

Security and Privacy of Current and Emerging IoT Devices and Systems

Bruno Crispo^{*1}, Alexandra Dmitrienko^{*2}, Gene Tsudik^{*3},
Wenyuan Xu^{*4}, and Christoph Sendner^{†5}

- 1 University of Trento, IT. bruno.crispo@unitn.it
- 2 Universität Würzburg, DE. alexandra.dmitrienko@uni-wuerzburg.de
- 3 University of California – Irvine, US. gts@ics.uci.edu
- 4 Zhejiang University – Hangzhou, CN. xuwenyuan@zju.edu.cn
- 5 Universität Würzburg, DE. christoph.sendner@uni-wuerzburg.de

Abstract

This report summarizes the program of Dagstuhl Seminar 24312 on “Security and Privacy of Current and Emerging IoT Devices and Systems” by providing short overviews over all talks and discussions as well as a list of open problems and a short outlook to the future.

Seminar July 28 – August 2, 2024 – <https://www.dagstuhl.de/24312>


2012 ACM Subject Classification Security and privacy → Embedded systems security; Security and privacy; Security and privacy → Security in hardware; Security and privacy → Systems security

Keywords and phrases IoT Security, Trust, Cryptography, Authentication

Digital Object Identifier 10.4230/DagRep.14.7.170

1 Executive Summary

Bruno Crispo (University of Trento, IT)
Alexandra Dmitrienko (Universität Würzburg, DE)
Christoph Sendner (Universität Würzburg, DE)
Gene Tsudik (University of California – Irvine, US)
Wenyuan Xu (Zhejiang University – Hangzhou, CN)

License  Creative Commons BY 4.0 International license
© Bruno Crispo, Alexandra Dmitrienko, Christoph Sendner, Gene Tsudik, and Wenyuan Xu

Over the past two decades, there has been a surge in the popularity of Internet-of-Things (IoT) devices and Cyber-Physical Systems (CPS). These devices are now commonplace in private settings, such as homes, offices, and factories, and public spaces like cultural, entertainment, and transportation facilities. They are also extensively used in farming, industrial, and vehicular automation. Furthermore, they are often interconnected and connected to the global Internet. These devices are typically built using low-end microcontroller units (MCUs), which have strict cost, size, and energy constraints and lack security features compared to their higher-end counterparts. As a result, these embedded devices, including sensors, actuators, and hybrids, have become attractive targets for various types of attacks. The focus of these attacks ranges from privacy concerns in the context of sensing, to safety and security issues in the context of actuation, and even zombification, as seen in the infamous Mirai botnet.

* Editor / Organizer

† Editorial Assistant / Collector



Except where otherwise noted, content of this report is licensed under a Creative Commons BY 4.0 International license

Security and Privacy of Current and Emerging IoT Devices and Systems, *Dagstuhl Reports*, Vol. 14, Issue 7, pp. 170–207

Editors: Bruno Crispo, Alexandra Dmitrienko, Gene Tsudik, and Wenyuan Xu



DAGSTUHL
REPORTS Dagstuhl Reports

Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The goal of the Dagstuhl Seminar was first to explore the landscape of attacks on current and emerging devices and then to identify and discuss promising research directions for effective countermeasures, both reactive and proactive. The relationship between academic research and industry was also of interest; specifically, to what extent is there a flow of ideas and innovation from the research community and device manufacturers, and what can be done to improve it.

The original proposal for this Dagstuhl Seminar included nine topics. However, once the seminar was approved and attendees were confirmed, it turned out that some of the topics simply did not have sufficient numbers of interested participants. In the end, five topics “survived” to the actual seminar and became – together with one new topic – individual sessions. (The session leader(s) are mentioned in parenthesis.):

1. **Security and Privacy Challenges in IoT-instrumented spaces** (Gene Tsudik) – originally named **Implications of increasing human immersion in instrumented spaces**. The increasing human immersion in instrumented spaces, such as smart homes, offices, and cities, brings new security and privacy challenges. The proliferation of interconnected devices that collect, store, and transmit personal data creates a larger attack surface for cybercriminals. Additionally, users may not be aware of the privacy implications of these devices and the data they generate. The seminar participants will focus on emerging privacy concerns and discuss the ways to protect users’ personal data while still enabling the functionality of these devices. Another challenge is the lack of standardization, which makes it difficult to create uniform security and privacy mechanisms and ensure the interoperability of different devices.
2. **Realizing Security/Privacy Services Across Hardware and Software Boundaries** (Alexandra Dmitrienko) – originally named **Scope of potential security/privacy services and how they should be realized across the SW/HW boundary**. Currently, microprocessors and many hardware platforms implement many security mechanisms, such as PAC, MTE, BTI, PUF, shadow stacks, and others, in hardware. However, more high-level trusted services (such as remote attestation, authentication, etc.) implemented in software on these platforms only partially, if at all, utilize these available mechanisms. To fully realize the potential of these security features implemented in hardware, a more systematic co-design of hardware and software is required. This approach can result in more efficient implementation of existing trusted services, as well as the design of new ones, thereby enhancing the overall security and privacy of IoT platforms.
3. **The Role of Secure Hardware (Trusted Computing) in IoT Security** (Bruno Crispo) – originally named **The Role of Trusted Computing in providing robust security services for IoT**. Trusted Execution Environments (TEEs) and Roots of Trust (RoTs) are common Trusted Computing tools in the academic literature related to IoT security. Specific instances have also been implemented in the industry (e.g., ARM TrustZone, Intel SGX, etc.). However, the first generation of TEEs has shown to be vulnerable to security issues. Therefore, major vendors and initiatives like RISC-V are revisiting trusted computing architectures to avoid past pitfalls. Hence, it is important to establish what types of Trusted Computing technologies are needed for different types of devices and under what types of attacks to ensure effective security measures.
4. **Balancing mission-criticality, safety, and security in system design** (Wenyuan Xu) – originally named **Mission-criticality/safety vs. security/privacy**. When it comes to mission-critical systems, striking a balance between safety and security can be challenging. Security measures often come with real-time overhead such as timing delays, interruptions, and increased bandwidth usage. In critical settings where safety

is the primary concern, these impacts can have significant consequences. Unfortunately, safety and security requirements are often treated in isolation during the design process, without considering their natural implications and the correlation between them. This separation is also reflected in the evaluation of these systems, with different and separate standards and regulations for assessing safety and security. To address this challenge, it is important to consider these two concerns jointly rather than in isolation. By doing so, unexpected interferences between the two subsystems can be avoided. A comprehensive approach to designing and evaluating mission-critical systems should take into account both safety and security requirements in an integrated manner. This will help ensure that these systems operate reliably and securely, without compromising on safety.

5. **Security Challenges in Unattended (IoT) Environments, e.g., Low-Orbit Satellites** (Wenyuan Xu and Bruno Crispo) – originally named **Space and other challenging (unattended) environments**. Low-orbit satellites are becoming increasingly popular. Deployed on a large scale, they are expected to provide ubiquitous Internet connectivity. However, these satellites operate in challenging, unattended environments that are physically inaccessible to humans. Despite the absence of attacks on low-orbit satellites thus far, it is only a matter of time before they become a target. The central challenge for designers of low-orbit satellite systems is to develop resilient and fault-tolerant security methods that can mitigate attacks from both far away and nearby sources. The remoteness of these satellites makes it difficult to detect and respond to attacks in real time, which increases the importance of designing security measures that can withstand attacks and continue operating even if a compromise occurs.
6. **Addressing the scalability challenge in securing large IoT deployments** (Alexandra Dmitrienko and Gene Tsudik).

2 Table of Contents

Executive Summary

<i>Bruno Crispo, Alexandra Dmitrienko, Christoph Sendner, Gene Tsudik, and Wenyuan Xu</i>	170
---	-----

Overview of Talks

Security and Privacy Challenges in IoT-instrumented spaces <i>Gene Tsudik</i>	176
Security Challenges in Internet of Autonomous Things (IoAT) <i>Alfred Chen</i>	176
Datasets for Security and Privacy Research in IoT <i>Murtuza Jadliwala</i>	176
Fingerprinting Encrypted Virtual Reality Traffic <i>Stefanie Roos</i>	177
Privacy Policy Enforcement for IoT Instrumented Spaces <i>Veelasha Moonsami</i>	177
Challenges in Compositional Secure Autonomy <i>Berkay Celik</i>	178
The Long Island Iced Tea Approach: Leveraging Different Techniques to Achieve Lightweight Privacy-Preserving Computation <i>Nader Sehatbakhsh</i>	178
DeeperAttest: End-to-end HW-Based Attestation of Embedded Deep Learning and LLM models <i>Farinaz Koushanfar</i>	179
Challenges of deploying PETs in practice <i>Jorge Guajardo-Mechan</i>	179
Discussion	180
Realizing Security/Privacy Services Across Hardware and Software Boundaries <i>Alexandra Dmitrienko</i>	181
Medical Device Cybersecurity <i>Kevin Fu</i>	181
Cyber-Physical Vulnerabilities: Definitions, Examples & Future Work <i>Yongdae Kim</i>	182
Symbolic Analysis for IoT Software: Challenges and Benefits <i>Xuhua Ding</i>	182
Security Challenges in IoT Firmware <i>Surya Nepal</i>	183
Complex Threats and Integration Problems in Large Deployments <i>Kasper Rasmussen</i>	183
Privacy by Birth: Protecting Data with in-Sensor Strategies for IoT Device <i>Wenyuan Xu</i>	184
Discussion	184


The Role of Secure Hardware (Trusted Computing) in IoT Security <i>Bruno Crispo</i>	186
TEEs for IoT Controllers 2016-2024: What, and What For <i>Jan Erik Ekberg</i>	187
Why and How to Verify RoT-Device Binding <i>Xuhua Ding</i>	187
Trusted Computing for the Internet of Collaborative Things <i>Nader Sehatbakhsh</i>	188
Conflicts Between Availability, Isolation, and Integrity in Real-time Operating Systems for MCUs <i>Ivan de Oliveira Nunes</i>	188
Open Issues with Existing TEE Implementations <i>Bruno Crispo</i>	189
Arguments for Active RoTs for IoT Devices <i>Gene Tsudik</i>	189
Balancing mission-criticality, safety, and security in system design <i>Wenyuan Xu</i>	191
Security of Private 5G for Safety-Critical Applications <i>Yongdae Kim</i>	191
Signal Injection Detected: What Do We Do Now? <i>Kasper Rasmussen</i>	192
Security for Embodied AI <i>Wenyuan Xu</i>	192
Analog Security <i>Kevin Fu</i>	193
Trustworthy Position & Time <i>Panagiotis Papadimitratos</i>	193
Discussion	193
Security Challenges in Unattended Environments, e.g., Low-Orbit Satellites <i>Bruno Crispo and Wenyuan Xu</i>	195
The Curse of Autonomy in IoAT Security <i>Alfred Chen</i>	195
Emerging Threats in Underwater Cyber-physical Systems <i>Sara Rampazzi</i>	196
Securing the Internet of Energy <i>Surya Nepal</i>	196
Orbiting Threats: Security & Privacy in Space <i>Ahmad-Reza Sadeghi</i>	197
Space Networks meet 5G Terrestrial Networks – Thoughts on Threats and Defenses in Large-scale Networks <i>Christina Pöpper</i>	197
Discussion	198

Addressing the scalability challenge in securing large IoT deployments <i>Alexandra Dmitrienko and Gene Tsudik</i>	199
You can have your cake and eat it too: Ensuring practical robustness and privacy in IoT Federated Learning <i>Farinaz Koushanfar</i>	199
IoT Devices During Internet Shutdowns <i>Stefanie Roos</i>	200
Rethinking the Role of the Cloud in IoT Systems <i>Earlence Fernandes</i>	200
Thoughts about Network Management in Secure IoT Environments <i>David Hock</i>	201
Just “Build, provision, deploy”? Obstacles Faced by SMBs when Building Secure IoT Devices <i>Markus Wamser</i>	201
Challenges of Scaling Security Services in IoT Networks <i>Alexandra Dmitrienko</i>	202
Scaling credential management in IoT <i>Panagiotis Papadimitratos</i>	202
Discussion	203
Open problems	
Open Issues <i>Bruno Crispo, Alexandra Dmitrienko, Christoph Sendner, Gene Tsudik, and Wenyan Xu</i>	204
Key Outcomes	204
Future Outlook	206
Participants	207

3 Overview of Talks

3.1 Security and Privacy Challenges in IoT-instrumented spaces

Gene Tsudik (University of California – Irvine, US)


License  Creative Commons BY 4.0 International license
© Gene Tsudik

The increasing human immersion in instrumented spaces, such as vehicles, homes, offices, and cities, prompts some new security and privacy challenges. Also, the proliferation of interconnected devices that collect, store, and transmit personal data creates a larger attack surface for and attacks. Furthermore, users may not be aware of the privacy implications of these devices and the data they generate. These issues are exacerbated by the current lack of standardization, which makes it difficult to create uniform security and privacy mechanisms and ensure the interoperability of various devices.

Consequently, this initial session focused on emerging privacy concerns and discussed ways to protect users' personal data while still enabling the functionality of IoT devices.

3.2 Security Challenges in Internet of Autonomous Things (IoAT)

Alfred Chen (University of California, Irvine, US)

License  Creative Commons BY 4.0 International license
© Alfred Chen

The speaker started with some background on autonomous systems and their future, particularly the Internet of Autonomous Things (IoAT). The talk traced the evolution of IoT from the 1980s to the present, highlighting the transition from basic sensing technologies to advanced networked and controlled systems. The talk included a range of examples of autonomous technologies, such as Waymo self-driving cars, dog-bots, food delivery robots, and drones, emphasizing their growing presence in everyday life.

The second part of the talk focused on critical security challenges faced by autonomous systems. The speaker stresses the high stakes involved, citing incidents, such as crashes of Uber and Tesla autonomous vehicles and recent malicious activities, such as protesters disabling driverless cars with traffic cones. The discussion extended to system vulnerabilities, including failures in LIDAR and camera detection and sophisticated attacks, e.g., LIDAR spoofing and IRL speed sign alterations. Despite exploring potential solutions, such as cryptographic measures and cross-domain validation, the speaker concluded that no definitive, provable solutions have been established to address these complex cyber-physical security challenges.

3.3 Datasets for Security and Privacy Research in IoT

Murtuza Jadliwala (University of Texas - San Antonio, US)

License  Creative Commons BY 4.0 International license
© Murtuza Jadliwala


The speaker highlighted critical challenges researchers face in accessing robust datasets, emphasizing their importance for advancing IoT research in areas, such as home automation,

healthcare, smart cities, and wearables. While there are numerous public datasets for diverse purposes (such as intrusion detection and activity recognition), they often have limitations, including data collection bias, static nature, as low as low variability, volume, and quality.

To address these issues, the speaker proposed the development of domain- and application-specific community IoT research infrastructures. These infrastructures, hosted by a few (trusted?) entities, would provide flexibility for researchers to conduct experiments and facilitate collaborative data collection across multiple nodes or locales. Current examples include Mcity test facility and FIT IoT testbed that offer controlled environments for testing and data collection. Whereas, initiatives (e.g., IoT Inspector and Scooterlab) demonstrate innovative approaches to user-owned device data collection. However, sustaining these infrastructures presents challenges, such as funding, regulatory compliance, and resource maintenance. Looking forward, there is a strong advocacy for expanding community IoT infrastructures, supporting advanced data analysis techniques, and fostering public-private partnerships to enhance resource pooling and research collaboration.

3.4 Fingerprinting Encrypted Virtual Reality Traffic

Stefanie Roos (RPTU Kaiserslautern-Landau, DE)


License  Creative Commons BY 4.0 International license
© Stefanie Roos

The talk presented fingerprinting of encrypted traffic, focusing on privacy issues in AR/VR/XR environments. These technologies, utilized in education, gaming, medical therapy, and sports, can inadvertently reveal sensitive information, such as user interests, reaction times, and physical attributes (e.g., height), depending on whether headsets or other sensors are used. Despite encryption, traffic patterns remain discernible, posing privacy risks. Potential adversaries include communication partners, ISPs, and anyone monitoring the traffic.

In experiments involving PhD students playing VR games, traffic was sniffed at WiFi routers to analyze patterns. The testbed consisted of two players, WiFi routers, and a game server. Using SVM, researchers could detect the type of hardware used, the game played, and the winner, although DNN was ineffective due to limited data. The study demonstrated that activities within VR environments could be inferred from traffic analysis, highlighting the need for more diverse participant samples and advanced analytical techniques. A comparison between WiFi and Ethernet showed negligible differences in traffic patterns.

3.5 Privacy Policy Enforcement for IoT Instrumented Spaces

Veelasha Moonsamy (Ruhr-Universität Bochum, DE)

License  Creative Commons BY 4.0 International license
© Veelasha Moonsami


The talk started with an overview of the importance of GDPR and its challenges. GDPR, enforced since May 2018, has garnered significant interest from companies aiming to avoid fines and ensure compliance. The implementation is complex, especially without a legal background, and involves working with lawyers to interpret and implement GDPR. The primary focus has been on web-based applications, addressing data subject rights, but the growing use of AI in IoT systems adds another layer of complexity. The talk highlights the

difficulty in transitioning legacy systems and emphasizes the need for robust solutions to manage data subject rights effectively.

Current approaches, e.g., RuleKeeper, Fontus, and WebTTC, each offer different technical means of GDPR compliance, though with limitations. RuleKeeper uses static manifest files for rule enforcement, Fontus from SAP employs classical security methods with data-flow tracking, and WebTTC combines formal verification with tainting and logic-based approaches. However, none fully meet all GDPR requirements, with WebTTC being the only one to cover user rights comprehensively. The challenges include determining the appropriate level for privacy enforcement, ensuring data provenance, and achieving interoperability in IoT spaces where devices and software from different vendors often do not work seamlessly together. The talk concluded by emphasizing the need for more integrated and adaptable privacy enforcement solutions.

3.6 Challenges in Compositional Secure Autonomy

Z. Berkay Celik (Purdue University - West Lafayette, US)

License  Creative Commons BY 4.0 International license
© Berkay Celik

The talk started with the overview of the evolution of computing, emphasizing the commoditization of sensing, computation, and actuation programming. The discussion then delved into the complexity of autonomous systems, which integrate multiple interacting components equipped with diverse sensors and actuators, often relying on large deep-learning models. These systems, such as robotic vehicles and drones, process various deterministic and non-deterministic inputs to make command decisions, highlighting the intricate integration of physical processes with digital connectivity.

The talk also examined specific examples, such as object tracking and sensor spoofing attacks on drones, underscoring the challenges of modeling adversaries and the complexity of these systems. The discussion extended to hybrid modeling approaches that combine formal methods and program analysis to ensure the correctness and unified behavior of autonomous systems. As autonomous systems become more connected and cooperative, their complexity and the challenges in securing them will increase. The future will see advancements in cognitive architectures and human-like perception. Still, significant challenges remain, such as dealing with uncertainty, adaptive attacks, and the need for expertise across various domains. Collaboration and establishing benchmarks will be crucial for addressing these challenges in secure autonomy.

3.7 The Long Island Iced Tea Approach: Leveraging Different Techniques to Achieve Lightweight Privacy-Preserving Computation

Nader Sehatbakhsh (University of California at Los Angeles, US)

License  Creative Commons BY 4.0 International license
© Nader Sehatbakhsh

The talk delved into privacy-preserving computation, particularly in the context of machine learning inference at the edge of IoT devices. The problem involves computing data locally

on these constrained devices while balancing privacy, security, latency, and accuracy. The talk evaluated the pros and cons of various methods, noting that no single approach is a clear winner and suggesting a combined strategy.

Three primary methods were explored: homomorphic encryption and multi-party computation (FHE/MPC), TEE, and obfuscation/information removal techniques. FHE/MPC offers strong privacy and security but suffers from poor latency, though hardware accelerators show promise. TEEs provide secure computation with better latency but have system-level vulnerabilities and hardware limitations. Obfuscation, while providing weaker privacy guarantees, ensures low latency and fewer system-level concerns. The talk compares these methods across privacy/security, accuracy, and latency, suggesting improvements such as better latency for FHE/MPC and TEE, as well as stronger privacy for obfuscation. The conclusion emphasizes a “cocktail” approach, combining these techniques to optimize privacy-preserving computation while addressing hidden problems like data guarantees on devices and unintentional data leaks.

3.8 DeeperAttest: End-to-end HW-Based Attestation of Embedded Deep Learning and LLM models

Farinaz Koushanfar (University of California at San Diego, US)

License  Creative Commons BY 4.0 International license
© Farinaz Koushanfar

This talk explored the concept of tracing and attestation extended to LLMs. It began by contrasting traditional data/algorithm cycles with a new end-to-end design that links automation, emphasizing the need for components to work together seamlessly. The focus is on deep learning and LLMs due to their output-driven nature, and the talk highlights significant resources required to train these models, underscoring the importance of safeguarding the investments in knowledge and money.

The discussion covered the AI landscape at the edge, with devices like Nvidia Jetson and products from Qualcomm, Apple, and Huawei. It outlined the challenges in the ML market related to hardware, software, and services. Key issues include proving ownership, usage control, IP tracing, and ensuring the safety and integrity of models for end users. The talk then covered various methods for attestation and watermarking, including hardware and DL fingerprints, LLM output and model watermarks, and proof of provenance using zero-knowledge proofs. The overarching idea is to robustly and unobtrusively embed information in the distribution, which is challenging for large models. There is a need for research to adapt these techniques to the evolving landscape of AI, particularly as synthetic data becomes more prevalent than real data on the internet.

3.9 Challenges of deploying PETs in practice

Jorge Guajardo Merchan (Robert Bosch LLC - Pittsburgh, US)

License  Creative Commons BY 4.0 International license
© Jorge Guajardo-Merchan

The talk addressed the challenges of deploying PETs in practice, focusing more on security than privacy. It began by underscoring the complexity of security when collaborating

with many stakeholders. The speaker discussed various domains at Bosch, including mobility solutions, industrial technologies, consumer goods, and energy and building technology. These domains share characteristics, such as connectivity, performance, intelligence, personalization, and convenience, which introduce system-level complexities, vulnerabilities, and the handling of big (and personal) data. The focus was particularly on automotive security, covering individual ECUs, in-vehicle networks, connected vehicles, and cloud services. The discussion emphasized the importance of intrusion detection and prevention systems, mandated by government regulations, which operate at multiple levels to detect, analyze, and respond to security events.

The talk elaborated on developing host-based IDS for detecting compromised ECUs using low-cost solutions (e.g., power-trace analysis) despite the inherent constraints of microcontrollers compared to PCs. The talk also covered the challenges in designing detection algorithms with low sampling rates and discussed anomaly detection within vehicles, focusing on low false positive rates, distributed deployment, and real-world performance. The talk also addressed the scaling of data collection for IDS purposes, proposing a configurable and customizable testbed to collect semi-synthetic data. Collaboration with different OEMs was highlighted to build a comprehensive platform for data collection, network simulation, and environment simulation involving engineers, pen-testers, and researchers. The talk concluded by acknowledging challenges such as distribution fidelity, reverse engineering of DBC dictionaries, and the privacy effects on trace correctness.

3.10 Discussion

The last segment of this session was a lively discussion. Topics included the following:

- There is no optimal algorithm for determining who should act first or who is the fastest in certain (IoT/CPS) domains.
- Autonomous vehicles are challenging for research due to the difficulty of reverse engineering and parameterization. When an intrusion is detected, it is unclear what actions should be taken in real-time situations.
- Research should include attacks that assume limited access to vehicle software stacks, e.g., fuzzing UDS protocols, and responses often involve degrading car functions, such as slowing down and stopping safely.
- Balancing safety and security in autonomous driving systems is a complex issue, with safety often (rightfully) taking precedence over security in critical situations.
- In human-driven systems, security is intertwined with safety concerns, such as slowing down a car while overtaking, leading to potential accidents.
- False positives in real-time detection systems can misinform users – this needs to be addressed in system designs.
- Adversary models vary by system, focusing on tamper detection in vehicle software as a key step in preventing attacks.
- Remote access to cars through cloud services or wireless connections is a significant security risk, as is re-flashing ECUs without attestation.
- Testing object recognition systems in vehicles is complex due to proprietary black-box models used by manufacturers, and extensive testing environments are required to gather sufficient data.
- Current research in automotive security includes attacks that manipulate vehicle systems through remote access, infotainment systems, or OBD connections, while minimizing

hardware assumptions.

- Discussions on solutions to security issues in autonomous driving include real-time updates and detection systems that ensure changes in ECU software are detected promptly.
- Questions about broader attacks on vehicles, as opposed to isolated incidents, highlight concerns about large-scale vulnerabilities.
- Other topics include the role of cloud services in vehicle security, the necessity of remote operators for autonomous cars, and privacy concerns surrounding IoT devices and vehicle cameras capturing individuals.
- GDPR and other privacy regulations were discussed, particularly regarding their applicability to IoT systems, where users are often unaware of being sensed or recorded by devices.
- The challenge of handling sensitive data (e.g., in facial recognition) in public spaces was highlighted, with potential technical solutions like automated obfuscation being suggested but questioned for practical and scalable implementation.
- Solutions to privacy concerns in IoT involve balancing the need for safety and security in public systems with the rights of individuals to privacy.

3.11 Realizing Security/Privacy Services Across Hardware and Software Boundaries

Alexandra Dmitrienko (Universität Würzburg, DE)

License  Creative Commons BY 4.0 International license
© Alexandra Dmitrienko

In an increasingly interconnected digital landscape, the boundaries between hardware and software are becoming more porous, giving rise to both innovative opportunities and complex security challenges. This session aims to explore the multifaceted nature of security and privacy in modern computing environments.

As devices evolve and systems integrate, ensuring robust security and privacy measures becomes paramount. This session aims to address the unique challenges posed by heterogeneous environments, including IoT ecosystems, cloud computing, and edge devices. It delves into emerging methodologies and frameworks that facilitate the seamless implementation of security and privacy services across these boundaries, as well as the potential implications for users, organizations and researchers.

3.12 Medical Device Cybersecurity

Kevin Fu (Northeastern University - Boston, US)

License  Creative Commons BY 4.0 International license
© Kevin Fu


The talk begins with an overview of the speaker's background and an introduction to the topic of medical device cybersecurity. It delves into the history of medical devices, highlighting early findings such as the absence of cryptography in wireless medical devices and the potential for inducing fatal heart rhythms via RF replay or induction. The discussion evolves to address the rise of malware and ransomware, mainly targeting hospitals and the power grid, leading to significant disruptions, including the shutdown of hospitals during

ransomware attacks. Real-world examples from the Ukraine-Russia conflict illustrate the severe impact of cyberattacks on healthcare, revealing plans to target over 400 hospitals and causing disruptions in critical treatments like cancer care.

The speaker also explores the regulatory landscape, detailing the pathways for medical device approvals and the responsibilities of manufacturers to submit risk audits to the FDA, provide software, and handle vulnerabilities. Challenges include the distribution of malware through firmware updates, with examples of ventilators being recalled due to infected firmware. The scope of FDA regulation is discussed, noting that therapeutic and diagnostic devices are regulated, but not personal devices like step trackers. The talk concludes with a discussion on threat modeling, the difficulties in addressing legacy devices, and the point at which liability shifts from manufacturers to hospitals for end-of-life devices.

3.13 Cyber-Physical Vulnerabilities: Definitions, Examples & Future Work

Yongdae Kim (KAIST - Daejeon, KR)

License  Creative Commons BY 4.0 International license
© Yongdae Kim

The presentation defines cyber-physical vulnerabilities and provides examples to illustrate their complexity. A detailed explanation of how drone control works is given, including the role of the IMU and the control unit. The speaker presents a case study from a 2015 paper on “rocking drones,” demonstrating how resonating the IMU with sound can disrupt the drone’s control, causing it to fall. Videos and formulas illustrate the effects of sound-induced resonance on drones, although commercial applications are limited by the short travel distance of sound.

Further discussion covers the use of sound pressure and explosives to disrupt sensors, with insights from military research. The concept of electromagnetic injection is introduced, showing how random sensor data can paralyze drones. The range of this attack is discussed, highlighting the dependency on power and the mainboard of the drone. The talk concludes with open problems and a video example involving a Tesla, showing how laser pointers can interfere with control systems, raising questions about future research directions in cyber-physical security.

3.14 Symbolic Analysis for IoT Software: Challenges and Benefits

Xuhua Ding (SMU - Singapore, SG)

License  Creative Commons BY 4.0 International license
© Xuhua Ding

This talk focuses on symbolic execution as a method for analyzing IoT software, emphasizing its ability to generate mathematical descriptions of control and data flow for more rigorous program analysis. The workflow of dynamic symbolic execution (DSE) is explained, from translating binary/source code into intermediate representation to managing states with and without symbols. The potential of combining DSE with IoT is explored, highlighting benefits like bug hunting and exploit generation in controlled lab settings but noting challenges in modeling interactions with hardware and running DSE on real IoT devices.

The speaker outlines potential directions for real-time DSE on IoT devices and symbolic hardware emulation, discussing benefits like runtime anomaly detection and better understanding of hardware behavior. However, challenges remain, such as the lack of DSE engines for ARM architecture, high-speed execution requirements, and difficulties in capturing hardware interactions. The talk concludes with a call for novel symbolic execution methods tailored to IoT's unique needs, stressing the importance of continued research in this area to improve IoT security.

3.15 Security Challenges in IoT Firmware

Surya Nepal (CSIRO - Eveleigh, AU)

License  Creative Commons BY 4.0 International license
© Surya Nepal

The talk introduces the concept of data-driven security and its application in IoT firmware, starting with the transition from Robot Operating Systems (ROS) to ROS-Military and the use of large language models to detect vulnerabilities. The discussion covers threat modeling for large-scale IoT deployments, emphasizing the need for frameworks to simulate large-scale environments using technologies like Docker. The challenges and solutions of embedded firmware fuzzing are highlighted, particularly the use of multi-stream fuzzers like MultiFuzz to test monolithic firmware across different hardware platforms.

The speaker addresses the critical role of firmware in interfacing hardware and applications, detailing the potential issues with firmware updates, such as those seen in the CrowdStrike case. Dynamic patching is proposed as a solution to maintain device operation during updates, emphasizing the need for resilience in remote, contested, and safety-critical environments. The talk also touches on the contributions of governments, industry, and academia to solving these challenges, as well as the concept of Digital Twins for threat modeling and fuzzing in IoT environments.

3.16 Complex Threats and Integration Problems in Large Deployments

Kasper Rasmussen (University of Oxford, GB)

License  Creative Commons BY 4.0 International license
© Kasper Rasmussen



The speaker discusses the complexity of integrating security measures in large-scale IoT deployments, arguing that the scope of security problems often lies more in system and threat models than in errors in security analysis. Examples from recent IoT research, such as the Bluetooth vulnerability, illustrate how usability features can introduce security risks when threat models expand beyond their initial context. The talk emphasizes the need for realistic threat models that balance comprehensiveness with practicality and the challenges of agreeing on common threat models and experimental standards.

The talk also explores the expectations of reviewers for broader testing across more devices and environments, as well as the difficulty of defining adequate testing scopes. The speaker calls for a streamlined approach to adversary models, similar to those in cryptography and network security, to establish common standards for evaluating IoT security.

This standardization could facilitate more effective and scalable security solutions across diverse IoT ecosystems.

3.17 Privacy by Birth: Protecting Data with in-Sensor Strategies for IoT Device

Wenyuan Xu (Zhejiang University - Hangzhou, CN)

License  Creative Commons BY 4.0 International license
 Wenyuan Xu

The talk introduces the concept of “privacy by birth,” focusing on strategies to protect data at the sensor level in IoT devices. It highlights the vast amount of data generated by sensors such as biosensors, microphones, and cameras, as well as the regulatory challenges associated with sensitive data. The lifecycle of data from generation to destruction is discussed, with a focus on ensuring privacy from the moment data is created. The limitations of privacy measures applied after data is generated are noted, emphasizing the need for sensors to perform their tasks without compromising privacy.

The speaker proposes redesigning hardware to create “smart sensors” capable of ensuring privacy by birth while addressing the compatibility and usability challenges posed by legacy sensors. Examples like CAMPro and MicroPro sensors are provided, demonstrating how human activity recognition can be achieved without leaking sensitive information such as facial data. The talk concludes with a demonstration of techniques to anonymize voice data, ensuring that humans can understand speech while preventing machines from identifying voiceprints, and a video highlighting the potential for backdoors in sensors.

3.18 Discussion

The post-session discussion centered on key topics relating to privacy and the challenges of balancing functionality with user control in sensor technology. It highlighted a common theme: while privacy is a key concern in academic and regulatory debates, both consumers and vendors often deprioritize it in favor of cost, convenience, and economic interests. It also expands on several critical issues related to device security, threat models, and the challenges within the research community, especially regarding the peer review process and paper rejections.

3.18.1 Privacy by Design vs. Current Models

A question was raised about the contrasting ideas of privacy by design and current data collection models. It was noted that including privacy controls in sensors can limit their functionality, effectively taking control away from users. In contrast, existing models allow for extensive data collection but place the responsibility on users. It was questioned whether a middle ground could be found, as changing numerous sensors across a city would be impractical. The concept of a “software-defined sensor” was suggested, which could operate in different modes – one unrestricted and the other limiting sensitive information.

3.18.2 Government and Vendor Reluctance

Another viewpoint supported the idea of changing legacy sensors by altering parameters without needing a complete overhaul. Challenges faced by vendors in implementing these changes were discussed, particularly due to varying regulations across countries. It was also pointed out that governments, especially in democratic countries, are not always willing to regulate privacy features for devices like CCTV cameras. Complexities in convincing vendors to adopt privacy-enhancing configurations were acknowledged. An experience with a specific camera system was shared, highlighting the tension between user control and vendor interests and reinforcing the difficulty of implementing user-driven privacy protections.

3.18.3 Consumer and Vendor Behavior

It was discussed how most consumers are not genuinely interested in privacy unless it involves personal, sensitive information (e.g., intimate photos). Vendors, on the other hand, are hesitant to offer privacy features unless they can monetize them, but consumers are unlikely to pay extra for privacy. Suggestion was made for a possible middle ground by using IoT devices to transform legacy sensors into smarter, privacy-conscious ones. It was further questioned whether advanced privacy sensors would ever be adopted by the market.

3.18.4 Challenges in Market Adoption

It was noted that while academic discussions on privacy are valuable, they often don't translate to real-world applications, where many users prioritize cost over privacy. The conversation proceeded to discuss the motivations behind privacy concerns, suggesting that these issues often become relevant only when individuals experience loss or violation firsthand. Also, it was emphasized that most companies are more interested in collecting data for business purposes, and privacy-enhancing technologies often face pushback because they limit this data collection.

3.18.5 Regulatory and Economic Influences

It was pointed out that regulations like the Cyber Resilience Act in Europe are forcing vendors to comply with stricter privacy rules, but the driving force behind these laws is often economic, such as protecting European industries from cheaper, foreign competitors. Another observation highlighted that even if privacy-preserving solutions exist, their market viability depends on consumer interest and willingness to pay.

3.18.6 Proposal for Large-Scale Facilities

It was also suggested that experimental cybersecurity research might need to be approached similarly to other scientific fields, like astrophysics, where large-scale government-funded facilities enable research that no single university can support. To facilitate larger experiments, community investment in shared resources would be necessary.

3.18.7 Device Security & Threat Modeling

The discussion delved into the complexities of threat modeling in cybersecurity and system security, addressing challenges in accurately modeling real-world systems and the disconnect

between academia and practical applications. Participants explored cyber-physical vulnerabilities, such as drones, and discussed attacker models, emphasizing the need for realistic approaches that consider how complex systems behave.

The need for standardized threat models across industries, particularly for IoT, was highlighted, along with the importance of cost in threat modeling and its impact on security measures. Understanding the economic implications of attacks and distinguishing between attacker capabilities and attack scalability were identified as crucial for effective threat categorization.

Moreover, participants emphasized the necessity for evolving frameworks to address new attack vectors and technologies, including often-overlooked analog attacks. Overall, the conversation acknowledged the challenges in threat modeling and the need for collaboration among researchers to develop models that balance academic rigor with real-world applicability.

3.18.8 Concerns Related to the Peer Review Process

Concerns were raised about a prevailing mindset in the research community, where reviewers often reject papers based on arbitrary checklist criteria that do not accurately reflect research validity. This practice is perpetuated by advisors passing down these practices to students. Criticism focused on the incompetence of some reviews, which often set unrealistic expectations, such as excessive evaluations and extended threat models, highlighting the need for a rethinking of the review process. Participants also noted that experimental work frequently encounters impractical reviewer demands. They proposed developing standardized threat models and disseminating common principles for consistent evaluation of experimental research. Some suggested that refreshing the leadership of steering committees with younger researchers could bring new perspectives and reduce the tendency to reject papers based on outdated ambitions.

3.19 The Role of Secure Hardware (Trusted Computing) in IoT Security

Bruno Crispo (University of Trento, IT)

License  Creative Commons BY 4.0 International license
© Bruno Crispo

A secure and correct Root of Trust (RoT) is essential to anchor the security of all system components. IoT devices typically achieve this through Trusted Execution Environments (TEEs). Over the years, various TEE technologies have been developed and implemented. However, existing designs often reveal significant limitations and vulnerabilities.

This session examines the challenges that complicate RoT design within the IoT landscape. Some of these obstacles – such as restricted resources, limited energy availability, and connectivity constraints – stem from the inherent nature of IoT devices. Additionally, new threats have emerged, including micro-architectural level attacks. Finally, the session will explore novel design opportunities and areas that current approaches have yet to consider.

3.20 TEEs for IoT Controllers 2016-2024: What, and What For

Jan-Erik Ekberg (Huawei Technologies - Helsinki, FI)

License © Creative Commons BY 4.0 International license
© Jan Erik Ekberg

The talk discussed the evolution and application of TEEs in IoT controllers from 2016 to 2024, with a focus on extending these environments into various sensors. It highlighted the diverse IoT categories and use cases, such as smart cities, vehicular, military, home, and industrial IoT, noting that the volume of home IoT devices is expected to surpass that of mobile phones. The presentation emphasized the future of small, ubiquitous computing devices, often costing less than one Euro, with features like isolated key material, immutable trust roots, secure firmware upgrades, and self-assessment capabilities.

Different approaches to implementing TEEs were examined, such as ARM TrustZone and software-based solutions, detailing specific use cases like Apple's MFI and Xiaomi MiJia. The speaker also covered the deployment challenges of TEEs in mobile phones and various attempts to implement trusted environments, including ARMv8-M and ESP32-S3, highlighting their challenges in real-world applications. The final part addressed the need for secure home IoT despite the slow momentum and potential missing killer use cases, similar to how regulatory compliance, DRM, and financial services boosted mobile phone security.

3.21 Why and How to Verify RoT-Device Binding

Xuhua Ding (SMU - Singapore, SG)

License © Creative Commons BY 4.0 International license
© Xuhua Ding

This talk focused on the importance of verifying RoT for device binding, which is crucial for secure remote attestation. It discussed the issue of adversaries in the device under checking colluding with other devices to evade verification and the gap between cyberspace identities (IP, MAC, host) and physical identities (TV, WiFi access points, camera), exacerbated by compromised software such as kernels. The speaker emphasized the need for securely measured unique physical properties, like geolocation and fingerprints, that can be verified by a trusted verifier.

Potential solutions were explored, including human-assisted methods using devices as verifiers and the challenges of establishing a universal physical property for RoT binding. The talk highlighted the complexities of trustworthy device pairing and the need for scalable authentication solutions, concluding that while RoT binding is fundamental to trusted computing, it remains a challenging issue to resolve.

3.22 Trusted Computing for the Internet of Collaborative Things

Nader Sehatbakhsh (University of California at Los Angeles, US)


License  Creative Commons BY 4.0 International license
© Nader Sehatbakhsh

This talk introduced the concept of the Internet of Collaborative Things (IoCT), focusing on the idea of devices collaborating in terms of computing, sensing, perception, and networking. The speaker discussed the benefits of sharing resources among devices, such as efficiency in power usage, cost reduction, and enabling new applications like cooperative sensing, perception, and crowdsourcing. However, the focus was on the challenges rather than solutions, with a motivating example of a visiting robot needing to navigate a building and perform tasks based on received instructions.

The challenges identified included issues with the computation stack, security and privacy on devices, and ensuring confidentiality and integrity in device interactions. The speaker emphasized the need for systematic approaches to address these challenges, utilizing existing solutions, open-source infrastructure, and academic contributions. The discussion revolved around how to extend trust to other entities in the IoCT ecosystem, addressing availability, real-time constraints, and the integration of various trust mechanisms.

3.23 Conflicts Between Availability, Isolation, and Integrity in Real-time Operating Systems for MCUs

Ivan De Oliveira Nunes (Rochester Institute of Technology, US)

License  Creative Commons BY 4.0 International license
© Ivan de Oliveira Nunes

This talk provided a critical analysis of the integration of RTOS with trusted computing in MCUs. It focused on the Cortex-M series, which typically lacks memory management units and virtual memory, and the difficulties of combining real-time availability with integrity and isolation. The speaker highlighted the problems with current MCU RTOS implementations, such as FreeRTOS and Zephyr, and the conflicts between RTOS requirements and TEE requirements.

Examples of conflicts included time interference, where atomic execution of security services can disrupt real-time operations, and resource sharing, where spatial isolation can break real-time guarantees. The talk also discussed the lack of meaningful isolation in most current RTOS implementations, the low usage of memory protection units, and the absence of clear specifications for RTOS guarantees. The speaker concluded that while there are proposed run-time trusted computing services, significant challenges remain in integrating them with real-time operating systems.

3.24 Open Issues with Existing TEE Implementations

Bruno Crispo (University of Trento, IT)

License © Creative Commons BY 4.0 International license
© Bruno Crispo

This talk addressed the open issues with existing TEE implementations, starting with the global platform definition of TEE and summarizing the most popular implementations. The speaker pointed out that while there is a common API, differences in underlying implementations can create interoperability issues, making it difficult to write secure applications. Portability issues were also discussed, particularly the lack of support for bare-metal devices, GPUs, NPUs, TPUs, and ASICs, as well as the emerging requirements from new hardware platforms.

The talk highlighted the limitations of vendor-specific TEEs, the challenges of ensuring security and assurance, and the large TCBs that are becoming even larger with new architectures like ARMv9. Issues such as the lack of protection for cache evictions and interrupt latency, the need for extensibility, and the potential benefits of RISC-V for customizable TEEs were discussed. The speaker concluded that while TEEs offer significant security benefits, there are numerous unresolved issues that need to be addressed to improve their effectiveness and interoperability.

3.25 Arguments for Active RoTs for IoT Devices

Gene Tsudik (University of California - Irvine, US)

License © Creative Commons BY 4.0 International license
© Gene Tsudik

This talk argued for the need for active RoTs for IoT devices, highlighting that IoT device manufacturers often do not prioritize security or privacy due to budget constraints, rush-to-market pressures, and other factors. The speaker warned of an impending “IoT armageddon,” citing incidents like the Mirai DDoS attack as previews of potential widespread IoT vulnerabilities. The talk emphasized the ubiquity of IoT devices in various settings and the impact on users who are not device owners, raising the question of whether these users should be informed about nearby devices.

The proposed solution, PAISA (Privacy-Agile IoT Sensing and Actuation), involves IoT devices announcing themselves and utilizing active RoTs to control timers and network peripherals. This approach aims to inform all potentially impacted users about nearby devices, their capabilities, and their current software state without requiring hardware modifications. The talk also discussed the limitations of PAISA, such as compatibility issues with other platforms and the inability to apply to TEE-less devices, concluding that while active RoTs offer a proactive approach to IoT security, there are still significant challenges to be addressed.

3.25.1 Discussion

The post-session discussion focused on the challenges of achieving interoperability among various TEE technologies and attestation protocols. Participants also emphasized the growing trend among chip manufacturers to expand the size of the trusted software running

within TEEs, significantly increasing the attack surface as a result. The conversation concluded with an exploration of a novel concept: designing a mechanism that would allow device owners to deactivate advanced features, such as AI functionalities, to regain full control over a simplified, bare device. This approach would require transforming the TEE from a passive to an active component, capable of responding dynamically to specific events.

3.25.2 Management and Interoperability Challenges

Managing multiple vendors and technologies presents difficulties, particularly in the areas of automation and device interoperability. Challenges arise from diverse attestation protocols and trust issues between different entities, each with its own Root of Trust and protocols. Projects like Veraison and Matter IoT standard are attempting to standardize attestation methods to address these issues.

3.25.3 Trust and Verification Mechanisms

there are ongoing debates regarding the reliance on cloud-based verification for small devices that lack the capability to perform self-verification. Concepts such as authenticated watchdog timers and kill switches are proposed to defend against malware attacks, like Mirai. There is also discussion on whether simplifying the functionality within Trusted Execution Environments (TEEs) could bolster security, balanced against concerns of feature creep and maintaining a small, verifiable codebase.

3.25.4 Hardware vs. Software Security

A significant challenge lies in balancing hardware and software solutions for secure IoT environments. Hardware/software co-design is considered as a potential pathway for improved security. However, the lack of open-source GPUs and reliance on proprietary hardware add complexities. Securing real-time systems further complicates this balance, as trade-offs between hardware and software implementations must be carefully considered.

3.25.5 IoT Device Communication and Threat Detection

Ensuring secure communication among IoT devices in multi-room environments is problematic, with issues like RF signal vulnerabilities and the difficulty of establishing secure channels. Simple eavesdropping attacks using off-the-shelf devices highlight the practical obstacles in maintaining security in sensitive environments. Effective detection mechanisms for malicious devices remain an area of active research.

3.25.6 User Interface and Detection System Challenges

There are significant concerns related to the user interfaces for managing IoT device detection, as creating intuitive policy-based systems for device recognition is complex. Real-time detection using RF signals is being explored, but scaling such systems for large spaces, like government buildings, is difficult. Practical challenges persist in deploying reliable security solutions that can detect unauthorized or malicious devices in controlled settings.

3.26 Balancing mission-criticality, safety, and security in system design

Wenyuan Xu (Zhejiang University – Hangzhou, CN)

License © Creative Commons BY 4.0 International license
© Wenyuan Xu

Mission-critical systems have increasingly relied on IoT technologies to enhance their operational capabilities and efficiency, across various sectors, including transportation, healthcare, and energy. These IoT technologies collect data in real-time and allow systems to leverage information for improved decision-making and control. However, the security issues associated with IoT in mission-critical systems have emerged as a paramount concern. This session engaged with the multifaceted security challenges endemic to these systems.

This session discusses three special technologies that are more widely used in mission-critical systems than in the Internet, e.g., 5G networks, sensors, and position and time technologies. The threats to these technologies are typically analog instead of digital, and the results of attacks could lead to safety consequences, causing physical damage. The presentations in this section highlights the importance of interdisciplinary efforts in tackling these complex threats in the analog world, while most traditional mitigation strategies are insufficient.

3.27 Security of Private 5G for Safety-Critical Applications

Yongdae Kim (KAIST - Daejeon, KR)

License © Creative Commons BY 4.0 International license
© Yongdae Kim

Private 5G networks, dedicated cellular networks deployed for specific organizations, offer numerous advantages such as dedicated infrastructure, enhanced security, customization, improved reliability, lower latency, and higher capacity. These benefits make private 5G an attractive solution for safety-critical applications where traditional WiFi is deemed insufficient, as seen in Korea's push for 5G in critical infrastructure. Deployments in various sectors such as railroads, medical fields, and power utilities highlight the practical applications and benefits of private 5G. For example, in railroads, it aids in handling safety issues and maintaining infrastructure, while in the medical field, it supports telemedicine and surgical assistance.

However, security vulnerabilities persist across all generations from 2G to 5G, largely due to the need for backward compatibility and the complex ecosystem involving governments, carriers, and device vendors. These vulnerabilities pose significant risks, especially in safety-critical applications where even minor attacks, like detaching a user from the network, can have severe consequences. The talk underscores the importance of addressing these vulnerabilities and suggests future directions, including developing secure implementations for private 5G, creating cellular intrusion detection and prevention systems, and securing standards for the upcoming 6G.

3.28 Signal Injection Detected: What Do We Do Now?

Kasper Rasmussen (University of Oxford, GB)

License  Creative Commons BY 4.0 International license
© Kasper Rasmussen

Signal injection attacks, which manipulate sensor readings through electromagnetic interference, present a significant challenge to the integrity of sensor systems. These attacks exploit long wires acting as unintended antennas, altering the analog signals that sensors rely on. While detection strategies exist, such as monitoring for adversarial signals or deviations in sensor data, they are not foolproof and detecting an attack is only part of the problem. The real challenge lies in determining the appropriate response once an attack is detected.

Several proposed solutions, such as using additional sensors or entering a 'safe mode', each have their own limitations and costs. For instance, using more sensors increases expense and complexity, and stopping systems may not always be feasible, especially for vehicles or medical devices. Another approach involves recovering clean signals, but this often requires additional hardware and forethought. The talk calls for further research into practical and effective responses to signal injection attacks, particularly in scenarios where existing mitigation strategies are insufficient.

3.29 Security for Embodied AI

Wenyuan Xu (Zhejiang University - Hangzhou, CN)

License  Creative Commons BY 4.0 International license
© Wenyuan Xu

In the realm of IoT and autonomous systems, the interplay between digital (soul) and physical (body) components creates unique security challenges. Traditional vulnerabilities often target either the digital or physical domain, but IoT systems are particularly susceptible to out-of-band vulnerabilities that exploit the interactions between these domains. Examples include sound waves disrupting drone operations or side-channel attacks that leverage cross-field signals. These vulnerabilities highlight the risks inherent in trusting sensor data and the physical integrity of devices.

The increasing miniaturization of sensors and integration of multiple functions into single devices exacerbate these vulnerabilities. For instance, smaller microphones are more prone to out-of-band attacks, and integrating logic chips with wireless capabilities can lead to new attack vectors like the 'screaming channel'. The talk emphasizes the need for comprehensive security measures that address both digital and physical aspects of IoT devices. This includes developing tools for detecting out-of-band vulnerabilities, redesigning systems for better resilience, and fostering real-time tolerance to attacks.

3.30 Analog Security

Kevin Fu (Northeastern University - Boston, US)



License  Creative Commons BY 4.0 International license
 Kevin Fu

Analog security concerns the vulnerabilities in sensors that stem from their physical properties and interactions with the environment. Research has shown that sensors can be manipulated through various means such as sound waves and laser light, leading to significant security breaches in devices ranging from smartphones to medical equipment. For instance, sound waves can be used to hack a phone or inject false steps into a fitness tracker, demonstrating the broad range of potential attacks.

Addressing these threats requires a deep understanding of sensor physics and the development of robust countermeasures. Solutions like altering the design of micro-electro-mechanical systems (MEMS) to be less susceptible to interference or using ultrasound instead of sound waves for communication are being explored. The talk highlights the ongoing research and innovative approaches needed to secure sensors against emerging analog threats, underscoring the importance of interdisciplinary efforts in tackling these complex challenges.

3.31 Trustworthy Position & Time

Panagiotis Papadimitratos (KTH Royal Institute of Technology - Kista, SE)

License  Creative Commons BY 4.0 International license
 Panagiotis Papadimitratos

The reliability of positioning and timing information, especially from Global Navigation Satellite Systems (GNSS), is critical for numerous applications. However, GNSS signals are vulnerable to various attacks that can manipulate location and time data. These attacks range from simple signal interference to sophisticated relay and replay attacks that capture and retransmit GNSS signals to deceive receivers. Such vulnerabilities can have serious implications for any system relying on accurate positioning, including civilian infrastructure.

Defending against these attacks involves augmenting GNSS receivers with additional sensors, inertial measurement units, and network localization methods, though these solutions come with their own limitations in accuracy and feasibility. Another approach is time-based detection, which refines time solutions to ensure continuous trust in the data. The talk also discusses advanced methods like using UAVs for localizing attackers and mobile crowdsensing for enhanced detection capabilities. The ongoing challenge is to develop robust, practical defenses that maintain the accuracy and availability of GNSS data amidst evolving threats.

3.32 Discussion

The post-session discussion focused on key topics related to improve the security of IoT devices in the real world, including calling for collaborations between academic research and industry needs, building “Citizen Lab” to facilitate research on both offensive and defensive strategies, and creating standards and regulations as a compelling motivator for changes.

3.32.1 Academic research vs. Industry needs

There is a tension between the focus of academic research and the practical needs of the industry. However, neither academic researchers nor industry alone can improve the security of IoT systems in real world, and both parties play crucial role in enhancing the security of IoT systems. Collaboration and mutual understanding between academic researchers and industry professional are essential for effectively addressing emerging threats. One of the top priority of companies is to make profits and thus they are often reluctant to address security vulnerabilities immediately due to the cost concerns, with the exception of external pressures, e.g., standards or regulations. Nevertheless, to help companies to improve the security of their produces, researchers should not only demonstrate the consequences of attacks, but also provide accessible security solutions, e.g. develop tools and frameworks that can help industry to detect and fix security vulnerabilities easily.

3.32.2 Attack vs. Defense

There was a proposal to create a “Citizen Lab” that would enable research on both offensive (attack) and defensive (solution) strategies regarding security vulnerabilities. Firstly, for research on offensive, it is important to follow the responsible disclosure process, but should remain skepticism about its real-work impact on industry practise. The conversation highlighted the necessity of realistic attack demonstrations to push companies toward action on security improvements. However, even if the offensive research may seem unrealistic today, it is the valuable of academia in pushing the boundaries of attack research, because those attacks could become relevant in the future. Secondly, after demonstrating the vulnerabilities, we shall provide solutions to fix the issues and their cost-benefit, to facilitate companies to adopt the mitigation and government to create regulation.

3.32.3 Standard and Regulations

Standards and regulations have emerged as critical factors in compelling companies to effectively address security vulnerabilities. Furthermore, catastrophic security incidents that can damage an industry’s reputation may prompt companies to respond to these vulnerabilities, as evidenced by examples from the automotive sector. Consequently, regulatory and reputational pressures are essential for driving meaningful changes in industry practices regarding security. However, the process of creating regulations typically requires a significant amount of time, often spanning 10 to 15 years, as demonstrated by experiences in medical device security. It is vital to understand the unique practices of government entities, which will not enact regulations based solely on academic research. Advocates must clearly articulate the size of the community they represent, the real consequences of security issues, and practical solutions, all while maintaining persistence. Consistent presence and advocacy are crucial for the acceptance and implementation of ideas, ultimately influencing policy and practice.

3.33 Security Challenges in Unattended Environments, e.g., Low-Orbit Satellites

Bruno Crispo (University of Trento, IT) and Wenyuan Xu (Zhejiang University – Hangzhou, CN)

License  Creative Commons BY 4.0 International license
© Bruno Crispo and Wenyuan Xu

An interesting and challenging design space for security researchers is the one where IoT devices are unattended and in some case even without the possibility to be reached and physically repaired or replaced. Yet designing for such domains trust and security mechanisms that can dynamically adapt to configuration changes and to the discovery of new attacks is important.

This section explores examples of these demanding environments, such as outer space, low-orbit satellites, underwater networks, and smart grids. These domains are rapidly evolving, with significant investment and development from both public and private sectors. The session's discussions will highlight the unique security challenges and threats inherent to each domain. Additionally, it will address the complexities introduced by the increasingly competitive and open market dynamics, which make securing these environments even more difficult.

3.34 The Curse of Autonomy in IoAT Security

Alfred Chen (University of California, Irvine, US)

License  Creative Commons BY 4.0 International license
© Alfred Chen

The talk centers on the challenges and vulnerabilities faced by autonomous systems, particularly in ensuring security for fully unattended operations. One example highlighted is a “traffic cone attack,” where simple cones are used to immobilize driverless cars, posing a significant and practical threat to these systems. Compared to other sophisticated attack methods, using traffic cones is not only affordable and transferable but also highly stealthy, leveraging ordinary items to disrupt autonomous vehicles. This underscores a key point: low-cost, simple interventions can exploit vulnerabilities in highly advanced systems, raising concerns about their resilience.

The speaker discusses the pursuit of true autonomy and its inherent risks. Without human drivers, autonomous systems struggle to handle disruptions that a driver could easily solve, such as moving a blocking object. Possible solutions like adding mechanical arms or relying on remote operators either add complexity and cost or undermine the goal of complete autonomy. Even with remote assistance, replicating the situational awareness of a human driver is challenging, affecting safety and security. The speaker suggests that autonomy and security can sometimes be at odds, and achieving a balance may require sacrificing certain autonomous functions to enhance overall system safety.

3.35 Emerging Threats in Underwater Cyber-physical Systems

Sara Rampazzi (University of Florida - Gainesville, US)

License  Creative Commons BY 4.0 International license
© Sara Rampazzi

The presentation focuses on the security challenges of underwater cyber-physical systems, extending concepts previously explored in terrestrial and aerial environments. It begins by discussing physics-based vulnerabilities, such as physical adversarial attacks that exploit physical phenomena to manipulate automated behavior. One example mentioned is a laser interference attack demonstrated in a Usenix paper, which causes sensors to fail in detecting pedestrians. The concept of “oversensing,” where sensors detect more than intended, is also highlighted as a potential attack vector. The presentation then shifts to underwater environments, exploring how traditional vulnerabilities apply to the emerging “blue economy” that revolves around oceanic resources, energy harvesting, and resilience to climate change.

The underwater Internet of Things (IoUT) is presented as a crucial aspect of this new blue economy, comprising assets like pipelines, data centers, and communication networks. The focus on underwater data centers emphasizes natural cooling benefits and climate stability but introduces unique vulnerabilities, such as acoustic injection attacks that can manipulate server operations through sound-induced vibrations. Challenges for underwater IoT security include unstable communication channels, low-energy and sparsely distributed devices, and a lack of established security standards. The key question is whether existing security frameworks designed for land-based IoT can be effectively adapted to underwater environments, given the unique physical and operational constraints of the ocean.

3.36 Securing the Internet of Energy

Surya Nepal (CSIRO - Eveleigh, AU)

License  Creative Commons BY 4.0 International license
© Surya Nepal

The talk addresses the pressing issue of ensuring energy security against cyber-attacks on the increasingly connected and distributed energy systems. While energy production and distribution have seen massive advances, the security aspect remains lagging, with limited research and solutions currently in place. The speaker emphasized the need to consider security from the ground up as the energy landscape transforms, especially with the proliferation of distributed energy resources (DERs) and consumer energy resources (CERs). Australia’s push towards renewable energy, such as South Australia’s aim to be 100% renewable by 2027, and the increased use of household solar and battery systems highlight the urgent need for robust cybersecurity measures to secure the energy grid.

The challenges include dealing with a landscape that was developed without security in mind, vulnerabilities in unencrypted communication, lack of device management, and the absence of a standardized security framework for DERs. The speaker drew parallels between current energy device installations and insecure IoT camera installations, emphasizing the need for better threat modeling and adherence to standards. The integration of virtual power plants and smart applications only complicates this landscape further, leading to increased dependency on other critical infrastructures. As governments start paying more attention to

smart energy, the nexus of climate and cybersecurity becomes an important area of concern, necessitating a proactive approach rather than the current “install and pray” mindset.

3.37 Orbiting Threats: Security & Privacy in Space

Ahmad-Reza Sadeghi (TU Darmstadt, DE)

License © Creative Commons BY 4.0 International license
© Ahmad-Reza Sadeghi

The talk covers the growing security and privacy challenges in space, especially with the surge in low-Earth orbit satellite launches and evolving technology. With emerging trends like mega-constellations, interplanetary networks, and spacecraft autonomy, the focus shifts to how such systems will cope with cybersecurity threats. Highlighted were potential attack scenarios, such as “blackhole” attacks (where a satellite disappears), “ghost” attacks (fake satellite impersonation), and “residence evil” (rogue, self-contained satellites). The architecture of modern small satellites, such as Ireland’s EIRSAT-1, was discussed, emphasizing onboard sensors and ARM-based computing platforms. Challenges include secure communication in highly dynamic and constrained environments, prevention of satellite user localization, and implementation of robust PKI systems in space.

The talk also addressed the limitations of existing solutions for securing space assets, like traditional PKI models, which are unsuitable due to sporadic connectivity, dynamic topology, and restricted power and storage. Challenges surrounding user localization were stressed, as there is a real risk of privacy violations in situations where authoritarian regimes or military conflicts limit terrestrial communication, as seen in Ukraine. Existing privacy measures like encryption or Tor are insufficient against metadata correlation, necessitating custom protocols to maintain user privacy. Lastly, the speaker suggested the potential of overlay networks for satellite internet and discussed the implications of physical security, compromised nodes, and the need for optimized fake traffic to enhance user location privacy in space systems.

3.38 Space Networks meet 5G Terrestrial Networks – Thoughts on Threats and Defenses in Large-scale Networks

Christina Pöpper (New York University - Abu Dhabi, AE)

License © Creative Commons BY 4.0 International license
© Christina Pöpper

The presentation discussed the intersection of 5G terrestrial networks and space networks, exploring security challenges and potential defenses for these large-scale systems. It began by reviewing the evolution and complexities of cellular network security, highlighting vulnerabilities across different generations and attack surfaces like user equipment, network infrastructure, and configurations. Despite advancements, many 5G systems still lack complete security due to the complexity and optional implementation of certain security measures. The discussion then shifted to space networks, detailing the various segments (launch, ground, space, user, link) and their susceptibility to attacks, including fake location information, communication jamming, and message manipulation. Space systems often lack robust security mechanisms, as they are typically deployed for decades with limited updates.

The core of the talk addressed the convergence of space networks (NTN) with 5G/6G terrestrial networks (NR), enabling expanded coverage and connectivity for IoT devices in areas without terrestrial network access. However, this integration poses several challenges, particularly regarding how to extend the security guarantees of terrestrial networks to space-based systems. Key challenges include the relatively weaker security of NTN compared to NR, the impact of NTN-NR integration on attack surfaces, and the need to understand potential attackers in both domains. The speaker also highlighted opportunities to leverage the unique physical properties of space, such as orbital movements and signal propagation characteristics, to create secure systems through physically-backed security measures.

3.39 Discussion

3.39.1 Hardware Limitation and Security

The discussion on hardware security began with an examination of energy limitations and security architecture constraints in satellite systems. Participants explored the applicability of ARM Trust Zone and RISC-based processors, focusing on low-energy designs that can withstand radiation challenges. Additionally, the use of FPGAs in satellites was analyzed, particularly their limitations related to radiation and the need for fault tolerance, alongside the difficulties in implementing RadHard technology and enhancing FPGA flexibility. Other important security issues in space systems include the need of secure communication protocols, real-time requirements, and public key infrastructure (PKI).

3.39.2 Testbeds and Experiments

There are several research challenges in simulating real-world security issues for self-driving cars, underwater communication and satellites, particularly the limitation of existing testbeds. Emphasis was placed on the importance of living labs and controlled experiments as essential components of security research, noting the complications involved in securing industry support for these initiatives. Furthermore, discussions centered on the challenges of keeping testbeds up-to-date in a rapidly evolved technological landscape.

3.39.3 Industry Collaboration


The group emphasize the need for collaboration across industries to create realistic testing environments, with specific testbeds initiatives in Singapore and Australia highlighted as examples. Participants expressed the importance of fostering connections between academic research and industry needs, suggesting future workshops and collaborative efforts focused on testbeds to strengthen these ties further.

3.39.4 Funding Opportunities

The discussion concluded with a discussion on funding opportunities, where the potential sources such as the National Science Foundation (NSF) and the German Research Foundation (DFG) were mentioned. Participants acknowledged the challenges associated with securing funding for research that involves security experiments in critical infrastructure, space, and autonomous vehicles, underscoring the need for strategic approaches to overcome these obstacles.

3.40 Addressing the scalability challenge in securing large IoT deployments

Alexandra Dmitrienko (Universität Würzburg, DE) and Gene Tsudik (University of California – Irvine, US)

License  Creative Commons BY 4.0 International license
© Alexandra Dmitrienko and Gene Tsudik

In an era where the Internet of Things (IoT) continues to proliferate across various industries, the scalability of security measures has become a paramount concern. This seminar session focused on the complex interplay between security, usability, and user trust in the rapidly evolving IoT landscape. The main goal is to inspire actionable strategies that address multifaceted challenges of securing large IoT deployments, while addressing privacy and usability concerns.

3.41 You can have your cake and eat it too: Ensuring practical robustness and privacy in IoT Federated Learning

Farinaz Koushanfar (University of California at San Diego, US)


License  Creative Commons BY 4.0 International license
© Farinaz Koushanfar

The presentation introduced a framework called zPROBE, aimed at enhancing both privacy and robustness in FL for IoT networks. Federated Learning is a machine learning approach that trains a central model using data distributed across many IoT nodes, which often contain private information. The challenge addressed is protection of this data from privacy risks (such as model inversion attacks) and ensuring robustness against malicious clients who may try to degrade model performance. Traditional privacy measures, such as differential privacy and Secure Multi-Party Computation we discussed as well as their limitations in terms of utility and efficiency.

The zPROBE approach was proposed as a solution, leveraging Zero-Knowledge Proofs (ZKPs) and rank-based statistics to securely aggregate data and maintain robustness in the presence of adversarial threats. The system uses a semi-honest server that clusters clients randomly while each client provides a ZKP to ensure privacy during data aggregation. This approach enables the identification and mitigation of outlier attacks, such as Byzantine attacks, which malicious clients may use to disrupt the model. Results show that rank-based statistics help maintain robustness better than existing methods, keeping overhead low and the system scalable. The conclusion emphasizes the ongoing challenge of designing efficient cryptographic methods that enhance privacy without compromising the utility and scalability of IoT Federated Learning.

3.42 IoT Devices During Internet Shutdowns

Stefanie Roos (RPTU Kaiserslautern-Landau, DE)


License  Creative Commons BY 4.0 International license
© Stefanie Roos

The presentation addresses the challenges of maintaining IoT device communication during internet shutdowns, a scenario that often correlates with political unrest. When governments impose internet blackouts, censorship-resistant methods relying on traffic modification, such as disguising sensitive data as mundane videos, become ineffective since there is no connectivity to exploit. The proposed solution involves leveraging mobile ad-hoc communication, allowing local peer-to-peer connections even when internet access is severed. This approach aims to keep individuals connected to others in proximity and potentially those outside of the immediate range, despite adversarial efforts by authorities to control or surveil these networks.

The situation is complex, as mobile ad-hoc networks must contend with issues like scalability, intermittent device disconnection, and adversarial conditions where authorities partially restrict communication, especially for protest coordination. Techniques like ring signatures are being explored to enhance anonymity and resist flooding attacks, although these aren't applicable to all devices. Scaling communication to larger areas poses additional challenges, and while satellite communication could be an alternative, it may not be entirely secure or accessible for widespread use. The speaker underlines that even with limited connectivity, every small effort contributes to enabling communication in a highly restricted environment.

3.43 Rethinking the Role of the Cloud in IoT Systems

Earlence Fernandes (University of California - San Diego, US)


License  Creative Commons BY 4.0 International license
© Earlence Fernandes

This talk explores the current role of cloud services in IoT systems, focusing on their security and privacy challenges. It begins by examining typical cloud functions in IoT: remote control of devices, interoperability, software updates, and analytics. While these services provide significant functionality, they also create substantial vulnerabilities. For example, remote control mechanisms can be compromised, providing attackers with access to all connected devices. Similarly, integrators – cloud hubs that link multiple IoT products – are prime targets due to the elevated privileges they hold, making security breaches particularly severe. Privacy concerns also arise, as cloud services can see all device data and patterns, often beyond what's necessary for functionality.

The talk proposes a shift towards minimizing trust in cloud services by applying the principle of least privilege, aiming for a design that can handle cloud security failures gracefully. A case study on trigger-action platforms exemplifies the concept, demonstrating how small cloud-hosted scripts could operate with far fewer data than they currently access. The speaker emphasizes rethinking how we construct IoT services to ensure that cloud privileges are strictly limited, asking critical questions about which functionalities are essential and how they can be delivered securely with minimal cloud access.

3.44 Thoughts about Network Management in Secure IoT Environments

David Hock (Infosim - Würzburg, DE)

License  Creative Commons BY 4.0 International license
© David Hock

The presentation (with music) focuses on managing secure IoT networks, highlighting the expanding IoT landscape, which consists of a vast and diverse ecosystem of interconnected devices. Despite numerous security threats, the persistence of IoT devices necessitates proactive integration and automation approaches. The speaker emphasizes the need for practical solutions, particularly in integrating security measures into an expanding network of diverse devices. The presentation highlights a rising trend in cyberattacks and emphasizes the importance of measuring security consistently. This involves developing a “key security indicator” to understand security risks across various devices, such as audio sensors and active triggers.

In terms of network management, the importance of visibility, control, and automation is stressed, with a common saying: “You can’t protect what you cannot see.” Full understanding of network activity, along with a balance between centralized and decentralized control, is crucial for responding to threats effectively. Scalable security strategies include leveraging edge computing and employing holistic, collaborative approaches to ensure comprehensive IoT security. The concluding note underlines the importance of scalable network management, comprehensive security, and collaborative efforts to secure the future of IoT environments.

3.45 Just “Build, provision, deploy”? Obstacles Faced by SMBs when Building Secure IoT Devices

Markus Wamser (Ingenics Digital - Gräfelfing, DE)

License  Creative Commons BY 4.0 International license
© Markus Wamser


Small and medium-sized businesses (SMBs) face significant challenges when building secure IoT devices, particularly in key areas such as secure provisioning, deployment, and maintaining security throughout the device lifecycle. Typically, SMBs produce devices like kitchen utilities, lights, and robots, often in quantities of 10,000 to 50,000 units per year, with small development teams and limited security expertise. Regulatory requirements, intellectual property protection, and maintaining device reliability drive the need for security, but SMBs often struggle to implement proper key management and secure boot processes due to limited resources and knowledge. Existing frameworks like IANA or industry standards for secure CI/CD pipelines are often either too complex or impractical for smaller businesses to adopt, leading to difficulties in securely managing keys and provisioning devices.

Most SMBs lack dedicated security professionals, relying instead on developers who are not well-versed in security procedures, leading to potential vulnerabilities such as improper key storage and a lack of recovery mechanisms for lost or stolen keys. Current solutions for secure device provisioning and deployment, such as AWS IoT or Azure, are often targeted at larger customers, leaving SMBs to attempt DIY approaches like threshold signatures. Despite the existence of several standards and frameworks (e.g., TUF, SLSA, in-toto), these are often too complex or academic for SMBs to use practically. There is a need for simplified

and specialized procedures tailored to the requirements of smaller IoT deployments, allowing these companies to effectively secure their devices while managing resources efficiently.

3.46 Challenges of Scaling Security Services in IoT Networks

Alexandra Dmitrienko (Universität Würzburg, DE)


License  Creative Commons BY 4.0 International license
© Alexandra Dmitrienko

The presentation addresses the challenges of scaling security services in IoT networks, particularly in the context of a rapidly expanding “Internet of Everything” that will soon involve trillions of connected devices. Current security architectures, which rely heavily on centralized client-server models and trusted third parties, are inadequate for such a large-scale and decentralized system. The speaker emphasizes the difficulties inherent in using publish-subscribe (pub/sub) communication models, which are increasingly relevant in IoT networks. Security issues include handling malicious subscribers, compromised publishers, and untrusted brokers. Establishing end-to-end encryption is complex due to scalability challenges, the limited resources of IoT devices, the need for group/broadcast encryption, and the absence of trusted key management entities. Additionally, dynamic membership in groups complicates key revocation, and timely delivery of security updates through potentially untrusted brokers remains a significant hurdle.

Further complications arise when addressing compromised devices within the network. Attestation is critical for identifying compromised endpoints, but the network’s heterogeneity means that multiple attestation methods must coexist, each providing different security guarantees. The presentation also discusses the challenge of enabling on-demand attestation and securing attestation information against replay attacks, which is further complicated by time synchronization issues. Finally, the speaker outlines the role of projects like Simpl, which aim to address some of these challenges by managing key information, facilitating attestation, and identifying compromised devices. However, there remain open issues, particularly concerning the scalability of security solutions and the integration of heterogeneous security measures across diverse devices and communication models.

3.47 Scaling credential management in IoT

Panagiotis Papadimitratos (KTH Royal Institute of Technology - Kista, SE)

License  Creative Commons BY 4.0 International license
© Panagiotis Papadimitratos

The presentation discusses the challenges and solutions for scaling credential management in large-scale IoT environments, particularly focusing on vehicular communication systems. It emphasizes the need to manage multiple ephemeral pseudonyms for vehicles, ensuring both security and privacy requirements. The speaker highlights the complexities of designing and evaluating a Public-Key Infrastructure (PKI) suitable for vehicular applications (VPKI), addressing the management of short-lived credentials, the diverse types of entities involved, and the constraints of large-scale deployment. The system faces challenges such as handling malicious users, scalability, and balancing security, privacy, and efficiency requirements under different operational loads.

A cloud-based, scalable VPKI service is proposed for efficient credential management, enabling quick provisioning of pseudonyms and dynamic handling of credential loads. Additional topics include vehicle-centric revocation strategies and the use of specialized cryptographic methods to enhance privacy through mechanisms like mix zones and decoy traffic. The discussion highlights the importance of scalability, cost efficiency, and privacy preservation in managing credential operations in dynamic vehicular networks, ultimately aiming for a secure and privacy-respecting system capable of global deployment.

3.48 Discussion

Presentations were followed by a discussion on the following topics:

3.48.1 Security Scoring and Subjectivity

There is a need for an in-depth exploration of an IoT security scoring system, which would facilitate fair security comparisons across devices. One challenge is that such systems are not intended for tracking changes over time. Another challenge is subjectivity in scoring, which makes it difficult to justify and publish in high-tier venues, as the field prefers more objective measures.

3.48.2 Large Data Collection by Cloud Providers vs. Privacy

Large-scale data collection by cloud providers undermines privacy of users. Concerns were raised about the economic incentives for cloud providers and manufacturers, noting their reluctance to reduce data control, which impacts revenue. A two-tier system for users based on privacy preferences was introduced, highlighting that manufacturers often prefer to sell devices without ongoing management responsibility.

The importance of separating data from control was also discussed, advocating for user choice in data mining. While current privacy options are acknowledged, usability challenges for average consumers persist. Trust in manufacturers is essential in any connected device scenario. It was also noted that companies use data for service provision as well as to innovate in terms of their products, with suggestions for offering incentives to users for data sharing. The issue of resold data without ongoing compensation was also addressed.

3.48.3 Centralization, Privacy, and Security Trade-offs

Centralization is being driven by the simplicity of maintaining cloud systems. It was suggested that local actuation could minimize risks without reliance on cloud services. The discussion also covered how security breaches often arise from mis-configurations, while noting that addressing privacy issues is more complex. There was a consensus about the need for better security prioritization in product design and the importance of improved industry guidelines.

3.48.4 Data Ownership, EULAs, and Changing Industry Practices

Concerns about data ownership were discussed, questioning whether consumers truly own the data generated by their devices, as this often depends on the EULA signed. The stagnation of industry practices was debated, emphasizing the need for proactive change from the community. The discussion included the issue of the gap between larger manufacturers that embrace data ownership and smaller ones that prefer to avoid such liability.

3.48.5 The Role of Academia and Industry Practices

The pressures in academia is to produce novel contributions. The discussion leaned towards evaluating work based on practical impact rather than sheer novelty. The conversation also touched on the “paper chase” phenomenon in academia, acknowledging the pressures to publish a lot and quickly. The idea of drafting impact-ful position papers to articulate perspectives on data usage and industry practices was also considered.

3.48.6 Vulnerability Disclosure and Corporate Responses

There are certain challenges of responsible vulnerability disclosure. This issue varies quite a bit in different countries, which means that legal protections for researchers also vary. Incidents of corporate indifference toward vulnerabilities were recounted. The discussion touched upon the potential of using public shaming through competitions to incentivize improvements in security.


3.48.7 Cultural Attitudes Toward Cybersecurity and Final Reflections

There were comparisons made regarding international responses to vulnerabilities, noting cultural differences in accountability, particularly between various jurisdiction. The session concluded with encouragement for participants to reflect on the discussion and consider future challenges, emphasizing the importance of looking forward rather than focusing solely on past achievements.

4 Open problems

4.1 Open Issues

Bruno Crispo (University of Trento, IT), Alexandra Dmitrienko (Universität Würzburg, DE), Christoph Sendner (Universität Würzburg, DE), Gene Tsudik (University of California – Irvine, US), and Wenyan Xu (Zhejiang University – Hangzhou, CN)

License  Creative Commons BY 4.0 International license
© Bruno Crispo, Alexandra Dmitrienko, Christoph Sendner, Gene Tsudik, and Wenyan Xu

The final session serves as a comprehensive wrap-up, summarizing key topics covered during the whole seminar. It also introduces potential research directions to continue the exploration and address unresolved issues. This session emphasizes the insights gained from discussions, identifying critical gaps, and calls for fostering collaborative research in the field.

4.2 Key Outcomes

- **Emphasis on Privacy and Security Challenges in IoT.** In IoT environments, privacy and security challenges are pervasive, but often there is an important gap between theoretical frameworks and practical implementation challenges. The discussions highlight the complexity of creating robust security measures that address diverse threats, especially when real-world constraints make certain theoretical solutions difficult to deploy effectively.

- **Hardware versus Software Trade-offs, with a Focus on TEEs.** Exploring the trade-offs between hardware and software solutions, particularly in the context of Trusted Execution Environments (TEEs), highlights their advantages and limitations. While TEEs provide a secure enclave for sensitive computations, limitations such as scalability, interoperability, and vulnerability to certain physical attacks remain open research challenges.
- **The Role of Secure Hardware in IoT Security** Secure hardware plays a crucial role in enhancing IoT security, especially in environments where devices operate autonomously, such as satellites and self-driving vehicles. The discussions delved into the unique security challenges in these contexts, where unattended operation makes conventional security measures ineffective.
- **Critique on the Absence of Formal Methods and Usable Security Discussions** Participants reflect on the general lack of assurance in existing IoT solutions and the potential benefits formal methods could bring, such as more rigorously designed security solutions. This critique also covers usable security, emphasizing the importance of designing security solutions that end-users can effectively utilize without unnecessary complexity.
- **Sensitivity and Societal Awareness of Self-Driving Car Threats** The discussions addressed how societal awareness around the security threats to self-driving technology remains limited. By raising sensitivity to these issues, the seminar aimed to highlight the implications of security breaches in self-driving cars, especially as these vehicles become integral to public transportation and logistics.
- **Scalability Challenges in Securing Large IoT Deployments** As IoT systems expand, so do the challenges of securing these vast networks. The discussions explored the complexities of provisioning, key management, and device authentication in distributed systems. Addressing these challenges is essential for the scalable deployment of secure IoT solutions that can withstand high levels of connectivity and data exchange.
- **Balancing Mission-Criticality, Safety, and Security in IoT Design** The need to balance mission-critical functions, safety requirements, and security measures, especially in cloud-based IoT services emerged in the discussions as well as the need to foster further collaborations between the two research communities of dependability and cybersecurity.
- **Need for Common and Publicly Accessible IoT Testbeds** The seminar highlighted how policy priorities and funding allocations shape IoT security research and development. Calls for large-scale testbeds and collaboration between private and public sectors highlight the importance of policy and financial support for advancing IoT security solutions.
- **Broader Discussion on Threat Models and Attacker Motivations** It's important to distinguish between pure physical attacks, for example, placing a cone on a self-driving car to disrupt its operation, from digital ones that are the ones on which the community should focus on. This segment emphasizes the need for a comprehensive analysis of threat models that consider diverse attacker motivations, from denial-of-service (DoS) attacks to irrational and economically motivated threats. Understanding these motivations aids in designing more nuanced and resilient IoT security frameworks.
- **Advocacy for Resilient System Designs and Sensor Fusion Logic** Participants advocate for designing IoT systems with enhanced resilience to counter vulnerabilities. Integrating sensor fusion logic, which combines data from multiple sources, can improve system accuracy and reduce susceptibility to individual sensor failures or attacks. The seminar concludes with calls for ongoing collaboration, inviting participants to contribute

to future projects and discussions. It encourages follow-up meetings to foster a continued exchange of ideas and support for evolving research initiatives.

4.3 Future Outlook

The consensus among participants is that the IoT landscape will undergo significant transformation in the coming years, driven by the rapid digitalization of industrial and commercial sectors. This digital shift will likely lead to exponential growth in the deployment of IoT technologies, accompanied by the development of new generations of devices, more powerful, intelligent, and pervasive. As IoT devices increasingly replace human roles in critical safety applications, they will bring forth new security challenges. Addressing these challenges will require incorporating non-technical dimensions such as usability, inclusivity, and accessibility, which are essential to ensuring that IoT technologies serve all users effectively and safely.

As IoT-related attacks and incidents inevitably increase, ethical and social considerations will become increasingly central to the IoT research agenda. Participants noted that traditional security frameworks, previously used for IT ecosystems such as the web, may not provide adequate protection in safety-critical IoT systems, where failures could lead to loss of life. Therefore, new proactive and preventative security paradigms will be necessary to address the specific risks associated with IoT in these high-stakes environments.

Looking forward, participants identified emerging trends in IoT security, including a tighter integration of human and cyber systems. This integration raises unique ethical and security concerns, particularly as bionic enhancements and other human-cyber hybrids become more commonplace. These advancements suggest a future where the line between human and machine is increasingly blurred, presenting new dimensions of security and privacy challenges that must be addressed.

In light of these factors, participants agreed on the need for more frequent and collaborative forums like this seminar. Such gatherings will be crucial for the IoT community to assess and discuss the evolving security and privacy landscape, establishing priorities and refining approaches to meet the complex demands of future IoT systems.

Participants

- Z. Berkay Celik
Purdue University –
West Lafayette, US
- Alfred Chen
University of California –
Irvine, US
- Bruno Crispo
University of Trento, IT
- Ivan De Oliveira Nunes
Rochester Institute of
Technology, US
- Xuhua Ding
SMU – Singapore, SG
- Alexandra Dmitrienko
Universität Würzburg, DE
- Jan-Erik Ekberg
Huawei Technologies –
Helsinki, FI
- Earlence Fernandes
University of California –
San Diego, US
- Kevin Fu
Northeastern University –
Boston, US
- Jorge Guajardo Merchan
Robert Bosch LLC –
Pittsburgh, US
- David Hock
Infosim – Würzburg, DE
- Murtuza Jadliwala
University of Texas –
San Antonio, US
- Yongdae Kim
KAIST – Daejeon, KR
- Farinaz Koushanfar
University of California at
San Diego, US
- Veelasha Moonsamy
Ruhr-Universität Bochum, DE
- Surya Nepal
CSIRO – Eveleigh, AU
- Panagiotis Papadimitratos
KTH Royal Institute of
Technology – Kista, SE
- Christina Pöpper
New York University –
Abu Dhabi, AE
- Sara Rampazzi
University of Florida –
Gainesville, US
- Kasper Rasmussen
University of Oxford, GB
- Stefanie Roos
RPTU Kaiserslautern-
Landau, DE
- Ahmad-Reza Sadeghi
TU Darmstadt, DE
- Nader Sehatbakhsh
University of California at
Los Angeles, US
- Christoph Sendner
Universität Würzburg, DE
- Gene Tsudik
University of California –
Irvine, US
- Markus Wamser
Ingenics Digital – Gräfelfing, DE
- Wenyan Xu
Zhejiang University –
Hangzhou, CN

