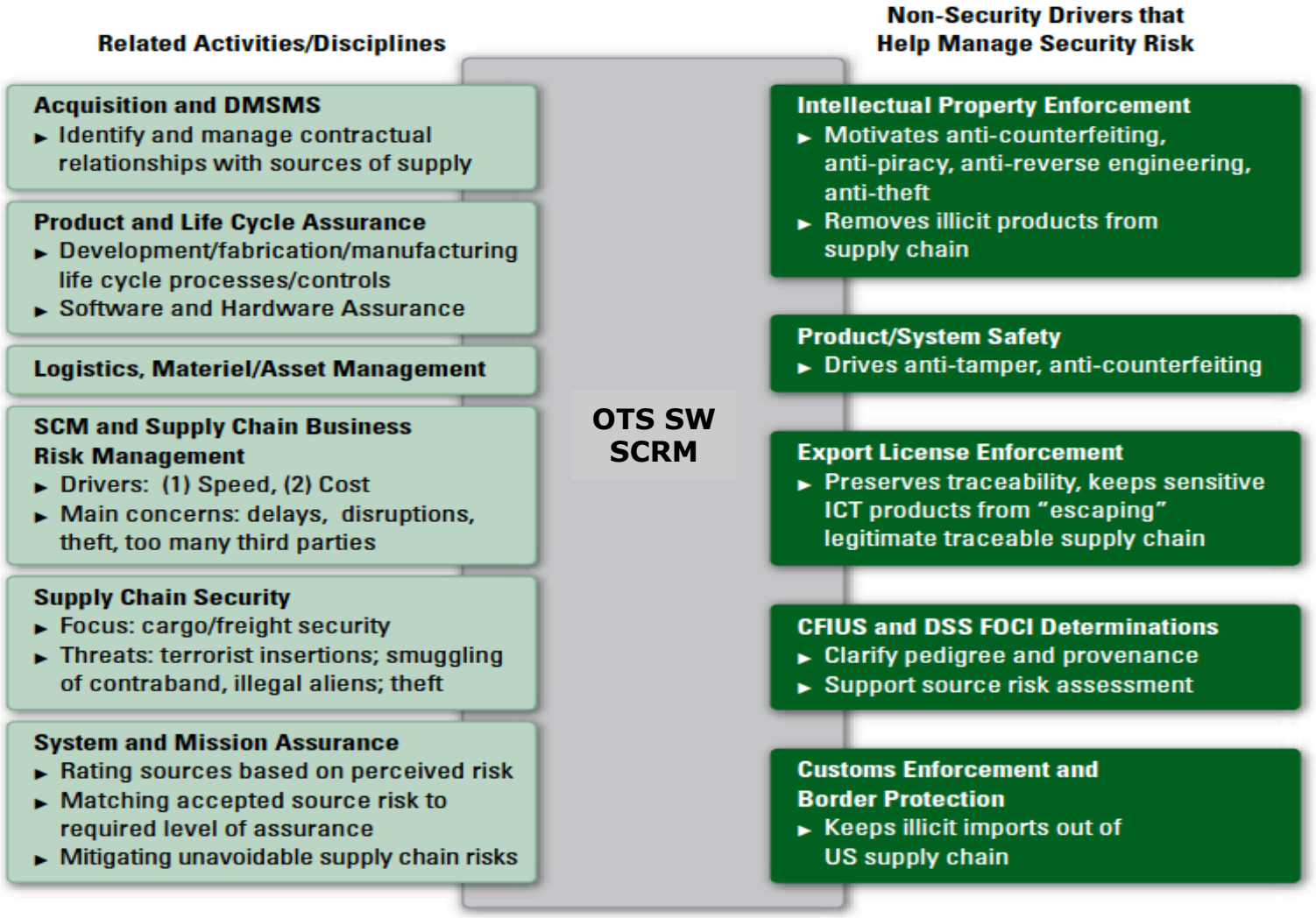
For the software supply chain to be secure, its constituent elements must exhibit certain properties.



Other properties enable the assurance that risks to supply chain properties have been adequately mitigated or avoided.



SCRM for the SW supply chain does not exist in isolation.



Each supply chain constituent is threatened in various ways.

- **Products:**
  - sabotage (building in malicious logic, backdoors, intentional vulnerabilities)
  - tampering (to add any or all of the above post-development)
  - counterfeiting, piracy (substitution of legitimate with illegitimate product)
  - theft (physical product, intellectual property, e.g., for reverse engineering)
  - destruction
- **Supply chain processes and product flows:**
  - disruption/delay
  - exfiltration (in aid of theft or disruption)
  - bypass of legitimate flows
  - infiltration, subversion
  - channel diversion (e.g., to piracy channels)
  - export control violations
  - insertion of undesirable items into physical product flows (e.g., bombs, bio/chem/radiation weapons, contraband, undocumented aliens)

Threats to supply chain constituents, *cont'd*

- **Supply chain data flows:**
  - penetration
  - diversion, rerouting
  - disruption/delay
  - corruption
- **Supply chain management data:**
  - tampering (illicit modification or augmentation)
  - counterfeiting (illicit substitution)
  - unauthorized disclosure, theft
  - deletion, destruction
- **Participants:**
  - subornation of insiders, e.g., through social engineering
  - "pseudo-insider threat" (undetected penetration of organization or network by criminal or adversary, with assumption of insider privileges)
  - Foreign Ownership and Control or Influence (FOCI) concerns (participants swayed by loyalties to hostile countries)

Malicious logic in software

- **What form does it take?**
  - Intentionally-Introduced Weakness (CWE-505)
  - Embedded Malicious Code (CWE-506)
  - Trojan Horse (CWE-507)
  - Trap Door/Back Door) (CWE-510)
  - Logic Bomb/Time Bomb (CWE-511)
- **How it gets there:**
  - Hidden in software's design (or even requirements)
  - Appended to legitimate software code
  - Added to linked library functions
  - Added to installation programs, plug-ins, device drivers, or other support programs
  - Integrated into development tools (e.g., compiler generates malicious code)

Malicious logic in software, *cont'd*

- **What SDLC vulnerabilities make it possible?**
  - Inadequate configuration control practices that allow for undocumented modifications or replacements of development artifacts
  - Lack of security-oriented design and code reviews
  - Inadequate testing that fails to exercise the software in ways that trigger anomalous behaviors or to identify such behaviors when they do occur
  - Ability of malicious code writers to reverse engineer legitimate executables (or analyze open source code) to better understand its workings, and thus more effectively craft malicious logic for insertion into later versions

Interesting statistics

- Percentage of all IT products that are counterfeit 10%

- Profit margin on cocaine 100%
- Profit margin on Microsoft Office 900%

- Value of counterfeit whiskey seized in 2008 $700,000,000
- Value of counterfeit IT seized in 2008 $100,000,000,000

SOURCE: Daniel Geer, Jr., and Daniel G. Conway, "Type II Reverse Engineering", in IEEE *Security and Privacy*, Sept./Oct. 2008

Distribution channels for counterfeit and pirated software

- Warez and peer-to-peer (P2P) file sharing sites and direct email exchanges between members of warez groups
- Surreptitious channel diversion through cross-site scripting (redirects customer browser away from legitimate download site to illegitimate – usually malicious – site)
- Software company employees and beta testers sharing pre-release versions
- "Grey market" channels:
  - online reuse repositories
  - open source repositories
  - freeware and shareware sites
  - individuals' Websites
  - third-party (esp. discount) commercial distributors

What's the big deal about counterfeiting and piracy?

- Counterfeits have proven to be less dependable than legitimate products.
- Counterfeiting provides an opportunity to subvert (e.g., malware, backdoors).
- Counterfeits and pirated copies, if detected, are not supported by legitimate vendors.
- Counterfeiting and piracy disrupt and obscure supply chain flows and participants.
- Counterfeiting and piracy violate intellectual property rights.
- Counterfeits and pirated copies threaten the business viability of legitimate vendors whose products are replicated.

Law enforcement vs. SW counterfeiting/piracy

- **Operation Fastlink (late 2000s):** multinational law enforcement action retrieves $50 million worth of illegally copied software, games, movies, and music, convicts and sentences 60 perpetrators.
- **Summer Solstice (2005-2007):** Joint operation by FBI and China's Ministry of Public Security seizes over 290,000 counterfeit software CDs and Certificates of Authenticity (estimated retail value $500 million) in China, $2 million worth in LA. 6 manufacturing and retail facilities in China dismantled. 8 master replication disks and 47,000 counterfeit Microsoft and Symantec CDs seized.

SW Supply Chain Risk Mitigation and Avoidance Measures

- **Security controls in software acquisitions**
  - ***Purchase only trustworthy software from trustworthy suppliers:***
    - Need to establish *sufficient* basis for trusting suppliers *and* their products.
    - Need to discover and trace pedigree and provenance of software products (including their components from contractors, third-parties, etc.).
    - Require Assurance Cases from software suppliers.
  - ***Prior to acceptance (better yet, prior to* acquisition*):***
    - Analysis to detect indicators of counterfeiting, piracy, license violations.
    - Examination to detect malicious logic, backdoors, vulnerabilities.
  - ***In DOD and Intelligence Community:*** Certain software constitutes Critical Program Information, requires Program Protection Plan.

SCRM in Government SW Acquisitions

- Government organizations that have addressed the need for improving security assurance in the SW acquisition process tend to emphasize:
  - Acquisition security criteria and requirements, security in contract language
  - Trusted supplier lists
  - Inspections and audits of supplier facilities, processes, and electronic flows
- Guidance available:
  - DHS: *Software Assurance in Acquisition: Mitigating Risks to the Enterprise*
  - OWASP: *Secure Software Contract Annex*
  - SANS Institute: template for application security requirements in contracts with software vendors
  - ISA Model Contracts Project
  - DOD Handbook 5000.60-H, *Assessing Defense Industrial Capabilities* defines "conditions in which reliance on foreign suppliers for specific products may constitute unacceptable foreign vulnerabilities"

SW Supply Chain Risk Mitigation and Avoidance, *cont'd*

- **Software assurance throughout SDLC**
  - Security analyses and tests: requirements reviews, design reviews, code reviews, security tests, anti-malicious logic, anti-vulnerability, and other checks.
  - Secure version, configuration, and inventory control to protect code, development artifacts, and tools from unauthorized changes, deletions, augmentations.
    - Limit insider access to pre-release software to deter inappropriate sharing of alpha and beta software (a source for pirates).
  - Physical and logical security of development facilities, servers, networks, to prevent unauthorized *and* inappropriate access.
  - Flow SWA requirements down to contractors, subcontractors, third-party sources.

Software Assurance and SCRM Guidance

- DHS portal at **`https://BuildSecurityIn.us-cert.gov`** provides extensive guidance and information resources for implementing software assurance throughout the SDLC.
- OWASP portal at **`http://www.owasp.org`** is a great source of guidance and tools for implementing application software assurance.
- SAFEcode portal at **`http://www.safecode.org`** focused on publishing free guidance that addresses software assurance (esp. for commercial software) from a supply chain risk management perspective.

SW Supply Chain Risk Mitigation and Avoidance, *cont'd*

- **Trusted distribution**
  - Add anti-reverse engineering and anti-tamper (deterrence and indication) mechanisms into executables (e.g., digital signatures).
  - Apply supplier source certification/authentication indicators (digital signatures, certificates of authenticity, RFID, etc.).
    - Certificate of authenticity must be protected against tampering and counterfeiting.
  - Apply tamper-deterrence/tamper-indication mechanisms to media and packaging (e.g., permanent printing, holographic seals, RFID, packaging that cannot be opened without visible damage).
  - Extend physical security controls throughout distribution chain for tangible software product (packaged) to prevent theft, tampering, diversion/delay.

SW Supply Chain Risk Mitigation and Avoidance, *cont'd*

- **Trusted distribution, *cont'd***
  - Extend physical and logical security to electronic supply chain product and data flows, and supply chain data.
    - Use authenticated, encrypted channels for supply chain data.
    - Secure download servers against unauthorized and inappropriate access.
    - Issue credentials for downloads: only to legitimate license holders.
    - Require authentication code/key for installation, with code/key delivered separately from the software itself (e.g., via email rather than download).

SW Supply Chain Risk Mitigation and Avoidance, *cont'd*

- **Post-acquisition:** Mitigate residual risk through pre-deployment system engineering.
  - System engineering measures (mainly architectural) can limit the extent and impact of unavoidable software risks.
    - Interpolation of security components to augment functionality of inadequate software (e.g., application firewalls, execution monitors, anomaly detectors)
    - Redundancy with diversity of critical software (avoid single points of failure, high value targets)
    - Enforced separation of trusted and untrusted components
    - Constrained execution environment for untrusted software (VMs, etc.)
    - Protected execution environment for trusted software (TPMs, HSMs, etc.)
    - Direct component modification (e.g., rewriting, wrapping, SDKs)
    - Reduce attack surface: Adjust system architecture to minimize exposure of less trustworthy software.

Guidance for Pre-Deployment Secure System Engineering

- NDIA: *Engineering for System Assurance*
  - **http://www.acq.osd.mil/sse/docs/SA-Guidebook-v1-Oct2008.pdf**
- NATO: *Engineering for System Assurance in NATO Programmes* (a NATO standard adapted from the NDIA guidebook)
  - **http://www.nato.int/docu/stanag/aep67/AEP-67(1)E.pdf**
- Ross Anderson: *Security Engineering, 2nd Edition* (Wiley, 2004)
  - **http://www.cl.cam.ac.uk/~rja14/book.html**

Face facts

- **OTS software is not suitable for all requirements.**
  - Some systems are too high-consequence, require too high confidence/assurance for *any* OTS software and associated supply chain risks to be acceptable.
- **The lifecycle cost of custom development does not always exceed the cost of using OTS.**
  - Need to factor in costs of:
    - Ongoing assessment and mitigation of supply chain risks
    - Analyses/tests to find vulnerabilities, backdoors, anomalies, malicious logic
    - (Re)engineering to minimize attack surface, mitigate vulnerabilities, eliminate potential malicious logic

Government concern over SCRM for the software supply chain

- **10 years of awareness-raising:**
  - 1999: *Final Report of the Defense Science Board (DSB) Task Force on Globalization and Security*
  - 2003: Government Accountability Office (GAO), *Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks*
  - 2005: GAO, *Offshoring of Services: An Overview of the Issues*
  - 2005: *Report of the DSB Task Force on High Performance Microchip Supply*
  - 2006: CNSS Global Information Technology Working Group, *Framework for Lifecycle Risk Mitigation for National Security Systems in the Era of Globalization*
  - 2007: *Report of the DSB Task Force on Mission Impact of Foreign Influence on DOD Software*
  - 2007: European Commission, *Availability and Robustness of Electronic Communications Infrastructures*
  - 2010: Department of Commerce Bureau of Industry and Security, *Defense Industrial Base Assessment: Counterfeit Electronics*

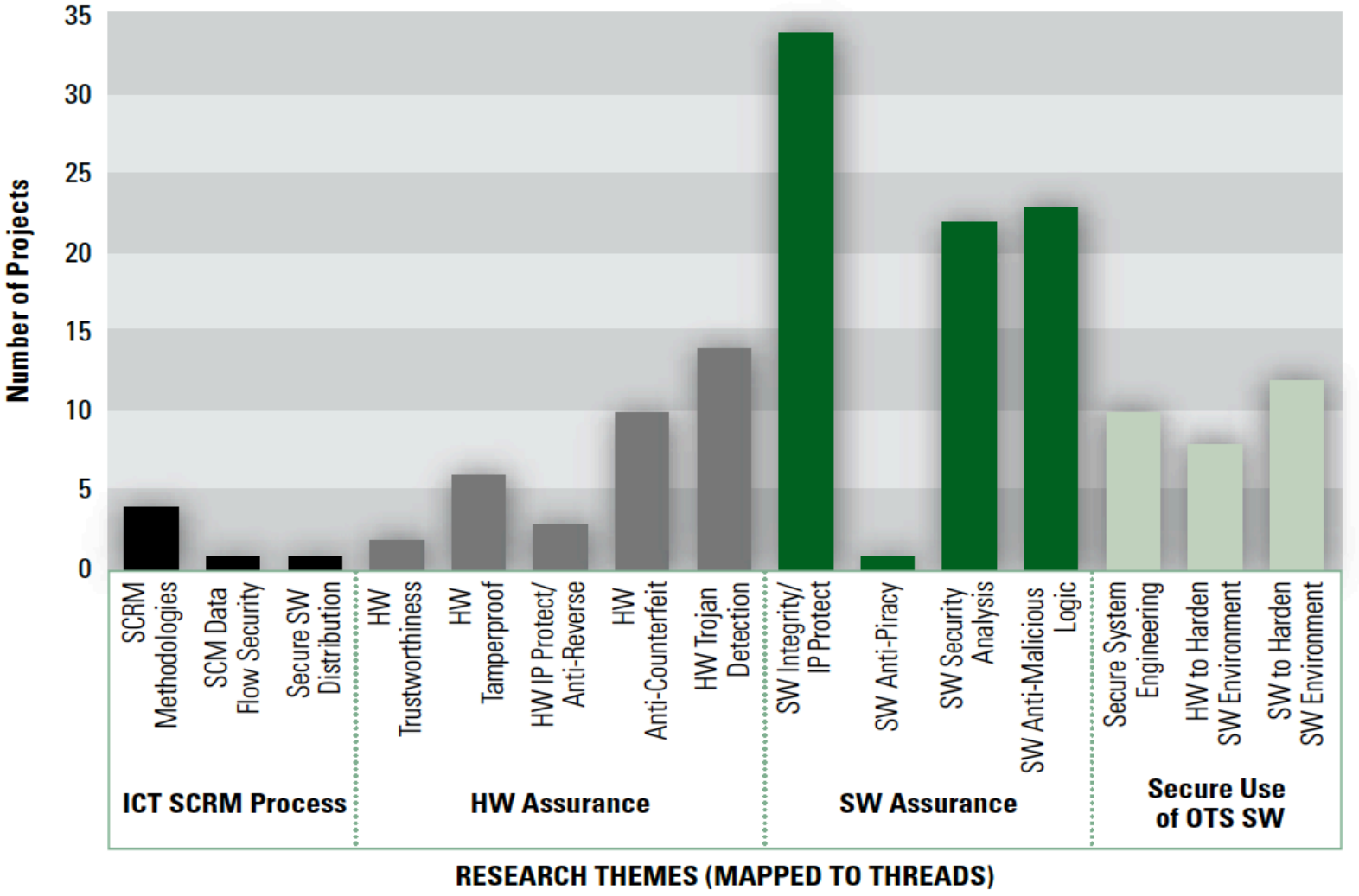
Government concern over SCRM for the software supply chain

- **CNCI Initiative 11:** "Develop Multi-Pronged Approach for Global Supply Chain Risk Management". Focus is on SCRM for the ICT (including software) supply chain.
- Government initiatives addressing SW supply chain risks include:
  - DOD SCRM Program, System Assurance Initiative, and Software Protection Initiative
  - NSA SCRM Special Program Office, Center for Assured Software, Assurance Development Processes, and Malicious Code Tiger Team
  - NIST ICT Supply Chain Risk Management Process and SAMATE
  - FSSCC-FBIIC Cyber Security Committee Supply Chain Working Group
  - DHS NCSD Software Assurance Program and DHS S&T Vulnerability Discovery and Remediation and Homeland Open Security Technology (HOST) Projects
  - Proposed FAR Amendment on Authentic IT Products
  - IARPA "Securely Taking on New Executable Software of Uncertain Provenance (STONESOUP)"

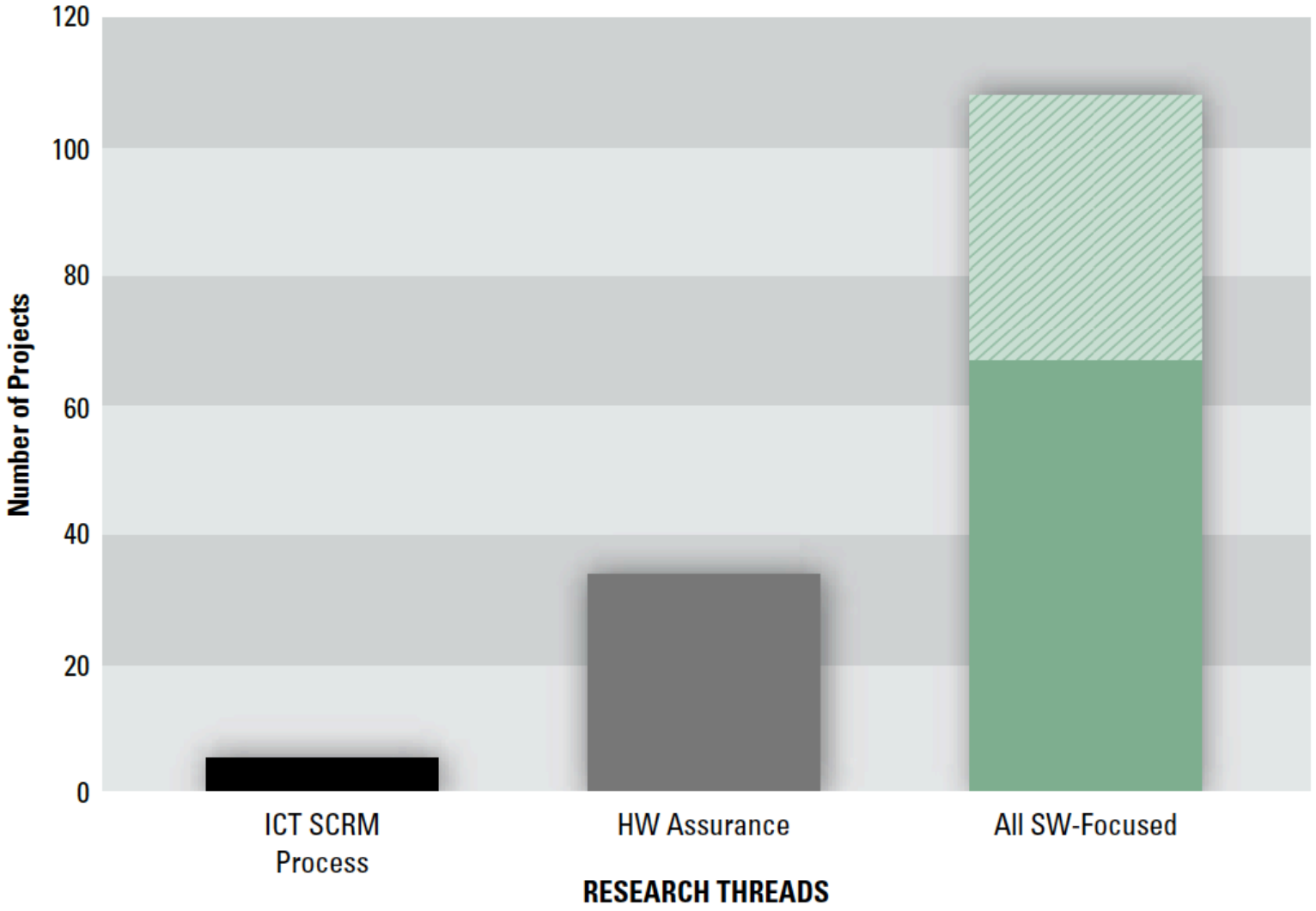
The Research Landscape

Research Thread	Recurring Themes
ICT SCRM Process	SCRM Methodologies
	supply chain data flow security
	secure software distribution
Hardware Assurance	hardware trustworthiness V&V
	hardware tamperproofing
	anti-reverse engineering of hardware
	anti-counterfeiting of hardware
	hardware Trojan detection
Software Assurance	tamperproofing and anti-reverse engineering of software
	anti-piracy of software
	software security analysis
	detection/prevention of malicious logic in software
Secure Use of Acquired Software	secure system engineering to mitigate risks from OTS software
	hardware-based hardening of software execution environment
	software-based hardening of software execution environment

The Research Landscape

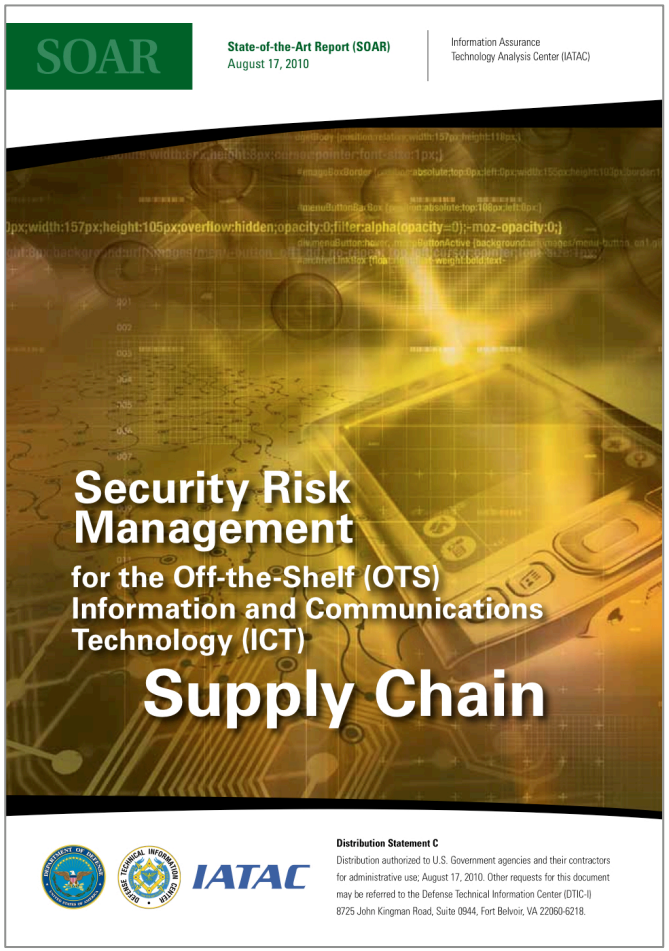


The Research Landscape, *cont'd*



Want to learn more?

- DOD Information Assurance Technology Analysis Center (IATAC) 2010 State of the Art Report on SCRM for the OTS ICT Supply Chain
- Available to federal government employees and contractors



- Download instructions on how to order from:
  - **http://iac.dtic.mil/iatac/download/limited_distro_sc.pdf**

Want to learn more?

- **Contact me:**

Karen Mercedes Goertzel, CISSP

Booz Allen Hamilton

703-698-7454

goertzel_karen@bah.com

Great Moments in Computer History:
Al Capone selling bootleg software.