Secure Systems Groups

Demo Day 2019
N. Asokan, Tuomas Aura, Valtteri Niemi
“State of the Union”
Who are we?

Aalto University
• 2 + 1 professors
• 4 (3+1) postdocs
• Several PhD/MSc students and research interns

University of Helsinki
• 1 + 1 Professor
• 2 senior researchers
• 2 postdocs
• Several PhD/MSc students
How are we funded?

3 Academy of Finland projects:
   SecureConnect (autumn '16 → autumn '20), SELIoT (spring '17 → autumn '19), BCon (autumn '17 → autumn '20)

1 Business Finland project:
   5G-FORCE (spring '19 → autumn '20)

2 EU projects:
   FENTEC (autumn '18 → spring '21), HELIOS (Spring '19 → autumn '21)

**Intel Institute for autonomous systems security (ICRI-CARS)**
   (autumn '17 → autumn '20, successor of ICRI-SC)

Other industry funding: research gifts from Zalando and Movial

Basic funding from universities (Aalto and UH)
What do we work on?

(Mobile) Platform Security
Machine Learning and Security
Other themes: Blockchains and consensus, Stylometry and security

5G Security
Applied cryptography

Security Protocol Engineering
Network Security
Security for Ubiquitous Computing

Protocol analysis: TLS, EMV, messaging
Formal verification
Foundations of cryptography
White-box cryptography
What do we work on?

Security

Usability

Deployability/Cost
Where are we publishing?

**Top-tier infosec venues:** Usenix SEC


**Focused thematic venues:** PETS

**Other venues:** BlackHat EU, IEEE Euro S&P, ACM ASIACCS

Self evaluation: Good but room to improve
What are we teaching?

Information Security courses
• Bachelor level course on Information Security
• MSc level courses on network security, cryptography, mobile system security
• Research seminar: ML and security
• Seminar and laboratory courses
• MOOC: Cybersecurity Base with F-Secure
• Shared courses between Aalto and UH

Courses taught by industry experts
• Reverse Engineering Malware, Software Security (F-Secure)

Recognition: Best Infosec thesis in Finland
Helsinki-Aalto Center for Information Security, HAIC

Mission:

**Attract** top international master’s students to Helsinki to specialize in information security

Activities:

**Scholarships** to top students donated by HAIC industry partners

**Industry contacts**: meet-and-greet events and company visits

**Public outreach**: HAIC Talks – lectures about information security + Annual Demo Days

@haic_fi  haic.fi  http://haic.fi
HAIC in 2019

Spring 2019: Sustained collaboration with Finnish industry
  New donations by F-Secure and Huawei (HAIC donors)
  Group visits of HAIC students to partner companies
Summer 2019: 30 incoming MSc students
  2-3 HAIC scholars, 21 Erasmus Mundus scholars
Demoday 2019: Enable companies to advertise opportunities to students

Company experts available to talk to students

Call to action: donors for next year
HAIC Public Outreach

“Information security affects everyone”

Initiative launched in Autumn 2017

HAIC Talks: public lectures on contemporary topics in information security

4 HAIC Talks since Demo Day 2018

https://haic.fi/talks/

March 1, 2019: 5G Security – the What, Why and How – with Alf Zugenmaier
## Secure Systems Group, Aalto University

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>Poster</th>
<th>Demo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Misbinding Attacks on Secure Device Pairing</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>2</td>
<td>Client-side Vulnerabilities in Commercial VPNs</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Making speculative BFT Resilient with Trusted Monotonic Counters</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Tolerating Common-Mode Faults in Byzantine Consensus</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pointer Authentication: What’s the point?</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>5</td>
<td>PACStack: Authenticated Call Stack</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>6</td>
<td>PARTE: Towards Pointer Integrity with Pointer Authentication</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Hardscope: Protecting Embedded Systems Against Data-Oriented Attacks</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Designing Trust: The Historical Insight into the Emergence of Trusted Execution Environment</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>S-FaaS: Trustworthy and Accountable Function-as-a-Service Using Intel SGX</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>10</td>
<td>APOC: Attesting Properties of Containers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Amplifying IoT Honeypots with Dynamic Traffic Replay</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>12</td>
<td>Detecting E-commerce Fraud by Identifying Self-similar Purchases</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>EAT2seq: Controlled Sentence Transformation without Task-specific Training</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>14</td>
<td>ParChoice: Effective Writing Style Imitation Using Combinatorial Paraphrasing</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>15</td>
<td>Making Targeted Evasion Attacks Effective and Efficient</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>16</td>
<td>Stealing Complex DNN Models: Limitations and Defense Strategies</td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>

## Secure Systems Group, University of Helsinki

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>Poster</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>Privacy issues of autonomous shared vehicles</td>
<td>x</td>
</tr>
<tr>
<td>21</td>
<td>Privacy Preserving AKMA in 5G</td>
<td>x</td>
</tr>
<tr>
<td>22</td>
<td>Embedded UICC in 5G AKMA</td>
<td>x</td>
</tr>
<tr>
<td>23</td>
<td>Functional Encryption on FPGAs: Multi-Core Architecture for Inner-Product Computations</td>
<td>x</td>
</tr>
<tr>
<td>24</td>
<td>Privacy Preserving 2-party Queries on Bipartite Graphs with Private Set Intersection</td>
<td>x</td>
</tr>
<tr>
<td>25</td>
<td>HELIOS - a Context-aware Distributed Social Networking Platform</td>
<td>x</td>
</tr>
</tbody>
</table>
Visitors: Cryptography group & Ambient Intelligence group, Aalto University

<table>
<thead>
<tr>
<th>Number</th>
<th>Title</th>
<th>Poster</th>
<th>Demo</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>White-box Cryptography</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>18</td>
<td>Collaborative Learning with Private Data and Binary Feedback</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>19</td>
<td>Closed Eye Gaze Gestures: Detection and Recognition of Closed-Eye Movements with Cameras in Smart Glasses</td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Change is Constant
N. Asokan

Professor and Cheriton Chair at University of Waterloo, from September 2019

Adjunct Professor, Aalto University (Sep 2019 – Aug 2024)
• Mobile Systems Security course, Spring 2020
• Graduating remaining doctoral students
• …
Janne Lindqvist

Currently, Associate Professor, Rutgers
https://www.lindqvistlab.org/

Appointed Associate Professor at Aalto, from Jan 2020
  HCI, security engineering, ...

Director of HAIC, from Jan 2020

Will visit Aalto in Fall 2019
Jan-Erik Ekberg

Appointed (part-time) Adjunct Professor from Nov 2018

Platform security
Lachlan Gunn

Appointed Secure Systems Group co-leader, from Sep 2019

Responsible for leading the “Platform security” theme
Samuel Marchal

Appointed (part-time) Research Fellow, from Sep 2019

Responsible for leading the “Machine Learning and Security” theme
Systems Security Professor-of-Practice

On-going call for Professor-of-Practice
(5-year term)

Decision expected in Autumn 2019
Logistics for the day
Logistics for today

For all:
Demos/posters downstairs at the library starting at 14:00

Follow volunteers

Coffee served by the library during the afternoon

For students:
Volunteers from companies are here to tell you about
  - internships
  - thesis positions
  - other opportunities