Data science and data security, Internet of Things

The IoT is coming... but can it be made secure?

Researchers from imec – COSIC – KU Leuven developed an innovative cryptography chip that can protect low-power sensors and even RFID tags.

Today, around the world, the Internet of Things is rolled out. One example is the Belgian city of Antwerp, which is on its way to becoming one of the world's largest living labs and technical test beds for IoT and smart city technology.

The basis of such a smart environment – its eyes and ears and fingers – are smart, unobtrusive sensors and tags. These gather data about air quality or traffic density but also about people's whereabouts and behavior. But here's an issue: most of these sensors are low-power electronics. They may have a hard time running the complex algorithms that are needed to protect your data ... if they can do it at all. Pieter Maene and Vladimir Rožić, researchers from imec – COSIC – KU Leuven talk about how their research group took up the challenge and developed an innovative cryptography chip that is up to the task, a chip that can even protect RFID tags.

Security for IoT sensors – an energy conundrum

Context-aware IoT applications are built around small processors, unobtrusively hidden in buildings, cars and bikes, clothes and wallets. To make them really useful, they should require no maintenance and have a long operating lifetime. They should run for maybe ten years on batteries or they could even be passive RFID tags, small processors that have no internal source of energy and that power up and start processing only if they come in the neighborhood of a power-providing antenna.

The applications they enable will exchange data with big data servers in the background. Data about e.g. people's location, shopping behavior, bank account, or health.

"But naturally," **says Pieter Maene,**"people
want that data to be secure; we wouldn't want e.g. our pharmacy shopping list to be shared with the world. Also, we want to keep some measure of privacy and anonymity. Not everyone should be able, e.g. to identify our RFID tags and know where we are.

Technically, this means that the sensors or tags you carry should only release data to the infrastructure you trust, e.g. to the smart city gateway. So the sensors and the gateway server should be able to mutually identify – 'authenticate' in security parlance. It also means that if a rogue server would try to contact e.g. an RFID tag you carry, the tag should not release any data or identifier that would make it possible to recognize and track you. In addition, when your data are sent to a gateway, nobody else should be able to read them – the data should be encrypted."

"But here is the catch," **adds Vladimir Rožić:** "The algorithms to authenticate and encrypt are complex mathematical functions. They do a good job on today's high-end to mid-range processors. But when running on lightweight processors or RFID tags, they might choke the processor or drain the energy resources."

The new IoT environments come with the unique challenge to make good use of the data from new devices, sensors and transactions, but at the same time protect the users' privacy and anonymity.

"The researchers at the COSIC research group of imec - KU Leuven are working on a number of aspects of this issue," **says Rožić.** "We
cover authentication and encryption, but also privacy enhancing technologies and anonymization. We look at these from the point of software and hardware. Which algorithms provide the right level of security while not consuming too much energy? How can we set up the hardware that supports these algorithms in the most energy-efficient way possible? And how can we co-design software and hardware to create the most secure IoT devices? And last but not least, we're also concerned with protocols and policies."

Talking about encryption

Encrypting data is scrambling the message so that it can only be understood by someone who knows the secret. A very simple encryption scheme, e.g., is to replace every character by a character that is three positions up in the alphabet. But the 'shift three positions' approach is not very secure: it's easy to guess; just try a few shifts and you have it. Through history, cryptographers have kept inventing more clever and complex schemes. And code breakers, eventually with the help of computers, have always tried to crack their secrets. They do so either to listen in on the communication and gain information, or if they are ethical hackers, to test and improve security.

Today's encryption schemes combine secret keys (a random string of bits) and clever scrambling algorithms. The algorithms are public so that they may be scrutinized, tested, and improved. They are designed so that even tomorrow's computing power will not be able to unscramble the message.

When two applications exchange data, the simplest way is to have them encrypt and decrypt the data using an identical key at both ends, a secret key that they both know. This technique is called symmetric encryption. It is fairly efficient but it shifts the security issue to how the applications can agree on a common secret key while talking over an insecure link and how they can both keep that key secret.

This problem – a safe key exchange – is one of the issues that has been solved by public key cryptography (PKC). In PKC, each party has two keys: a public key that it publishes for everyone to use, and a private key that it doesn't share with anyone.

Pieter Maene: "Your IoT sensor will encrypt a message using the public key of the server it wants to talk to. Only that server can now decrypt the message using its own private key. Similarly, the server can use the sensor's public key to encrypt messages, which only the sensor can decrypt using its private key. This scheme has two advantages: no keys have to be exchanged; everyone's private key is absolutely private and everyone's public key is in the open. And second: by using a public key of a specific computer to encrypt your message, you make sure that only that computer can decrypt that message, with its private key. So PKC also includes the basis for authentication."

A security processor for low-power devices and tags

"One of our latest efforts offers a good example of how we are innovating the field of security for IoT devices," **says Rožić.** "It is a processor that is flexible enough to support multiple cryptographic protocols. Its energy consumption while performing cryptographic operations is one of the lowest ever reported – low enough to serve as a basis for cryptography in passive RFID tags."

To operate, passive RFID tags draw their energy from the magnetic field of a nearby RFID reader. Close to that reader, the available power is highest. But increasing the distance results in a sharp drop. With a typical antenna and at a distance of 50cm, e.g., the tag may have a power budget nearing 300□W. At 70cm, the available power drops to 40□W.

Vladimir Rožić: "A tag without crypto processor may need less than 10□W, so that leaves maybe 250□W at 50cm for the security computations, but only 30□W at 70cm. At an operating frequency of 847.5 kHz, our processor consumes an average of 50.4□W. In this mode, it can easily provide cryptography for RFIDs up to the 50cm range. But we can lower our chip's average energy budget to 13.6□W by reducing the clock frequency to 211.9 kHz. And then it could be used for most RFID applications, with contact distances up to 70cm."

The PKC scheme used in the new chip implements elliptic curve cryptography (ECC), which is best-suited for energy-constrained devices. This is because its mathematics work with shorter numbers and it has a lower computational complexity, especially compared to the widely-used RSA system.

"To give an idea," **comments Rožić:** "to reach a security level that is equivalent with RSA keys with 1024-bits, ECC only needs to work with 163 bits."

There are many elliptic curve schemes available, but the researchers worked with one that is called K-163 and that is recommended by the USA National Institute of Standards and Technology (NIST). This curve achieves a fine balance between security, area and speed.

Testing the chip's security

The elliptic curve system is mathematically secure. The private keys cannot be cracked by conventional computers. But there are other ways that adversaries may try to break the system, through so called side-channel attacks. These involve measuring the time that specific computations take, or the power they consume. When a system is not carefully designed, such leaks may undermine its security.

RožiĆ: “We have taken great care in the implementation of the algorithms and the design of the hardware to avoid such side-channel leaks. To prevent timing attacks, for example, we implemented a fixed execution time regardless of the value of the keys. But our system is also sufficiently guarded against power analysis attacks, a protection which we have extensively tested because it is so important.”

This work was published in V. RožiĆ, O. Reparaz, and I. Verbauwhede, "A 5.1□J per point-multiplication elliptic curve cryptographic processor," International Journal of Circuit Theory and Applications 45(2), pp. 170-187, 2016.

Biography Vladimir RožiĆ

Vladimir RožiĆ obtained the Bachelor’s degree of Electrical Engineering from the University of Belgrade (Serbia) in 2007 and a PhD in Engineering Science from the KU Leuven (Belgium) in 2016. He is currently a postdoctoral researcher at the research group COSIC. His main research interests are related to embedded security with a special focus on hardware random number generators, physically unclonable functions and design of secure cryptographic chips.

Biography Pieter Maene

Pieter Maene received his M.Sc. in Electrical Engineering from the KU Leuven in 2014. He then started his PhD research at the COSIC lab under Prof. Ingrid Verbauwhede. He is specialized in lightweight trusted computing architectures, building technologies which give users more assurances about the software running on their devices.