15 October 2024

What Exploding Pagers in Lebanon tells us about the Security of the Electronics Supply Chain

WEAPONIZING THE GLOBAL ELECTRONICS SUPPLY CHAIN

On September 17, 2024, an unprecedented attack involving Hezbollah in Lebanon & Syria unveiled a new level of warfare involving "Trojan Horse" attacks through the global electronics supply chain. In a physical sabotage operation, electronic pagers & "walkie talkies" were turned into explosive devices representing a marked escalation from the typical digital hacks that target critical end applications such as networking and communications.

This incident stands apart from typical "Trojan Horse" attacks which embed malicious hardware or software into a system or product. The Hezbollah attack was a unique escalation in that it:

- involved physical sabotage that resulted in a direct kinetic effect, moving well beyond the digital realm and directly resulting in physical injury and death.
- was facilitated by corrupting an "authorized" distribution channel by leveraging a third-party licencing agreement.
- was simultaneously initiated by a relatively low-tech hack into the pager network.

The attack exposed critical vulnerabilities in the supply chain where compromised manufacturing and distribution allowed the modification of thousands of pagers. The exploitation required two critical actions to be successful: hardware tampering and remote access control. The POCSAG (**Post Office Code Standardization Advisory Group**) protocol, widely used in pagers, was particularly susceptible to spoofing and code modification, enabling attackers to remotely trigger the devices. The combination of physical tampering and digital control turned simple communication tools into deadly weapons, emphasizing the need for robust security across the entire supply chain. It also underscored the dangers of relying on outdated technology in modern warfare.

"If the supply chain was compromised to put explosives inside… it's impressive engineering to pull that off. But the actual compromise of the supply chain itself isn't that difficult," noted David Fincher, a China-based technologist. His observation highlights how easily older products with less oversight can be infiltrated. While manipulating the hardware requires sophisticated engineering, infiltrating vulnerable supply chains is alarmingly simple. This underscores the urgent need for stronger monitoring, testing, and control throughout the entire supply chain to prevent similar breaches. Source The Taipei Times Sun, Sep 22, 2024 page12

BEHIND THE CURTAIN: THE ILLUSION OF SECURITY

This is only the latest in a series of threats to the supply chain that go beyond the threat of untraceable assemblies and components, extending beyond the open, a.k.a. grey, market. It also encompasses outsourced and licensed production, and even original manufacturing, where third parties - or even foreign governments - can maliciously influence or compromise the supply chain. This creates vulnerabilities not only in independent distribution channels, but

also in “authorized” channels, where electronic components or assemblies can be altered or sabotaged, posing serious risks to product integrity.

These threats are part of a larger trend that goes beyond untraceable assemblies and components. For example:

- **Cloned assemblies and semiconductors** from original equipment manufacturers (OEM’s) and original component manufacturers (OCM’s) in countries like China that mimic authentic products but could be platforms for hidden modifications or vulnerabilities.
- **Distributors using fake certificates of authenticity** pushing suspect parts into legitimate supply chains, blurring the lines between genuine and fake products.
- **Licensed manufacturing agreements** that can be leveraged to present a product or component as the original manufacturer’s product but can also be corrupted by deviations in the bill of materials, quality controls, and changes to the product itself.

COULD MODERN-DAY ELECTRONCS BECOME A TROJAN HORSE IN CRITICAL INDUSTRIES?

The Hezbollah attack highlights the extreme risks associated with connected devices and systems in end applications for defense, communications, transportation, energy, and healthcare. As these devices become integral to operations, they may also introduce vulnerabilities that could be exploited by malicious actors.

The manipulation of electronics can serve as a form of sabotage, similar to the concept of a Trojan Horse, where seemingly harmless technology is used to infiltrate and disrupt systems. In industries like defense, a compromised connected device could jeopardize national security. In healthcare, it could endanger patient safety through unauthorized access to medical devices or equipment. The possibilities, and threats, are endless.

This sets out a case as to why organizations must safeguard against potential supply chain threats.

GUARDING AGAINST THE RISK OF MODIFIED ELECTRONIC ASSEMBLIES AND COMPONENTS

In industries like aerospace, defense, and critical infrastructure, “Trojan Horse” risks either through modified OEM assemblies or counterfeit electronic components, present serious security concerns. Advanced testing methods are essential to detect these hidden threats before they compromise safety or performance.

1. **Modified OEM Assemblies - Hidden “Trojan Horses”** when device functionality is maliciously altered, often by adding unauthorized functions or backdoors. These changes may go undetected by the end user, effectively turning products into “Trojan Horses”. Identifying these threats requires advanced testing methods:

- **VISUAL INSPECTION** remains one of the most effective methods for detecting suspect parts or assemblies. This process involves closely examining components for signs of prior use or refurbishment, such as damage, discrepancies in packaging, inconsistencies in physical dimensions, and other indications of tampering.
- **X-ray Imaging** offers a non-invasive internal view of components, ideal for detecting hidden hardware changes without disassembly. This testing is ideal for identifying changes not visible externally.
- **Functional Testing** assesses electrical performance to reveal deviations from expected behavior, ensuring that any operational anomalies caused by unauthorized modifications are identified.
- **RAMAN and FTIR Spectroscopy** methods analyze material inconsistencies, which may indicate unauthorized modifications.

2. **Counterfeit & Non-conforming Electronic Components - A Hidden Threat -** cloned, re-marked, or modified components present significant risks, particularly when extra functionality is introduced. These parts may seem genuine but can create vulnerabilities for sabotage or cyberattacks. To combat these risks, several testing methods are crucial:

   - **AS6171 Moderate Risk Level Testing -** this standard outlines comprehensive procedures to detect counterfeit or nonconforming components. It includes external visual inspection, X-Ray Fluorescence, Delid/Decapsulation Physical Analysis, and Radiological (X-Ray) inspection.
   - **AS6171 High-Risk Level Testing** - advanced testing techniques within AS6171 which require the use of RAMAN and FTIR spectroscopy, used to identify material anomalies, which may signal counterfeiting or tampering.
   - **Electrical Functional and Performance Testing** - used to identify components that do not perform the intended functions correctly or do not meet the manufacturers data sheet performance requirements over specified environmental conditions.
   - **Environmental Stress Testing** - exposes components to extreme conditions to ensure they are genuine components, weeding out counterfeit or nonconforming parts that would fail under harsh environmental stress.

SMT Corp, the leader in counterfeit electronics mitigation, recommends a multi-layered approach based on the techniques previously discussed to ensure the integrity of electronic assemblies and components. These methods help protect against malicious tampering, non-authentic products, and poor quality, ensuring system integrity and operational safety.

PRIORITIZING SUPPLY CHAIN SECURITY

Governments and organizations are adopting strategies such as AS6081, AS6171, ISO 9001, and NIST (National Institute of Standards & Technology) to improve supply chain security and accountability. Public-private partnerships and emerging technologies such as blockchain can also improve transparency and collaboration, although they require widescale industry buy-in which is not likely.

15 October 2024

CONCLUSION: THE NEED FOR SUPPLY CHAIN VISIBILITY

In today's globalized economy, supply chain transparency is essential to prevent counterfeiting and sabotage. Companies must adopt a proactive approach by working closely with suppliers, fostering collaboration, and thoroughly mapping their entire supply chain. Implementing rigorous testing for products from "untrusted" or "questionable" sources is crucial to securing these supply chains. Businesses that prioritize visibility and product assurance will strengthen their resilience and safeguard valuable assets in our increasingly interconnected world.

About SMT, Corp

SMT Corp is the industry leader for sourcing & authentication of DMSMS and hard-to-find electronics components, electrical testing services, and inventory management solutions. SMT Corp is a highly accredited and recognized expert with full on-site sourcing (AS6081), authentication (AS6171), and electrical testing to mitigate the risk of counterfeit, cloned, altered and substandard products from entering the critical infrastructure supply chain. https://smtcorp.com/

About Certify Holdings

Certify Holdings is a full lifecycle strategic partner for the defense and aerospace market, and other markets requiring high reliability electronic solutions. Certify Holdings supports our customers through the early project design stage with design-in support leveraging a wide range of Hi-Rel and RF electronic modules and components, throughout production with sourcing and distribution services, and into obsolescence / end of life with sourcing and authentication of hard-to-find electronics. Throughout the project lifecycle, Certify Holdings supports our customers with test solutions and services. https://certifyholdings.com/