Supply Chain Security

March 2012

Background

Governments, businesses, and consumers today rely upon information and communications technology systems to perform an increasingly important role in commerce and daily life. Some of the more important systems have become attractive targets for malicious actors who mount increasingly sophisticated attacks that have the potential to cause widespread damage or disruption, or give them unauthorized access to data.

A key area of interest is the supply chain of technology products, which the National Institute for Standards and Technology defines as "the set of organizations, people, activities, information, and resources for creating and moving a product or service (including its sub-elements) from suppliers through to an organization's customers."

The supply chain responsible for delivering information and communications technologies is globally distributed. The products themselves can be complex, made of many parts in many different companies all over the world. This raises concerns for some governments about the potential for hostile actors to introduce malicious or unwanted functions or counterfeit elements along the way. If products were compromised, they could potentially be used to conduct surveillance or to disrupt or otherwise degrade the trustworthiness of the information and communications technology systems of which the hardware or software will be a part.

Securing such a diverse and global supply chain presents a challenge for governments and businesses. Both need to recognize supply chain security as a shared problem and seek solutions that are built upon best practices, mitigate risks, and draw on international cooperation.

Microsoft Approach

Microsoft's strategy to help address supply chain risk to its products and services includes:

- **Identity and access management controls.** Microsoft works to help mitigate supply chain risk to its products and services by using policies, procedures, and technology that manage personnel access to Microsoft intellectual property.
- **The Security Development Lifecycle** is a foundational element for reducing the risk in the development of Microsoft software, and for protecting it against the introduction of product vulnerabilities, whether malicious or inadvertent.
- **Software integrity policies and procedures.** Microsoft employs policies, procedures, and technology to preserve the integrity of its software products, including checking for malware and code signing.
- **Anti-counterfeit measures.** To protect customers from the risks of counterfeit software, which could contain vulnerabilities, Microsoft actively identifies counterfeit versions of its software, works to maintain the integrity of its distribution models, and works closely with law enforcement agencies around the world to help reduce piracy.

Helpful Resources

www.microsoft.com/security/gssd
Microsoft Global Security Strategy and Diplomacy

www.microsoft.com/sdl
The Microsoft Security Development Lifecycle

www.safecode.org
The Software Assurance Forum for Excellence in Code (SAFECode)

Microsoft

Policy Considerations

A framework for managing supply chain risk should rest on these four principles:

- **Risk-based approach.** Governments should avoid using simplistic factors such as a product's country of origin to address risk. The global character of many products means that attempts to prohibit products based upon country of origin would result in a broad ban of products. This could lead to weakening the principles of open trade and relinquishing the benefits of global innovation. Instead, governments should rely on tested risk-management principles.
- **Transparency.** Governments have a right to expect IT companies to provide an appropriate degree of visibility into their business processes and the controls that ensure the security of their product development and operations. One example of such transparency is Microsoft's Government Security Program, which helps address security requirements by providing eligible, participating governments access to the source code for selected Microsoft products. While expecting transparency, however, governments also need to appreciate that businesses must protect their trade secrets and other intellectual property.
- **Flexibility.** When governments move to adopt standards governing supply chain security, control and mitigation standards need to remain flexible.
- **Reciprocity.** The development of reciprocal international standards for supply chain security is essential if we are to continue to realize the benefits of the Internet that rely on the security and integrity of information technology systems.

Key Points

- Governments worldwide have concerns about supply chain security, in particular the potential for hostile actors to insert malicious software into information technology products as they move through the supply chain. This could create vulnerabilities in the information and communications technology systems of which they will become a part.
- Microsoft employs a four-part strategy to manage the risks to its products and services in the supply chain. This strategy is grounded in identity and access management controls, the Security Development Lifecycle, policies and procedures that monitor the integrity of Microsoft software, and anti-counterfeit measures.
- Governments and businesses need to recognize that supply chain security is a shared problem and that they must work together using risk-based solutions, best practices, and international cooperation.