Don’t be the weakest link

All parts of the security chain need to be equally strong – whether it’s the device, the application or the system. By **Graham Pitcher**.

With the advent of the Internet of Things and the expectation that billions of devices will be ‘talking’ to each other in the near future, three words are finding increased usage – security, trust and authentication.

Amongst other definitions, security relates to making sure that your data goes where you expect it to, trust relates to whether the data being sent is what you expect and authentication is about ‘talking’ to the right device. These issues come on top of existing security problems, such as hacking, man in middle malware and even physical attacks.

Many IoT devices will never ‘talk’ to a human; rather, they will talk to each other, analyse data and make decisions according to a plan implemented at some point in the past. But how can we be sure that device A is the device which should be talking to device B? How then can device A identify itself as authorised to talk?

57% **of respondents are more concerned about embedded security than they were a year ago**

Communications, although important, is only one aspect of security. There is also device security – including counterfeiting – design security and physical security.

Looking to explore the issues, *New Electronics* surveyed its readers to find out their security concerns. According to the results, 57% of respondents were more concerned about embedded systems security than they were last year.

Asked what issue was of most concern, 35% of respondents pointed to data security, whilst 29% said design security.

We also asked whether your latest embedded system design accesses the internet. Surprisingly, perhaps, 61% of respondents said no. We asked whether your next embedded system design would access the internet. Again, rather surprisingly, the majority (52%) said no.

With the trend towards the use of FPGAs at the heart of embedded systems, we asked whether your latest design featured one. The answer was yes from 37% of respondents. Of these, almost three quarters said configuration data was held securely.

Meanwhile, 53% of respondents said they were implementing secure boot in their system, whilst 51% are designing in tamper resistance. Half of the respondents to the survey were aware of defensive programming and 65% of them are applying the technique in their latest design.

New Electronics convened a roundtable to discuss these issues. Taking part were Tim Morin, director of product marketing with Microsemi, and Alex Wilson, director of business development, aerospace and defence, for Wind River.

Asked for his response to the survey results, Morin said: “One of the things we all have to do is to challenge our assumptions about whether or not something needs security. Just because a system isn’t connected to the internet, doesn’t mean it’s secure.”

“Just because a system isn’t connected to the internet, doesn’t mean it’s secure.”
Tim Morin

Wilson noted: “A surprisingly low number of respondents to the survey appear to be thinking about security – and that’s a little worrying.”

Morin continued: “Security is tough from the engineer’s point of view. They design to requirements and need to meet those requirements; typically through features. When it comes to designing in security, they have to think about how their system might break.

“Making sure you have the procedures in place and that the system is secure is an extra step in

the process, which takes time, energy and money. Security is a complicated thing to get right."

Wilson pointed out: "Often, security is added as an afterthought, rather than being designed in from the start."

Trusted manufacturing

Microsemi makes a range of devices, including FPGAs, with many of its customers found in the military and aerospace supply chains. Because of this, it takes the security of the manufacturing process seriously. Morin explained: "We're concerned about all aspects of security, including how we make our devices. By developing a trusted supply chain, we can provide engineers with a foundation on which to build secure applications."

35% of respondents are most concerned about data security

The reason for the development of the trusted supply chain is the company perceives a range of threats, some of which could come from insiders.

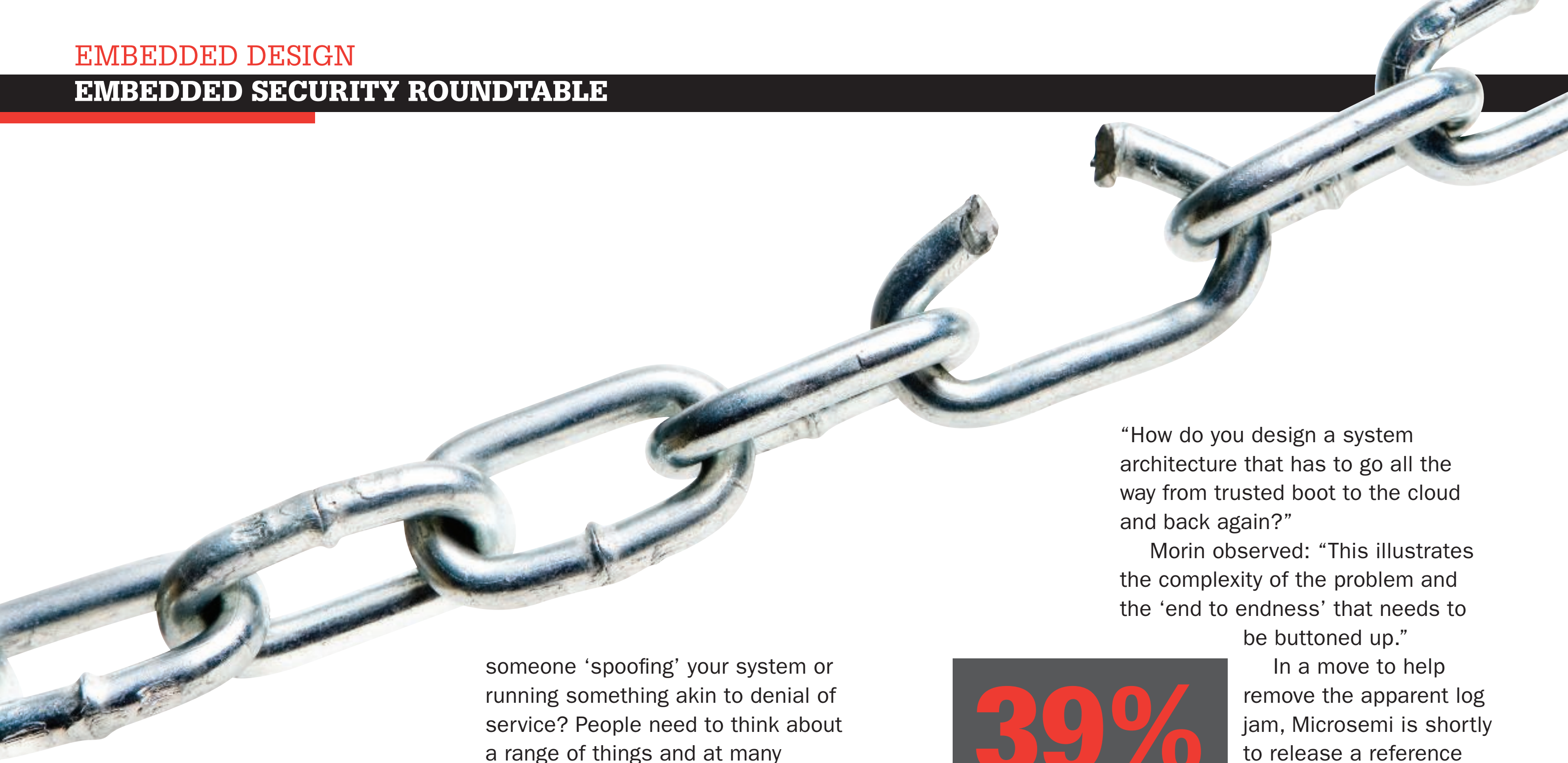
"We buy third party IP, for example," Morin said. "We make masks and wafers, then package devices. The part then gets out into distribution and someone uses it. There are a lot of steps in the process where security can be threatened. The problem is all these items are difficult to deal with."

One of the threats to that supply chain is counterfeiting. Morin noted: "The US Department of Defense has evidence of complete counterfeit mask sets getting through the supply chain and into military systems. Programmes are now in place to prevent this and it's one of the reasons why Microsemi is doing what it's doing."

Microsemi has been making FPGAs for 20 years – it acquired Actel in 2010 – and has made significant investments in security. The launch in 2012 of the SmartFusion2 SOC FPGA saw a number of features being integrated. "We embed a digitally signed certificate to show the part's authenticity," Morin explained. "If a Microsemi part claims to be industrial spec, users can read from it to confirm it is what it says and that it comes from the Microsemi supply chain."

The device is called an SOC FPGA because it includes fixed logic blocks related to security. And there's also anti tamper functionality. "There's an active metal mesh that covers sensitive areas of the chip," Morin said. "If someone tries an invasive attack, that's detected and a tamper flag is sent through one of the FPGA's ports. It's then up to the user to decide what to do. While we're offering programmable security, the customer knows best how to respond to threats."

"Engineers have to think about how to manage security and, to do that, have to think outside of their design rules."
Alex Wilson



System security

Wind River's Wilson said: “The results of the survey seem to suggest that engineers are building embedded systems, but haven't yet made the step of connecting them to the enterprise to get more value. That's how Wind River sees the IoT.

“There's a lot of hype around the IoT,” he continued, “but only a handful of companies have realised the benefits and we're seeing it happening more in the industrial sector than anywhere else – for example, smart buildings and companies leasing systems, where there's the need to monitor them and take responsibility away from the customer.”

In Wilson's opinion, there's more to the IoT than connecting a device to the internet. “It's taking data from the field, analysing it, extracting the value and then feeding back. That's very different from hooking up to the web; the IoT is about what you do with data.”

The security implications in the IoT are broad. Not only is there the need to secure the data being transmitted, there's also system maintenance. Wilson pointed out: “Once you've loaded software, how do you maintain it? How do you load patches? Is someone ‘spoofing’ your system or running something akin to denial of service? People need to think about a range of things and at many levels.”

28%

of respondents are most concerned about design security

A further complication is that many companies are starting from what Wilson calls ‘brownfields’, rather than ‘greenfields’. “They're trying to enable things already built and the IoT is all about how to connect to ‘back end’ systems.”

The ‘greenfield’ starting point allows designers to create intelligent systems which boot securely. But a ‘brownfield’ start invariably requires a gateway to extract data from sensors, aggregate the data and pass it on securely.

“These are the things which Wind River and Intel are working on,” he continued. “We're using Intel technology for secure boot, whilst hardening the OS and including anti tamper and encryption features. That creates a secure platform and enables connectivity and management.”

He believes that security – and software security in particular – is an important issue. “If you've never looked at how to secure software, there's a big learning curve. Engineers have to think about how to manage security and, to do that, have to think outside of their design rules. The problem is they can't think of every possible threat.”

“It's not just a software problem, it's a system problem,” he added. “How do you design a system architecture that has to go all the way from trusted boot to the cloud and back again?”

Morin observed: “This illustrates the complexity of the problem and the ‘end to endness’ that needs to be buttoned up.”

39%

of respondents think security is extremely important

In a move to help remove the apparent log jam, Microsemi is shortly to release a reference design that shows how to do M2M authentication over any kind of fieldbus. “It will demonstrate how to work out who is supposed to be talking to you, the exchange of keys and the enabling of traffic over a secure link,” Morin noted.

Wind River is taking a similar approach. “We have built an IoT gateway product with Intel. It's a hardware and software package that helps users to get started.”

Concluding, Morin said: “Security is complicated, but people think that because a system is embedded, it's secure. We're doing it from a programmable point of view, but it's only one aspect because security is all about layers. If you're building a secure system, then we can offer a secure FPGA.”

Wilson noted: “It's tough for customers to think about security; they expect it to be built in, free and easy to use. But it's a system level issue; for an IoT system to work, engineers have to start from a systems point of view and work out how it fits together.”

The Embedded Security roundtable was sponsored by Microsemi and Wind River

Microsemi

WIND RIVER