About Telit Cinterion

Company

Telit Cinterion, previously Telit, is a leading provider of communication modules powering the internet of things (IoT), services and solutions, formed through acquisition of the Cinterion line of IoT products and services from Thales in January 2023. Founded in 1986, Telit Cinterion launched its first module in 1998 and has over time expanded into adjacent areas like IoT platform services, connectivity services and solution design services. The Cinterion business started as a division of Siemens and emerged as a leading player in the wireless module industry from the onset after the launch of its first cellular module in 1996. In 2022, Telit Cinterion added custom IoT project and solution design services to its offering through the purchase of California-based Mobilogix.

Products and Services

Telit Cinterion provides a comprehensive portfolio of modules, connectivity services and software for enterprise and consumer applications. Cellular modules are offered under the Telit and Cinterion brands and are divided into families, where members have the same form factor and software interface. Much attention is given to ease of integration and backward and forward compatibility to ensure cost-efficient development and implementation of new technologies. Supported technologies include 4G LTE, including LPWA technologies such as LTE-M and NB-IoT, and 5G. The product portfolio also includes Wi-Fi, Bluetooth, BLE and GNSS modules, which can be easily integrated with the company's cellular modules but can also be used as standalone devices.

Security

Telit Cinterion places the security and integrity of our products and services, and the sanctity of our customer's data in transit or at rest, at the center of our planning and execution. Telit Cinterion products are security tested and bring features and tools for advanced security applications. With rigorous processes bolstered by best practices from Thales for critical infrastructure, our secure-by-design methodology and approach extends across our R&D, manufacturing, and supply base.

Risks and Challenges

US infrastructure faces three significant challenges, each with its potential risks. These challenges underscore the importance of a balanced and careful approach in evaluating the risks and benefits associated with using Chinese cellular modules in US infrastructure:

Security Risk.

Cellular modules are essentially communication computers that come with software code provided by the module manufacturer. Due to their communication capabilities, they can (and must given the nature of the cellular operation process) establish connections with remote servers. Moreover, all cellular devices can utilize the location of connected cell towers as a reference for tracking purposes. This combination of communication and location features poses potential security risks, as these modules could be exploited for tracking and unauthorized access.

Remote Maintenance.

Throughout their active lifespan, cellular modules require regular software and firmware updates. These updates are vital to maintaining security and stability, especially in response to network operator updates. Many nations find themselves heavily reliant on Chinese cellular module manufacturers to ensure the safety and security of critical industrial products throughout their usable life. Without ongoing support from these manufacturers, the modules may become insecure or prone to instability, posing risks to critical infrastructure.

Supply Dependence.

A pressing concern lies in the risk of becoming entirely reliant on Chinese module manufacturers to connect critical infrastructure. The Chinese government subsidies benefiting Chinese manufacturers may eventually disadvantage non-Chinese players, leading to potential crippling effects on their market presence. In this scenario, every nation would be dependent on Chinese suppliers to establish and safeguard their critical infrastructure, raising concerns about sovereignty and independence.

Case Study: PAX Technology

On October 26, 2021, U.S. federal investigators raided the Florida offices of PAX Technology, a Chinese provider of point-of-sale devices used by millions of businesses and retailers globally.

According to an article published by KrebsOnSecurity (link below), the raid was tied to reports that PAX's systems may have been involved in cyberattacks on U.S. and E.U. organizations.

More specifically, the article noted a major US payment processor became concerned when it noticed that the size of data packets transmitted from the company's PAX terminals didn't match the payment data they would be sending, nor did the packet size correlate to normal maintenance updates of terminals.

It is not uncommon for payment terminals to be compromised remotely by malicious software and made to collect and transmit stolen information.

Indeed, some of history's largest cyber-heists involved point-of-sale malware, including the 2008 breach at Heartland Payment Systems that exposed 100 million payment cards, and the 2013-2014 string of breaches at Target, Home Depot and elsewhere that led to the theft of roughly another 100 million cards.

https://krebsonsecurity.com/2021/10/fbi-raids-chinese-point-of-sale-giant-pax-technology/

Chinese Companies Dominate Global POS Market

Of the 135M POS terminal shipments worldwide in 2021, the top 15 companies accounted for 85.2% or 115M.

Among the top 15, Chinese companies accounted for 80.5% or 92.6M.

Figure 3.1: POS terminal shipments by manufacturer (World 2021)

Company	Shipments	Market share	Headquarters
Ingenico (Worldline)	14,100,000	10.4%	France
PAX Technology	12,000,000	8.9%	China
Newland Payment Technology	11,200,000	8.3%	China
Tianyu	11,500,000	8.5%	China
Centerm	8,800,000	6.5%	China
New POS	8,500,000	6.3%	China
Verifone	8,300,000	6.1%	USA
MoreFun	8,200,000	6.1%	China
Vanstone Electronic	6,500,000	4.8%	China
Nexgo (Xinguodu)	5,300,000	3.9%	China
JTact	4,800,000	3.6%	China
Dspread Technology	4,600,000	3.4%	China
Sunmi	4,500,000	3.3%	China
Castles Technology	3,900,000	2.9%	Taiwan
TopWise	2,800,000	2.1%	China
Others	20,000,000	14.8%	
Total	135,000,000	100.0%	
Includes mPOS devices			

Source: Berg Insight

Recommendations

Governments and industries must take proactive measures to address security vulnerabilities, ensure continuous support and maintenance, and diversify their supply chain to mitigate potential risks in the long term.

Recommendation 1: ***Establish and empower independent agency to certify module/devices as 'secure'.***

Trust is fundamental, but it needs to be pillared on independent audits like UL and CE. Finite State, F-Secure Consulting, NCC Group, and Synopsys Software Integrity Group (SIG) are examples of cybersecurity evaluation labs. These labs provide vendors an external review of vulnerabilities, which can help businesses identify areas for improvement. While these audits are beneficial, there is an inherent conflict of interest since they are paid for and cannot provide an objective and exempt seal of approval. Without a clear delineation between a commercial lab and lab certified by an independent regulatory agency, the lab's seal can be mistaken by the market as independent, creating a potentially dangerous false sense of trust.

Recommendation 2: ***Establish and maintain a public registry of secure module/devices.***

Transparency is fundamental. The market should have a place to turn for information on application date, status, certification date, number of prior (failed) applications and their dates, country of origin, etc. The information should be cross-referenced and searchable.

Recommendation 3: ***Establish and maintain a roster of accredited providers.***

Continuity of support and supply is fundamental. The market should have an easy way to identify businesses it can turn to for guidance and support on technical issues related to the selection, deployment and maintenance of IoT modules and devices.