CrossTalk would like to thank DHS for sponsoring this issue.

This sponsor's note is taken from an interview with **Joe Jarzombek*** *after he spoke at CodenomiCON, when he shared his thoughts about supply chain assurance from a perspective of enterprise risk management and user safety and security.*

Imagine a cyber-reliant society with the Internet of Things (IoT) in which connected devices and products have been evaluated and certified from a perspective of consumer safety and protection. Safe and secure use of cyber assets places responsibilities on operators and users; yet realization of cyber assurance requires more focus on cyber safety and security in the supply chain. It requires network-connectable devices to be developed with cyber-physical security and safety in mind. IoT devices need to be patchable to be responsive to a changing threat environment. They need to be evaluated to determine they do not have malware, known vulnerabilities and software security weaknesses. This includes relevant certification activities that focus on mitigating exploitable weaknesses that could have otherwise been vectors of zero-day exploits if not mitigated prior to use. Independent third-party evaluation and certification is desired to assure relevant mitigations have been accomplished prior to use. IoT trust can be enabled with verification and validation activities focused on quality, safety, and security of devices in the context of the environments in which they would be used.

Fortunately for consumers, many white-hat researchers and test centers now provide third-party analysis of IoT products relative to cyber-physical security and safety. Underwriters Laboratories (UL) has launched its Cyber Assurance Program (addressing the needs stated above) and will be putting its mark on IoT devices and products; starting with healthcare systems, industrial control systems and network devices. These efforts provide better synergy between cyber assurance and cyber insurance since both provide a focus for mitigating residual risk.

The use of standardized cyber security terms is vital for information exchange needed in supply chain assurance. The UL CAP offers extensive coverage in evaluating IoT products for resilience to exploitation, and it adopts the use of several internationally recognized standards in the ITU-T CYBEX Series X for cybersecurity information exchange that covers data networks, open system communications and security. Standardized cyber security terms and enumerations enable interoperability, reduce ambiguity, and provide precision for managing efforts seeking to mitigate known vulnerabilities, exploitable weaknesses, and malware in cyber-enabled capabilities. The ITU-T CYBEX uses several DHS-sponsored standardized enumerations and languages vital to understanding the resilience of IoT products. The Common Weakness Enumeration (CWE™) https://cwe.mitre.org/ -- ITU-T CYBEX Recommendation ITU-T X.1524 http://www.itu.int/rec/T-REC-X.1524/en provides a formal list of known software-related weakness types – a specific type of mistake or condition that, if left unaddressed, could under the proper conditions contribute to a cyber-enabled capability being vulnerable to attack, allowing an adversary to make items function in unintended ways. A "weakness" represents a potential source vector for zero-day exploits or unreported vulnerabilities. Known weaknesses are CWEs – those characterized, discoverable, and potentially exploitable weaknesses with known mitigations. A "vulnerability" is a weakness with an associated exploit that can be directly used by an adversary to get a cyber-enabled capability to function in an unintended manner. Typically, this is the violation of a reasonable security policy for the cyber-enabled capability resulting in a negative technical impact. Although all vulnerabilities involve a weakness, not all weaknesses are vulnerabilities. The existence (even if only theoretical) of an exploit designed to take advantage of a weakness (or multiple weaknesses) and achieve a negative technical impact is what makes a weakness a vulnerability. Common Vulnerabilities and Exposures (CVE™) leverages common names and identifiers for publicly know information security vulnerabilities that have standardized use in ITU-T X.1520 CVE https://cve.mitre.org/. A vulnerability is a mistake in software that can be directly used by a hacker to gain access to a product, system or network. A configuration issue or a mistake in exposure is a vulnerability if it does not directly allow compromise but could be an important component of a successful attack and is a violation of a reasonable security policy. An information security exposure is a configuration issue of a mistake in logic that allows unauthorized access or exploitation. Known vulnerabilities are equated with publicly reported CVEs with patches in the National Vulnerability Database (NVD).

CVEs are easily discoverable through binary analysis; yet suppliers seem to routinely deliver new IoT products with old CVEs (some for which the patch has been available for more than four years). Two thirds of all CWEs are at the code level; detectable via static code analysis. Many tools are available to detect and aid in mitigating CVEs and CWEs. Why are users left on their own to find those CWEs and CVEs and mitigate or patch those products when developers could have easily mitigated the known vulnerabilities and weaknesses prior to delivery or as part of a product release update? Suppliers have no liability associated with products tainted with malware, known vulnerabilities and weaknesses. Why do some suppliers prohibit security researchers and users from evaluating products for these discoverable flaws that put users at risk?

Everyone can agree that IoT products need to have malware removed, and for supply chain assurance to be realized, suppliers, acquirers, and operators must also seek to mitigate known vulnerabilities and weaknesses prior to the products being put into use. The fact that new products are still being released with known vulnerabilities and weaknesses causes many to question the cyber hygiene of supply chain actors. It seems supply chain assurance can best be achieved with adoption of independent evaluation and certification of IoT products because realization of risks attributable to known vulnerabilities and weaknesses are primarily on the use side; not the supply side. Cyber insurance should also be interested in this cyber assurance practice since history has demonstrated that there seems little incentive for suppliers to change practices for mitigating these risks without independent evaluation and certification of IoT products.

* **Joe Jarzombek** *has been involved with CrossTalk for nearly two decades. As the Director for Software & Supply Chain Assurance (SSCA) in Cyber Security and Communications in the Department of Homeland Security (DHS) he leads public-private collaboration efforts for government interagency teams with industry, academia, and standards organizations focused on the assurance of ICT/software products and services. Through co-sponsorship of the SSCA Forum and Working Groups, he co-leads community efforts addressing cyber security needs, addressing software, supply chain external dependencies, and security automation initiatives to enable scalable information sharing among organizations and security researchers.*