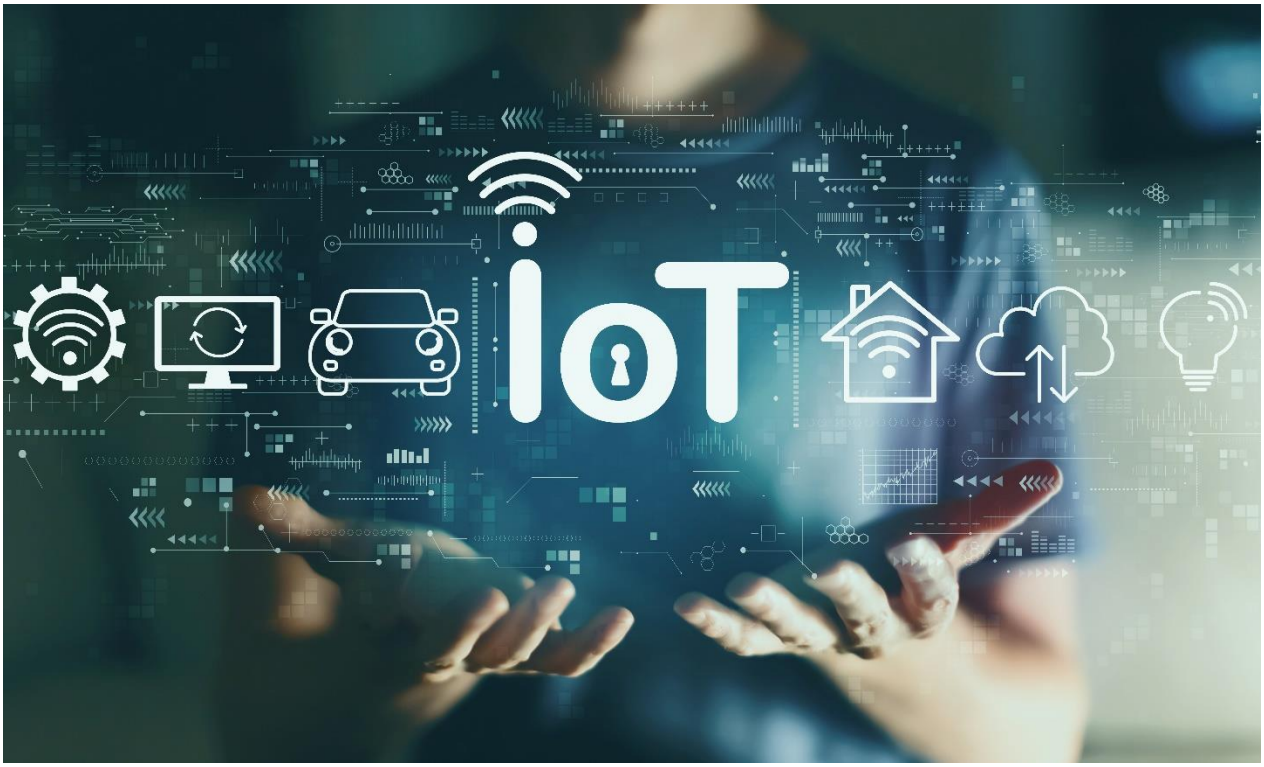
IoT Security Specialists: Pioneering a Secure Industry 4.0

Written by Joshua Bucheli, AI Ethics Researcher and Fellow at the ForHumanity Center, in Collaboration with Tobias Schläpfer, Cryptography Engineer at NatWest Services, and Peter Kosel, Founder of cyberunity



In 2017, an EU-US investigation shocked millions of parents when it uncovered a vulnerability in the Bluetooth interface of a German smart-doll that allowed hackers to listen and talk to the children playing with it. As horrific as this sounds, real life chuckies are the least of our worries if the Internet of Things (IoT) is not properly secured sooner rather than later.

The internet put the sum of human knowledge into the pocket of virtually every individual on the planet by connecting computers to one another, giving rise to innovations the likes of which Alan Turing could have only dreamed of. The Internet *of Things* (IoT) applies this concept to the rest of our environment, equipping the objects that surround us with the networking capabilities that have revolutionised our world once before.

For those who wish they had been ahead of the curve in the early days of the internet revolution, IoT represents a second chance at a once in a lifetime opportunity… so long as they are ready to invest in the right people to help them prevent the kinds of mishaps that could inspire a reboot of the Chucky franchise.

Where Does IoT Stand Today?

The internet connects computers to each other and allows them to record and exchange information. The IoT connects pretty much everything else to the net. From smart watches and toilets to traffic lights and nuclear plants – anything with an on/off switch is fair game.

With over 15 billion new devices expected to go online within the next decade, the IoT rivals innovations like quantum-computers and cloud-computing as the most significant revolution in modern tech. However, with new opportunities come new risks – in a totally digitised world pretty much everything around us becomes vulnerable to digital threats.

“The difference between IoT security and IT security begins with the fact that IoT devices exist in far greater numbers and are much more openly accessible. The IoT is bound to the ‘things’ themselves rather than secured locations like data centres or server rooms. This makes it far more difficult to secure, encrypt, patch, and update” says Tobias Schläpfer, Cryptography Engineer at NatWest Services.

In the early days of IoT, dedicated devices called ‘gateways’ connected ‘things’ to a centralized cloud, allowing them to be controlled remotely on the basis of data that they gathered and exchanged. Today IoT is transitioning away from the closed systems on which it was initially rolled out, eliminating gateways and shifting the issue of security onto IoT devices themselves.

Where is IoT Headed?

“As evidenced by the GDPR and initiatives like the ENISA Security-Label, even regulators are starting to recognise that IoT needs to be a legislative priority”, says Tobias.

With highly publicised incidents like the Las Vegas Casino fish tank hack on the rise, businesses are realising that they need to act and their clients are increasingly beginning to understand the perils that come with putting every ‘thing’ online. They are starting to ask more questions and it’s vital that companies stand ready with the answers.

Future-proofing is a holistic affair that must be integrated proactively and according to the Zero-Trust standards that underpin cybersecurity more broadly – something that OEMs who manufacture IoT devices have yet to fully acknowledge:

“Businesses need to be asking themselves how they are going to ensure that devices are not only smart but also *safe*. Instead, they still often overlook the issue of security until later stages in the design and production process”, warns Tobias.

One considerable pain-point that is yet to be addressed in IoT security is that these devices are far more limited than smartphones and computers in terms of processing power, storage space, and battery life – key attributes on which robust cybersecurity solutions like RSA-keys conventionally rely.

“Here, companies need to start exploring new avenues. For instance, they should be looking at token- or claim-based authentication solutions that rely on time sensitive credentials rather than on conventional PKI-authentication”, advises Tobias.

Luckily, as the industry wakes up to the security needs of IoT, tools and standard protocols like OAuth are making safe API-authorisation more openly available.

For those interested in the nitty gritty of PKI authentication, RSA keys, and the IoT, the following video offers a great technical overview.

IoT Security Specialists – Hard Skills and Qualifications

IoT is a matter of marrying devices (‘things’) with the networking capabilities of the digital world. Securing it will therefore take individuals who strike a balance between software- and hardware-related skills and who understand the intersections between the two.

“At the junction of hardware and software, IoT security specialists will need to be aware that it is *firmware* rather than software that is in focus and they will need to keep in mind that securing IoT may even be a matter of developing new hardware”, emphasises Tobias.

On the one hand, this means individuals who are familiar with the basics of security algorithms and methods, PKI authentication, access management and network engineering. It’s going to take people who understand the difference between RSA and elliptical cryptography and their respective influences on IoT systems.

On the other hand, strong IoT security specialists will also benefit from experience in electrical engineering. They will need to be able to practically and innovatively work around the finite resources and communication protocols that constrain these devices.

Thanks to the interdisciplinary nature of IoT security, those coming from less related fields will also be in high demand. Electrical engineers, embedded engineers, network security engineers, and cryptography specialists with a hankering for practical work and an interest in software development are well placed to help develop secure firmware for IoT.

In terms of qualifications, “it’s important to keep in mind that employers far prefer experience and demonstrated practical understanding over certificates or diplomas”, says Tobias.

Nevertheless, evidence of formal or academic training like the ZHAW Institute of Embedded Systems’ MAS program or the University of Geneva’s Internet of Things MAS program will give applicants a definite leg up. Qualifications in security related embedded C-programming, evidence of workshops like Ares’ upcoming IoT SECFOR 2021, and certificates like the IoTSF’s Foundations of IoT Security or Certnexus’ Certified IoT Security Practitioner will also make applicants stand out among the competition.

In terms of exciting employment opportunities at the frontier of IoT security, new companies like Sensiron, Kistler, Duagon, and Qiio sprout every day. Chip manufacturers like NXP, Renesas, and WISeKey also present interesting options for aspiring IoT security specialists.

Anyone interested in getting started in the world of IoT security is invited to reach out to Prof. Dr. Andreas Rüst, director of the ZHAW's IoT program, Jonas Conrad, Lead Researcher at ETH Zürich's pd|z, or Prof. Dr. Willenbacher from KIT for more information.

Beyond Technical Know-How:

When it comes to IoT security specialists, it's clear that engineers across the IT industry will be in high demand. But it takes more than just technical skills to help future-proof a technology of this magnitude.

It's going to take diligence and grit when dealing with lengthy troubleshooting and well-developed analytical skills will be critical for identifying security risks and potential solutions.

Finally, and often underestimated, communication skills are also an essential element of a well rounded IoT security specialist's repertoire. A crucial part of their job will consist in alerting management to the risks of IoT, making the ability to raise awareness and highlight problems, solutions, and the respective benefits of different courses of action absolutely pivotal.

Today's article has focused on networking in a *technological* sense – the current relevance and attractiveness of which cannot be understated. However, when it comes to recruiting the right people to successfully drive these technologies forward, networking in the *human* sense is also required.

Here again, technology-driven means like artificial intelligence and algorithms might be used to help identify the right specialists – indeed, doing so is already becoming increasingly commonplace. However, the key ingredient for companies who want that extra edge over the competition is maintaining authentic relationships with the right talents. Doing so makes it possible to get in touch with potential candidates efficiently and to quickly initiate collaboration.

A genuine passion for technology is commendable. But to really thrive, companies need to honestly invest in relationships with promising candidates well before they are hired. They must continuously cultivate these relationships and then win them over if they are to prevail in today's market.

'Time to candidate market' is an often-discussed key success driver for companies, yet it is still underrepresented in most corporate strategies. Indeed, in his daily work, Peter Kosel observes all too often how little attention is paid to the matter of fostering future top performers.

The KNOW YOUR TALENTS approach at cyberunity supports companies on precisely this journey – Peter Kosel actively guides businesses towards a successful future and is always eager to have a conversation. Reach out to him directly at pk@cyberunity.io and discover your talents today!