Open Access License Notice

A New Model for Managing ICT Supply Chain Risk

Abstract – **The risks to the Nation's ICT infrastructure and products, both in defense and in the private sector, are well understood. Yet nearly ten years after the initial classified initiative to address supply-chain vulnerabilities in the telecommunications sector, the United States still lacks a broadly-accepted process to remedy them. These risks currently pose the greatest single gap in this nation's perimeter defenses. This paper presents a novel approach to making the remediation of supply-chain risks at all levels of the public and private sectors feasible, affordable and enforceable, based on establishing PGP-style networks of hierarchically trusted suppliers.**

1. Introduction: Addressing the Risk

Risks to the Nation's supply chain for Information and Communications Technology (ICT) are manifold and diverse. In broad terms, the risks can be classified as threats to supply chain *security* (from theft), supply chain *resilience* (threats to the supply chain itself, from natural disaster, acts of civil unrest, or other unforeseeable events), or supply chain *integrity* (from malware in software or firmware; counterfeiting in any product; or introduction of functional but unauthorized components) (Opstal 2012). While these three areas may have synergies of solution, this paper focuses on the last.

2. Case Study I – The Legal Threat: Software Freedom Conservancy v. Best Buy, *et al.*

In 2010, Best Buy, Inc. and thirteen electronics equipment or component manufacturers were sued for distributing high-definition televisions in which it was determined that third-tier component suppliers had incorporated shareware into the firmware on certain microchips in violation of the GNU General Product License (GPL). A U.S. District Court held all defendants liable and required them to surrender all the televisions to the plaintiffs to be donated to charity. Additionally, at least one plaintiff was held liable for triple statutory damages in the amount of $90,000 plus the plaintiffs' legal fees for attempting to dodge the settlement by restructuring through a bankruptcy-like action in the state of California (Guyomard 2011).

It is worth noting that the end-item retailer and manufacturers were both sued for damages in this case, although it would not ordinarily be considered reasonable to expect a television retailer to research the reliability of the manufacturers of the microchips that go into its products.

The challenge of ensuring an untainted supply chain balloons when one considers a typical mobile device, which may contain over 300 components, each with its own supply chain and licensing issues. The Android operating system alone is composed of 165 projects and over 80,000 files (Guyomard 2011).

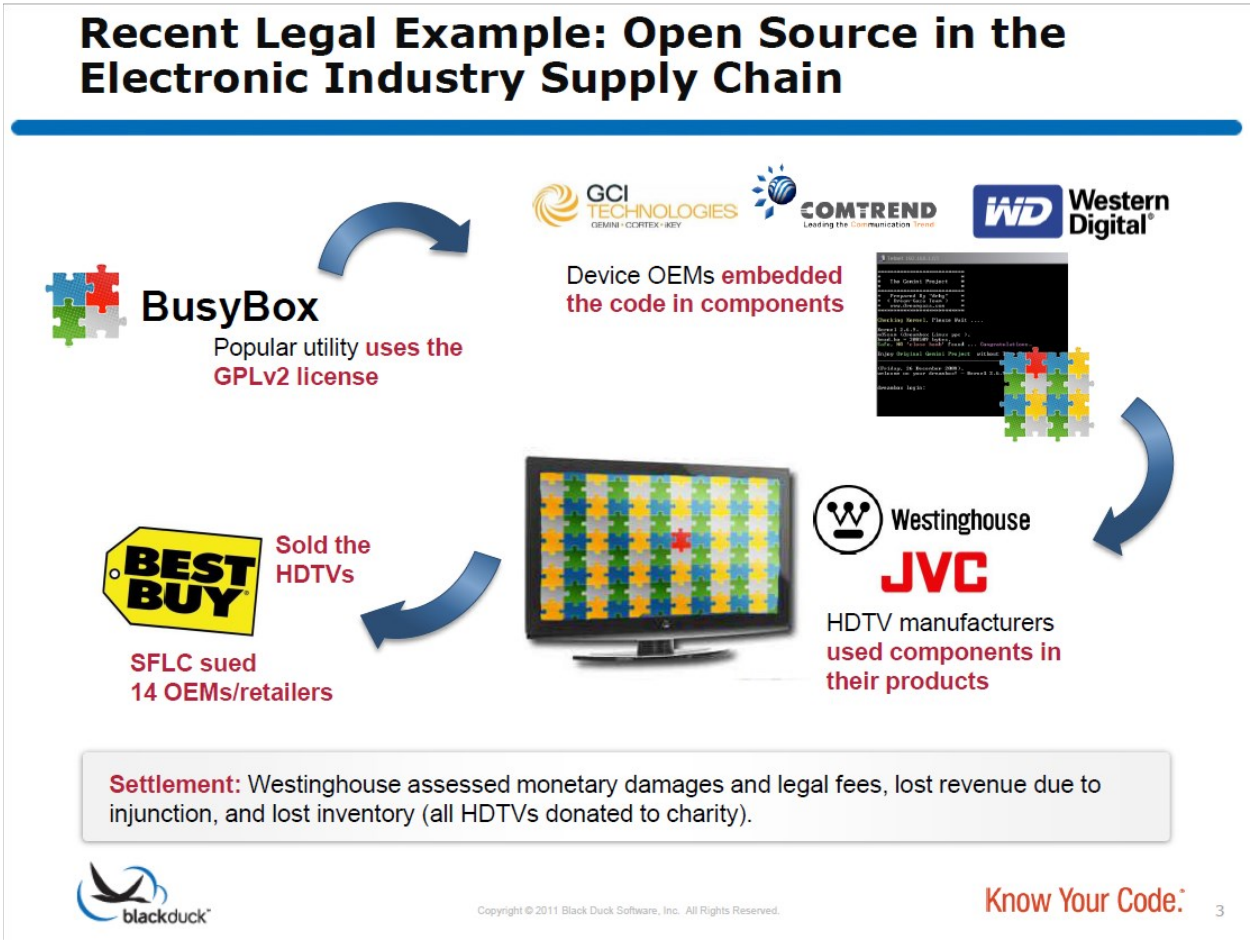

Figure 1: Software Freedom Conservancy v. Best Buy *et al.*

3. Case Study II – The Counterfeit Threat: Operation Network Raider

Between 2005 and 2010, federal authorities seized more than $143m worth of counterfeit Cisco hardware and labels in a coordinated operation between the FBI, Immigration and Customs Enforcement and Customs and Border Protection known as Operation Network Raider. The operation netted more than 700 seizures and 30 felony convictions over five years. In related actions, US authorities made more than 1,300 seizures of 5.6 million bogus semiconductors between 2007 and 2010. More than 50 shipments were falsely marked as military or aerospace grade devices.

Aside from concerns for U.S. corporations' intellectual property and brand value, much of the hardware of unknown provenance was destined for highly sensitive applications such as the Marine Corps' communications network in active combat zones. Counterfeit hardware and firmware is not subject to the same stringent quality requirements as genuine Cisco equipment and could fail under harsh conditions.

Worse, the equipment could introduce backdoors into critical components of infrastructure. In 2008, researchers from University of Illinois showed how they were able to modify a Sun Microsystems SPARC microprocessor to effectively create a hardwired backdoor capable of logging passwords or other sensitive data (Goodin 2010).

4. Spoiled for Choice: the Wealth of Competency Models

A wide variety of ICT supply-chain best practices is available, issued by a variety of entities – national and international, defense, government and industry – to forestall the types of threats described above.

Business and industry tend to follow the standards laid out by the International Standards Organization (ISO), which are typically adopted *in toto* by the Institute of Electrical and Electronics Engineers *(*IEEE):

International Standards Organization

ISO/IEC 12207-2008 (Systems and software engineering — Software life cycle processes) and **ISO/IEC 16085-2006** (Systems and software engineering – Life cycle processes – Risk management)

12207 defines all tasks involved in software/firmware acquisition, from initiation and requirements development through validation testing and project closure, and including product disposal. It covers 42 separate lifecycle and software-specific processes in seven areas. **16085** defines the risk management tasks for each of those processes. (Shoemaker, 2013)

ISO/IEC 15026-2 (Systems and software engineering – Systems and Software Assurance – Assurance Case) – discusses how to build the assurance case to show that supply-chain risks have been addressed

ISO/IEC 15408-2009 (Common Criteria for IT Security) – a coalition of national boards of 26 countries which accept each others' certifications of **hardware, firmware and software** packages

Society of Automotive Engineers

SAE AS5553 (Counterfeit Parts: Avoidance, Detection, Mitigation and Disposition)

Government agencies, by contrast, tend to follow standards set forth by the National Institute of Standards and Technology (NIST):

National Institute of Standards and Technology

NIST Information Technology Laboratory: Supply Chain Risk Management (http://scrm.nist.gov)

NIST IR 7622 (Notional Supply Chain Risk Management Practices for Federal Information Systems) – ten practices for ICT SCRM

DoD Information Assurance Certification and Accreditation Process (DIACAP)

Key Practices and Implementation Guide for the DoD Comprehensive National Cybersecurity Initiative 11: Supply Chain Risk Management Pilot Program. (https://diacap.iaportal.navy.mil/pages/scrm.aspx)

Carnegie-Mellon University Software Engineering Institute

Evaluating and Mitigating Software Supply Chain Security Risks – discusses how to build the assurance case to show that supply-chain risks have been addressed (Filsinger, et al. 2012)

5. Who Will Put the Bell on the Cat?

A popular children's story relates of a community of mice beleaguered by one very determined cat. None of the mice could leave their holes without risk of being attacked by the silent, crafty creature. After intensive conference, the mouse elders devised a brilliant plan: if a bell could be affixed to the cat's neck,

all the mice would have plenty of warning of the cat's approach. Only one challenge remained: which intrepid mouse would tie the bell around the cat's neck?

The Challenge

The current situation of ICT supply-chain control is analogous to the children's story. All of these standards are carefully thought-out collections of best practices. What all of them currently lack is teeth. Achieving these standards is labor-intensive, time-consuming, and therefore expensive; any supplier achieving them is arguably at a competitive disadvantage to one who is willing to cut corners. Furthermore, the current lack of agreement is a hurdle to enforcement efforts through either litigation or regulation. Common sentiment is that voluntary compliance is more effective than legal or regulatory guidance, due in large measure to the fact that the ICT domain evolves faster than legislation can effectively be brought to bear on it (Telecommunications Industry Association 2012); (Filsinger, et al. 2012). So the question remains: who will enforce the standards?

The British Solution

The United Kingdom must be commended for its effective engagement of this challenge. In 2007, the British Standards Institute, working with a consortium of leading members of the British ICT business community, established not only a standard by which ICT suppliers could be fairly and independently evaluated, rated and accredited, but also established a national authority – AccredIT UK – to execute the standard. This authority exists simultaneously to certify ICT providers, and to make its ratings available to potential business ICT consumers. Further motivation to attain certification comes from a business partner that offers significant discounts on Professional Indemnity insurance to any company holding an AccredIT UK certification. In the intervening six years, AccredIT UK has certified nearly eighty providers of ICT goods and services to English business consumers.

Accredit UK certification is available in five specialty areas:

- Communications Infrastructure
- Software Product Design and Development
- ICT Consultancy
- Solutions and Support (covers all hardware assembly, supply and integration activities, including telephony, and all managed ICT services)
- e-Media and e-Commerce

The AccredIT UK standard encompasses the following five areas of control measures for business operations:

- **Business Generation** – how well does a business go about generating new custom?
- **Delivery & Operations** – how well does a business carry out its activities?
- **Customer Relationships** – how well does a business manage its customers?
- **Business Management** – how well does a business manage itself and its personnel?
- **Business Direction** – how well has a business planned its strategy? (AccredIT UK 2007)

Disadvantages

Unfortunately, the British model has several shortcomings which make it unsuitable for adoption in the U.S. One is that its list of control measures is more limited than any of the U.S. industry or international

standards currently in use. Further, it is unclear whether it is positioned to certify suppliers of specialized firmware to defense customers and contractors – a key sector of the U.S. ICT SCRM effort. Its most pressing limitation, however, is one of scale: AccredIT UK certifies only UK suppliers to British Commonwealth customers. This prevents it from effectively addressing the problem of the global web of *n*th-tier suppliers which comprises the U.S. ICT supply chain.

6. Proposed Scheme

We propose establishing a framework for a network of trust. Consider the scenario in Figure 2, in which an ICT supply contractor A has relationships with its subcontractors B and C. The subcontractors, in turn, have relationships with *their* subcontractors D, E, F and G. In this model, A certifies B and C as trustworthy; B certifies D and E; and C certifies F and G.

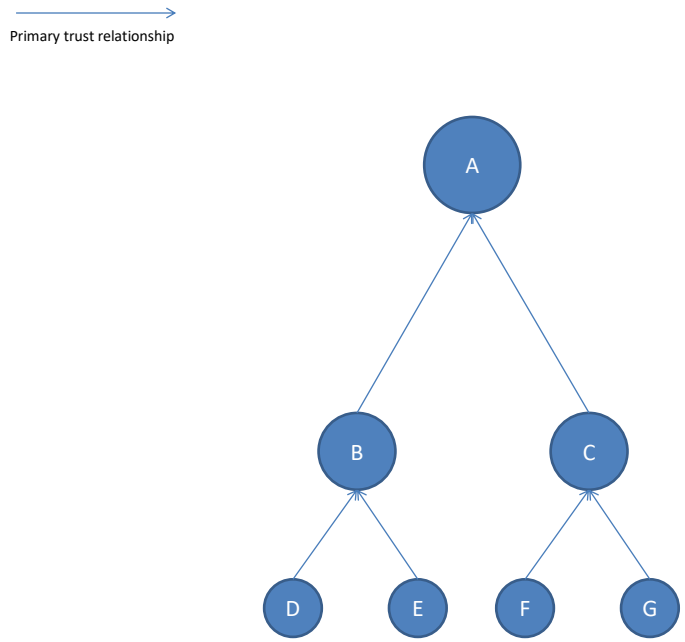

Figure 2: Network of trust

This diagram may look familiar to professionals in networks and distributed systems: it is closely analogous to the widely-used model established by PGP to establish networks of trust for secure e-mail transmission. Here, it has been translated from the network domain into the business realm.

7. Certification

Certification could take place using the consolidated model proposed by (Shoemaker and Wilson 2013) or any of the principal existing frameworks, with one addition: In order to gain full certification, a contractor must show that it is capable of certifying *its own* subcontractors. Thus, each contractor or subcontractor would need at least one individual, and possibly a team, on staff who can train other organizations in compliance with the standard of choice.

Note that it is not necessary for every subcontractor to be able to certify its own sub-subcontractors, or even to be certified itself, as discussed below.

8. Advantages

Under this schema:

- Each certifying entity is responsible only for the entities with which it directly does business. This reduces the certification workload to a manageable level.
- Each certifying entity can set the standards in each competency area as high as it feels necessary based on its specific requirements, given the nature of the business it conducts.
- The certificate is held, not by the subcontractor, but by the contractor. In essence, the certification packet constitutes a "get out of jail free" card (perhaps literally) for the contractor. In fact, a better term for the packet would be an *attestation*, rather than a certificate, as it is the subcontractor who is attesting that it is competent to meet the standards set by the contractor.
- In the event of litigation over some element of taint entering the supply chain, a contractor's liability could be limited to proving that it had set its standards high enough to prove due diligence. Any residual liability would then be transferred to the subcontractor. The subcontractor, in turn, can transfer liability to its sub-subcontractors. In this way, an entity's liability is limited to those areas over which it has control and visibility.
- Note, as mentioned in Section 6, that it is not necessary for a contractor to certify (or get an attestation from) every subcontractor in order to do business with them. The decision falls to the contractor: Is it more cost-effective to mitigate its supply-chain risk by certifying the subcontractor, or to accept the risk of an uncertified supplier? This is a classic risk-assessment paradigm familiar to every business.

9. Ramifications of the Decentralized Approach

Certificate sharing

As the decentralized approach described here plays out in the business world, several business arrangements may spontaneously evolve. One is depicted in Figure 3. Contractors A and H have each developed their own networks of trust. Subcontractor C wishes to do business with contractor H without having to go through the expense of proving its practices all over again to a different customer whose requirements might be slightly different. Contractors A and H, if they trust each others' business practices, can choose to trust each others' certificates, reducing the overhead for both entities.

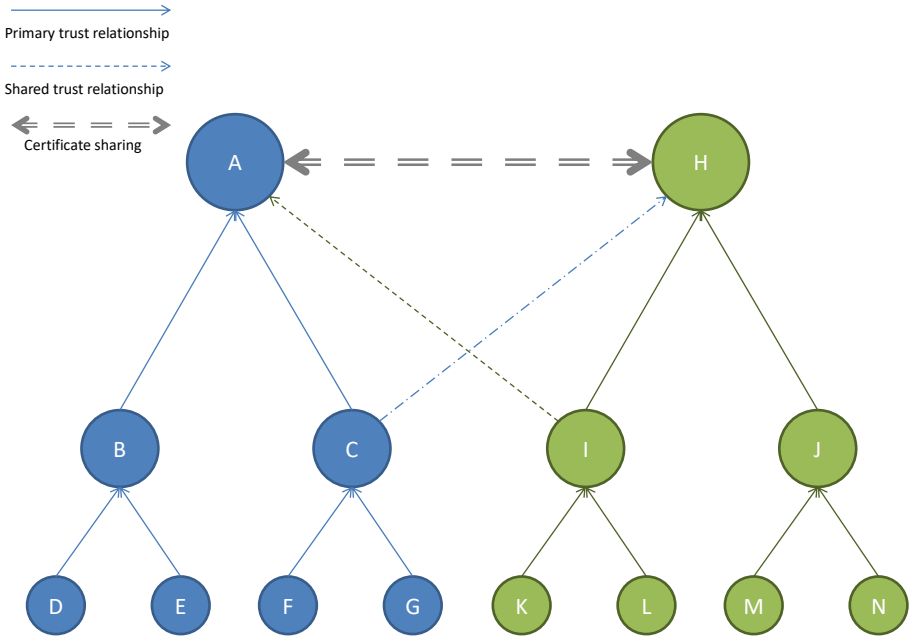

Figure 3: Certificate sharing

De facto certificate authorities

It is inevitable that the largest contractors will develop the largest networks of trusted suppliers, and will probably be the first to establish mature certification practices. Smaller contractors, or those moving into a new area of development, may wish to use subcontractors that have already been certified in the field in which they wish to work. This creates a business opportunity for the largest contractors to sell or license their attestations for a given subcontractor out to other contractors. In this way, what was a major expense becomes a potential source of revenue. See Figure 4.

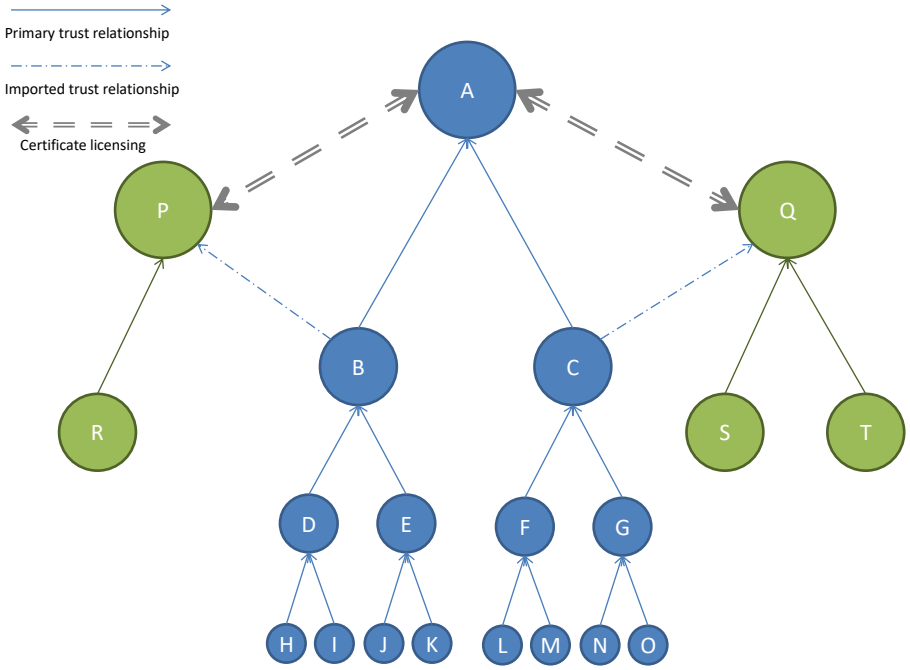

Figure 4: *de facto* certificate authority

10. Challenges, Requirements and Opportunities

The entire premise set forth in this paper is fueled by litigation. Thus, it requires that certain standards be accepted in case law as meeting the criterion of due diligence for avoiding the taint of counterfeit or compromised products in the supply chain. Some may despair at the seeming impossibility of holding *n*th-tier suppliers in foreign countries accountable through litigation; however, experience has shown that taking foreign suppliers to court *in their own countries* – notably in China – may indeed be the most effective way to combat incursions on intellectual property. (Fuchs, 2011)

Federal government agencies, and even state governments, can facilitate and accelerate the acceptance process by reinforcing the standards with laws imposing criminal penalties for lack of due diligence, particularly in cases of defense or SCADA acquisition. Here again, this requires a certain level of consensus on which standards can or should be imposed.

Possibly the greatest challenge to adoption of this model is getting contractors, who may be small businesses, to embrace the need to train and certify their own subcontractors. We posit that teaching something is the best way to become familiar with it, and thus having a training team can only enhance a contractor's own security practices; and since the contractor holds the purse-strings, they are uniquely well-positioned to ensure the subcontractor's compliance with the contractor's own standards. In any case, opportunities will abound for qualified organizations to "train the trainer."

11. Conclusion

In this paper, we present a model for a distributed system of supply-chain risk mitigation measures. By creating a system in which each tier of the supply chain is held responsible only for actions over which it

has direct control and oversight, we hope to foster a system that is at once fair, effective, enforceable, and responsive to the evolving needs of the ICT development and acquisition community.

References

AccredIT UK. "The Standard for Purchasers and Suppliers of ICT Solutions." Coventry: National Computing Centre, 2007.

Filsinger, Jarrellann, Barbara Fast, Daniel G. Wolf, James F.X. Payne, and Mary Anderson. *Supply Chain Risk Management Awareness.* Armed Forces Communication and Electronics Association Cyber Committee (AFCEA-CC), 2012.

Fuchs, Hans Joachim. "Setting Precedents: A Case of Anti-Counterfeiting in China." *Business Forum China*, Jan. 2011: 62-64.

Goodin, Dan. "Feds seize $143 million worth of bogus networking gear." *The Channel*, May 7, 2010.

Guyomard, Hervé. "Legal Issues for FOSS-based Supply Chain Management – Black Duck Software." *EOLE - European Opensource and Free Law Event.* November 3, 2011. http://www.eolevent.eu/sites/default/files/Legal Issues for FOSS-based Supply Chain Management - Herve.pdf (accessed April 1, 2013).

Opstal, Debra van. "“Aha” Findings from the Workshop on Securing the Smart Grid: Best Practices in Supply Chain Security, Integrity, and Resilience." *The CIP Report*, August 2012: 6-9, 21.

Shoemaker, Dan, and Charles Wilson. "The Weakest Link - The ICT Supply Chain and Information Warfare." *Proceedings of 8th Annual Conference International Conference on Information Warfare (ICIW).* Denver, 2013.

Stallings, William. "Pretty Good Privacy." In *Cryptography and Network Security*, by William Stallings, 568-587. Prentice Hall, 2011.

Telecommunications Industry Association. "Securing the Network: Cybersecurity Recommendations for Critical Infrastructure and the Global Supply Chain." *TIA Online.* July 24, 2012. http://tiaonline.org/sites/default/files/pages/TIACybersecurityWhitePaper_0.pdf (accessed April 1, 2013).