A Brief Introduction to Secure Systems Group @KTH

N. Asokan, Secure Systems Group
https://asokan.org/asokan/
@asokan.org *@nasokan*

Who am I?

Visiting Professor and Wallenberg Chair, KTH (from January 2026)

University Professor, University of Waterloo

Fellow of the Royal Society of Canada (2023), IEEE Fellow (2017), ACM Fellow (2019)

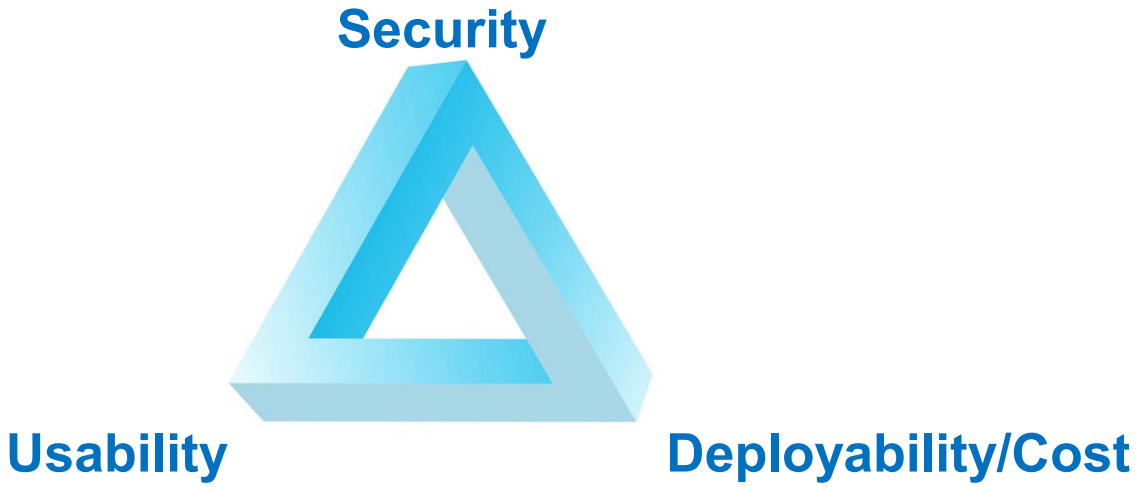
Previously: Professor, Aalto University (2013-2019), **Nokia** (14 y; built up Nokia security research team), **IBM Research** (3 y)

Industry collaborations: Private-AI Institute, ICRI-CARS, Google Awards

https://asokan.org/asokan/ for more background

Systems security and privacy

How to make it possible to build systems that are simultaneously easy-to-use and inexpensive to deploy while still guaranteeing sufficient security?



Our research interests

Systems Security and Privacy

AI and Security/Privacy

- How to use AI to improve security/privacy solutions
- How to ensure security/privacy of AI-based systems

Platform security

- How to design/use hardware assistance to secure software?

https://ssg-research.github.io/

How to use AI to improve security?

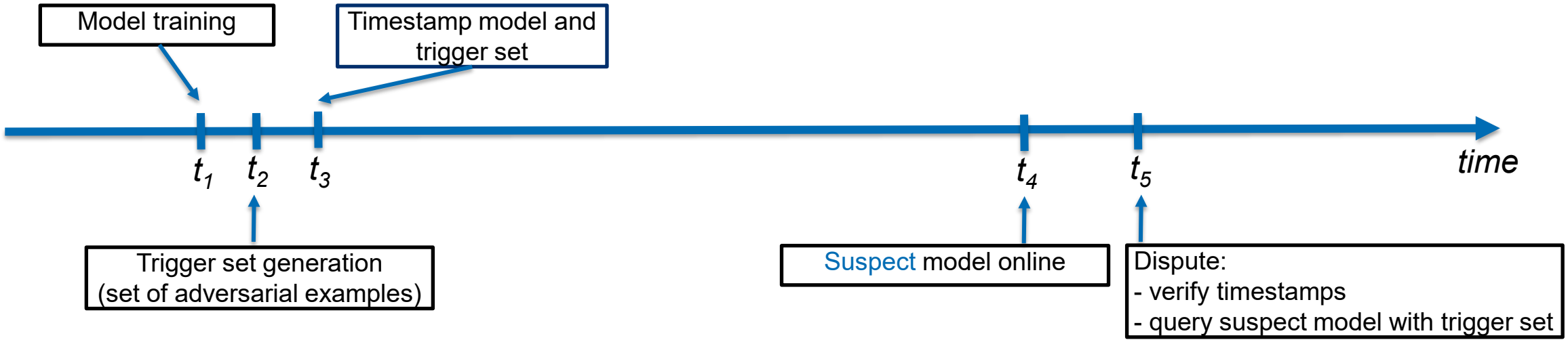
Example: Can we protect vulnerable IoT devices effectively?

- **IoT is a "brown field" setting. Analyze traffic to identify vulnerable/infected devices**
- **IoT Sentinel: Automated Device-Type Identification for Security Enforcement in IoT (ICDCS 2017)**
- **AuDI: Toward Autonomous IoT Device-Type Identification Using Periodic Communication (IEEE JSAC 2019)**
- **DÏoT: A Federated Self-learning Anomaly Detection System for IoT (ICDCS 2019)**

How to ensure security/privacy of AI (1/2)?

Example: Are AI security/privacy proposals correctly modeling adversarial behavior?

- **Current model watermarking/fingerprinting techniques overlook malicious accusers**
  - **Malicious suspect:** tries to evade verification (e.g., pruning, fine-tuning, noising)
  - **Malicious accuser:** tries to frame an independent model owner
    - (secure) timestamping (watermark/fingerprint and model) is the only defense in prior work



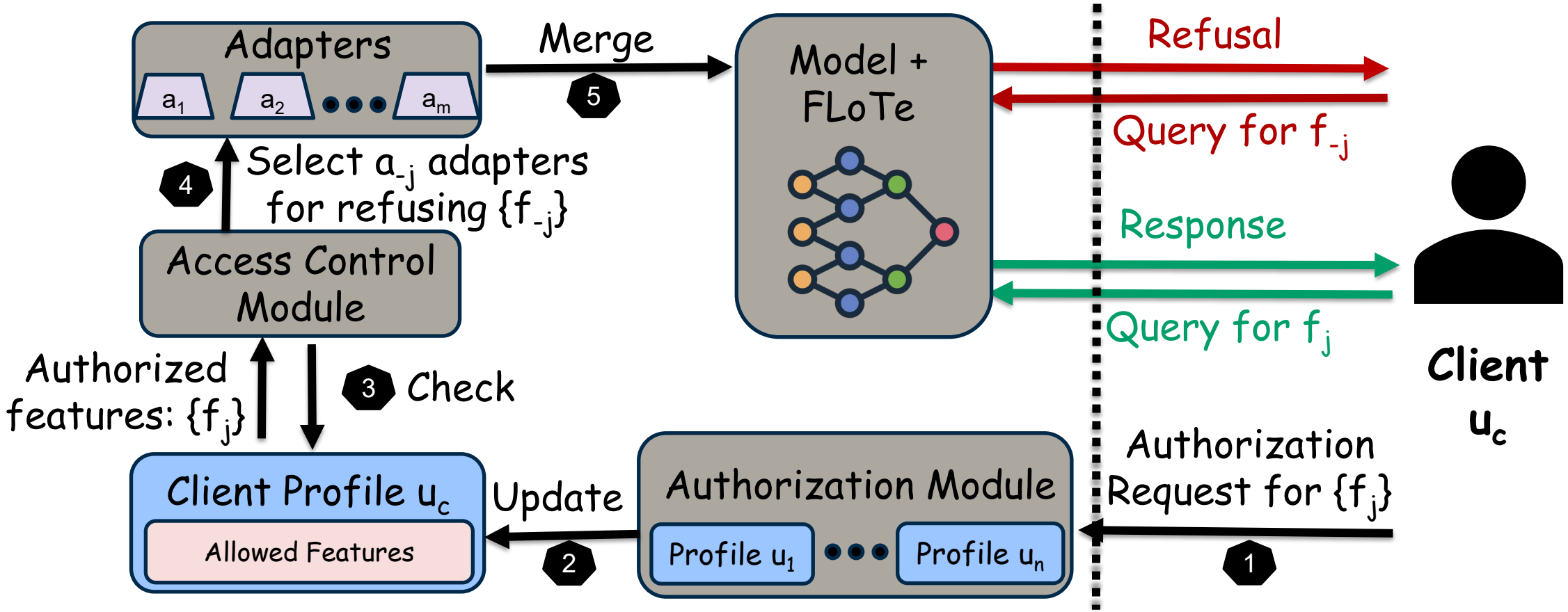
- **False Claims against Model Ownership Resolution (Usenix Security 2024)**

How to ensure security/privacy of AI (2/2)?

Example: Can We Enable Pay-to-Unlock for Chatbot Services?

- **For blackbox adversaries, policy decision can be separated from enforcement**
- **Locket: Robust Feature-Locking Technique for Language Models (ACL 2026)**
  - Train LoRA adapters for refusing each premium feature

Locket Design: LoRA Adaptors for Scalability



Refusal training for adapter → One adaptor per feature to lock

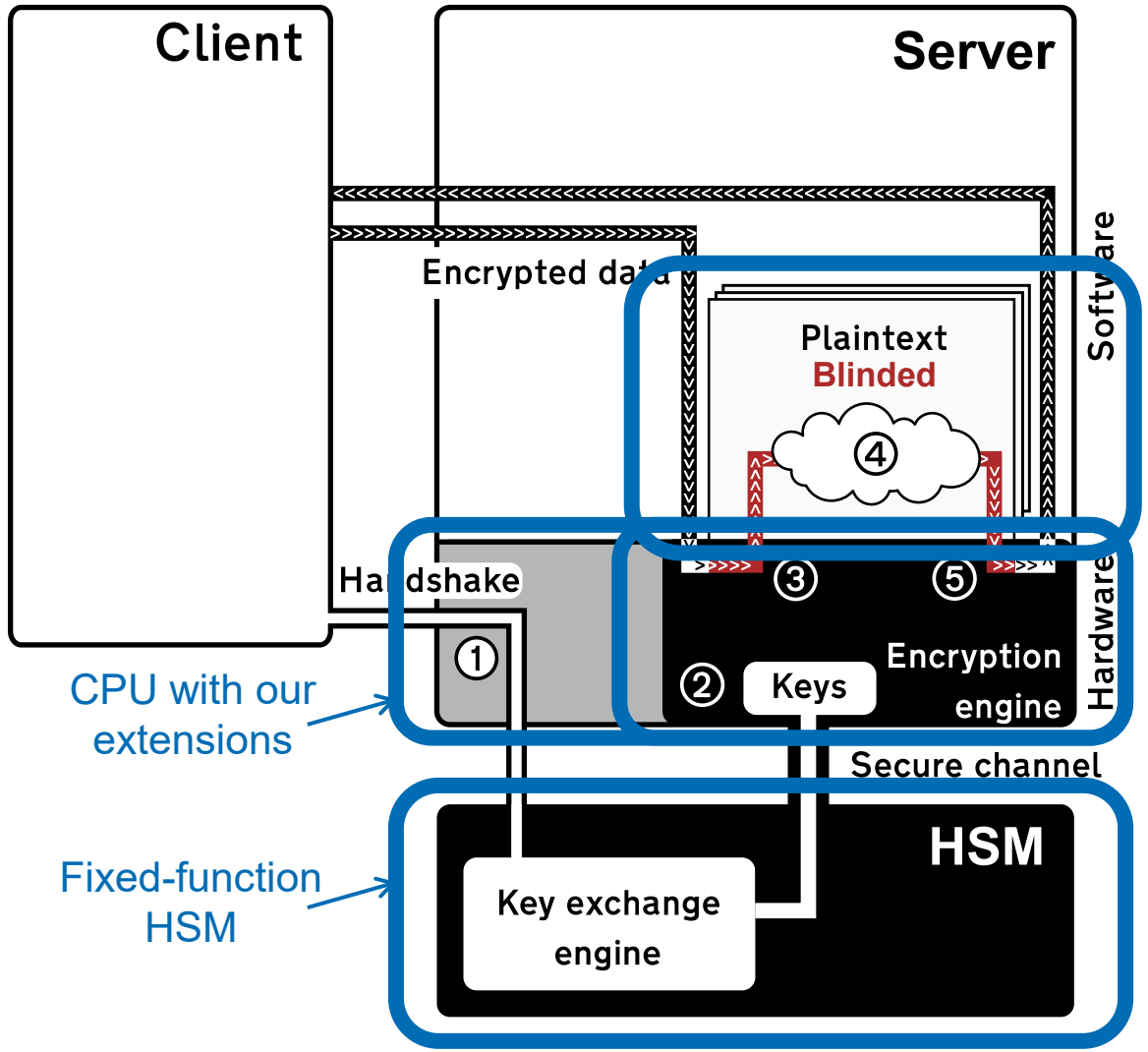
How to use hardware assistance to secure software?

Example: Can h/w assistance efficiently protect client data in outsourced computing

- **Hardware-assisted taint-tracking can afford efficient protection**
- **BliMe: Verifiably Secure Outsourced Computation with Hardware-Enforced Taint Tracking (NDSS 2024)**

BliMe Architecture

1. **Handshake (incl. remote attestation)**
2. **Shared secret key**
3. **Atomic data import (inputs)**
   - Decrypt & blind (Blinded ← true)
4. **Safe (“blinded”) computation**
   - Enforced by BliMe HW extensions
5. **Atomic data export (result)**
   - Encrypt & unblind (Blinded ← false)



How to use hardware assistance to secure software?

Example: Can we effectively combine side-channel protection and memory safety?

- BLACKOUT: Data-Oblivious Computation with Blinded Capabilities **(CCS 2025)**

SSG@KTH

Goal: Strengthen systems security research at KTH and Sweden

Approach: with support from WASP

- Build SSG@KTH around two postdoctoral researchers
- Recruit two doctoral students to work with the postdocs
- Collaborate closely with Prof. Panos Papadimitratos / Networks Systems Security
- KTH and WASP commit to open an assistant professor position in ~2 years

Success criteria:

1. Both postdocs are compelling assistant professor candidates at top institutions
2. A new assistant professor @KTH can take over SSG@KTH

Today’s speakers (1/3)

Sebastian Szyller, SSG Alumnus

- **Assistant Professor, Aalto University**
- **AI security/privacy**

Buse Atli, SSG Alumna

- **Assistant Professor, Linköping University**
- **AI security/privacy**

Today’s speakers (2/3)

Thomas Nyman, SSG Alumnus

- **Expert, Ericsson Product Security**
- **Platform security**

Merve Gülmez, SSG Research Collaborator

- **Researcher, Ericsson Security Research**
- **Platform security**

Today’s speakers (3/3)

Panos Papadimitratos, SSG Collaborator

- **Professor, KTH**
- **Networked Systems Security**

Logistics

30 minutes for each talk including Q/A

- **Seb Szyller**
- **Buse Atli**
- **[Short 10-min break]**
- **Merve Gülmez and Thomas Nyman**
- **Panos Papadimitratos**
- **Feedback and conclusion**

Talk abstracts at https://nss.proj.kth.se/asokan_workshop.html

Refreshments at the back

https://ssg-research.github.io/