We can apply **network protocol analysis** techniques to analyze automatically the **security of Internet of Things devices**.

Automated Security Analysis for Real-World IoT Devices

Lelio Brun, Ichiro Hasuo, Yasushi Ono, Taro Sekiyama

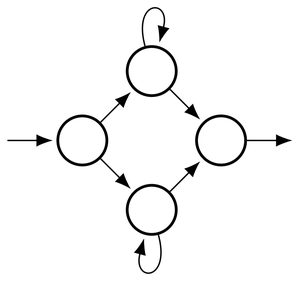
Introduction

- IoT devices are everywhere
- Security is important
- Automatic analysis with the Tamarin model checker

Method

Modeling protocols and verifying security properties with Tamarin

Model:



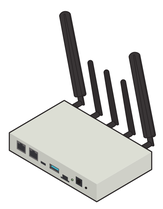
Properties:

$$\begin{cases} \phi = \forall \ldots \exists \ldots \\ \psi = \forall \ldots \\ \zeta = \exists \ldots \end{cases}$$

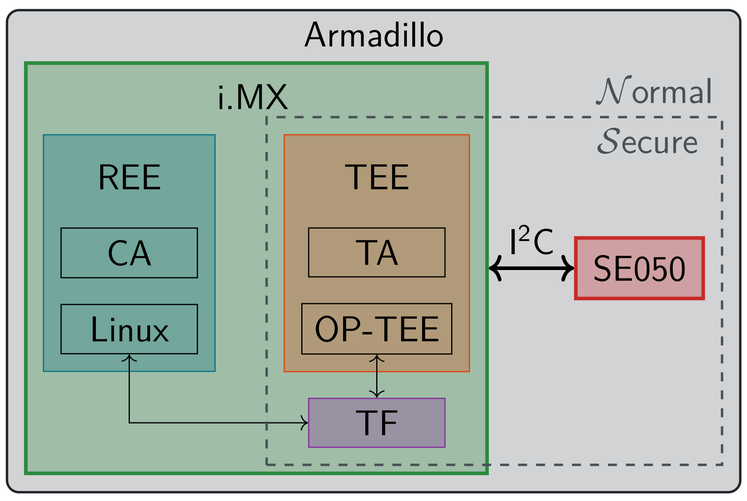
Verification:

$$\begin{cases} \phi & \checkmark \\ \psi & \times \\ \zeta & \infty \end{cases}$$

Case study



The Armadillo-IoT G4 device for high performance AI



Model:

1. Binding process
2. Key derivation
3. TA execution

Properties: Authentication and secrecy

Verification: 15s – 150s

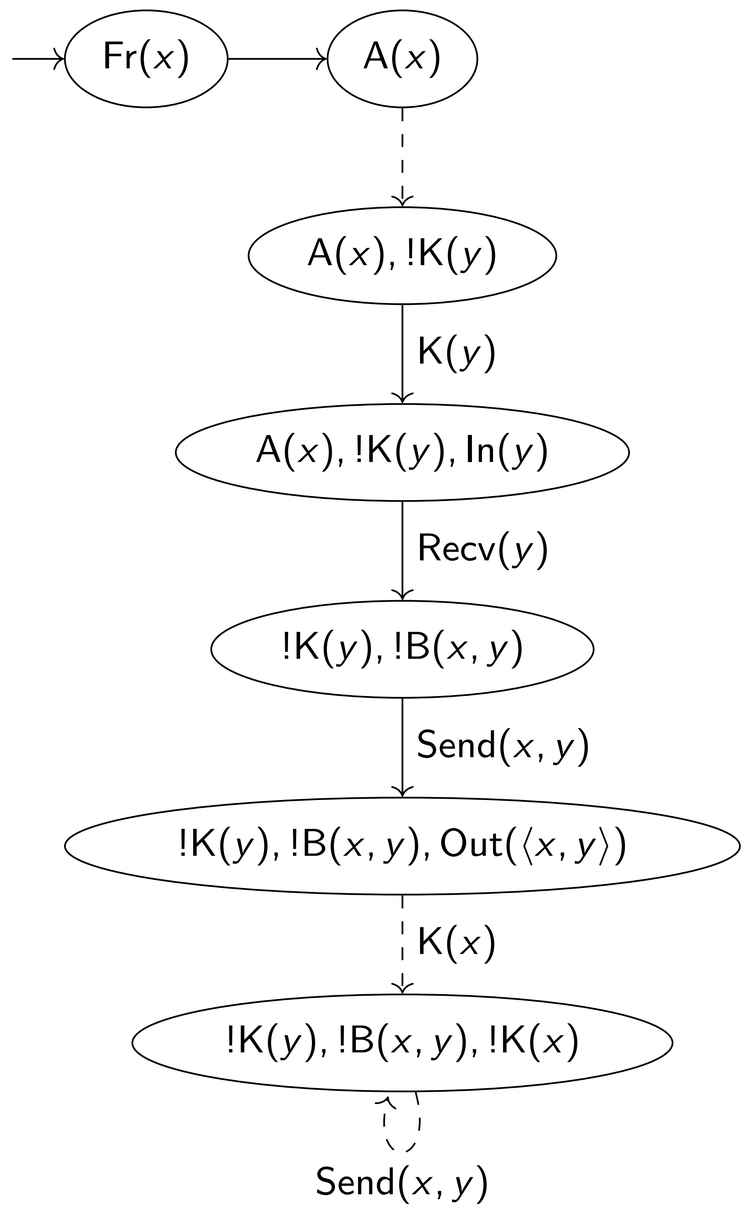
Extra figures

$$\frac{}{\mathsf{Fr}(x)} \qquad \frac{\mathsf{Out}(x)}{!\mathsf{K}(x)} \qquad \frac{!\mathsf{K}(x)}{\mathsf{In}(x)}[\mathsf{K}(x)]$$

$$\frac{\mathsf{Fr}(x)}{!\mathsf{K}(x)} \qquad \frac{!\mathsf{K}(x_1) \cdots !\mathsf{K}(x_n)}{!\mathsf{K}(f(x_1, \ldots, x_n))}$$

$$\frac{\mathsf{Fr}(x)}{\mathsf{A}(x)} \qquad \frac{\mathsf{In}(y) \qquad \mathsf{A}(x)}{!\mathsf{B}(x,y)}[\mathsf{Recv}(y)]$$

$$\frac{!\mathsf{B}(x,y)}{\mathsf{Out}(\langle x,y\rangle)}[\mathsf{Send}(x,y)]$$



National Institute of Informatics
Information Systems Architecture Science Research Division
ZT-IoT project – https://zt-iot.nii.ac.jp
lelio_brun@nii.ac.jp

download the full paper