Case Study

Sternum Simplifies Telit's Security Lifecycle from Integration to Post-Deployment Monitoring

Background

Telit is a leading manufacturer of cellular modules that are used for Internet of Things devices.

With over 20 years of experience, the company has significant insights into the scope and challenges facing the IoT market. They work with major OEMS which embed Telit market-ready cellular modules into their devices. Last year, over 30 million Telit-powered IoT devices were sold.

As a major manufacturer of IoT devices, Telit knows that their devices have to be secure. Malicious actors ranging from criminal groups to state actors can attack IoT devices, causing outages of service, harness them for botnets like Mirai, and compromise their integrity. They can be leveraged as gateways to breach a network and steal valuable information such as intellectual property.

Challenge

For Telit's SVP Software and Services, Product Management Alon Segal, security for IoT devices is done correctly when it is implemented from the start. "It's very hard to instrument security post-deployment as the risk is too great," says Segal. "Once you've released a system, security threats will chase you, so it becomes a question of liability and risk and how much of it you are willing to initially assume."

One of the primary challenges for Telit and their customers in incorporating security is integrating security tools into their diverse range of devices. "This is a complex expense scenario," says Segal. "To integrate an agent for each device means that I have to allocate time and expenses on R&D, which is taking away from my revenue generating abilities."

Adding to the challenge of securing their devices is the dearth of effective holistic solutions available in the market. Segal says that security vendors are siloed and fractured.

"They are focused on solving one issue or another, but leaving other avenues open to attack," he says, adding that, "Many vendors, unable to secure the devices themselves, shift to defending the network, which still leaves the devices open to attacks."

> ***"To integrate an agent for each device means that I have to allocate time and expenses on R&D, which is taking away from my revenue generating abilities"***
>
> *Alon Segal, SVP Software and Services, Telit*

Faced with these challenges, and having examined solutions from other vendors in the IoT security space, Telit found Sternum's approach offers significant advantages.

Solution

Sternum provides a holistic solution that prevents exploitations on IoT devices in real-time. Their approach recognizes that the number of vulnerabilities and malware types are infinite. By contrast, paths of exploitation

are far more limited and therefore a more viable chokepoint for blocking attacks. Understanding that all exploits work according to a similar course of corrupting or overriding memory in the heap or stack, taking control of the execution flow, and finally executing its own shellcode, Sternum has developed their Embedded Integrity Verification (EIV) technology for securing IoT devices.

When integrated directly into the system code, EIV identifies the execution flow and verifies that it behaves as intended. Calls to execute code in a path that violates the integrity of the flow are blocked in real-time, preventing exploitation and shutting down the attack on the spot.

With an overhead of only **3%**, EIV provides powerful, lightweight protection. "Sternum fits in very well into our security stack without adding another layer into the mechanism," says Segal, noting that in resource-sensitive environments, Sternum can offer secure coverage **using less than 1% overhead**. "There was no memory consumption or impact on the device's performance," he adds.

> ***"What really impressed us was how quickly we started receiving insights considering the light footprint of their technology"***
>
> *Alon Segal, SVP Software and Services, Telit*

The ease of integrating Sternum into Telit's code was a key factor according to Segal "They're streamlined into your existing build environment, "so the effort of integration is fairly low."

Describing a recent installation, Segal says that Sternum was able to complete a complex integration in a matter of hours. "We were quickly able to see processes and files that were accessed on the Sternum dashboard," he says. "Despite its light footprint, after the integration we quickly began receiving alerts to issues, including some 0-day memory corruptions. Normally we require a significant amount of additional equipment and time to detect these kinds of concerns."

Benefits

By integrating Sternum into their modules, Telit provides direct value to their customers with security visibility into their devices.

"Sternum succeeded in delivering visibility inside our devices, not only into what is happening with our proprietary code but 3rd party software including open source components as well," says Segal. "What really impressed us was how quickly we started receiving insights considering the light footprint of their technology."

Zooming out from the individual device to the macro level, Sternum's security monitoring allows Telit's customers to receive notifications to security issues throughout their fleet of devices.

"Our customers are able to receive an added valuable layer of security into their device management platform. Sternum alerts users to any attempts to compromise one of their deployed devices, providing early security intelligence that can warn them to large scale threats," explains Dr. Mihai Voicu, CISO at Telit.

"Because Sternum's technology is precompiled into our modules, our customers benefit from the advantages of detection and prevention. All without any changes to their code or action from their end. It is seamless, baked in security with none of the added investment or complexity."

> ***"It is seamless, baked in security with none of the added investment or complexity"***
>
> *Mihai Voicu, CISO, Telit*