ROUTING AND ACTION

MEMORANDUM

ROUTING

TO:(1) Network Sciences Branch (Wang, Cliff)

Report is available for review

(2) Proposal Files Report No.: Proposal Number: 66733-NS.13

DESCRIPTION OF MATERIAL

CONTRACT OR GRANT NUMBER: W911NF-16-1-0536

INSTITUTION: University of California - Irvine

PRINCIPAL INVESTIGATOR: Gene Tsudik

TYPE REPORT: Final Report

DATE RECEIVED: 12/28/21 4:32AM

PERIOD COVERED: 9/1/16 12:00AM through 8/30/21 12:00AM

TITLE: Final Report: Remote Attestation of Critical Infrastructure Components

ACTION TAKEN BY DIVISION

(x) Report has been reviewed for technical sufficiency and IS [x] IS NOT [ ] satisfactory.

( ) Based on my technical review, I have identified no OPSEC or Technology Protection concerns that need to be addressed regarding this report.

(x) Perfomance of the research effort was accomplished in a satisfactory manner and all other technical requirements have been fulfilled.

(x) Based upon my knowledge of the research project, I agree with the patent information disclosed.

Approved by SSL\CLIFF.WANG.2 on 8/9/22 2:33PM

ARO FORM 36-E

REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
28-12-2021	Final Report	1-Sep-2016 - 30-Aug-2021

4. TITLE AND SUBTITLE
Final Report: Remote Attestation of Critical Infrastructure Components

5a. CONTRACT NUMBER
W911NF-16-1-0536

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
University of California - Irvine
141 Innovation Drive, Suite 250

Irvine, CA 92697 -7600

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
66733-NS.13

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Gene Tsudik
UU	UU	UU	UU		19b. TELEPHONE NUMBER 949-824-3410

RPPR Final Report
as of 09-Aug-2022

Agency Code: 21XD

Proposal Number: 66733NS **Agreement Number: W911NF-16-1-0536**
INVESTIGATOR(S):

Name: Gene Tsudik
Email: gene.tsudik@uci.edu
Phone Number: 9498243410
Principal: Y

Organization: **University of California - Irvine**
Address: 141 Innovation Drive, Suite 250, Irvine, CA 926977600
Country: USA
DUNS Number: 046705849 EIN: 952226406

Report Date: 30-Nov-2021 Date Received: 28-Dec-2021
Final Report for Period Beginning 01-Sep-2016 and Ending 30-Aug-2021
Title: Remote Attestation of Critical Infrastructure Components
Begin Performance Period: 01-Sep-2016 **End Performance Period:** 30-Aug-2021
Report Term: 0-Other

Submitted By: Gene Tsudik Email: gene.tsudik@uci.edu
Phone: (949) 824-3410

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 2 **STEM Participants:** 2

Major Goals: Major Goals include:
* Exploration of software/hardware co-design in constructing secure and efficient techniques for Remote Attestation of embedded (IoT) devices. This encompasses investigating current and emerging attacks/adversary types, including those mounted via software, side-channels as well as physical means. We also aim to provide assurance by formally verifying proposed techniques.
* Research into efficient, robust/resilient and scalable Remote Attestation in the context of groups(swarms) of potentially heterogeneous devices, with dynamic membership and support for device mobility.

Accomplishments: For a detailed description of accomplishments, please see enclosed PDF document.

RPPR Final Report
as of 09-Aug-2022

Training Opportunities: The project directly contributed to training of two UCI CS PhD students and one postdoctoral researcher.

One PhD student (Norrathep Rattanavipanon) conducted research on swarm attestation and hybrid attestation. The former involvee careful specification of the attestation process for each prover device that is being attested as part of the swarm, while the latter involves fusing the formally verified sel4 microkernel with hybrid attestation to attain a prover with minimal hardware requirements (only secure bootloader).

This student graduated with a PhD in Computer Science in December 2019. His dissertation was entirely related to this project. Since January 2019 he is an Assistant Professor at the Prince of Songla University in Phuket, Thailand.

The second PhD student (Ivan Oliveira Nunes) worked on several topics related to this project. One topic was presence attestation -- techniques for human users (owners) to verify the presence of DRTM (Dynamic Root of Trust) on their devices. He also worked on Swarm RA, formally-verified RA and related topics.

This student graduated in July 2021 and started as Assistant Professor in the Computer Science Department at the Rochester Institute of Technology (RIT) in August 2021.

The postdoctoral scholar (Xavier Carpent) worked on swarm attestation, temporal consistency of integrity-ensuring functions and autonomous (verifier-free) attestation and several other related topics. He obtained valuable research experience which facilitated his transition to a researcher position at UCSD. He is now an Assistant Professor at the University of Nottingham (UK).

RPPR Final Report
as of 09-Aug-2022

Results Dissemination: -------- 2017-2018

X. Carpent, K. Eldefrawy, N. Rattanavipanon, A. Sadeghi and G. Tsudik
Reconciling Remote Attestation and Safety-Critical Operation on Simple
IoT Devices,
QCM/IEE Design Automation Conference (DAC), 2018.

X. Carpent, N. Rattanavipanon and G. Tsudik
Temporal Consistency of Integrity-Ensuring Computations and Applications
to Embedded Systems Security,
ACM ASIACCS, 2018.

X. Carpent, N. Rattanavipanon and G. Tsudik
Remote Attestation of IoT Devices via SMARM: Shuffled
Measurements Against Roving Malware,
IEEE HOST, 2018.

X. Carpent, N. Rattanavipanon and G. Tsudik
ERASMUS: Efficient Remote Attestation via Self-Measurement for
Unattended Settings,
IEEE/ACM Design, Automation, and Test in Europe (DATE), 2018.

-------- 2018-2019

K. Eldefrawy and G. Tsudik
Advancing Remote Attestation via Computer-aided Formal Verification of
Designs and Synthesis of Executables
ACM WISEC, 2019.

I. De Oliveira Nunes, K. Eldefrawy, N. Rattanavipanon, M. Steiner and G. Tsudik
VRASED: A Verified Hardware/Software Co-Design for Remote Attestation
USENIX Security Symposium, 2019.

I. De Oliveira Nunes, K. Eldefrawy, N. Rattanavipanon and G. Tsudik
PURE: Using Verified Remote Attestation to Obtain Proofs of Update,
Reset and Erasure in Low-End Embedded Systems
IEEE/ACM International Conference On Computer Aided Design (ICCAD), 2019.

I. De Oliveira Nunes, G. Dessouky, A. Ibrahim, N. Rattanavipanon,
A. Sadeghi and G. Tsudik
Towards Systematic Design of Collective Remote Attestation Protocols
IEEE International Conference on Distributed Computing Systems (ICDCS), 2019.

A. Ibrahim, A. Sadeghi, G. Tsudik:
HEALED: HEaling and Attestation for Low-End Embedded Devices
Financial Cryptography 2019, pp. 627-645.

-------- 2019-2020

M. Ammar, B. Crispo and G. Tsudik
SIMPLE: A Remote Attestation Approach for Resource-Constrained IoT devices
International Conference on Cyber-Physical Systems (ICCPS/CPSWeek), 2020.

I. De Oliveira Nunes, K. Eldefrawy, N. Rattanavipanon and G. Tsudik
APEX: A Verified Architecture for Proofs of Execution on Remote Devices Under
Full Software Compromise
USENIX Security Symposium, 2020.

RPPR Final Report
as of 09-Aug-2022

-------- 2020-2021

I. De Oliveira Nunes, S. Jakkamsetti, N. Rattanavipanon, G. Tsudik:
On the TOCTOU Problem in Remote Attestation.
ACM CCS 2021: 2921-2936

I. De Oliveira Nunes, S. Jakkamsetti, G. Tsudik:
DIALED: Data Integrity Attestation for Low-end Embedded Devices.
ACM/IEEE DAC 2021: 313-318

I. De Oliveira Nunes, S. Jakkamsetti, G. Tsudik:
Tiny-CFA: Minimalistic Control-Flow Attestation Using Verified Proofs of Execution. ACM/IEEE DATE 2021: 641-646

I. De Oliveira Nunes, X. Ding, G. Tsudik:
On the Root of Trust Identification Problem.
ACM IPSN 2021: 315-327

M. Ammar, B. Crispo, I. De Oliveira Nunes, G. Tsudik:
Delegated attestation: scalable remote attestation of commodity CPS by blending proofs of execution with software attestation.
ACM WISEC 2021: 37-47

Honors and Awards: Gene Tsudik was the recipient of the 2017 ACM SIGSAC Outstanding Contributions Award.

Gene Tsudik was elected AAAS Fellow in November 2016, Citation: For Contributions to Internet Security and Privacy.

Gene Tsudik was awarded the TUV Sud Foundation Visiting Professorship, at TU Dresden (Germany), 2017-2018.

Best Paper Award, IEEE International Conference on Computer Communications and Networks (ICCCN), 2017.

Gene Tsudik was appointed a Fulbright Specialist at the University of Information Technology, Yangon, Myanmar, October-November 2019. This selective appointment focuses on cybersecurity curriculum design with particular emphasis on IoT and embedded systems security.

Gene Tsudik was appointed Distinguished Professor of Computer Science at UCI effective July 1, 2019. (He was previously Chancellor's Professor of Computer Science). NOTE: at UCI, the Distinguished Professor title is a campus-level distinction and is reserved for Above Scale faculty who have achieved the highest levels of scholarship over the course of their careers. Distinguished Professors will typically have earned national and international level distinctions and honors of the highest level.

Gene Tsudik presented a keynote talk at the ACM AsiaCCS 2020, titled: "Proofs or Remote Execution and Mitigation of TOCTOU Attacks".

Gene Tsudik was elected IFIP Fellow in 2020, as part of IFIP's inaugural cohort of fellows.

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Gene Tsudik
Person Months Worked: 10.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Postdoctoral (scholar, fellow or other postdoctoral position)
Participant: Xavier Carpent
Person Months Worked: 8.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Norrathep Rattavipanon
Person Months Worked: 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Ivan De Oliveira Nunes
Person Months Worked: 11.00 **Funding Support:**
Project Contribution:
National Academy Member: N

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: the 2017 ACM
Date Received: 03-Oct-2017 Conference Date: 02-Apr-2017 Date Published:
Conference Location: Abu Dhabi, United Arab Emirates
Paper Title: Lightweight Swarm Attestation
Authors: Xavier Carpent, Karim ElDefrawy, Norrathep Rattanavipanon, Gene Tsudik
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)
Date Received: 03-Oct-2017 Conference Date: 26-Jun-2017 Date Published: 17-Jul-2017
Conference Location: Denver, CO, USA
Paper Title: FUsing Hybrid Remote Attestation with a Formally Verified Microkernel: Lessons Learned
Authors: Karim Eldefrawy, Norrathep Rattanavipanon, Gene Tsudik
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 09-Aug-2022

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: the 10th ACM Conference
Date Received: 03-Oct-2017 Conference Date: 18-Jul-2017 Date Published: 19-Jul-2017
Conference Location: Boston, Massachusetts
Paper Title: HYDRA: HYbrid Design for Remote Attestation (Using a Formally Verified Microkernel)
Authors: Karim Eldefrawy, Norrathep Rattanavipanon, Gene Tsudik
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: the 2016 ACM SIGSAC Conference
Date Received: 03-Oct-2017 Conference Date: 24-Oct-2016 Date Published: 26-Oct-2016
Conference Location: Vienna, Austria
Paper Title: C-FLAT: Control-Flow Attestation for Embedded Systems Software
Authors: Tigist Abera, N. Asokan, Lucas Davi, Jan-Erik Ekberg, Thomas Nyman, Andrew Paverd, Ahmad-Reza S
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: ACM WiSeC
Date Received: 17-Oct-2019 Conference Date: 15-May-2019 Date Published:
Conference Location: Miami, Florida
Paper Title: Advancing remote attestation via computer-aided formal verification of designs and synthesis of executables
Authors: Karim Eldefrawy, Gene Tsudik
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 28th USENIX Security Symposium (USENIX Sec'19)
Date Received: 17-Oct-2019 Conference Date: 14-Aug-2019 Date Published: 16-Aug-2019
Conference Location: San Jose, CA
Paper Title: VRASED: A Verified Hardware/Software Co-Design for Remote Attestation
Authors: Ivan De Oliveira Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, Michaek Steiner, Gene Tsudik
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE/ACM ICCAD
Date Received: 02-Nov-2020 Conference Date: 04-Nov-2019 Date Published: 06-Nov-2019
Conference Location: Westminster, CO
Paper Title: PURE: Using Verified Remote Attestation to Obtain Proofs of Update, Reset and Erasure in Low-End Embedded Systems
Authors: Ivan De Oliveira Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, Gene Tsudik
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)
Date Received: 17-Oct-2019 Conference Date: 07-Dec-2018 Date Published: 07-Jul-2019
Conference Location: Dallas, TX
Paper Title: Towards Systematic Design of Collective RemoteAttestation Protocols
Authors: Ivan De Oliveira Nunes, Ghada Dessouky, Ahmad Ibrahim, Norrathep Rattanavipanon, Ahmad-Reza Sa
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 09-Aug-2022

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2020 ACM/IEEE 11th International Conference on Cyber-Physical Systems (ICCPS)
Date Received: 02-Nov-2020 Conference Date: 21-Apr-2020 Date Published: 21-Apr-2020
Conference Location: Sydney, Australia
Paper Title: SIMPLE: A Remote Attestation Approach for Resource-constrained IoT devices
Authors: Mahmoud Ammar, Bruno Crispo, Gene Tsudik
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 29th USENIX Security Symposium (USENIX Security'20)
Date Received: 02-Nov-2020 Conference Date: 12-Aug-2020 Date Published: 12-Aug-2020
Conference Location: Virtual
Paper Title: APEX: A Verified Architecture for Proofs of Execution on Remote Devices under Full Software Compromise
Authors: Ivan De Oliveira Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, Gene Tsudik
Acknowledged Federal Support: **Y**

DISSERTATIONS:

Publication Type: Thesis or Dissertation
Institution: University of California, Irvine
Date Received: 02-Nov-2020 Completion Date: 12/1/19 11:40AM
Title: Secure Remote Attestation for Safety-Critical Embedded and IoT Devices
Authors: Norrathep Rattanavipanon
Acknowledged Federal Support: **Y**

WEBSITES:

URL: http://sprout.ics.uci.edu/projects/attestation/
Date Received: 03-Oct-2017
Title: Remote Attestation of Embedded Devices
Description: Project Web Site

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Gene Tsudik
Signature Date: 12/28/21 4:32AM

2017/2018

Presence Attestation

Many popular modern processors include an important hardware security feature in the form of a DRTM (Dynamic Root of Trust for Measurement) that helps bootstrap trust and resists software attacks. However, despite substantial body of prior research on trust establishment, security of DRTM was treated without involvement of the human user, who represents a vital missing link. The basic challenge is: how can a human user determine whether an expected DRTM is currently active on her device? We define the notion of "presence attestation", which is based on mandatory, though minimal, user participation. We constructed three concrete presence attestation schemes: sight-based, location-based, and scene-based. They vary in terms of security and usability features and are suitable for different application contexts. After analyzing their security, we assess their usability and performance based on prototype implementations.

Robust and Efficient Swarm Attestation

Our main goal is to advance swarm attestation by bringing it closer to reality. To this end, we make two contributions: (1) a new metric, called QoSA: Quality of Swarm Attestation, that captures the information offered by a swarm attestation technique; this allows comparing efficacy of multiple protocols, and (2) two practical attestation protocols – called LISA-A and LISA-S – for mobile swarms, with different QoSA features and communication and computation complexities. Security of proposed protocols is analyzed, and their performance is assessed based on experiments with prototype implementations.

Efficient Attestation via Self-Measurements

All prior RA techniques require on-demand operation, i.e., RA is performed in real time. We identify some drawbacks of this general approach in the context of unattended devices: First, it fails to detect mobile malware that enters and leaves the prover between successive RA instances. Second, it requires the prover to engage in a potentially expensive (in terms of time and energy) computation, which can be harmful for critical or real-time devices.

To address these drawbacks, we introduce the concept of self-measurement where a prover device periodically (and securely) measures and records its own software state, based on a pre-established schedule. A possibly untrusted verifier occasionally collects and verifies these measurements. We present the design of a concrete technique called ERASMUS: Efficient Remote Attestation via Self-Measurement for Unattended Settings, justify its features and evaluate its performance. In the process, we also define a new metric – Quality of Attestation (QoA). We argue that ERASMUS is well-suited for time-sensitive and/or safety-critical applications that are not served well by on-demand RA. Finally, we show that ERASMUS is a promising steppingstone towards handling attestation of multiple devices (i.e., a group or swarm) with high mobility.

Fusion of Formally Verified Components with Attestation

In this work, we construct the first hybrid RA design – called HYDRA – that builds upon formally

verified software components that ensure memory isolation and protection, as well as enforce access control to memory and other resources. HYDRA obtains these properties by using the formally verified seL4 microkernel. (Until now, this was only attainable with purely hardware-based designs.) Using seL4 imposes fewer hardware requirements on the underlying microprocessor. Also, building upon a formally verified software component increases confidence in security of the overall design of HYDRA and its implementation. We instantiate HYDRA on two commodity hardware platforms and assess the performance and overhead of performing RA on such platforms via experimentation; we show that HYDRA can attest 10MB of memory in less than 250msec when using a Speck-based cryptographic checksum.

Control Flow Attestation of Simple IoT Devices

Remote Attestation is a crucial security service particularly relevant to increasingly popular IoT (and other embedded) devices. It allows a trusted party (verifier) to learn the state of a remote, and potentially malware-infected, device (prover). Most existing approaches are static in nature and only check whether benign software is initially loaded on the prover. However, they are vulnerable to run-time attacks that hijack the application's control or data flow, e.g., via return-oriented programming or data-oriented exploits. As a concrete step towards more comprehensive runtime remote attestation, we design and implement Control-Flow ATtestation (C-FLAT) that enables remote attestation of an application's control-flow path, without requiring the source code. We describe a full prototype implementation of C-FLAT on Raspberry Pi using its ARM TrustZone hardware security extensions. We evaluate C-FLAT's performance using a real-world embedded (cyber-physical) application and demonstrate its efficacy against control-flow hijacking attacks.

2018/2019

Secure Software/Firmware Update

Secure firmware update is an important stage in the IoT device lifecycle. Prior techniques, designed for other computational settings, are not readily suitable for IoT devices since they do not consider idiosyncrasies of a realistic large-scale IoT deployment. This motivated our design of ASSURED, a secure and scalable update framework for IoT. ASSURED includes all stakeholders in a typical IoT update ecosystem, while providing end-to-end security between manufacturers and devices. To demonstrate its feasibility and practicality, ASSURED is instantiated and experimentally evaluated on two commodity hardware platforms. Results show that ASSURED is considerably faster than current update mechanisms in realistic settings.

Protecting RA against Roving Malware

Malware that is aware of ongoing or impending RA and aims to avoid detection can relocate itself during computation of an attestation measurement. To thwart such behavior, prior RA techniques are either non-interruptible or explicitly forbid modification of storage during measurement computation. However, since the latter can be a time-consuming task, this curtails availability of device's other (main) functions, which is especially undesirable, or even dangerous, for devices with time- and/or safety-critical missions. To this end, we designed SMARM, a light-weight

technique, based on shuffled measurements, as a defense against roving malware. In SMARM, memory is measured in a randomized and secret order. This does not impact device's availability – the measurement process can be interrupted, even by malware, which can relocate itself at will. We analyze various malware behaviors and show that, while malware can escape detection in a single attestation instance, it is highly unlikely to avoid eventual detection.

Temporal Consistency of Integrity-Ensuring Computations

Assuring integrity of information (e.g., data and/or software) is usually accomplished by cryptographic means, such as hash functions or message authentication codes (MACs). Computing such integrity-ensuring functions can be time-consuming if the amount of input data is large and/or the computing platform is weak. At the same time, in real-time or safety-critical settings, it is often impractical (or even undesirable) to guarantee atomicity of computing a lengthy integrity-ensuring function. Meanwhile, standard correctness and security definitions of such functions assume that input data (regardless of its size) remains consistent throughout computation. However, temporal consistency may be lost if another process interrupts execution of an integrity-ensuring function and modifies portions of input that either or both: (1) were already processed, or (2) were not processed yet. Lack of temporal consistency might yield an integrity result that is non-sensical or simply incorrect. Such subtleties and discrepancies between (implicit) assumptions in definitions and implementations can be a source of inconsistencies, which might lead to vulnerabilities. Motivated by this, we systematically explored the notion of temporal consistency of cryptographic integrity-ensuring functions. We showed that its lack in implementations of such functions can lead to inconsistent results and security violations in protocols and systems using them, e.g., remote attestation, remote updates, and secure resets. We considered several mechanisms that guarantee temporal consistency of implementations of integrity-ensuring functions in embedded systems with a focus on remote attestation. We also assessed performance of proposed mechanisms on two commodity hardware platforms: I.MX6-SabreLite and ODROID-XU4.

Remote Attestation of Dynamic Swarms

Most prior RA schemes focus on attesting a single device and do not scale. In recent years, schemes for collective (group or swarm) RA have been designed. However, none is applicable to autonomous and dynamic network settings. We therefore constructed US-AID – the first collective attestation scheme for large autonomous dynamic networks of embedded devices. US-AID verifies overall network integrity by combining continuous in-network attestation with a key exchange mechanism and Proofs-of-non-Absence. Using device absence detection US-AID defends against physical attacks that require disconnecting attacked devices from the network for a non-negligible time. We demonstrated feasibility of US-AID via proof-of-concept implementations on a state-of-the-art security architecture for low-end embedded devices and on an autonomous testbed with six drones. We also assessed its scalability and practicality via extensive simulations.

2019/2020

Formal Verification of Security Services for low-end IoT/CPS/Embedded Devices

Despite much prior work, state-of-the-art RA techniques unfortunately still lack any solid foundation and offer no ironclad security, safety, or robustness guarantees. We argue that computer-aided formal verification and synthesis of executables of RA protocols and hybrid(software-hardware) architectures is required and currently unaddressed. We believe that this is achievable with current (computer-aided) methods frameworks and tools, and that this can help advance and mature RA research if used to establish more rigorous and clear security arguments. To support our opinion, we highlight several examples where subtle issues were missed in the design and security analysis of RA techniques. Despite deceptive simplicity of such protocols, manual analyses and ad hoc implementations often lead to over-simplification of (and subsequent glossing over) important details in the underlying processor and system architectures. Computer-aided formal verification forces a more scrupulous and disciplined consideration of such details, since, otherwise, verification simply fails. The key objective of the research direction we propose is to increase confidence in correctness and security guarantees of current and future RA techniques and their implementations.

As the first concrete step towards formal verification of Remote Attestation (RA), we design and verify an architecture called VRASED: Verifiable Remote Attestation for Simple Embedded Devices. VRASED instantiates a hybrid (HW/SW) RA co-design aimed at low-end embedded systems, e.g., simple IoT devices. VRASED provides a level of security comparable to HW-based approaches, while relying on SW to minimize additional HW costs. Since security properties must be jointly guaranteed by HW and SW, verification is a challenging task, which has never been attempted before in the context of RA. VRASED is the first formally verified RA scheme. It is also the first formal verification of a HW/SW implementation of any security service. To demonstrate VRASED's practicality and low overhead, we instantiate and evaluate it on a commodity platform (TI MSP430). VRASED's publicly available implementation was deployed on the Basys3 FPGA.

As the next step, we show how a secure RA architecture can be extended to enable important and useful security services for low-end embedded devices. We extend the formally verified VRASED RA architecture to implement provably secure software update, erasure, and system-wide resets. When (serially) composed, these features guarantee to Vrf that a remote Prv has been updated to a functional and malware-free state and was properly initialized after such process. These services are provably secure against an adversary (represented by malware) that compromises Prv and exerts full control of its software state. Our results demonstrate that such services incur minimal additional overhead (0.4% extra hardware footprint, and 100-s milliseconds to generate combined proofs of update, erasure and reset), making them practical even for the lowest-end embedded devices, e.g., those based on MSP430 or AVR ATMega micro-controller units (MCUs). All changes introduced by our new services to VRASED trusted components are also formally verified.

Collective (Group/Swarm) Remote Attestation Methods

Networks of and embedded (IoT) devices are becoming increasingly popular, particularly, in

settings such as smart homes, factories and vehicles. They can include numerous (potentially diverse) devices that collectively perform certain tasks. To guarantee overall safety and privacy, especially in the face of remote exploits, software integrity of each device must be continuously assured, e.g., via Remote Attestation (RA). While RA of a single device is well understood, collective RA of large numbers of networked embedded devices poses new research challenges. Unlike single-device RA, collective RA has not benefited from any systematic treatment. Thus, unsurprisingly, prior collective RA schemes are designed in an ad hoc fashion. We initiate the approach to systematic design of collective RA, to help place collective RA onto a solid ground and serve as a set of design guidelines for both researchers and practitioners. We explore the design space for collective RA and show how the notions of security and effectiveness can be formally defined according to a given application domain. We then design and evaluate a concrete collective RA scheme systematically designed to satisfy these goals.

Collective RA is a very useful security service that allows to verify the integrity of devices' software state remotely and securely, thus allowing detection of potential malware. However, current collective RA schemes focus on detecting whether devices are infected by malware, but not on disinfecting and/or restoring them to a benign state. To this end, we develop HEALED – the first collective RA scheme that allows both detection of software compromise and disinfection of compromised devices. HEALED uses Merkle Hash Trees (MHTs) for measurement of software state, which allows restoring a device to a benign state in a secure and efficient manner.