Key Considerations in Building and Operating Trustworthy Systems: The Role of the Trustworthy Vendor

Executive Summary

In the 21st century, the world has come to depend on local and wide-area data networks to support essential economic, social, and government services. To achieve their respective missions without interruption or human interference, private and public organizations need to deliver their services from a foundation of trustworthy information systems.

The trustworthy system concept encompasses networked products that provide continuously improved, evolving security designed to effectively anticipate and deter critical human-originated threats. Since no purposeful system or product generates itself by random chance, the creation and operation of trustworthy systems require the efforts of equally trustworthy vendors possessing the system knowledge, process expertise, and ethical compass to make good on the promise of trustworthy network platforms.

This paper provides an overview of Cisco’s vision of the verifiable trustworthy system. It covers key considerations of how organizations can achieve trustworthiness based on processes, technology development capabilities, and vendor partnerships. It explains the importance of creating a system that serves as a “root of trust” to meet the needs of governments, business, and citizens.

The trustworthy system model calls for building security directly into customer networks throughout their development and operational lifecycle, as supported by vendor processes, independent certifications, and supply chain practices. The paper examines the trustworthy system model and then reviews Cisco’s qualifications as a trustworthy vendor. While trustworthy systems can add to the cost of solutions through more rigorous product development practices, value-added features, supply chain processes, documented transparency, and post-production maintenance required for trustworthiness, the added cost more than pay for itself in the form of higher levels of service availability, asset and intellectual property protection, and public confidence in an enterprise’s integrity.

Building Trust in a Network-Dependent World

Today’s global society increasingly depends on the smooth and unimpeded operation of complex computing and communications networks for its very existence. Vital services, infrastructure, and institutions all rely on the availability and trustworthiness of local and global data networks. This includes air transportation, highways, railroads, global shipping, power grids, water supplies, and global financial networks, food supplies, government, universities, business, churches, school systems, and military organizations. Cisco predicts that the total amount of global Internet traffic will quadruple between 2011 and 2015, reaching 966 exabytes1 per year2. By 2016, the number of networked devices will reach three times the world’s human population3.

As society evolves, we create increasingly pervasive, networked technologies to meet changing demands. Networks touch more people using wider ranges of devices than ever before. In just one Internet minute, people today send more

---

1 966 *1018 bytes, or nearly a billion trillion bytes of data.
3 IBID.
than 204 million emails, view 20 million photos, access 6 million Facebook pages, and watch 1.3 million YouTube video clips.

No matter how we access networked services, we need to trust the information we consume along with the systems that deliver them. But the very richness and openness of the network creates the motive and opportunity for malevolent actors to misuse and misappropriate network-borne data, services, and resources. And even those who strive to add value to the network experience can inadvertently enable harmful behaviors. Consider social media companies who dangle attractive “free” services to users at the hidden cost of privacy. Or organizations that bypass security checks and balances to rush a new service to market.

Creating a truly secure network environment becomes even more complex as governments and business invest in mobility, collaboration, cloud computing, and other forms of virtualization. These capabilities improve resiliency, increase efficiency, and reduce costs, but also introduce additional risks. The security of the manufacturing processes creating information technology products is also now at risk, with counterfeit and tampered products becoming a growing problem. As a result, today’s government and corporate leaders overwhelmingly identify cybersecurity and associated trust issues as top concerns.

Five Hallmarks of Trustworthy Systems

Trustworthy products differentiate themselves from generic equivalents in five ways:

1. **Trustworthy products incorporate built-in security features and functions rather than adding them on as overlays to “ethically neutral” hardware and software.** To defending against the rapidly evolving body of threats to the integrity of network-enabled services increasingly requires the ability to secure business infrastructure and data through embedded protections built directly into IT infrastructures. The days of treating security as an overlay on top of ethically neutral, “universal machine” computing processes are over. Most of all, vendors need to set trustworthiness as a design goal in product development, and back this with appropriate and effective trustworthiness-directed design review and revision processes.

2. **Built-in trustworthy features include state-of-the art security technologies such as encrypted internal communications, usage and access controls, and policy management controls.** Trustworthy products incorporate security-focused features and functions that often go beyond those found in generic equivalents. These features can represent a positive enhancement to “standard” feature sets such as encrypted data communications that harden products and avoid design mistakes that increase product vulnerabilities to external attack.

3. **Trustworthy products comply with industry and government security standards relevant to customer business requirements.** Public sector buyers, for example, expect compliance with standards such as the Federal Information Processing Standard (FIPS) 140-2, Federal Information Security Management Act (FISMA), and international Common Criteria standards. Health Insurance Portability Accountability Act (HIPAA) patient information security standards apply to both private and public sector healthcare organizations, while retailers look for compliance with Payment Card Industry (PCI) data security standards.

4. **Trustworthy product vendors take steps to secure their product manufacturing and distribution supply chains against counterfeiting, tampering, or installation of unauthorized features and functions such as “back doors.”** Trustworthy vendors take care to maintain the integrity of their products against counterfeiting and tampering in the manufacturing and distribution processes. This can include authenticity and tampering protections embedded into products in addition to external procedural controls and audits.

---

Source: GO-Globe.com
5. **Perhaps most importantly, trustworthy vendors stand behind trustworthy products and systems, and are always ready to validate features, functionality, supply chain integrity, and business practices.** No matter how strong the security features and operational processes embedded into a network may be, we cannot trust the output of a networked system unless we can trust the vendors and service providers responsible for the system. Trustworthiness is easy to claim, but difficult to prove. Trustworthiness begins with transparency as the defining virtue of a truly trustworthy vendor. Vendors must candidly reveal their process for building secure products, enabling secure network architectures, protecting the integrity of manufacturing products, and delivering long-term solution maintenance and support.

**Trustworthiness Throughout the Solution Lifecycle**

Trustworthy systems provide the foundation for a continuous improvement approach to security that anticipates and preempts new threats. Such infrastructures not only protect critical information, but more importantly, help avoid interruptions of critical services. Trustworthy products supported by trusted vendors enable their users to minimize the costs and reputation damage stemming from information misappropriation, service outages, and information breaches.

Trustworthy systems, however, should not be confused with immunity from external attack. Information technology customers and users have an important role to play in maintaining the effectiveness of trustworthy systems in fending off attempts to corrupt their operations. This includes timely installation of security-focused updates and patches, constant vigilance in recognizing abnormal system behavior, and effective countermeasures against attack.

Technologies do not stand still, and neither do attackers. Ensuring system trustworthiness needs to cover the full lifecycle of a networked from initial design, through to manufacturing, system integration, daily operation, maintenance and updates, and ultimate decommissioning of the solution.

**Trustworthy Systems Require Trustworthy Vendors**

Vendor choice guides all forward steps in the trustworthy systems journey. Choosing a truly trustworthy vendor marks a significant step toward maximizing the economic and social returns of an information technology system over its lifetime. Choosing the wrong vendor can significantly damage enterprise information security and degrade overall return on information technology investment.

Trustworthy is as trustworthy does when evaluating vendor attributes. While almost all vendors will claim trustworthiness, vendor transparency will be the first and most telling indicator of trustworthy behavior. Trustworthy vendors will not hesitate to offer clear and independently verifiable information regarding:

- Product development methodologies and practices
- Solution architecture precepts and techniques
- Manufacturing supply chain security
- Post-installation system maintenance and support practices

**Choosing the Right Vendor**

As IT administrators invest in new products to help improve resiliency, increase efficiency, and reduce costs, they must choose a vendor that can offer a framework that supports the design, development, and operation of core infrastructures to meet high levels of security. Organizations should also challenge themselves to scrutinize the vendor’s reputation and behavior during of the buying decision-making process.

**You get what you pay for.** Many organizations continue to make network technology investment decisions based solely on low-cost bidder criteria. They rationalize this decision-making style on their perceptions of long odds against an attack on their particular infrastructure, plus a belief that any attacks that have occurred have proven to be relatively mild. To this
class of buyer, the risks posed by security breaches do not justify the added cost of trustworthy IT products and technologies.

This line of thinking ignores the growing destructive capabilities of hackers in our increasingly networked world, and the proliferation of vulnerabilities enabled by the shift to mobility, cloud computing, social media, and other new technologies. Although these new capabilities are not inherently dangerous, experience has shown that any new technology carries with it vulnerabilities unforeseen by its developers.

**Not all vendors are created equally trustworthy.** Because of past practices, limited resources, government requirements, experience, or business philosophies, not all vendors are qualified, willing, or able to develop trustworthy systems. Vendors are not inherently wicked, but trustworthiness, at least in the sense described in this white paper, is a new concept, and relatively few vendors have cultivated the disciplines required to make, sell, support, and validate the bona fides of trustworthy systems.

**Not all vendors are transparent about security processes.** IT customers need and should require visibility into vendor product, design, validation and manufacturing processes; supply chain management/outourced product quality assurance; cryptography policies; and other factors relevant to system trustworthiness. Most vendors do not provide this information, nor do they have organized, end-to-end programs to document trustworthiness, largely because most IT customers have not yet demanded this level of disclosure.

**Assumed Trustworthiness Versus Verifiable Trustworthiness**

If we increasingly rely on trustworthy systems to provide a foundation for improved IT security, it is important to distinguish between assumed trustworthiness and verifiable trustworthiness. Furthermore, once we understand these differences, we must figure out how to verify and maintain trustworthiness over the lifecycle of an IT solution.

Assumed trustworthiness is what we live with every day. We assume that other people walking down a street do not intend to harm us or that buying a sandwich in a shop will not immediately poison us. We base these assumptions on experience, and we apply the same assumptions in IT. If a system functions normally, we tend to believe that it will continue to behave normally and that malfunctions are exceptions, not the rule. We only question the trust we place in a system when it misbehaves.

Verifiable trustworthiness, by contrast, measurably and objectively validates ongoing system trustworthiness based on independently confirmable data and processes. Trustworthiness indicators may include the presence and use of signed software, hardware encryption checks and anchors, and regular system audits. A vendor’s reputation can serve as independent trustworthiness validation based on their history in the industry, customer references, analyst recommendations, and independently conferred product certifications.

Verifiable trustworthiness isn’t so much a goal as an ongoing process that continues through a product or solution’s lifecycle. Security standards, practices, and threats constantly evolve. Consequently, technology vendors must continuously improve product and solution security through:

- Building security checkpoints throughout the product and architecture solution development lifecycle
- Designing products to meet recognized international security standards, within a secure supply chain process
- Providing timely patches and updates to maintain trustworthiness and adherence to standards throughout product lifecycles
- Collaborating with other companies and institutions across the industry in the areas of threat intelligence, incident response, and development of ever more powerful and effective standards

The IT customer also has a role to play in verifying trustworthiness—by holding vendors accountable for keeping promises, checking customer and analyst references, validating vendor compliance to standards, and operating
trustworthy systems in ways that keep them trustworthy. Operational disciplines that maintain trustworthiness include taking a best practices approach to staying current with evolving standards, installing updates, remediating security vulnerabilities, and responding to threats.

Cisco as a Trustworthy Vendor
Cisco’s overall security vision is based on three principles:

1. Protect the entire network.
2. Protect anything and anyone connecting to a network.
3. Protect information that crosses the network.

Cisco’s approach to trustworthy systems calls for providing long-term, constantly evolving protection of data and services processed and delivered by an IT solution. Based on the concept of “trusted computing,” the trustworthy system integrates verifiable hardware, software, firmware, and services that provably demonstrate trust and effective risk management. Reinforced by multiple layers of security across the network, trustworthy products support the highest degrees of information assurance and availability.

Equally important, Cisco’s trustworthy systems initiatives incorporate the policies and processes that drive development of secure technologies, products, and solutions. Powerful security procedures throughout the manufacturing process protect users against counterfeit components and subsystems, malicious modifications to technology, and misuse of intellectual property.

Security Checkpoints Throughout the Product Lifecycle
Developing trustworthy systems means building security in from the ground up, from beginning to end of a product’s lifecycle. The Cisco Secure Development Lifecycle prescribes a repeatable and measurable methodology designed to build in product security at the product concept stage, minimize vulnerabilities during development, and increase resiliency of products in the face of attack.

Cisco establishes a “root of trust” at the heart of each trustworthy system element, with each hardware and software component validated throughout the process. Such an approach provides customers, developers, and partners with a comprehensive and secure design paradigm, well understood secure coding practices, and a background of thorough vulnerability testing and threat modeling. These processes create a baseline from which customers, developers, and system integrators can build secure solutions.

This baseline also applies to creating trustworthy network architectures. No longer walled gardens, today’s increasingly mobile-focused network environments are borderless, with access privileges defined primarily by who the user requesting services is rather than where a device resides. Securing this fluid new infrastructure requires a layered security approach that protects critical data through robust policies and their effective enforcement. Both network architectures and products are designed and built for compliance with international certification specifications through a secure supply chain process.

As a result, networks can validate policy-compliant operating hardware and applications when they join a network, and thereby help ensure the continued trustworthy operation of the entire network.

Within this protected infrastructure, data should be defended with state-of-the-art encryption. Cryptography provides confidentiality, integrity, authentication and non-repudiation of communications in public networks and storage centers. For an encryption system to have a useful shelf life and securely interoperate with other devices throughout its life span, the network must be designed to meet evolving security needs anticipated for the next ten or more years.

Cisco’s trustworthy systems concept provides developers with guidelines to incorporate secure, agile, high performance, and validated cryptography across its product portfolio. Cisco bases its products on a Trust Anchor Technology (TAT) that encompasses a number of hardware-rooted security building blocks:
First, the Trust Anchor Module helps to ensure customer device integrity through an anti-tamper smartcard secure processor providing secure storage, dedicated entropy source channel capacity, and immutable identity.

Second, Secure Boot procedures (through a secure processor, memory, and boot ROM) validate the system boot of a signed Cisco image on a Cisco platform.

Third, Cisco products carry a Standardized Secure Unique Identity set at the time of manufacture using anti-tamper storage. This unique ID validates the authenticity of the Cisco product when the system boots up.

Each area of the system embeds additional protections. For example, the Cisco Secure Development Lifecycle runs “signed” software, which safeguards against on-host threats that modify software processes while they run, at next reboot, or at some predefined moment.

Standards Compliance and Certification

As noted earlier, trustworthy systems need to meet international security certification and supply chain standards. Governments have stepped up international collaboration to combat cyber threats through development and enforcement of new, more consistent standards. International certifications also help ensure that users can confidently purchase standards-compliant equipment, that this equipment performs as advertised, lives up to security claims, and is compatible and interoperable with existing infrastructure.

Currently supported by 26 participating nations, the international Common Criteria standard has been extremely successful in providing capital equipment purchasing guidelines for government and business, and has been widely adopted as a purchasing requirement. Not surprisingly, Common Criteria compliance has become a defining element of trustworthy systems. Cisco strongly supports the Common Criteria effort as well as the U.S. Federal Information Process Standard (FIPS) 140-2.

Supply Chain Security

Global manufacturing and distribution supply chains have also fallen prey to attacks on their integrity through such means as product tampering, counterfeiting, theft, and intellectual property piracy. Along with meeting international design, feature, function, and quality standards for their products and services, vendors need to help ensure security of the manufacturing supply chain, combining traditional management practices with auditable, verifiable system security procedures. According to the US Department of Commerce (2010), 39 percent of companies and organizations unwittingly purchased counterfeit electronics between the years 2005-2008, with the number of counterfeiting incidents increasing from year to year. Supply chain security concerns show no signs of abating. A US Department of Defense (DoD) investigation in 2011, for example, showed that no fewer than 93 separate DoD suppliers had provided suspect parts on at least one occasion, and some did so up to more than 10 times.

Cisco’s supply chain processes feature multiple checkpoints to embed physical and logical security assurance verifications at each link of the company’s manufacturing and distribution chain. These combine traditional supply chain management practices with added emphasis on assuring specified security functionality of Cisco products, focusing on malicious modification or substitution of technology, misuse of intellectual property, disruption of the supply chain, and/or sales of counterfeit products. These processes strive to ensure that resulting Cisco technology platforms remain uncompromised by any threat vector, from early-phase product concept development to final delivery and installation in a government or corporate network.

---

Cross-Industry Collaborative Incident Response and Standards Maintenance

The final steps to maintaining confidence in a trustworthy system involves long-term post-installation interaction with IT infrastructure to support an effective incident and continuous-improvement approach to industry and government security standards compliance.

Trustworthy vendors must extend proactive intelligence to customers, and also provide a rapid and effective incident response to security attacks. This can be addressed by coordinated vendor programs that work to observe, protect, and create new standards for trustworthy systems.

Cisco’s Security Intelligent Operations (SIO) team is an industry leader in this area, maintaining interactive, collaborative relationships among Cisco customers and partners to integrate real-world information and intelligence into design processes, products, and after-sales service and maintenance. Although this effort primarily focuses on strengthening Cisco products, it takes an enlightened self-interest approach to sharing information with customers, partners, and even competitors to raise the general level of security features and functionality across the IT industry. In multivendor IT infrastructures, security can only be as strong as the environment’s weakest link.

Cisco also supports a 24/7 dedicated global task forces to manage the receipt, investigation, repair, and public reporting of security vulnerabilities related to products and networks. This team works closely with users, independent security researchers, consultants, industry organizations and other vendors to gather information, identify, and quickly counteract possible security problems. Cisco also supports monitoring of internal and external security threats, assessing third-party vendor products as well as Cisco products.

Cisco actively contributes to the work of industry organizations working on trusted computing and trustworthy networking initiatives. Cisco plays an important role as a member of the Trusted Computing Group, the Open Group, the Institute of Electrical Engineers (IEEE) Standards Association, and the Internet Engineering Task Force (IETF). Cisco also works closely with governments worldwide, and microprocessor makers (Intel, AMD, Cavium, Freescale, etc.) to establish the guidelines for the future of trustworthy systems. These organizations work to create more demanding standards for cybersecurity to improve the defense systems, companies, and nations against ever-changing attack vectors.

Trust, Confidence, Security, and Return on Investment

The concept of trust is taking center stage in the national and international conversation regarding supply chain, software, and hardware security. To establish the levels of trust sufficient to enable reliable IT-based economic and social processes, security must be a foundational priority covering all phases of product and solution development, IT operations, and service delivery.

To maintain public confidence in information technologies as the basis for economic and social benefit, we need confidence in the vendors that develop and deliver them. Vendors selling into, servicing, and supporting economically and socially vital marketplaces must therefore possess a proven track record of IT security trustworthiness. Trustworthiness is a customer-side issue as well. Businesses, governments and institutions that expect the public to trust them must be willing to invest in the operational disciplines required to deliver trustworthy products and services to their stakeholders.

Make no mistake. Trustworthy products and services cost more to produce and purchase than generic alternatives. But the extra cost of trustworthy products, services, and processes will be far less than the risks to reputation, property, assets, and ability to do business posed by taking a trust-agnostic approach to investment and operational budgeting decisions.

Those seeking trustworthy IT solutions and operations should expect vendors to provide full, transparent disclosure of development practices, product standards conformance certifications, supply chain integrity assurance processes, key employee credentials, and other evidence of product, solution, and business practice trustworthiness. IT customers need to rely on verified products that do precisely what they are installed and configured to do, not just assume that they will perform as desired.
Beyond the dynamics of one-to-one customer-vendor relationships, vendor public reputations also build confidence in the trustworthiness of their products, solutions, and services they provide. Don’t hesitate to verify customer and industry references of any vendor claiming trustworthiness as a selling point.

**Summing Up**

Cisco produces trustworthy systems that enable public and private organizations around the world to deliver goods and services over computer networks with maximum possible confidence. From the first days of its founding, Cisco has embedded trustworthiness in its culture, based on the understanding that networks cannot fulfill their potential as economically, socially, and culturally relevant infrastructures if they betray the expectations of their owners, users, and beneficiaries. Cisco also knows that trust is easily claimed, but difficult to earn and maintain. We welcome questions on product and solution certifications, standards compliance, and validations and are happy to refer customers, prospects, and partners to independent references.

Building trust into enterprise information technology is not cost-free. The end products of trust—reliable delivery of information technology-derived goods, services, and communications—generate positive returns to society, the economy, and the world at large.

[www.cisco.com/go/trustworthy](http://www.cisco.com/go/trustworthy)