FELIPE BOEIRA

Security Researcher

PROFILE

I am a security researcher currently enrolled as a PhD candidate in the Computer Science Graduate School at Linköping University, Sweden. I have a combination of industry and academic experiences, which ranges from ethical hacking to formal verification of security properties in the context of cryptographic protocols and software security.

CONTACT

PHONE NUMBER:
+46 76 555 62 91

WEBSITE:
http://felipeboeira.eu

LINKEDIN:
https://www.linkedin.com/in/fboeira/

EMAIL ADDRESS:
felipecboeira@gmail.com

LANGUAGES

English - Fluent
Portuguese – Native
Spanish – Basic
Swedish – Basic

EDUCATION

Linköping University (Sweden)
2018-present (Expected defence in September 2023)
PhD in Computer Science

Universidade Federal do Rio Grande do Sul (Brazil)
2016-2018
MSc in Computer Science

Universidade do Vale do Rio dos Sinos (Brazil)
2009-2012
Major in Information Security

HIGHLIGHTED ACHIEVEMENTS

- I have been a speaker within the security community in events such as Blackhat São Paulo and Hackers to Hackers Conference (H2HC)
- I have recently presented my research paper in a prestigious conference in formal methods for security in Haifa, Israel
- In Samsung, I helped to design and implement a security subsystem for the Linux Kernel that is now integrated into flagship smartphones
- Using a threat modelling methodology, I have identified a weakness in 5G networks, designed and formally verified a security solution which is accepted for publication

ACADEMIC WORK EXPERIENCE

Linköping University – PhD Candidate
2018-2023
Focused on security research of vehicular and 5G mobile networks employing threat modelling and formal methods to the analysis of cryptographic protocols. Furthermore, I am involved in teaching courses and supervising Bachelor's/Master's theses.

University of California Irvine – Visiting Security Researcher
Sep-Dec 2022
In this collaboration I have been working on a formally verified implementation of task availability for safety-critical systems.

Halmstad University/Linköping University – Research Engineer
2017-2018
Security research on position falsification attacks and mitigations in the automotive domain.

INDUSTRY WORK EXPERIENCE

Samsung Electronics – Security Researcher
2013-2017
Involved with security Research & Development on mobile devices, wearable devices, and Internet of Things. I have performed security analyses of protocols to identify weaknesses and propose mitigations, worked with personal data leakage prevention and mobile privacy, reverse-engineered Android malware to identify its *modus operandi* and designed novel security solutions. Our main project is now integrated into flagship smartphones to increase resilience against malicious exploitation.

Defenda – Penetration Tester (Ethical Hacker)
2012-2013
I have worked with large organizations performing security assessments of applications and network infrastructures to exploit vulnerabilities and provide recommendations to mitigate security risks. I was involved with discussing the outcomes of the penetration tests with the responsible teams for the implementation of countermeasures. In this position, I was Certified Ethical Hacker v7 (CEH) by EC-Council.

Defenda – Cyberfraud Incident Response
2010-2012
I responded to cyberfraud incidents related to phishing and malware distribution to shut down the attackers. This involved Brazilian organizations in the areas of finance, health, and airline companies, as well as governmental entities.

TRAINING

Android Application Hacking - Pentesting Mobile Apps – **Blackhat USA 2014**
Offensive Internet of Things (IoT) Exploitation – **Blackhat USA 2015**
Exploit Laboratory: Master – **Blackhat USA 2016**

PATENTS

Method for multi-factor transaction authentication using wearable devices
US 20160086176 A1 and BR 10 2014 023229-0, 5 inventors including myself

Method to compare binary files
BR 10 2014 026608 9, 6 inventors including myself

Method for providing a secure mode for mobile applications
US 15/167,270, 5 inventors including myself

SELECTED PUBLICATIONS/PRESENTATIONS

Provable Non-Frameability for 5G Lawful Interception
16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) - May 2023
Felipe Boeira, Mikael Asplund, and Marinho Barcellos

Towards Self-Monitoring Enclaves: Side-Channel Detection using Performance Counters
NordSec 2022
David Lantz, Felipe Boeira, Mikael Asplund

Exploiting Partial Order of Keys to Verify Security of a Vehicular Group Protocol
35th IEEE Computer Security Foundations Symposium (CSF) - August 2022
Felipe Boeira, Mikael Asplund

No Doppelgänger: Advancing Mobile Networks Against Impersonation in Adversarial Scenarios
15th ACM Conference on Security and Privacy in Wireless and Mobile Networks - May 2022
Felipe Boeira, Mikael Asplund, and Marinho Barcellos

Decentralized Proof of Location in Vehicular Ad Hoc Networks
Elsevier Computer Communications - November 2019
Felipe Boeira, Mikael Asplund, and Marinho Barcellos

Mitigating Position Falsification Attacks in Vehicular Platooning
IEEE Vehicular Networking Conference (VNC) - November 2018
Felipe Boeira, Mikael Asplund, and Marinho Barcellos

Effects of Colluding Sybil Nodes in Message Falsification Attacks for Vehicular Platooning
IEEE Vehicular Networking Conference (VNC) - November 2017
Felipe Boeira, Marinho Barcellos, Edison P. de Freitas, Alexey Vinel and Mikael Asplund

On the Impact of Sybil Attacks in Cooperative Driving Scenarios
IFIP Networking - June 2017
Felipe Boeira, Marinho Barcellos, Edison P. de Freitas, Alexey Vinel and Mikael Asplund

Android Resiliency Defense Strategy
H2HC (Hackers to Hackers Conference) - October 2016
Felipe Boeira

Yet Another Android Security Feature
Blackhat SP - November 2014
Felipe Boeira, Breno Silva

Defeat Android Kernel Exploitation
H2HC (Hackers to Hackers Conference) - October 2014
Felipe Boeira, Breno Silva