Gartner

Market Analysis and Statistics
G00238476

Maverick* Research: Living in a World Without Trust: When IT's Supply Chain Integrity and Online Infrastructure Get Pwned

Published: 5 October 2012

Analyst(s): Neil MacDonald, Ray Valdes

Enterprise IT supply chains will be targeted and compromised, forcing changes in the structure of the IT marketplace and how IT will be managed moving forward. (Maverick research deliberately exposes unconventional thinking, and may not agree with Gartner's official positions.)

Key Findings

- A lack of trust in information security technology solutions will fragment information security spending along geopolitical lines by 2018.
- Supply chain issues don't end when a system is delivered. Supply chain integrity must extend to include "operational supply chain" issues, such as updates and maintenance.
- Open source does not eliminate software supply chain integrity issues. Rogue or outdated open-source libraries and frameworks are significant risks.
- An architectural shift to software-defined IT architectures running on standardized hardware will result in more transparency and higher IT supply chain assurance.
- Within an IT system, trusted virtualization platforms on trusted CPUs will be used to establish a stronghold of trust on systems that are otherwise considered untrustable.

Recommendations

- IT procurement processes must be updated to address IT supply chain integrity issues.
- Shift to architectures using standardized hardware, which moves intelligence out of hardware and into software layers that can be more readily tested.
- If open source is used, ensure that the frameworks and libraries used are legitimate and up-to-date, and that the compiler used hasn't been compromised.

- Adopt trust models that reduce the scope of trust to defendable strongholds, and then extend the trust to allow the use of untrusted systems and components.
- In the longer term, all sensitive data, including fixed desktops and servers within enterprise data centers, should be encrypted, reducing the scope of trust required.

Table of Contents

List of Figures

Strategic Planning Assumptions

By 2015, 70% of applications delivered via app stores will be mandatorily scanned for security vulnerabilities, backdoors and outdated libraries.

By 2016, a new, publicly disclosed, IT supply-chain-integrity-related incident, costing millions in remediation and data loss, will affect at least 25% of the Global 2000.

By 2017, IT supply chain integrity will be identified as a top three security-related concern by Global 2000 IT leaders.

By 2018, 50% of new information security market spending will be fragmented along geopolitical lines.

By 2018, IT procurement, in at least half of the G20 for critical, nonmilitary infrastructure, will explicitly ban several IT systems produced by vendors in hostile, competitive, geopolitical groups.

By 2018, at least one multibillion-dollar, Western-aligned, enterprise IT vendor will spin out a Chinese subsidiary as a wholly owned and independent entity with isolated engineering and production to help alleviate supply chain integrity concerns.

By 2020, more than one-half of the data in enterprise storage will be encrypted, up from less than 5% in 2012.

Analysis

*Maverick Research

This is "Maverick" research, designed to spark new, unconventional insights. Maverick research is unconstrained by our typical broad consensus-formation process to deliver breakthrough, innovative and disruptive ideas from our research incubator. We are publishing a collection of more than a dozen Maverick research lines this year, all designed for maximum value and impact. We'll explore each of these lines of research to help you be ahead of the mainstream, and take advantage of trends and insights that could impact your IT strategy and your organization (see Note 1 and Note 2).

In December 2011, after a short evaluation period, the U.S. Air Force Special Operations Command (AFSOC) announced plans to procure nearly 3,000 of Apple's iPads to replace bulky flight manuals carried on board by pilots. The evaluation had determined that only the iPad met the project's requirements. The procurement bid specified the use of the GoodReader application, which is developed by Moscow-based Good.iWare.

In February 2012, plans for adoption of the iPads were put on hold, reportedly due to concerns over the use of Russian-developed software in the project.[1] Michael McCarthy, director of the U.S. Army's smartphone project, questioned the AFSOC project, stating "I would not use encryption software developed in Russia ... I don't want to put users at risk." He added that he was concerned about the integrity of the supply chain with GoodReader.[2] A spokesperson for the AFSOC stated, "We continue to look at each component of the program to ensure we do the right thing for our airmen, don't introduce unnecessary risk into operations and provide the best tools available to conduct the mission." The groundwork for banning such a product was laid in the 2011 U.S. National Defense Authorization Act, which authorizes the Secretary of Defense or the Secretaries of the Army, Navy and Air Force to exclude vendors or their products if they pose an unacceptable supply chain risk.

But what if IT supply chain concerns spread beyond defense and intelligence? And what if the rapidly growing Chinese or Russian markets for enterprise IT were cut from Western-aligned firms for similar reasons?

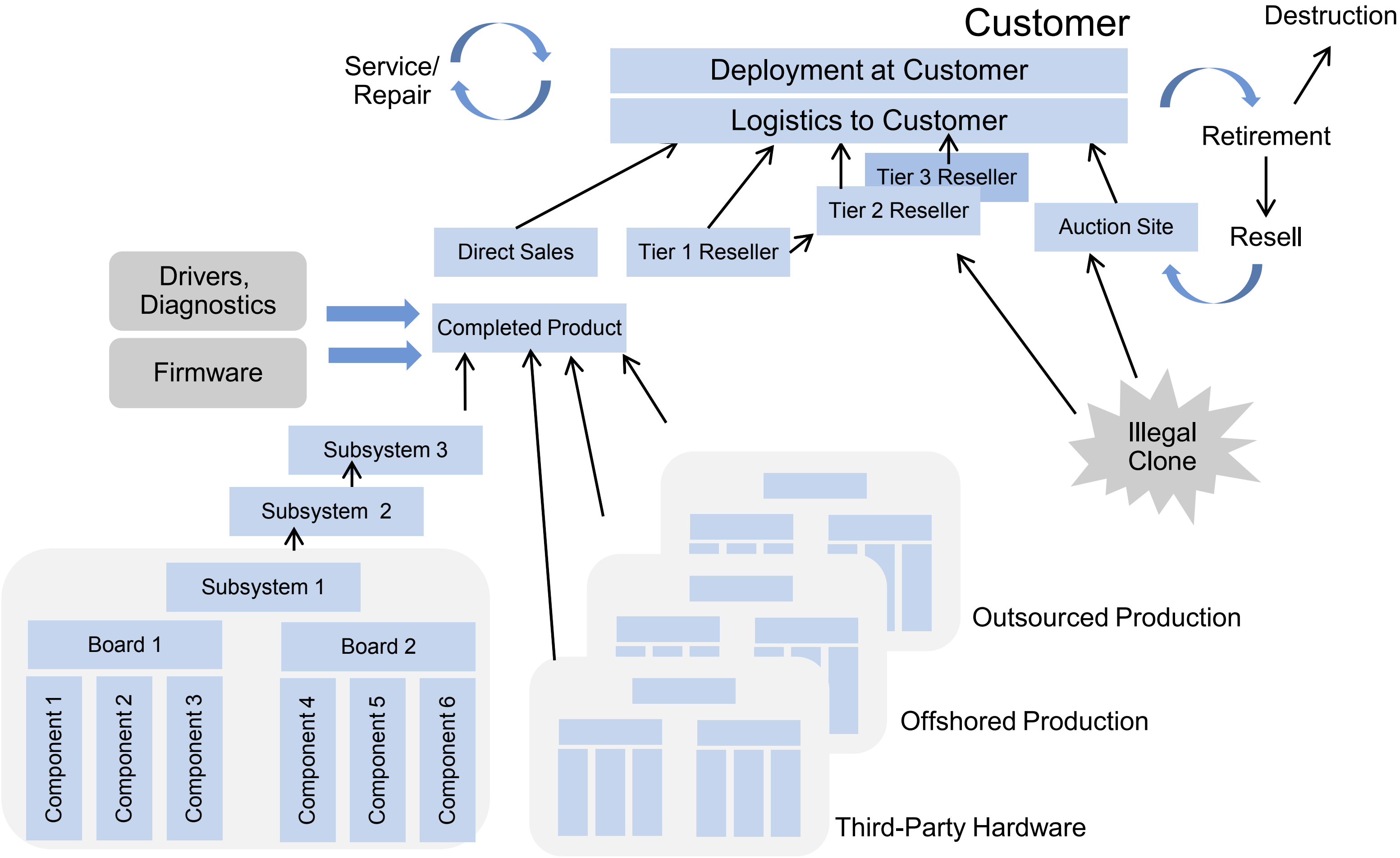
The use of Russian software in iPads is just one of the ever-increasing examples of IT supply chain integrity concerns that will reshape the IT landscape during the next several decades.

Supply Chain Integrity Is Increasingly Relevant to Enterprise IT

Supply chain integrity is the process of managing an organization's internal capabilities, as well as its partners and suppliers, to ensure all elements of an integrated solution are of high assurance. The need for integrity in the supply chain is necessary, whether the solution is developed in-house or purchased from a third party. The term "supply chain" often has implications of physical goods. In the technology sector, it relates to hardware, such as computers, networking equipment, mobile devices and servers.

The IT supply chain has become more complex, fine-grained, globally distributed and volatile in the sense that rapid change provides the opportunity to introduce compromises. Hardware vendors are increasingly outsourcing not just manufacturing, but also design to OEM suppliers and contractors located in Asia and India. In some cases, established Asian suppliers are outsourcing to emerging economies, such as Brazil, Vietnam and Indonesia. This is a complex problem, since most hardware systems are a conglomeration of components and subsystems procured from a large number of individual providers (see Figure 1).

Figure 1. Typical IT Supply Chain for Hardware

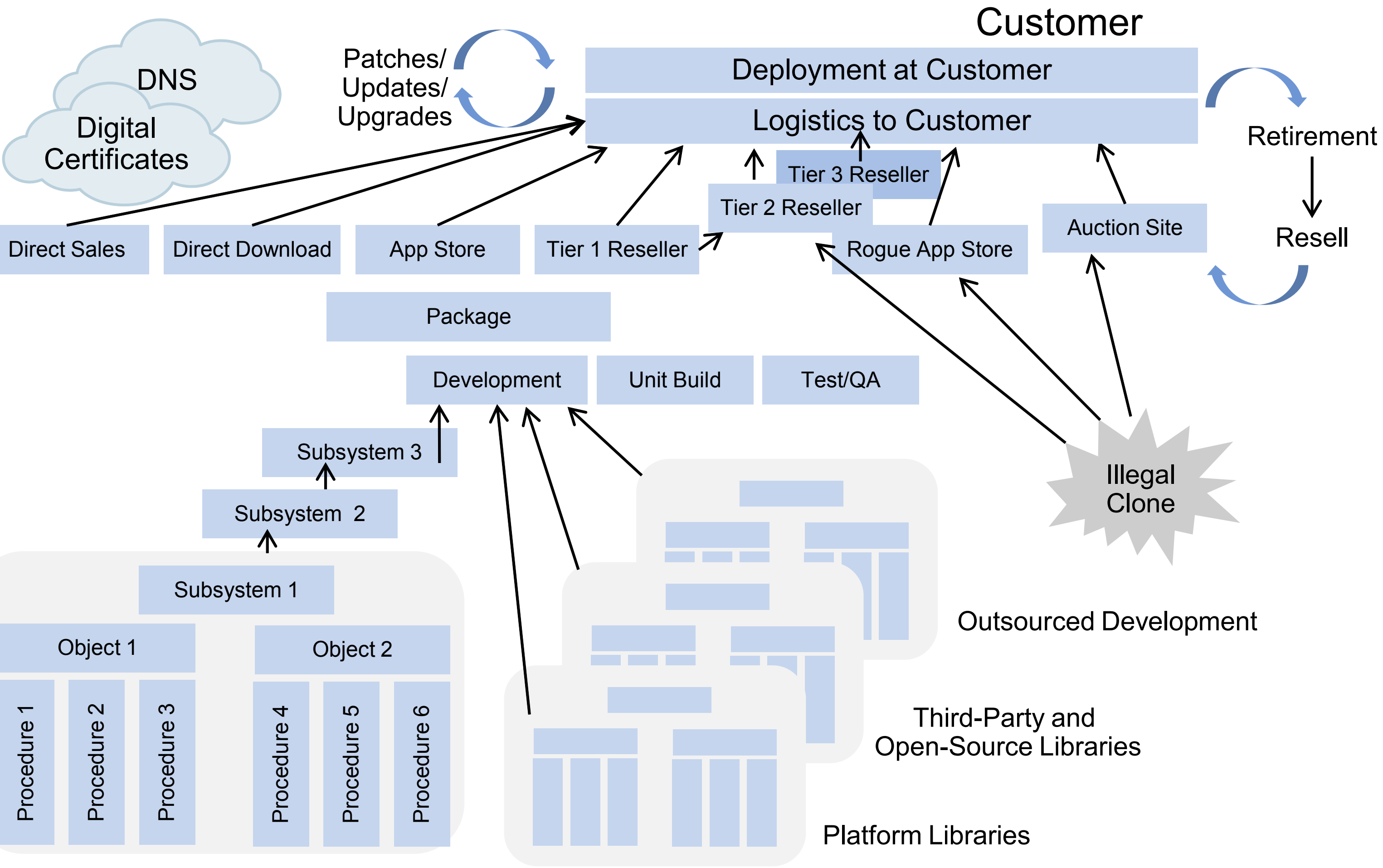


Source: Gartner (October 2012)

However, most hardware systems include software-based elements (at a minimum, firmware and drivers), with the trend to shift more intelligence out of hardware and into software. In an information- and software-based economy, IT supply chain integrity must extend to include the following:

- **Software supply chains —** This includes components, frameworks, middleware, language platforms, virtual machines (VMs) and operating systems (OSs), but also the software infrastructure and environment for software distribution and updates (such as DNS, identity, application store packaging, and digital certificates; see Figure 2).

Figure 2. Typical IT Supply Chain for Software



Source: Gartner (October 2012)

Ensuring the integrity of software supply chains is a more difficult problem because of the increased use of offshore development, the relative ease of cloning software, and the ongoing need to keep software patched and updated via trusted mechanisms.

- **Information supply chains —** Information is now becoming available from a variety of sources — from partners, suppliers and cloud-based services, such as data from Google Maps, Twitter, Facebook and Amazon. This information can be incorporated into connected applications, information marketplaces and the information integrated from partners in an extended supply chain ecosystem. Critical decisions will be based on information assembled from many other sources, creating a similar supply chain integrity issue to that of hardware and software.

Supply Chain Integrity Is Not New, but Problems Are Increasing

The serious implications of supply chain integrity issues are not new. Consider the quality issues in the 1990s with the production of Firestone tires used on the Ford Explorer, or the use of contaminated hamburger in the supply chain of U.S.-based, fast-food chain Jack in the Box.

Specifically pertaining to IT supply chain integrity, a January 2010 report by the U.S. Bureau of Industry and Security's Office of Technology Evaluation summarized the use of counterfeit electronics in the U.S. defense industrial base.[4] The assessment covered a total of 387 companies and organizations from 2005 to 2008, representing multiple segments of the defense industry and including several types of IT system hardware elements, such as discrete electronic components, microcircuits and circuit boards. The study found that, during the four-year period, 39% of the organizations surveyed had experienced counterfeit IT issues. More concerning, there had been a marked increase in the number of counterfeit incidents detected, growing to 9,536 incidents in 2008 from 3,868 in 2005 — more than double over the three-year period.

Likewise, in 2011, the U.S. Government Accountability Office (GAO) did a test. It purchased 16 military-grade parts via the U.S. Department of Defense (DoD) Internet purchasing platforms that listed DoD-authorized suppliers, finding that 12 of them were "suspected counterfeit" and four were bogus parts with purposely provided, invalid part numbers.[5] All of the parts were purchased from China.

In these cases, the root cause of the IT supply chain issue was the use of counterfeit, refurbished and/or substandard hardware components being sold to weapon manufacturers as new and compliant parts, such as the substandard memory chips found in the weapon systems that were marked as compliant. The problem is exacerbated in the military industrial sector by the use of weapon systems for extended periods of time, whereas the electronic hardware used within them evolves much faster, making it difficult to source older components. In these cases, the goal was not to steal sensitive information, but to profit by passing off noncompliant, substandard and possibly forged goods as being compliant. A failure of such a component in use could have catastrophic consequences, including full system failure, with the potential for damage or death.

Although the previous IT-related studies pertained to defense and intelligence agencies, Gartner believes the issue of IT supply chain integrity is now of critical concern to all enterprise IT organizations.

Why IT Supply Chain Integrity Is Becoming a Critical Issue Now: Motivational Changes

The motivations of hackers are shifting, creating IT supply chain integrity issues that will also impact enterprise IT organizations:

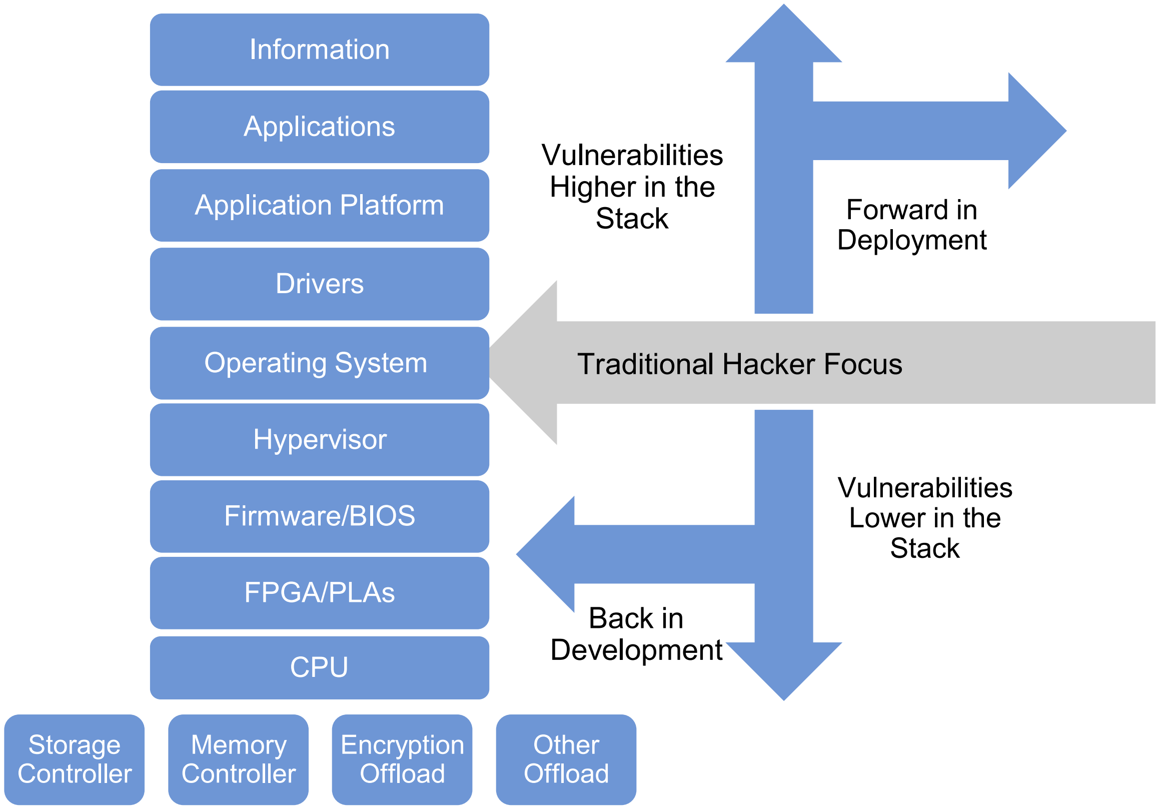
- **The changing motivations of attackers —** The most notable shift is the move away from "noisy" mass attacks, with the motivation of gaining attention or vandalism, to stealthier, targeted and financially motivated attacks for political, military or financial gain, or to make a political statement ("hacktivism"). The targets of supply chain integrity attacks are no longer isolated to defense and intelligence targets. They now include the critical infrastructure of nation states, such as the recently publicized Stuxnet attack on Iranian nuclear infrastructure, as well as sensitive manufacturing, financial service and pharmaceutical infrastructures.
- **Market mechanisms now at work —** Hackers are organizing their own supply chains, with some focusing on finding new "zero-day" vulnerabilities in systems, others on malware assembly and still others on malware delivery systems. Automation is being brought to the hacker supply chain in the form of toolkits that can quickly assemble custom malware. Reportedly, there are markets and middlemen that buy and sell zero-day information, in which exclusive access to a bug in Flash or Java may fetch $40,000 to $100,000, while one in the Apple iOS may be priced between $100,000 and $250,000.[6] The ecosystem is growing in part because the sale of this information is technically not illegal in most regions, since the laws have not kept up. In response, some vendors have established their own markets or bounty programs. For instance, Google pays $60,000 for a zero-day bug in the Chrome browser, and TippingPoint established the Zero Day Initiative as a market between "researchers" and affected vendors.
- **Since enterprises are getting better at defending perimeters, attackers are targeting IT supply chains —** Rich targets, such as financial services, defense and intelligence, are well-defended, so attackers are looking for new approaches to compromise these targets. For a well-defended target, it is easier to compromise an IT system before it is deployed, rather than compromise a production system.

Why IT Supply Chain Integrity Is Becoming a Critical Issue Now: Technical Changes

There are multiple technical challenges making enterprise IT supply chain integrity an issue:

- **Opportunities to place vulnerabilities abound —** A successful attack requires a vulnerability to exploit in technology, people or processes. Attackers are shifting their focus up and down the stack, and left and right in the IT supply chain, in search of vulnerabilities (see Figure 3).

Figure 3. Shifting Attacks Up and Down in the IT Stack



BIOS = basic input/output system; FPGA = field-programmable gate arrays; PLA = programmable logic array

Source: Gartner (October 2012)

Further, each one of these layers has its own supply chain, compounding the complexity of assuring the integrity of the completed solution. In addition to moving up and down the stack, attackers are also shifting their focus horizontally in time — to the left, further back into the creation and assembly of IT systems, and to the right, as IT systems are updated, replaced, retired and refurbished.

- **Hardware compromises are increasingly difficult to detect and harder to execute —** As attackers shift their focus further down the stack to the hardware layer, compromises are more difficult to detect, but also harder to implement. While a counterfeit motherboard might be observable using visual inspection without specialized equipment, refurbished memory chips or additional circuitry added to a system requires specialized equipment, skills and techniques beyond the capability of most enterprises, such as destructive testing, the removal of layers of integrated circuits one at a time, scanning electron microscopes, x-ray scanning and so on.
- **IT software supply chains are easy targets —** The ability to defend an IT software supply chain is complicated by multiple factors:

- **Increased use of outsourcers for software development —** Even if creators use their own developers, many use external third-party libraries and frameworks to speed development, including open source (which we will discuss in more detail later in this research).
- **Increasingly active code at many layers —** The use of software-based platforms on top of OSs is increasing, providing new opportunities for compromise with vulnerabilities or backdoors (for example, Microsoft Office macros, Java VMs, Adobe Flash and custom WebGL shaders loaded from a website running on a graphics processing unit [GPU]).
- **Content itself can be used to carry attacks —** Exploits against hidden application-layer vulnerabilities can transform a seemingly static piece of information to active code that's capable of carrying an attack (such as malformed images and music handled by deliberately buggy media players or malformed Web requests handled by vulnerable Web applications).

- **Application update infrastructure will be targeted —** Attackers will look for operational supply chain issues, and, increasingly, the update mechanisms for executable code will be targeted. This concern applies not only to traditional OSs and application software, but also hardware, since most firmware and BIOS have mechanisms for updating. At the application layer, the number of auto-updated applications is proliferating, with examples including Apple iTunes, Apple Safari, Mozilla Firefox, Adobe Reader, Google Chrome and so on. All these update infrastructure mechanisms create multiple sources of "authorized" changes outside the control of centralized IT. These mechanisms will and have become prime targets for compromise.
- **Executable code below the OS —** Hypervisors and hardware virtualization introduce another layer of software below the OS that, by design, mediates all system access to memory, CPU, network and storage. Because of its unique and privileged vantage point, a compromise of the hypervisor integrity represents a worst-case security scenario, since the integrity of the entire system is dependent on the integrity of the hypervisor. Not surprisingly, in April 2012, an attack that gained access to VMware's ESX source code was publicly disclosed.[7] In another example, the Unified Extensible Firmware Interface (UEFI) standard replaced a legacy BIOS firmware, with a much richer set (and, thus, more opportunity for compromise) of networking and storage services. These lower layers represent a compelling target for compromise, since they are difficult to detect and provide easy access to layers of the IT systems running above them.
- **Intelligence bypassing the CPU —** Out of band (OOB) management technologies, such as Intel's Active Management Technology (AMT), bypass the central processing unit for remote system management. In some cases, these OOB access technologies provide access to encrypted hard drives for the purposes of patching. Likewise, technologies such as direct memory access (DMA) provide the ability to access and manipulate memory outside the control and visibility of the main processor. Network and storage controllers with their own onboard intelligence and DMA represent similar opportunities for supply chain compromise.
- **Attacks on Internet infrastructure mechanisms of trust —** In lieu of direct ownership and control, the Web has evolved multiple mechanisms to establish and propagate trust between

digital entities and IT systems that need to communicate and share information over the Internet (for example, DNS, digital certificates and alternative authentication mechanisms). Since the ongoing, operational supply chain integrity of an IT system depends on the integrity of this infrastructure, it will be, and has been, targeted.

- **The shift to public-cloud-based computing models —** The industry transition to cloud platforms is occurring at all levels of the technology stack, and will become an integral part of extended IT supply chains. In a system with many "moving parts" distributed across organizational boundaries, there will be opportunities to introduce deliberate weaknesses in the form of bugs, misconfigurations and design flaws.
- **The shift to horizontal integration of enterprises —** Enterprises are opening up their internal IT networks and systems to collaborate and share information with customers, partners and suppliers. As a result, all of these become targets for IT supply chain compromise. If an attacker can't find a weakness in your enterprise people, processes or systems, they will look for opportunities in your extended enterprise supply chain.
- **Information itself becomes a target for compromise —** As enterprises increasingly rely on information that is generated outside of their direct control, information supply chains will emerge, and be targeted with bad information, misinformation and/or corrupted information for consumption by information supply chain participants. Here, the goal would be to cause an incorrect decision by the target that. in some way, wastes its resources and damages its ability to correctly respond (for example, shifting resources to target a nonexistent opportunity).

The Result: Unmanageable Complexity, Unmanageable Risk

The result is a set of intertwined, distributed, multilayered, complex IT infrastructures, with the complexity moving beyond the simple understanding of a single individual that can no longer be trusted. All endpoints, servers and systems are at risk of compromise. However, we believe that there are ways that enterprises can better protect themselves in such an environment.

With this in mind, let's look at some recently publicized IT supply chain compromises. There are lessons to be learned from these incidents and applied to enterprise IT.

Insights and Recommendations From Recent IT Supply Chain Issues

Incident No. 1: Counterfeit Cisco Routers in the Supply Chain

A 2008 summary report by the U.S. Federal Bureau of Investigation (FBI) into the use of Cisco equipment within various agencies of the U.S. government indicated the purchase and deployment of millions of dollars of counterfeit Cisco equipment.

What Happened

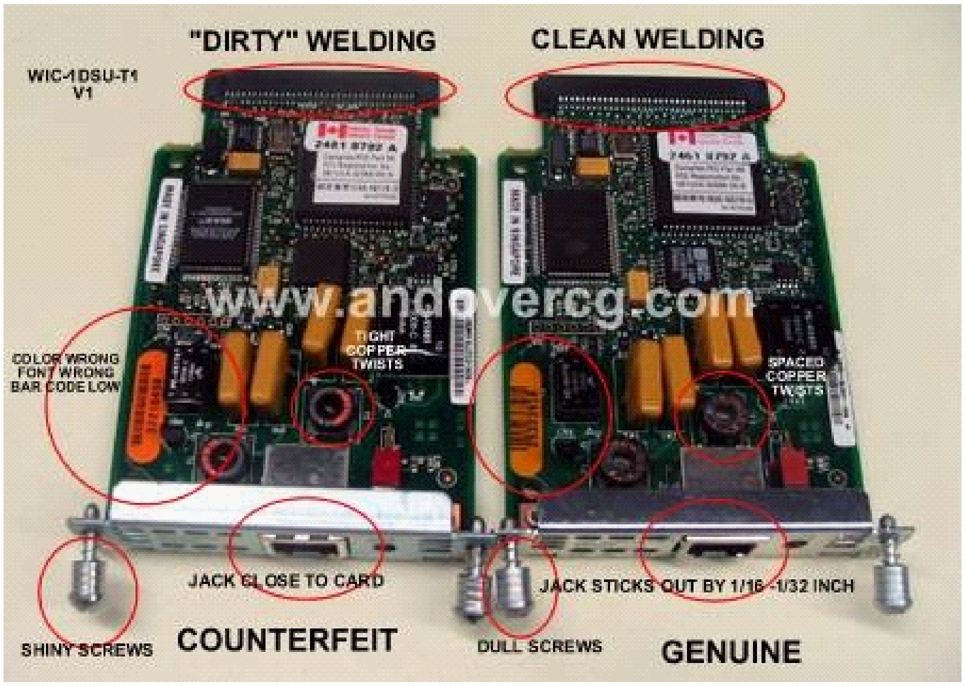
- Counterfeit routers, switches, gigabit interface converter and WAN interface cards were identified.

- The counterfeit equipment was used within multiple agencies in the U.S. government and commercial enterprises, including the U.S. Navy and FBI itself.
- The motivation of the attackers was profit. The motivation of the government agencies was cost savings.
- All counterfeit equipment originated in China and was subsequently sold through multiple channels, including sales on eBay.
- The compromise was detected due to equipment failures (in one case, a faulty power supply caused a fire), media access control (MAC) address conflicts and upgrade failures.

Insights

- Espionage is not the only goal for IT supply chain compromises.
- All cases were a direct result of weak procurement processes.
- For physical systems, the use of holograms on motherboards and shipping tape to seal boxes is a small but useful countermeasure to counterfeiting.
- A detailed physical inspection would have discovered the counterfeit systems, but one was not performed, or baselines for comparison were not known (see Figure 4).

Figure 4. Physical Differences in Counterfeit Cisco Routers



Source: Andover

Recommendations

Enterprise IT organizations can't spend the same amount of money for testing, or perform the type of destructive testing that a nation-state-level defense or intelligence agency can. However, there are specific steps a typical enterprise can take to protect the integrity of its IT supply chain:

- Require proof of an explicit chain of custody from your IT suppliers. Make sure this includes any third-party hardware and software components they use in the solution.
- Require your IT system provider to supply proof of a periodic sampling and testing of its final solution to ensure adherence to specification and integrity.
- If you trust the geopolitical axis with which you are aligned, use the specific IT hardware and software solutions tested and approved for use by government agencies.
- Strengthen your procurement processes. Deal directly with IT vendors, when possible. When it is not, the ideal situation is to purchase only through trusted, certified resellers with an established reputation. Don't force procurement to go with the lowest-cost provider.
- Explicitly ban the purchase of new or used IT hardware or software from eBay, Craigslist or similar public auction sites.

Incident No. 2: Huawei Banned From Western Government Deals

It was reported in March 2012 that the Australian federal government had banned Chinese telecom giant Huawei from bidding on a US$38 billion new project to build the next-generation National Broadband Network (NBN) because of national security concerns.[8] According to The Australian, the decision was prompted by fears from the Australian Security Intelligence Organization (ASIO), which stated that there was "credible evidence" that Huawei was connected to the People's Liberation Army.[9] Additionally, on 13 September 2012, the U.S. House Permanent Select Committee on Intelligence held a hearing on two of the biggest Chinese telecommunications companies doing business in the U.S.— Huawei and ZTE — reviewing "the extent to which these companies have ties to the Chinese government or otherwise provide the Chinese government with an opportunity for greater foreign espionage."[10]

What Happened

- China is Australia's largest trading partner. Huawei has participated in large telecom projects in Australia before (with Vodafone Group and Optus, for example), as well as in NBN-style networks in the U.K., New Zealand, Singapore, Malaysia and other countries. In 2011, it overtook Ericsson to become the world's largest telecom equipment vendor. Huawei counts 45 out of the world's 50 largest telecom operators as customers.
- Huawei's $1 billion supply contract bid was blocked by Australian Attorney General Nicola Roxon on advice from the ASIO, a decision defended by Prime Minister Julia Gillard after the story broke.

- Huawei was founded by an ex-member of the People's Liberation Army. Reportedly, there are concerns about possible ties between the company and the Chinese military, leading the Australian and U.S. governments to block the company from sensitive projects.
- In 2008, the U.S. Department of the Treasury blocked the sale of U.S. vendor 3Com to Huawei, and, in 2010, Sprint denied Huawei's bid to build out its 4G network in the U.S. In 2011, Huawei's bid to build a wireless network for first responders (that is, police and firefighters) was denied, according to the U.S. Department of Commerce, "due to national security concerns."
- Neither the Australian government nor the U.S. government has provided any detail beyond the basic facts of turning down bids or blocking proposals.

Insights

- The broad outline of these events demonstrates that political factors (perceived national self-interest) trumps economic self-interest.
- Fault lines have emerged in the political/economic landscape. These lines track geographic regional boundaries, but also reflect long-standing historical relationships (such as between Australia and the U.S.).
- The geopolitical alignment of regional centers of influence will continue to strengthen, since there is a self-reinforcing cycle under way.

Recommendations

- Require all IT system providers to provide complete transparency to their hardware and software supply chain processes. For example, to counter the perception that its products may be compromised, in late 2010, Huawei opened up a Cyber Security Evaluation Center in Banbury, U.K. The company provides full access to each product and code release to validate the integrity of the design, that no backdoors are present, and that its hardware and software products meet British government standards.[11]
- Even if you don't have the capability to inspect these IT systems, nation states do. Align your procurement practices with those tested and approved by one you trust.

Incident No. 3: Stuxnet Cyberwarfare Attack on Iranian Nuclear Infrastructure

Stuxnet, a nation-state-created piece of malware, became public knowledge in 2010. Although it is an excellent example of an advanced targeted attack, Stuxnet also demonstrates an IT supply chain integrity issue because of the way digital certificates were used to compromise a system's operational software supply chain.

What Happened

- Weaponized malware, which was reportedly created by the U.S. and Israel, targeted Iran.

- The targeted systems were not Internet-connected, so the compromise was carried out via USB transfer.
- The attack used a combination of attacks on Microsoft Windows zero-day vulnerabilities and ostensibly legitimate, digitally signed drivers. It targeted Siemens process control systems that were using embedded Windows.
- Before injecting its malicious payload, the attack was designed to look for specific Siemens settings to detect that it had been installed on a specific programmable logic controller (PLC) device.
- There were stolen certificates used to digitally sign code. They were signed by VeriSign, a leading, high-assurance provider of digital certificates worldwide.
- The Iranians turned to Eastern European malware firms for assistance with identifying the malware. Stuxnet was discovered by a Belarus-based, anti-malware firm.

Insights

- Supply chain issues don't end at the point the system is delivered. Supply chain integrity must extend to include operational supply chain issues.
- The goal of a compromise isn't always to acquire sensitive information and send it out. In this case, the goal was to cause physical damage to Iran's nuclear capabilities.
- Application control (also referred to as whitelisting) would have stopped this attack.
- This case highlights the risk of over-reliance on digital certificates for trust, as well as the limited way Windows-based systems deal with revoked certificates.
- Weaponized malware created by nation states will catalyze the fragmentation of the information security market. In February 2012, Iran announced it would ban the import of all foreign security software.[12]
- As an example of fragmentation of the Internet, in August 2012, Iran announced it was creating a second, parallel Internet for use by key agencies.[13]

Recommendations

- Even air-gapped systems are at risk. Look at all the ways executable code can be introduced to a system, and exercise disciplined change control processes on sensitive systems.
- Just because something is digitally signed doesn't mean it can be trusted. Stolen or compromised code-signing certificates are significant risks if they are trusted blindly. In addition to Stuxnet, a September 2012 incident, when Adobe certificates were compromised and used to sign malware, illustrates this point.[14] Augment the use of signed code with community-based certificate and file reputation services.
- Ensure that all software and firmware you are loading on a system is genuine:

- Receive software directly from manufacturer's media or website. Scan the files for known malware before installation.
- For open source, use only high-assurance repositories, using the latest versions and in compliance with a trusted compiler.
- Require strong digital signatures on all code that is received and verify.
- For sensitive systems, embedded systems or servers, use application control solutions built into the OS or from third-party providers that are designed to validate and restrict systems to running only high-assurance code (see "How to Devise a Server Protection Strategy" and "Toolkit: Application Control Evaluation and Selection Tool"; note: the latter document has been archived; some of its content may not reflect current conditions).

Incident No. 4: Flame Disclosed as Reconnaissance Element of Stuxnet

In 2012, Kaspersky Lab announced the discovery of Flame. Based on the company's analysis, Flame was written by the same organization as Stuxnet, and is the reconnaissance element of Stuxnet that was used to gather intelligence before Stuxnet was deployed. Once again, this is an excellent example of an advanced targeted attack, but also demonstrates another weakness in the IT software supply chain. With Flame, a compromise of digital certificate trust infrastructure was used to automatically load software updates to Windows-based systems.

What Happened

- Weaponized malware had the same genetic underpinnings as Stuxnet.
- Like Stuxnet, Flame was geographically targeted at Windows-based systems.
- The compromise was disclosed by Russian anti-malware company Kaspersky. It was not detected by Symantec, McAfee or others until after Kaspersky's discovery.
- Flame can turn on camera, microphone and other system capabilities without user acknowledgment or any indication to the user that these capabilities are active.
- According to a Symantec researcher, Flame is also capable of deleting files.
- Flame uses a "man in the middle attack" on Windows software update services by registering itself as a proxy server for update.microsoft.com. It served a fake, malicious update that was signed with a Microsoft code-signing certificate.
- An MD5 collision was used to create "legitimately signed" Microsoft code.

Insights

- There is a growing fracture of trust of information security vendors along geopolitical axes.
- The compute cost to calculate the MD5 collision for the malicious code was estimated by cryptographic research to require as much as $200,000 worth of computing resources in a

traditional data center, although one-tenth of the cost when using alternative resources, such as Amazon Web Services (AWS), combined with more efficient algorithms.[15]

- Cloud computing will be used to help attackers.
- MD5 has been known as vulnerable since 1993, and was proven vulnerable in 2008. New Microsoft certificates are issued from a different root and signed with SHA-1.
- Certificates can no longer be blindly trusted, nor can automatic updates.
- Automatic updaters of all types represent an attractive target, and should be considered as part of a broader strategy for operational supply chain integrity.
- Most organizations don't have insight into the certificates and updaters in use on their systems.
- The techniques used will have future spillover effects into enterprise Windows systems.

Recommendations

- Now that MD5 collisions have been shown to be financially feasible and exploitable, ban the use of MD5 and, specifically, MD5-signed certificates. Furthermore, begin a survey of all digital certificates in use on your systems to identify and document the ones active on the network and the attributes they carry.
- Your enterprise process of certificate life cycle management should be documented and tested specifically for the following:
  - Document the process of certificate revocation across your IT systems that use them and how this will vary from system to system.
  - If internally created certificates are used, managing the keys associated with the certificates is a top priority.
  - Monitor security intelligence feeds for indications of compromised third-party certificates.
  - Consider the use of emerging certificate reputation systems.
- Disable or ban autoupdating applications, or restrict to only those from providers you trust and for which you have vetted the security of the update mechanism. Ideally, coordinate all software updates through centralized IT.
- Restrict access to sensitive infrastructure management systems via security or management tools (for example, software updates or VM live migration). Use a separate security and management control plane for servers, and tightly restrict access to these sensitive networks:
  - Check controls on software distribution and patch management systems to limit the number of people and systems that have access to these tools. Verify the strength of the authentication mechanism used.
  - If Intel's AMT or other similar OOB management system is used for system management, tightly control access to these systems. Require that they be placed on a separate network segment for servers and, ideally, for desktops as well.

Incident No. 5: ZTE Phone Backdoor

In May 2012, ZTE, a mobile phone manufacturer in China that is the fourth largest in the world, admitted that one of its Android smartphones had a backdoor installed in its software. This backdoor allowed an application that knew the hard-coded password to gain full root access to the system.

What Happened

- The problem was only found in smartphones shipped to the U.S. (the Score M model running Android 2.3.4 and distributed by MetroPCS).
- The discovery was made by an anonymous individual posting on Pastebin.com, and later confirmed by security researchers at Symantec and CrowdStrike.
- An application can grant itself superuser privileges, which allows for the installation of arbitrary applications and full access to any device-resident data.
- ZTE confirmed the presence of a "vulnerability" and apologized, but did not provide technical details about the backdoor. The company said that an over-the-air patch was being developed to fix the problem.
- Security research firm CrowdStrike said that its analysis of the backdoor indicated that it was used for pushing software updates. It was a crude mechanism in lieu of using official Google APIs for this task.
- Symantec indicated that physical access to the device was not needed to exploit the vulnerability, only the ability to trick the user into installing a rogue application.
- In testimony before members of U.S. Congress on 13 September 2012, ZTE reaffirmed its assertion that this was a "software bug," no different than those of other IT vendors.

Insights

- Details of the case are sparse, with the fact that only U.S.-destined phones were affected leading to wide speculation. There is no way to know whether this is the first and only backdoor or just the tip of an iceberg. In theory, there could be many backdoors like this on many devices from different manufacturers, although, if the number were large, there would likely be multiple discoveries similar to the ZTE case.
- The backdoor is not necessarily an indicator of official company policy. Instead, it could be developed and installed by a disgruntled or rogue employee, assuming he or she circumvented source-code control and deployment management systems.
- Comprehensive, operational software supply chain integrity must include disclosure and investigation into the robustness of the software update mechanisms.
- In the future, a clever hacker could install a backdoor and camouflage it as a configuration or system management process error, in which the backdoor has an ostensible, legitimate

purpose (that is, debugging or software update support) as well as a hidden, more nefarious one.

Recommendations

- The code in question was possibly a poorly implemented software update mechanism. Ask all hardware and software suppliers for specific information on their mechanisms for updating firmware and software elements:
  - How are updates performed? Are they pushed or pulled?
  - What channel do they use, and from what location?
  - Can my organization block updates and coordinate these centrally?
  - How is authentication performed? If certificates are used, what type? How are certificates managed?
  - How is integrity of the conversation protected from snooping and tampering?
  - If the platform (Google's Android, in this case) provides code update mechanisms, why aren't they used?

Incident No. 6: 2012 Backdoor in Chinese-Manufactured FPGAs

In the most recent example, Sergei Skorobogatov, a Ph.D. candidate at the University of Cambridge released a draft paper in June 2012 on his research into silicon chips exploits.[16] In his research, he announced that he had discovered a backdoor built into the silicon in the Microsemi/Actel ProASIC3 FPGA chips manufactured in China. A technique called Pipeline Emission Analysis (PEA) was used to discover the backdoor. According to his paper, "This backdoor has a key, which we were able to extract. If you use this key, you can disable the chip or reprogram it at will, even if locked by the user with [his or her] own key. This particular chip is prevalent in many systems, from weapons [and] nuclear power plants to public transport. In other words, this backdoor access could be turned into an advanced Stuxnet weapon to attack potentially millions of systems."

The incident was real, but overhyped. Since that time, other researchers have reported that the backdoor did not originate from its original Chinese manufacturers, and that Actel (a California-based company) inserted the backdoor as a built-in debugging interface. According to Errata Security researcher Robert Graham, the backdoor required physical access to the chip via its Joint Test Action Group (JTAG) interface, which was created to test circuit boards.[17],[18] JTAG technology is widely used as a debugging practice to avoid expensive and customized debugging interfaces for each chip.

What Happened

- A backdoor was documented in FPGA chipsets.
- The chips were manufactured in China, creating a significant amount of initial speculation of a hardware supply chain integrity issue.

- Since disclosure, the backdoor has been traced to U.S.-based Actel, which claims the backdoor was there for the testing of circuit boards.

Insights

- The amount of coverage the incident received is indicative of the amount of hype, sensitivity and growing awareness of the issue of IT supply chain integrity, especially when competing geopolitical alignments are involved.
- Advanced techniques, such as PEA, are necessary to find compromises, backdoors and vulnerabilities in FPGAs.
- Backdoors are an issue with any system and used for a variety of legitimate reasons, such as debugging code and testing paths.

Recommendations

- Require IT suppliers to be transparent about the functions that are implemented in firmware, PLAs or FPGAs. However, the vendors' need to protect the sensitive intellectual property (IP) embedded in FPGAs is at odds with the need for transparency by potential customers. In cases where direct access is not provided, independent third-party inspection and verification are needed.
- Static or predictable default passwords represent a similar IT supply chain risk. Ask specifically about the presence of default or hard-coded passwords.
- Ensure that all testing and debugging interfaces (hardware or software) are disabled and, ideally, removed when the IT system is shipped.

Other Examples of Potential IT Supply Chain Integrity Compromises

- **Backup keys built into Windows —** In 1999, Windows NT 4 Service Pack 5 was released. Microsoft failed to remove its debugging symbols in advapi32.dll, a security and encryption driver. Andrew Fernandes, chief scientist with Cryptonym, found a primary key stored in the variable _KEY and a second key labeled _NSAKEY. Although there was knowledge of a second key in Windows, the disclosure of the "NSA" naming scheme set off a firestorm of speculation that it was owned by the U.S. National Security Agency (NSA), and could be used to subvert Windows cryptography. In addition, a third key was discovered in Windows 2000 by Dr. Nicko van Someren.[19]
- **Attempt to place backdoor in Linux kernel —** In 2003, an attempt was made to place a deliberate bug into the main Linux distribution that would have enabled backdoor root access. The bug was discovered during review, and no distributions were compromised. It did highlight, however, the importance of disciplined change control processes for Linux kernel source code management, including digital signatures and hashing to detect tampering (at the time, BitKeeper, which was later replaced by Git).

- **Loss of key randomness in Debian Linux —** In 2006, a reported mistake by a Linux distribution maintainer commented out a critical set of randomization commands within the Debian OpenSSL implementation that remained undetected for more than two years. This critically weakened the security of the keys created to the extent that every key pair recreated during that time had to be considered compromised and replaced. This incident again highlighted a risk: Although the open-source software (OSS) culture values forward redistribution, this allows anyone who can modify the code to do so, often without the changes being reviewed by the original code developers.

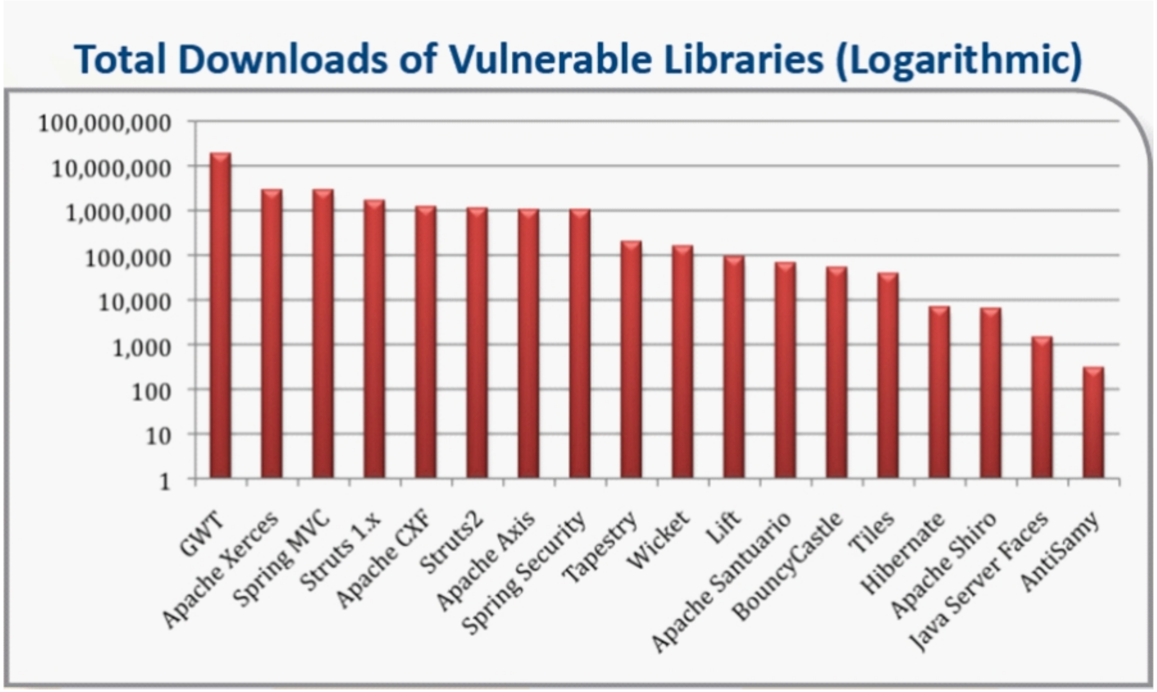
- **Loss of key randomness in Windows —** In 2007, a weakness in Windows cryptography via its pseudorandom number generator was disclosed, affecting all versions of Windows 2000 and XP. This vulnerability was not addressed until Windows XP Service Pack 3 in 2008.[20] The implication of the weakness was that a buffer overflow or a similar attack could be used to learn a single state of the random number generator, which can then be used to predict all random values, such as those used on Secure Sockets Layer (SSL) keys.[21]

- **Unknown root certificates in browsers —** In 2010, the Mozilla open-source project disclosed that the Firefox browser contained a root certificate authority that, at the time, appeared to not have a known owner, and that it had been present for an unknown amount of time (the same certificate was also discovered on the Apple OS). The presence of an unknown root certificate on multiple systems created a significant concern, since the use of the certificate by the owner would have enabled unlimited access to decrypt SSL traffic for an extended period of time. Later, RSA, The Security Division of EMC, claimed ownership of the certificate, raising questions on how a vendor trusted with this critical element of Web trust infrastructure had demonstrated such poor certificate management processes, losing track of the certificate.

- **Claims of backdoors in OpenBSD —** Also in 2010, Theo de Raadt, OpenBSD founder and developer, published an email he received claiming that the U.S. FBI had paid OpenBSD developers to leave backdoors in its IPsec network security stack. Since that time, audits found some questionable code, which was believed to be unintentional mistakes. However, the original source stands by his assertion of compromise. Contributors have denied any wrongdoing, and the allegations remain unproven.

- **Study of vulnerable libraries and frameworks —** In 2012, a joint study by Aspect Security and Sonatype found that 26% of the 113 million OSS downloads they analyzed from more than 60,000 organizations over a six-month period contained known vulnerabilities. The most notable impact came from the download and usage of known-vulnerable versions of Google Web Toolkit (GWT), but many outdated and vulnerable libraries and frameworks were routinely downloaded (see Figure 5).[21] The use of contaminated software in the creation of a finished software offering, whether inadvertent or intentional, is conceptually no different than the use of contaminated meat to create hamburgers. Both result in a final product that is compromised from creation.

Figure 5. Vulnerable Library Downloads



Source: Aspect Security and Sonatype

- Open source doesn't necessarily mean more secure. It just means more transparent. Commercial software and OSS contain risks.
- The OSS strength of allowing forward redistribution and changes by anyone is also a critical weakness if changes are not carefully reviewed by competent developers. There is also a weakness if Linux distribution maintainers, who may or may not be developers, make changes independent of Linux developers.
- Disciplined change management to source code requires a disciplined development process, whether commercial or open source, to reduce the chance of tampering and backdoor insertion.
- Although not a backdoor, weak cryptography implementations can create a false sense of security if the algorithms are believed to be strong, but compromised by mistake or design.
- Rather than write explicit backdoor code, hackers can create backdoors through deliberate coding errors that can later be explained as an unintentional mistake.
- Backdoors and duplicate keys represent significant risk if poorly implemented or misused.
- Certificates used as trust mechanisms will be targeted. This is the first of several attacks we will discuss that specifically target certificates.

- Usage of older, outdated and vulnerable libraries and frameworks, whether by mistake or by design, represents a significant threat to enterprise IT software supply chain integrity.

Recommendations

- If OSS is used, ensure that the libraries and frameworks are current, and compile the code yourself using a known, noncompromised compiler.
- Scan source code repositories and source code for the use of outdated and vulnerable versions of OSS libraries. Commercial solutions from vendors such as Palamida and Black Duck Software can help with this process.
- If commercial OSs are used, require the right to compile it yourself instead of receiving precompiled binaries from the vendor:
  - Where binaries are received, used commercially available binary scanning solutions to identify possible security vulnerabilities and backdoors.
  - Require proof of independent application security testing for all third-party applications, including any third-party libraries used in applications developed in-house.
  - Perform application security testing on all internally developed applications.
  - For internally developed applications, implement a source code management system within a broader application life cycle management framework to minimize developer access to the source code.

Absolute Trust in IT Supply Chains Is Naive: Adopt Mistrust as a Guiding Principle

Consider the following:

- There are no silver bullets. Perfect security is impossible. Absolute trust is misguided. Trade-offs are necessary.
- It is easier to attack software than hardware. Hackers will take the path of least resistance to attack software supply chains, including operational aspects.
- For trusted computing, you must have a foothold of trust from which to work.
- Information and IP theft is almost always the goal, not physical damage.
- In IP theft cases, information must be communicated out for it to be useful. Thus, even if the compromised system isn't initially detected, it may be possible to detect the exfiltration of the information.
- Your IT supply chain is only as strong as its weakest link. Contractors, outsourcers and third-party suppliers will be targeted if their security practices as not as strong.
- Whitelist-based IT ecosystems are inherently more secure than blacklisting-based systems, but harder to manage. The whitelisting mechanisms will be attacked.

- The mechanisms of trust for software and information interactions, such as digital certificates, strong authentication and DNS, will be increasingly targeted, and must be strengthened.
- Just as with other types of military arms, weaponized malware will find its way into the hands of traditional criminals and hackers.

Rebuilding Trust in the IT Supply Chain: Maverick Implications

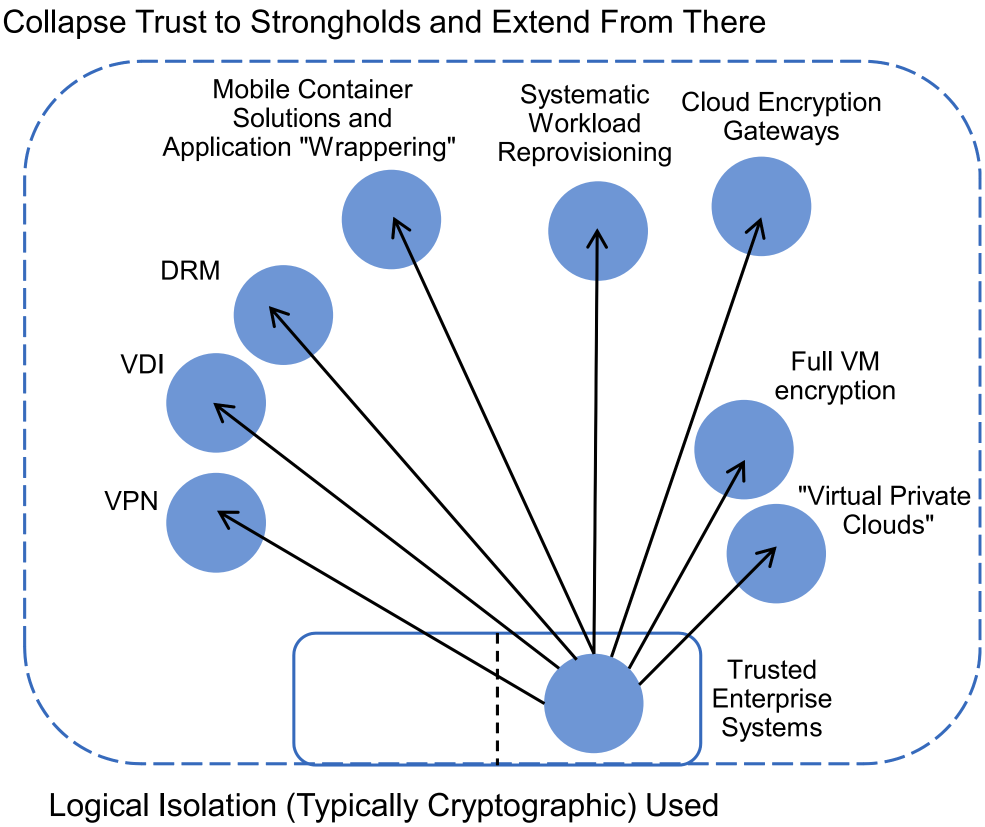
IT supply chain integrity issues are expanding from hardware into software and information. They are growing more complex as IT systems are assembled from a large number of geographically diverse providers, and, now of mainstream concern to enterprise IT. These issues are not just about defense and intelligence. This has significant implications for businesses, governments and individuals moving forward in a world where the integrity of the IT supply chain is no longer completely trustable, and where all layers of the IT stack will be targeted for supply chain compromise.

As a result:

- Information security market spending will fragment along geopolitical lines. Specific early examples of this fragmentation are already occurring:
  - In 2005, the U.S. government blocked the acquisition of Sourcefire by Check Point Software Technologies.
  - In 2008, the U.S. government blocked the acquisition of 3Com by Huawei.
  - Several agencies within the U.S. government have banned the use of Kaspersky Lab.
- China's 2007 specification for the multilevel protection of information security imposes several requirements on the security products used in sensitive IT systems. It requires that companies are invested in or controlled by Chinese citizens, or legal people of the state, and have independent legal representation in China.[22]
- More recently, in 2012, Iran banned the use of foreign security products, stating its intent to create its own anti-malware industry.[23]
- The OS market for defense and intelligence will fragment, and fragment again within critical enterprise industries along geopolitical lines, where there will be a determined shift away from the use of Microsoft Windows for critical industries and process control systems. Specific examples of this fragmentation include the following:
  - Cuba is replacing Windows with Nova.[24]
  - Within China, several initiatives are occurring:
    - China is requiring the use of Red Flag Linux in Internet cafes.[25]

        - A Chinese alternative to Windows is being developed for national defense and PC makers to improve IT security, according to China's Ministry of Industry and Information Technology.[26]
        - Another Chinese OS, Kylin, has been developed by the National University of Defense Technology.[27]
    - In 2010, North Korea began its rollout of Red Star Linux.[28]
    - At the end of 2010, it was reported that Russian Prime Minister Vladimir Putin issued a directive that all Russian enterprises move from Windows to open-source Linux by 2015, although the effort appears to have stalled.[29]
- "Trusted" chip fabrication programs, such as the Trusted Foundry Program in the U.S., will be required for use by the defense and intelligence industries, with an associated preference for onshore production of chips for use by defense/intelligence within geopolitically aligned countries.[30]
- Trust rooted in geopolitical alignment will become a factor in the decision to offshore software development, impacting the use of Russia and China for engineering, software development and manufacturing by enterprises aligned with Western aligned nations.
- The need for transparency and inspection will be one factor in the shift away from proprietary hardware onto standardized x86-based and ARM-based platforms, combined with a shift of intelligence into software for transparency (such as software-defined networking, storage and information security controls).
- Reduced scope of trust (RSOT) strategies will become a mainstream approach for the use of untrusted systems. RSOT-based systems establish footholds of trust in a small number of IT systems, using them to extend into untrusted systems in a hub-and-spoke-type model (see Figure 6).

Figure 6. RSOT


Collapse Trust to Strongholds and Extend From There
Mobile Container Solutions and Application "Wrappering"
Systematic Workload Reprovisioning
Cloud Encryption Gateways
DRM
VDI
VPN
Full VM encryption
"Virtual Private Clouds"
Trusted Enterprise Systems
Logical Isolation (Typically Cryptographic) Used

DRM = digital rights management; VDI = virtual desktop infrastructure

Source: Gartner (October 2012)

This strategy reduces the scope of trust to a smaller number of high-assurance systems and images, including the following:

- The use of trusted hypervisors and processors to gain footholds on otherwise untrusted systems
- Encryption and tokenization to logically contain sensitive information on untrusted networks, storage, systems and memory
- A shift toward containerization of applications/computing sessions as an alternative to full system isolation

- Some enterprises are separating Internet access from systems that handle sensitive information. For some, strong military-grade, multilevel-type separation will be required. For most, "good enough" isolation, using commercial-grade hypervisors and application containers, will be sufficient.

- New mechanisms and distributed models of trust will emerge to support the shift to software and information-based economies, where absolute trust, based on direct ownership and control, is replaced by a notion of "trustworthiness" supplemented by reputation services at all layers of the IT stack (for example, IP reputation, URL reputation, certificate reputation, identity reputation and information reputation services).
- Compromised software will be more likely than compromised hardware. For this reason, most enterprise efforts should focus here. For protection from IT software supply chain compromise, consider the following:
  - Enterprises will begin a shift to a whitelisting-based computing model, using default deny environments for desktops and servers (see "Predicts 2012: Sophisticated Attacks, Complex IT Environments and Increased Risks Demand New Approaches to Infrastructure Protection").
  - To enable user flexibility within whitelisted environments, curated app stores and enterprise app stores will play an increasing role for enterprise IT.
  - IP, URL and application reputation services will become increasingly important elements of enterprise information security strategies.
- As information supply chains become common, information itself will become a target for compromise.
- Tokenization and format preserving encryption will become mainstream strategies for the protection of information on untrusted systems, including within enterprise data centers. By 2020, more than one-half of the data in enterprise storage will be encrypted, up from less than 5% in 2012.
- In the longer term, mechanisms for trust fault-tolerant systems and commercially feasible homomorphic encryption will offer alternative approaches for securing IT supply chains.

Changes in Mindset for Enterprise IT

In addition to the recommendations discussed in the previously mentioned incidents, there are further changes necessary in the way that IT systems are developed, procured, deployed and supported within enterprise IT departments.

Here are some recommended changes:

- Enterprises should formalize their vendor risk management programs to incorporate IT supply chain risk management. Governance, risk and compliance (GRC) vendors, such as EMC (RSA Archer), Symantec and Agiliance, have risk management capabilities that are extendable to IT supply chain risk management functions. Furthermore, vendors such as Veracode have integrated their software risk analysis output into these risk management platforms.
- Avoid new investments in proprietary hardware for new IT systems, and use standardized CPUs, such as x86 or ARM, where possible. Favor vendors that provide solutions based on standardized hardware, ideally, with the alternative deployment option of using virtual, rather than physical, appliances. This shifts most supply chain integrity concerns into software, which

is more readily assessable for security risks. For example, Check Point's security appliances and EMC's storage array appliances are now based on x86 architectures. For ARM-based systems, use silicon from high-assurance providers only.

- Move intelligence out of hardware and into software where it is more transparent, and can be more readily assessed for backdoors and hidden vulnerabilities. This applies to networking, storage, printing and security functionality (also referred to as software-defined networking, storage and security). The hardware in question performs simple functions such as packet forwarding, reading/writing bits to media, printing bits, allowing/denying packets to be forwarded and so on. The intelligence of these hardware systems shifts into software-defined systems that are driven by policy.

- Assume IT systems will be compromised. For a compromised system to be useful, the sensitive information it collects must be communicated out. Although this doesn't stop the initial supply chain compromise, it makes it more difficult to exfiltrate sensitive information. Activate IP and URL reputation services on all inbound and outbound communications through next-generation security policy enforcement solutions, such as network firewalls, network intrusion prevention systems (IPSs), secure Web gateways, secure email gateways, and URL and file reputation at endpoints. For example, such policies could block users from navigating to websites with low reputation cores or outbound communications to IP addresses in specific geographic locations that your organization doesn't trust.

- Upgrade to modern desktop and server hardware and OSs that support hardware-based, root-of-trust mechanisms to ensure the integrity of the firmware (BIOS or UEFI), bootloader, OS, drivers, and the network and management stack. Examples include Windows 7, which supports Trusted Execution Technology (TXT)-based root-of-trust measurements with BitLocker. Windows 8 takes this further with the use of TXT and UEFI to perform a secure and trusted boot process (see "Effectively Securing Windows 8 Requires Rethinking Endpoint Security Approaches").

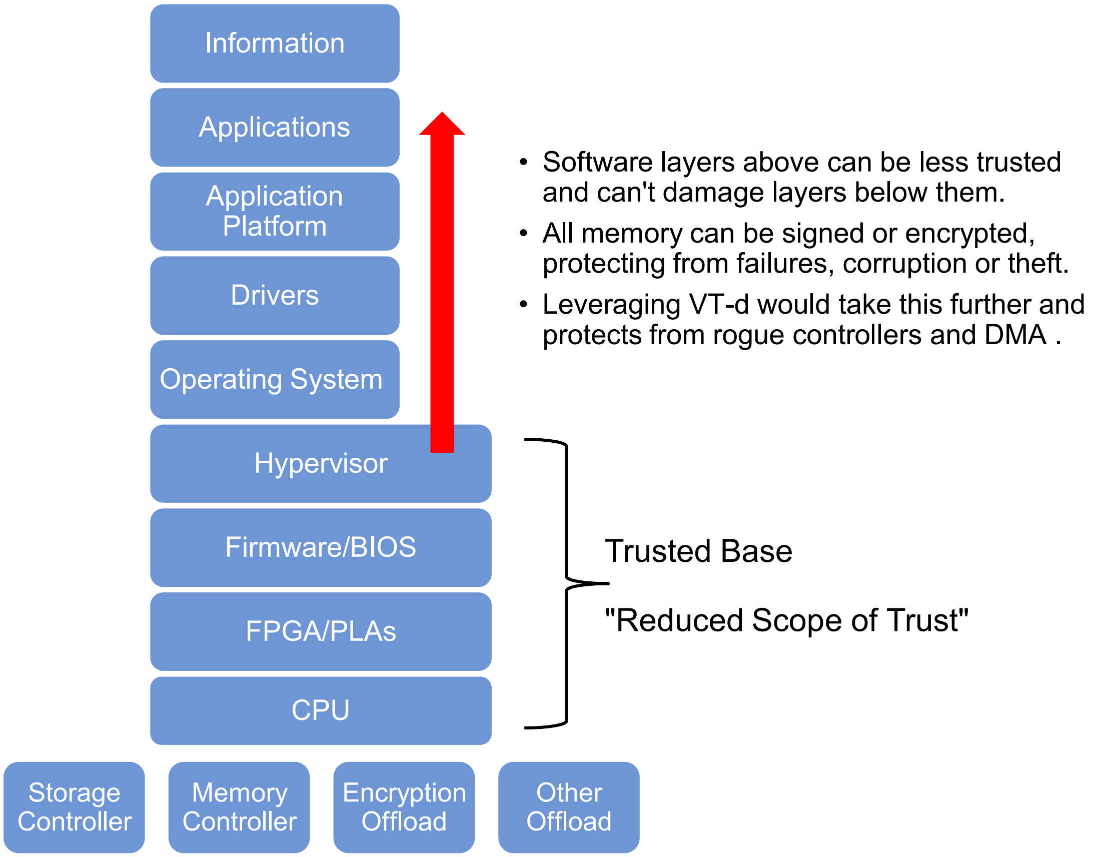
- To protect against exploits of intentional coding mistakes, such as a buffer overrun, upgrade to modern desktop and server OSs with better vulnerability mitigation capabilities. For example, the latest versions of Windows, Linux and Mac OS support the AMD No eXecute (NX) and the Intel Execute Disable hardware-based memory protection. They also address stack layout randomization to thwart attacks that rely on a specific memory offset to work. In addition, control the use of DMA to protect physical memory from unauthorized access. A modern IT system's firmware should enable this protection as early as possible, preferably within the initial boot firmware.

- To isolate potentially compromised applications, use a containerlike approach, where applications dealing with untrusted data (such as from browsing the Internet, handling content that originated from outside the enterprise and so on) are "sandboxed" from the core set of trusted applications and data. This can be accomplished without requiring VMs by using application sandboxing solutions from vendors such as Trustware, Invincea and Quarri. However, full virtualization could make this isolation stronger. The most sensitive systems require general Internet access, Web conferencing and arbitrary applications to be provided through a separate VM, such as a VDI session running in the demilitarized zone (DMZ). Sensitive system access would be through a separate, isolated session or vice versa, where the VDI session in the data center is used to handle sensitive system access. More recently, Bromium has introduced a technology that achieves strong application isolation through the use of Intel's Virtualization Technology, without having to hook the Windows kernel or use multiple, full VMs.

- Adopt a controlled application environment for systems dealing with sensitive data. Consider the adoption of application control/whitelisting for end-user desktops that handle sensitive information (for example, solutions from vendors such as Bit9, McAfee, Lumension Security, CoreTrace and others). In controlled application ecosystems, file reputation services based on communities (Web) of trust will be increasingly used to fill in the shades of gray when files are not known to be either "good" or "bad," such as those being developed by Bit9, Microsoft, Symantec, Trend Micro, Lumension Security and McAfee.
- At the data level, consider "disinformation" strategies, so that useful sensitive information is difficult to discern from a larger amount of useless sensitive information. This technique is useful for commercial enterprises as well. In a recently reported incident, this approach was implemented by an organization using salesforce.com. False customer and sales information was placed into the system. When the information (or disinformation) showed up later in the hands of a competitor, the information breach was traced back to a recently fired employee.
- Use a trusted hypervisor to gain a trusted foothold in the IT stack. This is a form of an RSOT system, which was discussed earlier. VMware and Citrix have thin hypervisors suitable for most enterprise separation requirements. For military-grade security, separation kernels are also available from Green Hills Software, LynuxWorks and others. More recently, PrivateCore has entered the market with a hardened hypervisor that is capable of strong separation, including memory encryption.

  In addition to providing strong separation among untrusted VMs, virtualization provides a layer of isolation of the hardware from the OS and applications, potentially providing protection from attacks on compromised hardware that require software running on the system to activate the compromise (see Figure 7).

Figure 7. Trusted Processor and Virtualization Platform



- Software layers above can be less trusted and can't damage layers below them.
- All memory can be signed or encrypted, protecting from failures, corruption or theft.
- Leveraging VT-d would take this further and protects from rogue controllers and DMA .

VT-d = Intel Virtualization Technology for Directed I/O

Source: Gartner (October 2012)

Virtualization layers provide the ability to "introspect" the contents of the VMs running on them to provide an "outside-in" perspective of the VM, as well as security controls that may run in the VM itself (see "Radically Transforming Security and Management in a Virtualized World: Concepts" and "Radically Transforming Security and Management in a Virtualized World: Considerations"; note: these document have been archived; some of their content may not reflect current conditions). This provides the ability to detect deeply rooted systems and abnormal OS behaviors that traditional anti-malware solutions running within the VM would not be able to detect.

- Whenever a trusted system communicates with, stores or has another untrusted IT system handle its data, the information should be encrypted or tokenized:
  - Although encryption isn't perfect, it reduces the scope-of-trust problem to one of key management/dictionary management and memory protection while keys are being handled.

- Largely a result of Payment Card Industry (PCI) security guidelines, tokenization techniques are gaining traction where a dictionary is used to map sensitive information to the tokenized information stored. Unlike encryption, there is no mathematical way to arrive at the original data, collapsing the scope of trust to the protection of the system holding the mapping dictionary and function.
  - Beyond encrypting the data that moves to untrusted systems, enterprises should encrypt all important data within their data centers. This acts as a form of whitelisting, where only the systems that require access to the sensitive data have the keys. This reduces the scope of trust to key management, and decreases the aperture for the theft of sensitive data.
- This also applies to information being stored on consumer mobile devices or the public cloud, which are also equally untrusted.[31]
- In the longer term, homomorphic encryption offers promise by enabling mathematical manipulation and analysis of encrypted information, without sacrificing confidentiality.[32] However, no commercially feasible implementation has yet been delivered.[33]

Trust Resiliency

A longer-term protection mechanism against compromises in supply chain integrity at the hardware level for extremely sensitive systems is the concept of "trust resiliency." Just as a highly available system can be created out of individual, less highly available parts, a highly trustable system can be created out of individual, less trustable parts. The approach will use multiple systems from different hardware providers — for example, different OEMs and, ideally, different chipsets that are placed on logically separate network segments, fed the same input and monitored for differences using a voting mechanism. Expanding the notion of resiliency to security and trust raises the bar for IT supply chain compromises. To succeed, each system would have to be compromised in exactly the same way at the same time across multiple hardware system providers and network segments.

Bottom Line

IT supply chain integrity issues are real, and will have mainstream enterprise IT impact within the next five years. In the shorter term, the market for information security offerings will fragment along geopolitical lines. In the longer term, the same will happen for OSs and other IT system infrastructure software, reshaping the IT landscape moving forward. Enterprise IT departments must begin to make changes today to protect their systems and information in a world where all IT systems are suspect. These changes in information protection strategies will help enterprises embrace and adopt cloud computing and consumerization, which have strikingly similar issues with untrusted systems.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Toolkit: Create and Implement a Supply Chain Risk Management Framework"

"DoD Supply Chains Face 21st-Century Threats"

"Sharing Your Data Without Losing It: Controlling Your Data on Their Desktop"

"Cloud IaaS: Security Considerations"

"Assessing the Security Risks of Products and Services"

Note 1 Roots of the Word "Maverick"

Derived from the name of Texas rancher Samuel Maverick and his steadfast refusal to brand his cattle, "maverick" connotes someone who willfully takes an independent — and frequently disruptive or unorthodox — stand against prevailing modes of thought and action.

Note 2 Commonly Held Belief

The issue of supply chain integrity is not new. However, it is usually referred to in the context of enterprise supply chain management (SCM). Issues with IT SCM are usually considered to be a concern of government defense and intelligence organizations, with little impact on enterprise customers. This is a mistake. Another commonly held belief is that, even if IT supply chain compromises occur, there is little that a typical enterprise can do to protect itself. We disagree. Here, we explore the implications of issues in the IT supply chain, including hardware, software and information supply chains. We believe this will become a mainstream issue for all enterprise IT departments within the next five years. Many of the implications and strategies explored in this research are new, with no substantive prior art in this area.

Evidence

[1] Meinck, C. (22 February 2012). "Air Force Special Ops Command Cancels Plans to Purchase iPads." Retrieved from www.everythingicafe.com/air-force-special-ops-command-cancels-plans-to-purchase-ipads/2012/02/22.

[2] Brewin, B. (17 February 2012). "Air Force Special Operations Command Eyes Russian Security Software for iPads." Retrieved from www.nextgov.com/defense/2012/02/air-force-special-operations-command-eyes-russian-security-software-for-ipads/50667.

[3] Ike Skelton National Defense Authorization Act for Fiscal Year 2011, H.R. 6523. 111th Congress, Section 806 (2011).

Section 806 defines the term "supply chain risk" as the risk that an adversary may sabotage, maliciously introduce an unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

[4] U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology. (January 2010). "Defense Industrial Base Assessment: Counterfeit Electronics Evaluation." Retrieved from

www.bis.doc.gov/defenseindustrialbaseprograms/osies/defmarketresearchrpts/final_counterfeit_electronics_report.pdf.

[5] U.S. Government Accountability Office. (February 2012). "DoD Supply Chain: Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platforms." GAO-12-375. Retrieved from www.gao.gov/assets/590/588736.pdf.

[6] Greenberg, A. (23 March 2012). "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits." Forbes. Retrieved from www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits.

[7] Greene, T. (25 April 2012). "VMware Source Code Stolen, Impact Unclear." Network World. Retrieved from www.networkworld.com/news/2012/042512-vmware-source-code-258680.html.

The hacker taking responsibility for the leak claimed that he possessed a total of about 300 megabytes of VMware source code, part of which was posted. He said the data was part of a cache taken from a previously reported breach of a network belonging to the Beijing-based China National Electronics Import & Export Corporation, which works with the Chinese military.

[8] Barker, G. (27 July 2012). "China's Huawei Banned From NBN." Financial Review. Retrieved from www.afr.com/p/technology/china_giant_banned_from_nbn_9U9zi1oc3FXBF3BZdRD9mJ.

[9] Maley, P. and Bingemann, M. (28 March 2012)."Spies Feared China Was Hacking the NBN." The Australian. Retrieved from www.theaustralian.com.au/national-affairs/defence/spies-feared-china-was-hacking-the-nbn/story-e6frg8yo-1226311796483.

[10] "Update 2 — China's Huawei Negotiating Conditions to Join U.S. Hearing." (7 September 2012). Retrieved from in.reuters.com/article/2012/09/06/huawei-hearing-idINL2E8K69XO20120906.

[11] Espiner, T. (7 December 2010). "Huawei Opens Cybersecurity Testing Centre in U.K." ZDNet. Retrieved from www.zdnet.com/huawei-opens-cybersecurity-testing-centre-in-uk-3040091082.

[12] Isayev, S. and Jafarov, T. (20 February 2012). "Iran Bans Import of Foreign Computer Security Software." Trend. Retrieved from en.trend.az/regions/iran/1994160.html.

[13] Isayev, S. (7 August 2012). "Iran to Unplug Key Agencies From Internet." Trend. Retrieved from en.trend.az/regions/iran/2053991.html.

[14] Arkin, B. (27 September 2012). "Inappropriate Use of Adobe Code Signing Certificate." Retrieved from blogs.adobe.com/asset/2012/09/inappropriate-use-of-adobe-code-signing-certificate.html.

[15] Sotirov, A. "Analyzing the MD5 Collision in Flame." Retrieved from trailofbits.files.wordpress.com/2012/06/flame-md5.pdf.

[16] Skorobogatov, S. and Woods, C. (5 March 2012). "Breakthrough Silicon Scanning Discovers Backdoor in Military Chip." Retrieved from www.scribd.com/doc/95282643/Backdoors-Embedded-in-DoD-Microchips-From-China.

[17] Graham, R.D. (28 May 2012). "Bogus Story: No Chinese Backdoor in Military Chip." Retrieved from erratasec.blogspot.com/2012/05/bogus-story-no-chinese-backdoor-in.html.

[18] JTAG Technologies — www.jtag.com

[19] _NSAKEY — en.wikipedia.org/wiki/NSAKEY

[20] Dorrendorf, L; Gutterman, Z.; and Pinkas, B. (4 November 2007). "Cryptanalysis of the Random Number Generator of the Windows Operating System." Retrieved from eprint.iacr.org/2007/419.

[21] Williams, J. and Dabirsiaghi, A. (March 2012). "The Unfortunate Reality of Insecure Libraries." Retrieved from www.aspectsecurity.com/uploads/downloads/2012/03/Aspect-Security-The-Unfortunate-Reality-of-Insecure-Libraries.pdf.

[22] China's Article 21, Multi-Level Protection Scheme Management policy document No. 43, issued 22 June 2007.

[23] Isayev, S. and Jafarov, T. (20 February 2012). "Iran Bans Import of Foreign Computer Security Software." Trend. Retrieved from en.trend.az/regions/iran/1994160.html.

[24] Israel, E. (11 February 2009). "Cuba Launches Own Linux Variant to Counter U.S." Reuters. Retrieved from www.reuters.com/article/2009/02/11/cuba-software-idINN1137270420090211?rpc=44.

[25] Racicot, J. (5 December 2008). "China's Red Flag Linux." Cyberwarfare Magazine. Retrieved from cyberwarfaremag.wordpress.com/2008/12/05/china-red-flag-linux.

[26] China Daily. (17 December 2010). "China Developing Own Operating System to Challenge Microsoft." Retrieved from www.chinadaily.com.cn/business/2010-12/17/content_11717626.htm.

[27] Xinhua News Agency. (5 December 2006). "Computer Server Operating System Developed." Retrieved from www.china.org.cn/english/China/191263.htm.

[28] Clarke, G. (7 April 2010). "North Korea Mobilizes Red Star Linux Rollout." The Register. Retrieved from www.theregister.co.uk/2010/04/07/linux_north_korea.

[29] Brownlee, J. (28 December 2010). "Russia to Adopt Linux as National Operating System by 2015." Retrieved from www.geek.com/articles/news/russia-to-adopt-linux-as-national-operating-system-by-2015-20101228.

[30] Trusted Foundry — www.trustedfoundryprogram.org

[31] For example, one of the branches of the U.S. Armed Forces used a solution from Voltage Security to protect veteran's healthcare information being analyzed by outsourced firms and universities. Through careful consideration of how and what data was tokenized, external service

providers were able to provide statistical analysis and summaries of the data without handling the sensitive data directly.

[32] "IBM Researcher Solves Longstanding Cryptographic Challenge." (25 June 2009). Retrieved from www-03.ibm.com/press/us/en/pressrelease/27840.wss.

[33] Hayes, B. (September/October 2012). "Alice and Bob in Cipherspace." American Scientist. Retrieved from www.americanscientist.org/issues/pub/2012/5/alice-and-bob-in-cipherspace.

[34] Naehrig, M.; Lauter, K.; and Vaikuntanathan, V. (6 May 2011). "Can Homomorphic Encryption Be Practical?" Proceedings of the Third ACM Workshop on Cloud Computing Security (pp. 113-124).

This is part of a set of related research. See the following for an overview:

- Drive Disruptive Innovation With Maverick* Research

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.