Titouan Lazard

http://perso.eleves.ens-rennes.fr/people/titouan.lazard/

Education

2017–2019 **Master and Magister of Science in Computer Science**, *ENS / Universite de Rennes 1*, Rennes.
Research in Computer Science

2016–2017 **Bachelor of Science in computer Science**, *Université de Rennes 1*.
Computer Science

2014–2016 **DUT in IT**, *IUT*, Orléans.
Learning Software developpement and conception. The DUT is a two year cursus, focused on practice.

Experiences

2019-2020 **HP Labs Research Engeneer**, *HP Labs* , Bristol, United Kingdom.
I work on the PCIe security DMA Attack and IOMMU protections.

2019 **Internship in the HP Security Lab**, *HP Labs*, Bristol, United Kingdom.
I worked on the security of PCIe components and their interaction with the main platform.

2018 **Internship for first year of Master**, *FAU*, Erlangen, Germany.
Developpement of TEEShift, a tool to selectively shift function of a compiled software into a Trusted Execution Environment to insure Code Confidentiality. It leads to a publication at SysTEX 2018 and a Best Paper Award: https://doi.org/10.1145/3268935.3268938

2017 **Internship for Bachelor's**, *Orange Cyberdéfense*, Rennes, 3 months.
I mainly did Pentest (Penetration Testing). I tested security of websites and IoT devices like smartligth. I also did some Reverse Engineering on Android and iOS applications.

2016 **Internship for DUT**, *INSA Centre val-de-loire (College of engeneering)*, Bourges, 2 months.
I worked on virtualization system for students workspaces. I also created and administrated an ELK server to manage logs from different devices in the school network.

Skills and Interest

Low Level Security — I am interested in low level software security such as Operating systems and Firmware. I practiced DMA attack over PCIe during my work at HP.

Hardware Assisted security — I like to explore the combination of hardware and software, more specifically, when software security relies on modern hardware security features like TPM or Trusted Execution Environment (Intel SGX, ARM TrustZone).

Challenges — I am contributor and administrator of the challenge platform Root-Me.