SECURITY THROUGH MODULARITY

As more connected devices appear, so the concept of modularity is being used to tackle the problem of security. By **Neil Tyler**

While the world of connected devices continues to grow unabated the issue of building security into these devices has tended to be an afterthought, in many cases, and the impact of this is being felt on a daily basis by both consumers and companies.

Whether device security and brand protection, operational cost containment or the user experience, the costs associated with poor security are growing exponentially and it remains a fact that despite the amount companies are willing to spend on R&D, too many are still failing to invest in security to ensure that their IoT devices are made secure.

According to Dan Potts, CEO of Cog Systems, attitudes towards security remain diverse.

"In truth, attitudes towards security, and the risks associated with it, are hard to measure, especially when companies are not looking at, or addressing the issues around security.

"In terms of the companies we work with there's a real mixed bag out there in terms of their attitude towards security. Some are blissfully unaware of security, others turn a blind eye as it is seen as a big distraction if they are trying to get 'cool' consumer devices to market ahead of the competition.

"Those who view security in this way are usually companies whose focus is on driving innovation and getting to market first.

"Smaller businesses tend to overlook security until they are successful - when they have sold 1000s or even 100,000s of devices a hack could have a profound impact on their business - only then do they become worried about how a hack may affect their brand or a device's functionality."

According to Potts there is a degree of apathy, or inertia, when it comes to addressing the issue. Security, however, can't be ignored and that is especially true for a business whose devices could be handling sensitive information and data.

"Some companies are blissfully unaware of security, others turn a blind eye as it is seen as a distraction."
Dan Potts

"Cog, which was founded in 2014 and is based in Australia, was established to provide security for connected device architectures," explained Potts. "We wanted to build better security from an operating point of view."

According to Potts, the architecture of connected devices has created far too many vulnerabilities and therefore opportunities for hackers to compromise devices, resulting in a growing number of companies having to accept much higher levels of risk which can, in turn, restrict access and make life more difficult for users.

"When it comes to security we have adopted an embedded solution that's built on the concept of modularity, as well as proactive security, trustworthiness and adaptability to enable highly secure connected devices," Potts said.

"We look to leverage modularity in order to isolate critical functions

elenabsl/stock.adobe.com

and services on connected devices and by doing so we are pro-actively securing these devices by reducing the attack surface. At the same time we are increasing reliability by eliminating single points of failure."

According to Potts, Cog focuses on securing the kernel, data, and network as the baseline to the company's security solution.

"We also look to isolate specific applications, operating systems, or services to further achieve a full defence-in-depth based solution. The system can scale linearly and infinitely, reducing bottlenecks while at the same time preserving performance."

This approach not only provides high level grade security for the device but it also means that customers no longer have to worry about security – they can focus solely on what they're best at, delivering IoT applications for their customers.

But is a failure to address the problem of security becoming a bigger issue? Potts suggests it might be and a growing number of reports point to a similar trend.

Modular v Monolithic

"At Cog we have a strong background in operating systems and ours is a philosophical approach when it came to security and our decision to take a more modular, rather than monolithic, approach," explained Potts.

"From our experience with working in the connected device ecosystem, we wanted to work out how best we could help connected devices build better security from an operating point of view. The motivation was simply that we were seeing an ever increasing trend, largely mobile related to begin with but then with the Internet of Things, in which an increasing number of connected things and devices are coming to market.

"We felt that a monolithic architecture, typically Linux based, was more vulnerable from a threat perspective to attacks, and we wanted to take a more modular approach, much the same as with hardware components, so that we could improve security.

"I've already mentioned our philosophical approach to security and our modular approach was a result of a lot of research which encompassed componentisation, defence in depth and so forth. We wanted an approach that would enable companies to solve a variety of problems – providing them with both better engineering outcomes and more flexibility.

"We began by working with defence firms, who are highly regulated, to build the chain of trust, using encryption for example, and to productise our concept to make it more usable," Potts explained.

"D4 Secure is the result of this work and is a software toolkit, in essence, which has building blocks to help device manufacturers quickly build in modularity; they can add data encryption etc., as well as mix and match different operating systems.

"It's a framework for providing security and extensibility to connected devices. The architecture isolates certain system processes and capabilities by leveraging Type 1 Virtualization to separate the functions into multiple virtual machines (VMs)."

According to Potts, by splitting the system into multiple functional areas it allows for much greater operational integrity, more granular system control, and, crucially, a much reduced attack surface.

"Various rules of operation govern the interactions across functional areas and between virtual machines and these ensure that the system functions in very specific ways, as defined by the specific use case.

"Developers can use as much or as little of it to solve their problems," he explained.

The components of D4 Secure comprise of modularity, security, value added modules and scalability.

Modularity provides multiple levels of containerisation that serve to isolate applications and components while enabling plug and play virtual machines and components, faster system development and software reuse. This approach makes it possible to securely run legacy software together with updates and third-party software, according to Potts.

In terms of security it provides storage encryption technologies and device policies that ensure defence-grade embedded security.

Additional layers of security can be added to D4 Secure to provide the highest degree of assurance that the device and data is protected, including: Full Disk Encryption (FDE) and a Nested VPN i.e. a second VPN to the operating system, to run a truly 'nested' VPN solution on the device, which provides double Data in Transit (DIT) protection.

Finally, D4 Secure provides scalability and the ability to concurrently run software with vastly different Operating System (OS) and platform requirements as well as run a common set of software over a variety of different hardware devices.

"This speeds up development by eliminating the need to refactor or rewrite old code and also easily supports new hardware," according to Potts.

Cog Systems is now engaging with some of the world's leading companies including Qualcomm and Arm.

"Our aim is to secure the edge and allow people to innovate using our high performance virtualisation capabilities. We've just partnered with Qualcomm and will be embedding our software into their Snapdragon chips – what we provide device makers with is a very high level of security, that doesn't impact the device's performance due to the use of our modular approach," explained Potts, who concluded: "No matter what type of business you are, our approach enables you to very quickly get away from security and get back to focusing on what you, as a company, do best which is innovate and bring products to market."

"We approach security from an operating point of view and wanted to take a more modular approach to security."
Dan Potts