Kryptotag @ Uni Regensburg, 25./26. Mai 2023

Donnerstag, 09.06.2022			**Talk**	**Speaker**	**Affiliation**	**Title**
13:00	13:30	0:30	**Get Together**			
13:30	13:35	0:05	Welcome	Michael Nüsken	b-it, Bonn	Hello
13:35	14:20	0:45	*Keynote Talk*	Elif Kavun	Uni Passau	Symbiotic Security from RISC-V and PUFs
14:20	14:45	0:25	Talk	Tobias Guggemos	Uni Wien	Demonstration of quantum-digital payments
14:45	15:15	0:30	**Coffee Break**			
15:15	15:40	0:25	Talk	Janik Schug	Uni Hamburg	Securing Biometric Access Control
15:40	16:05	0:25	Talk	Nico Mexis	Uni Passau	An Improved Machine-Learning Model for the Identification and Classification of Memory-Based PUF Responses
16:05	16:30	0:25	Talk	Tobias Tefke	FH Schmalkalden	Exchanging messages between constrained devices ensuring confidentiality and authenticity
16:30	17:00	0:30	**Coffee Break**			
17:00	17:25	0:25	Talk	Maximiliane Weishäupl	Uni Regensburg	Committing Authenticated Encryption
17:25	17:55	0:30	GI FG Krypto	Leitungsgremium FG KRYPTO		GI Fachgruppentreffen “Angewandte Kryptographie”
17:55	18:30	0:35	"Kofferpause"			
18:30			**Social event**			
Freitag, 10.06.2022			**Talk**	**Speaker**	**Affiliation**	**Title**
9:00	9:30	0:30	**Good Morning Coffee**			
9:30	10:00	0:30	Talk	Kai Hendrik Wöhnert	HAW Hamburg	Artificial Intelligence Based Identity Learning for Malware Detection Using Fuzzified Advanced Robust Hashes
10:00	10:30	0:30	Talk	Shashank Tripathi	HAW Hamburg	Malware Identification and Static Analysis using FaR Hash
10:30	11:00	0:30	**Coffee Break**			
11:00	11:30	0:30	Talk	Antoine Gansel	University of Twente	Privacy-Preserving Cohort Selection
11:30	12:00	0:30	Talk	Giang Nam Nguyen	TU Darmstadt	SageMath–A Great Environment for Experimenting with Isogeny-based Cryptography
12:00	12:30	0:30	Talk	Knud Ahrens	Uni Passau	Putting an End to VDFs: A verifiable delay function using the endomorphism ring
12:30	13:00	0:30	**Farewell**			

Exchanging messages between constrained devices ensuring confidentiality and authenticity

Tobias Tefke[1] and Ralf C. Staudemeyer[1]

[1]Faculty of Computer Science, Schmalkalden University of Applied Sciences, 98574 Schmalkalden, Germany

35th Crypto Day, 25/26 May 2023

Protecting confidentiality and authenticity of data when exchanging information between severely constrained devices poses a major challenge due to the lack of computational resources. In our use case, we would like to pass a sensor value from one device to another. For this, we use the Zolertia RE-Mote (Lignan, 2016) Internet of Things (IoT) devices. These have only 32 kB of main memory available for the operating system and all applications running on top of it. Nevertheless, we would like to ensure confidentiality and authenticity of exchanged information.

The RE-Motes are supported by the IoT operating system Contiki-NG (Oikonomou, Duquennoy, Elsts, Eriksson, Tanaka & Tsiftes, 2022). For exchanging data between devices we use the CoAP protocol (Shelby, Hartke & Bormann, 2014). Data transmitted via CoAP is encrypted with DTLS (Rescorla, Tschofenig & Modadugu, 2022). This is also known as CoAPs (Bormann, Lemay, Tschofenig, Hartke, Silverajan & Raymor, 2018).

In Contiki-NG, CoAPs can be enabled with the tinyDTLS library (Contiki-NG, 2022). For ensuring authenticity, we would like to use the ECDSA algorithm (Raimondo & Locascio, 2023). In order to exchange data, we adopt the JSON Sensor Signature format (JSS) (Pohls, 2015). During JSS generation, the data is hashed with SHA-256 (Pritzker & May, 2015). Afterwards, the hash is signed with ECDSA (Raimondo & Locascio, 2023). Then, the data is forwarded to another device within the IoT network infrastructure. The recipient can validate the authenticity of the confidential message with the public key of the sender. This key was broadcasted previously during initialisation of the IoT-network.

The main challenge is making all cryptographic procedures work despite of only having 32 kB of RAM. The lowest power mode of the RE-Mote only allows using half of the CPU's memory (Texas Instruments, 2013), which is not sufficient for our application and has therefore been disabled. However, open challenges remain in fitting the whole application into the available memory. The aim of this contribution is to provide an overview about the current status of the implementation and how we plan to move forward.

References

Carsten Bormann, Simon Lemay, Hannes Tschofenig, Klaus Hartke, Bill Silverajan & Brian Raymor (2018). CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets. RFC 8323. URL https://www.rfc-editor.org/info/rfc8323.

Contiki-NG (2022). tinyDTLS. URL https://github.com/contiki-ng/tinydtls.

Antonio Lignan (2016). *Zolertia RE-Mote platform.* Zolertia. URL https://github.com/Zolertia/Resources/wiki/RE-Mote.

George Oikonomou, Simon Duquennoy, Atis Elsts, Joakim Eriksson, Yasuyuki Tanaka & Nicolas Tsiftes (2022). The Contiki-NG open source operating system for next generation IoT devices. *SoftwareX* **18**. URL https://doi.org/10.1016/j.softx.2022.101089.

Henrich C. Pohls (2015). JSON Sensor Signatures (JSS): End-to-End Integrity Protection from Constrained Device to IoT Application. In *2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing.* IEEE. URL https://doi.org/10.1109/imis.2015.48.

Penny Pritzker & Willie E. May (2015). Secure Hash Standard (SHS). URL https://doi.org/10.6028/nist.fips.180-4.

Gina M. Raimondo & Laurie E. Locascio (2023). Digital Signature Standard (DSS). URL https://doi.org/10.6028/nist.fips.186-5.

Eric Rescorla, Hannes Tschofenig & Nagendra Modadugu (2022). The Datagram Transport Layer Security (DTLS) Protocol Version 1.3. RFC 9147. URL https://www.rfc-editor.org/info/rfc9147.

Zach Shelby, Klaus Hartke & Carsten Bormann (2014). The Constrained Application Protocol (CoAP). RFC 7252. URL https://www.rfc-editor.org/info/rfc7252.

Texas Instruments (2013). CC2538 System-on-Chip Solution for 2.4-GHzIEEE 802.15.4 and ZigBee®/ZigBee IP®Applications. Texas Instruments CC2538™ Family of Products. URL https://www.ti.com/lit/ug/swru319c/swru319c.pdf.