Improving cybersecurity in an increasingly technological world

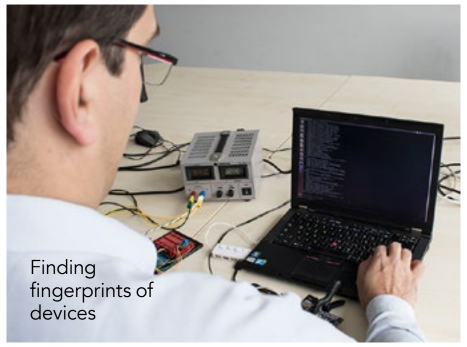
Prof Dr Stefan Katzenbeisser is a Professor for Security Engineering and a member of the Cybersecurity (CYSEC) Profile Area at Technische Universität Darmstadt in Germany. He is a Principal Investigator in the Collaborative Research Center CROSSING and the Center for Research and Privacy (CRISP). He conducts research into IT security solutions for critical infrastructures.

Technology is now more and more ubiquitous. Devices are increasingly embedded in everyday items, such as consumer electronics, and critical infrastructures, such as industrial equipment and the power grid. This has been termed the 'Internet of Things': a phrase which describes how low-end technological devices, that have the capacity to communicate via the Internet, are an intrinsic part of everyday objects.

While these devices have obvious benefits (being able to programme your heating from your phone, for example), the greater interconnectedness increases the attractiveness of these devices for cyber attacks – there are profitable outcomes to targeting software and hardware. In addition, these devices generally lack security hardware to protect against attacks, making them easy, as well as profitable, targets.

Software is more vulnerable to attack from hackers than hardware: to compromise hardware an attacker has to physically change it, unlike software which can be hacked remotely. Therefore, the most reliable way of securing a device is to include a 'trust anchor' within the hardware. This trust anchor is generally a small piece of hardware that can bootstrap security for the whole device by confirming that the rest of the device has not been hacked. By installing the trust anchor as hardware, it will not be compromised if the software is corrupted (easy once an attacker has broken in).

Dr Katzenbeisser's work focuses on two main areas to improve the security of everyday technology: identifying a device and verifying that it is running the correct software.



Finding fingerprints of devices

FINGERPRINTING DEVICES

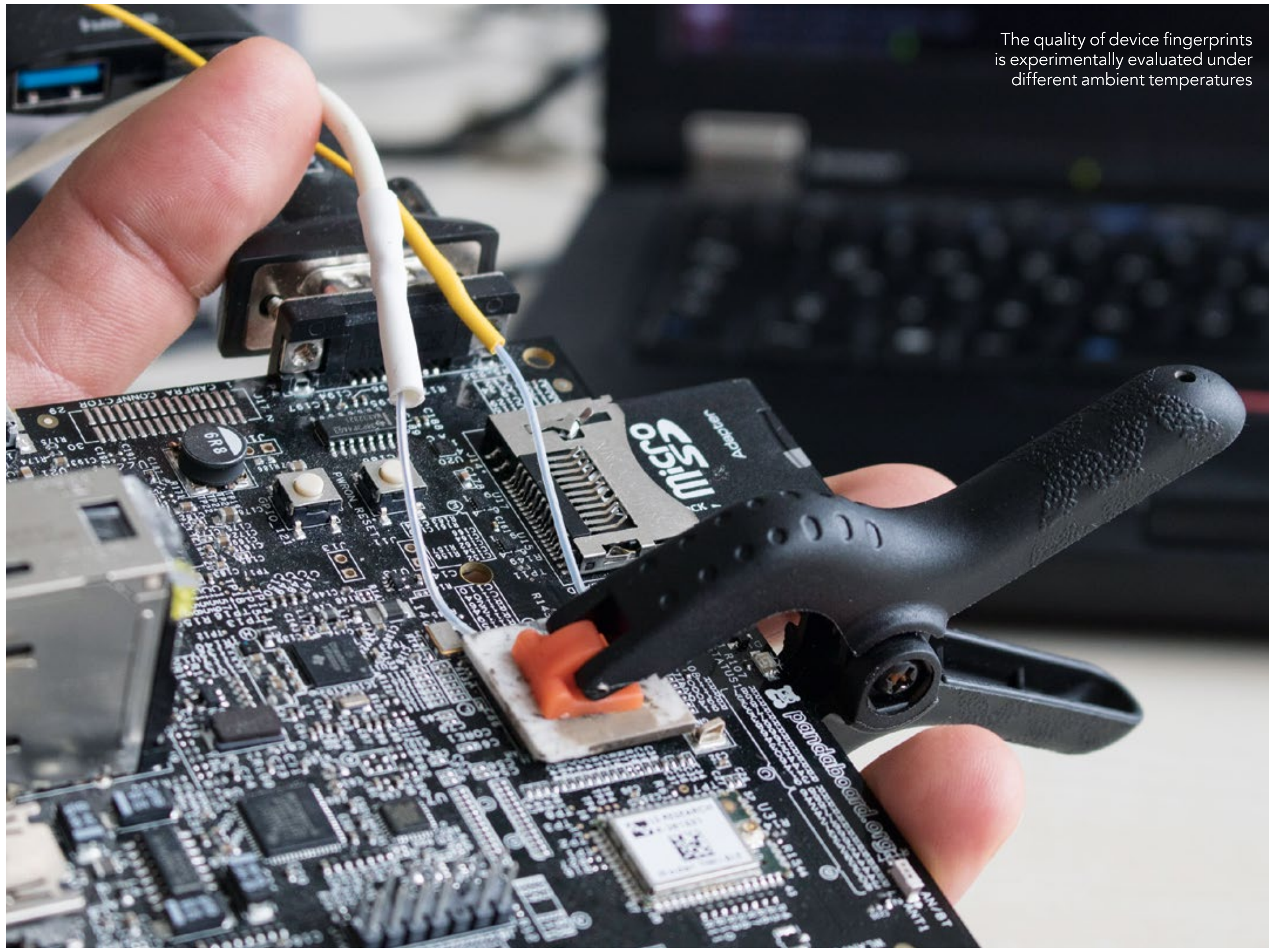
In order to communicate as a device with other devices in the network, a central element of security is knowing who you are talking to.

To identify the different members of a communication network, Dr Katzenbeisser's team makes use of tiny variations that arise during the manufacturing process, which distinguish devices from one another, giving them a unique signature or fingerprint. These are called Physically Unclonable Functions (PUFs) and can be exploited to implement security in low-tech devices without secure hardware.

Because PUFs are an embodied physical entity, they act as a trust anchor – they can be assumed to be uncompromised. PUFs can be readily evaluated to confirm the device's identity, but their behaviour cannot be predicted, even if somebody knows the exact manufacturing process that was used. This means they are easy to make, but virtually impossible to duplicate.

PUFs can also link the use of a particular type of software to a specific device, which protects the programmed code against manipulation by external sources, such as attackers who would like to reproduce it.

> **Because PUFs are an embodied physical entity, they act as a trust anchor – they can be assumed to be uncompromised**



The quality of device fingerprints is experimentally evaluated under different ambient temperatures

DYNAMIC IDENTIFICATION

Specifically, the research group of Dr Katzenbeisser and his collaborators have developed a novel type of PUF called a DRAM PUF, which makes use of the dynamic random access memories (where the ‘DRAM’ part of the name comes from) that computers need to function.

DRAM PUFs are an improvement on the ‘intrinsic’ PUFs that are already inherently present in many commodity devices. Traditional intrinsic PUFs can only be accessed when the device starts up. DRAM PUFs, on the other hand, can be accessed while the device is running, so the identity and security of a system can be queried at any time.

SHHH… IT’S A SECRET

Cryptography relies on the use of keys, small ‘secrets’ which must be kept secure. These keys are pieces of information that control the cipher. The PUF can not only generate a unique key – a device’s fingerprint – but it can also be used as a storage medium for cryptographic keys. This way, keys can be protected even on a compromised device.

REMOTE ATTESTATION

Dr Katzenbeisser’s research also focuses on identifying whether or not a device is running the correct software. This is important because hackers will often try to alter the device's programs to realise their own ends. This verification process is called ‘remote attestation’. Dr Katzenbeisser has been working on creating protocols to detect the misuse and malfunctioning of devices as early as possible.

Several techniques have been proposed to verify whether or not individual devices have been compromised. A new challenge arises when there are multiple devices in a network, because the amount of information that needs to be transmitted soars at a much greater rate than the number of devices added to the network.

The protocol developed by Dr Katzenbeisser’s team confirms whether devices in a large network have been compromised using ‘heartbeats’. Each device in the network is connected to some other device, and can transmit and receive information. The novelty of Dr Katzenbeisser’s approach is that one ‘leader’ device periodically transmits a heartbeat signal, which is logged and retransmitted by neighbouring devices, together with its own software state. Each device must transmit the most recent heartbeat to be considered uncompromised. Because hackers have to take devices offline to physically tamper with hardware, compromised devices will miss the most recent heartbeat, and therefore be detectable.

The resulting protocol is scalable and can be used in networks of any size without issue. It has several advantages over previously developed methods. Firstly, it is much more efficient, which is especially important when networks are large. Secondly, it can precisely identify which devices are compromised, as long as the total number of compromised devices is less than half the network. Other methods cannot pinpoint the problem device, but merely detect that the whole network is unsafe. Thirdly, it also prevents the problem of false positives, whereby issues other than security breaches (e.g., technical failures) cause the protocol to consider the network insecure.

This work is performed in the Collaborative Research Center CROSSING, funded by the German Research Foundation. CROSSING is dedicated to providing security solutions for new and next generation computing environments.

All of Dr Katzenbeisser’s work aims to improve trust and security in an increasingly technological world. His research protects critical code and data from malicious exploitation.

> **Dr Katzenbeisser’s work aims to improve trust and security in an increasingly technological world. His research protects critical data and code from malicious exploitation**

Q&A

How much is at risk due to the increasing prevalence of technology in everyday items?

A lot. We increasingly rely on networked devices in our daily life. At home, hacked devices may only cause annoyance for their users but, when used to control critical infrastructures, unprotected devices may even undermine the core functions of our society.

How common are cyber attacks on commodity devices?

Hackers have recently identified attacks against devices in the 'Internet of Things' as attractive targets, due to their low level of protection as well as their sheer number. We have recently seen massive Denial of Service attacks, threatening core Internet services, which originated from web cameras and other 'Internet of Things' devices. Attacks against small networked devices are already happening now!

Does the ‘Internet of Things’ represent a positive development?

Yes. Still, we need to assess the risk posed by networked devices. At the moment, many manufacturers simply add network interfaces to existing products, which were never designed with security in mind. This is the root cause of many security incidents we see in the Internet of Things. We need to establish a new “security culture”: vendors need to care about security as much as they care about user convenience and safety.

How important is it to protect devices from attacks?

Compromised networked devices do not only pose a threat to their owners, but can also serve as a basis for large-scale attacks. At the same time, we need to make sure that devices controlling critical infrastructures are adequately protected.

What kind of variations are detectable as PUFs?

Digital PUFs rely on small manufacturing variations in electronic circuits, such as voltage differences, signal delays or sizes of transistors. Even using advanced production technologies, such minuscule variations cannot be completely controlled by manufacturers.

Detail

RESEARCH OBJECTIVES

Dr Katzenbeisser’s research focuses on developing IT security solutions tailored to critical infrastructures. He and his team are continuously developing methods and tools to improve cybersecurity and privacy.

FUNDING

- The German Research Foundation (DFG)
- The German Federal Ministry of Education and Research
- The European Commission

COLLABORATORS

Jakub Szefer (Yale University)

BIO

Following the completion of his PhD in Computer Science at the Vienna University of Technology, Prof Dr Katzenbeisser has enjoyed a distinguished career as a researcher and professor. He currently works as a Professor at Technische Universität Darmstadt.

CONTACT

Prof Stefan Katzenbeisser
Technische Universität Darmstadt
Mornewegstrasse 32
D-64293 Darmstadt
Germany

T: +49 6151 1625620
E: katzenbeisser@seceng.informatik.tu-darmstadt.de