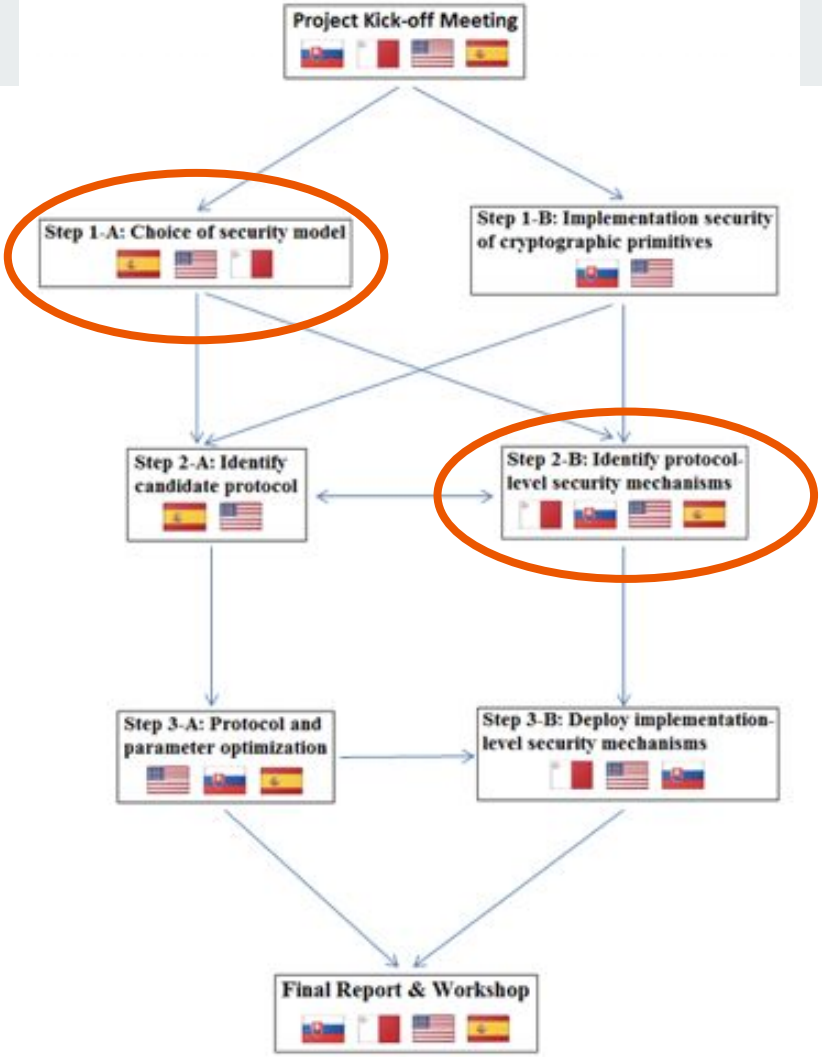
The Proposed Runtime Verification Setup for Cryptographic Protocol Execution

Secure Communication in the Quantum Era (SPS G5448)
Smolenice Project Meeting, March 2020

L-Università
ta' Malta



L-Università ta' Malta

NATO OTAN

Cryptographic Protocols

Design

Proofs to validate design against threat models

Implementation

Difficult to make it fully secure…
So many things can go wrong!

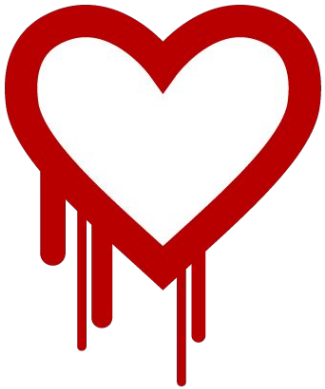
Cryptographic Protocols

Design

Proofs to validate design against threat models

Implementation

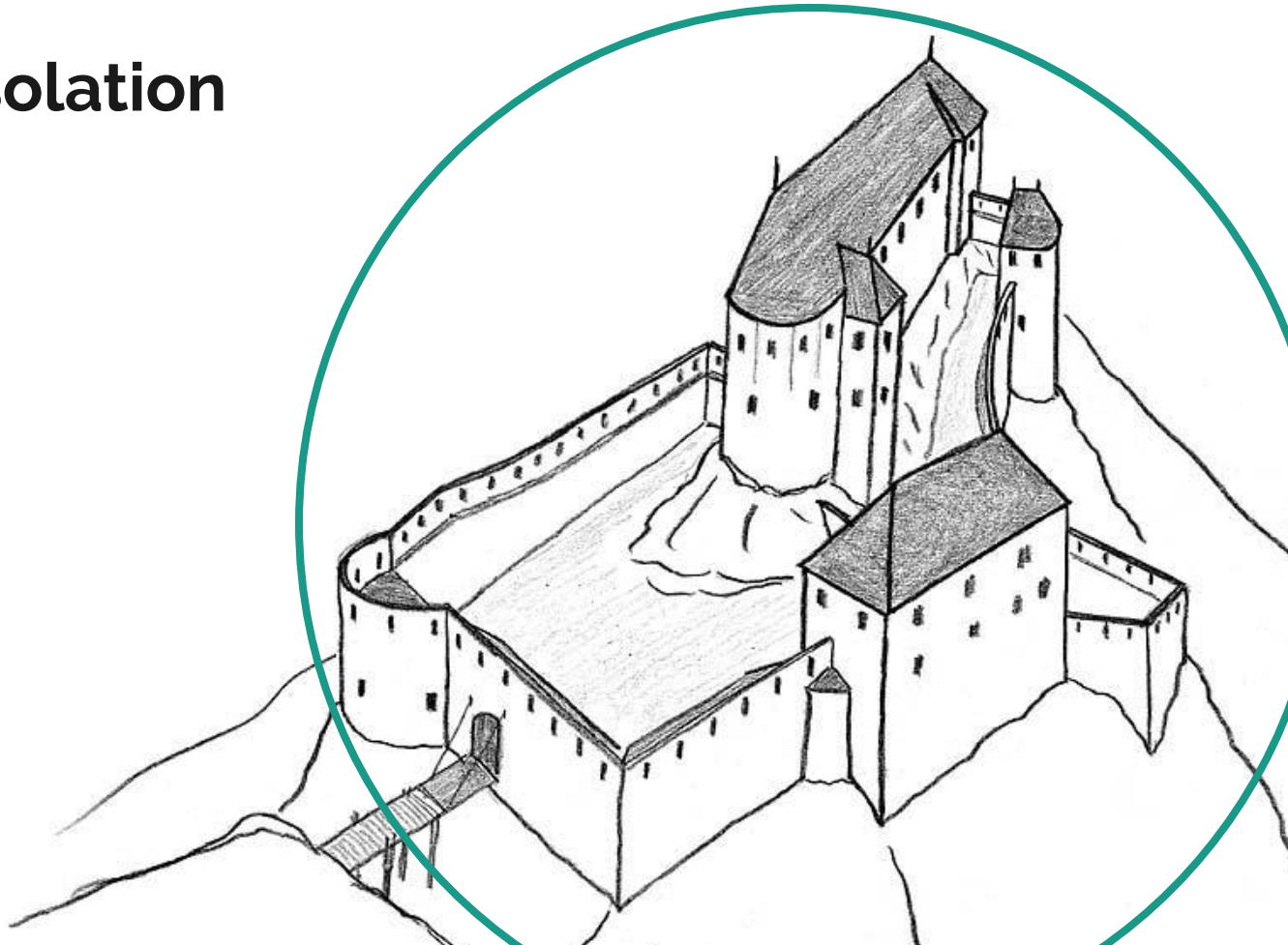
Difficult to make it fully secure…
So many things can go wrong!



Many things can go wrong on many different levels

(High level) Wrong protocol implementation	The protocol implementation might deviate from the verified (theoretical) design
Medium level threats	Malware, Data leaks, etc
Low level threats	Arithmetic overflows, undefined downcasts, and invalid pointer references
Hardware	Can hardware be trusted? Side Channel attacks?

Concept 1: Isolation



L-Università ta' Malta

Concept 1: Isolation

Medium level

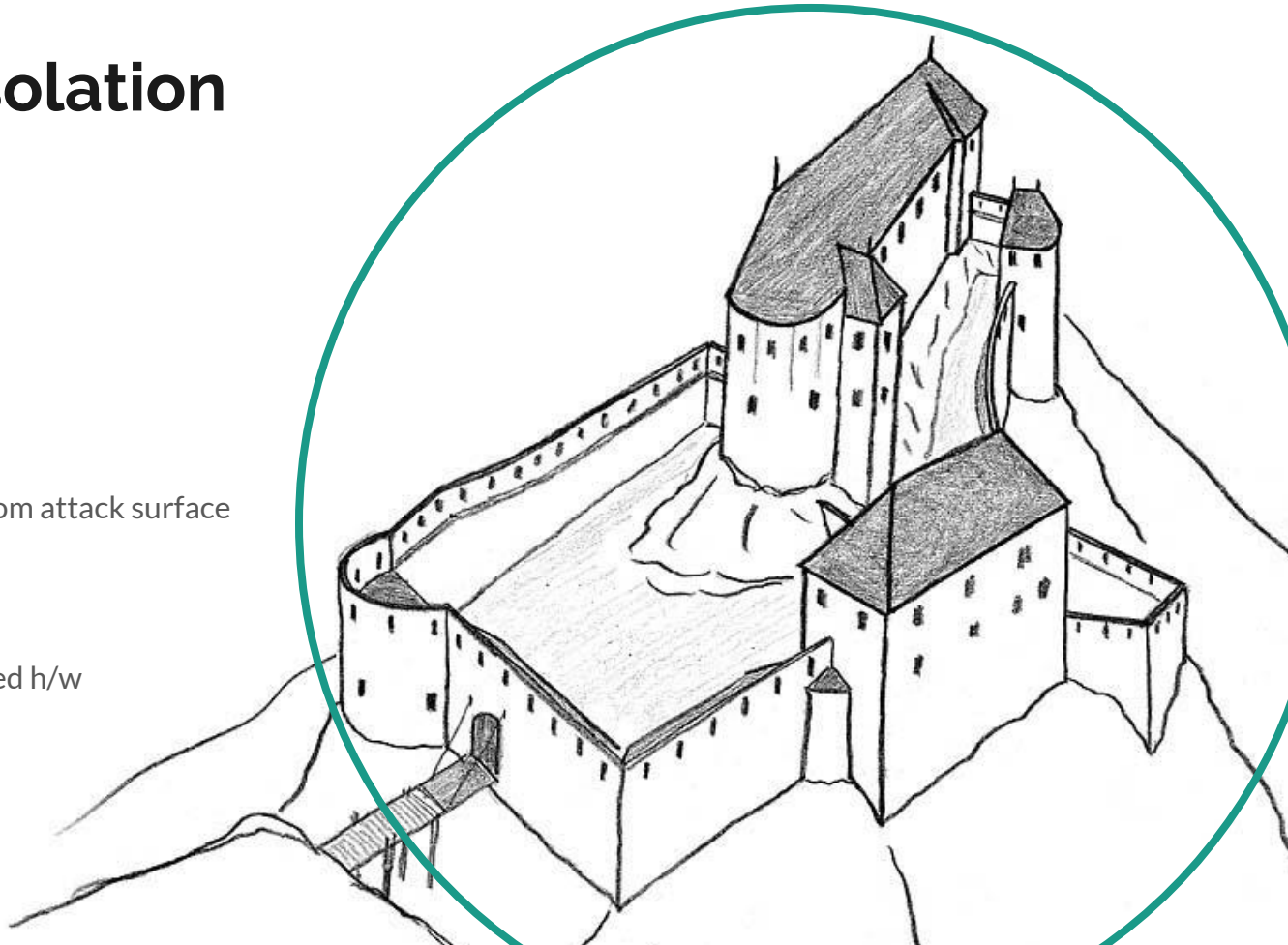
- Crypto keys

Low level

- Hide memory errors from attack surface

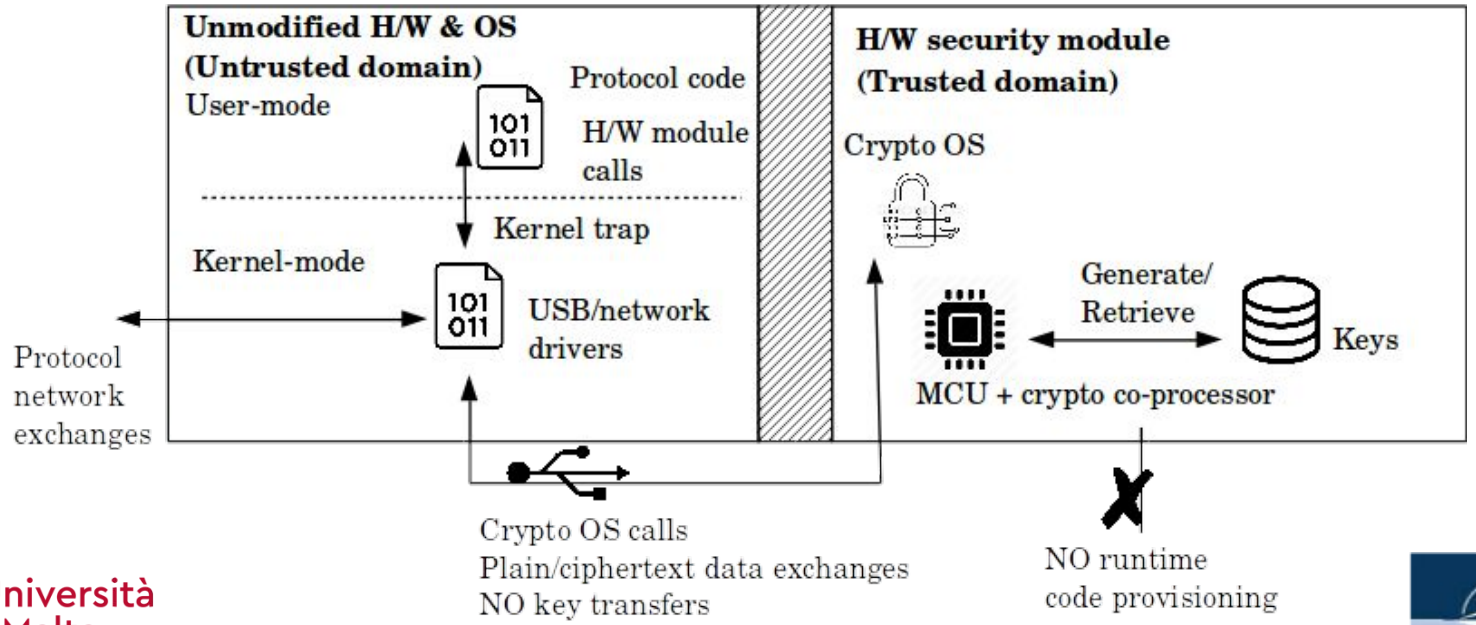
Hardware

- Bring-your-own certified h/w

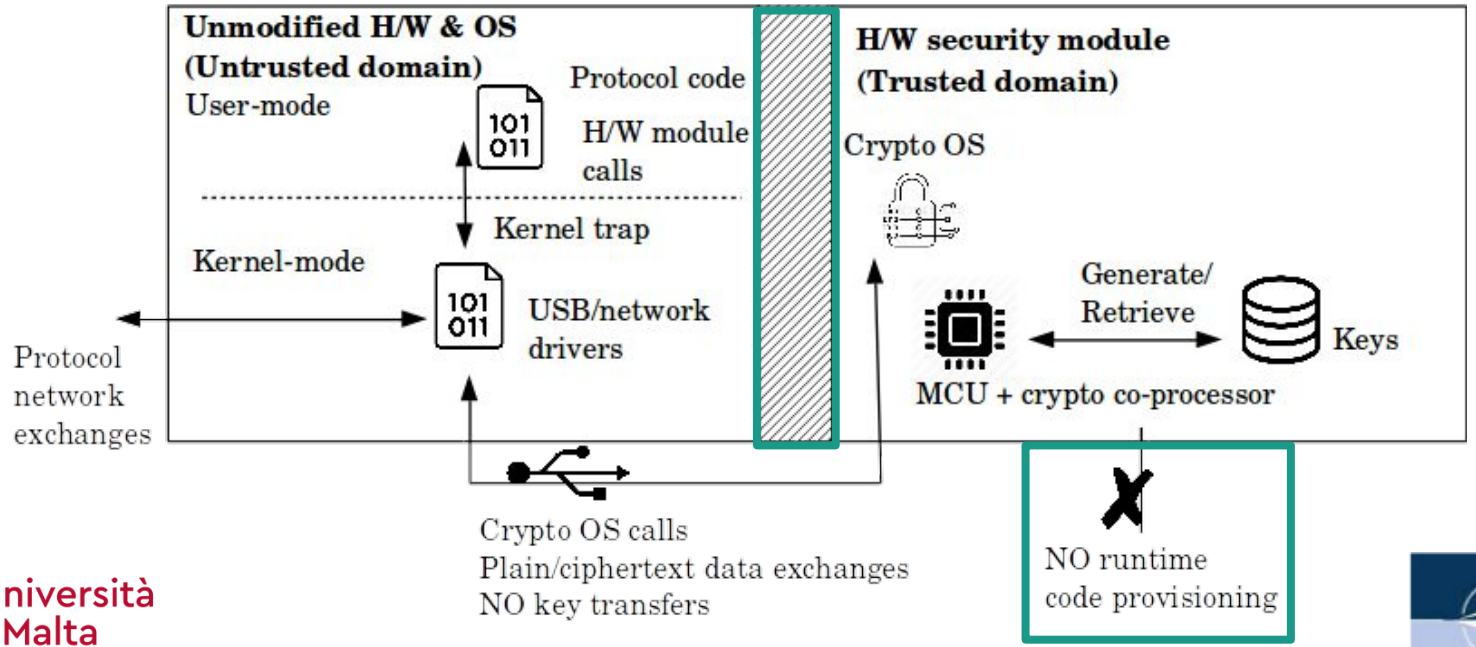


L-Università ta' Malta

Concept 1: Isolation



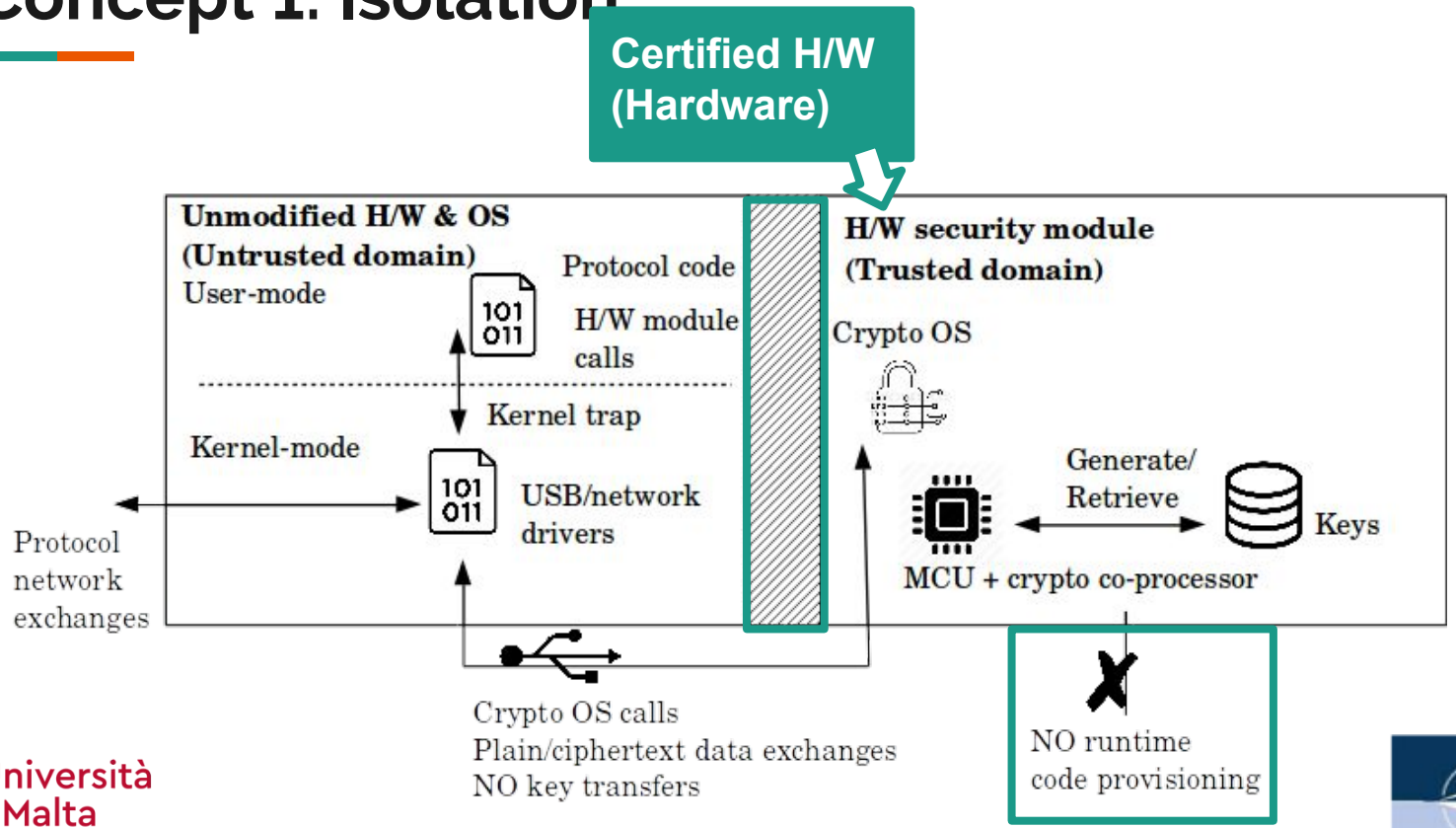
Concept 1: Isolation



L-Università ta' Malta

NATO OTAN

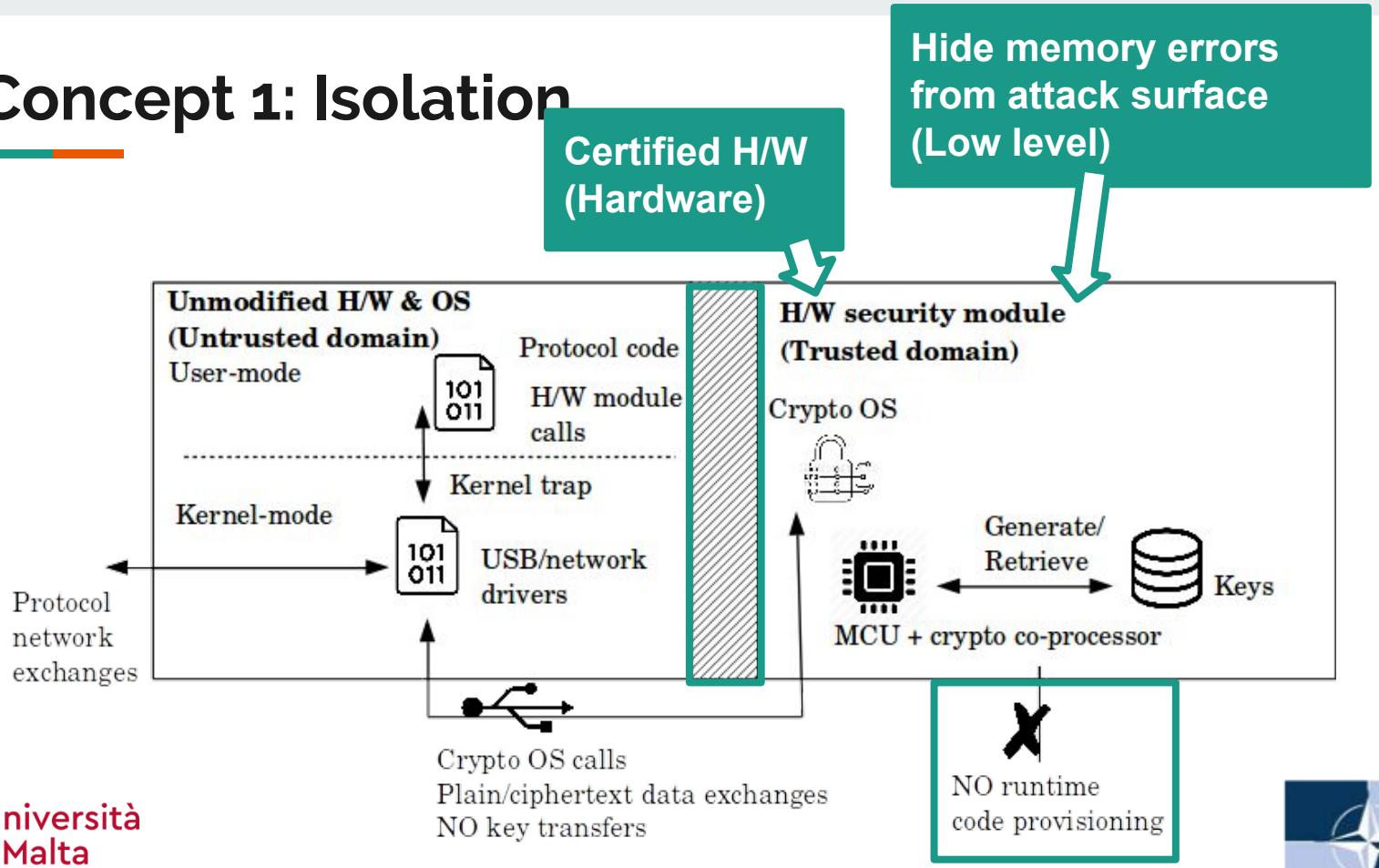
Concept 1: Isolation



L-Università ta' Malta

NATO OTAN

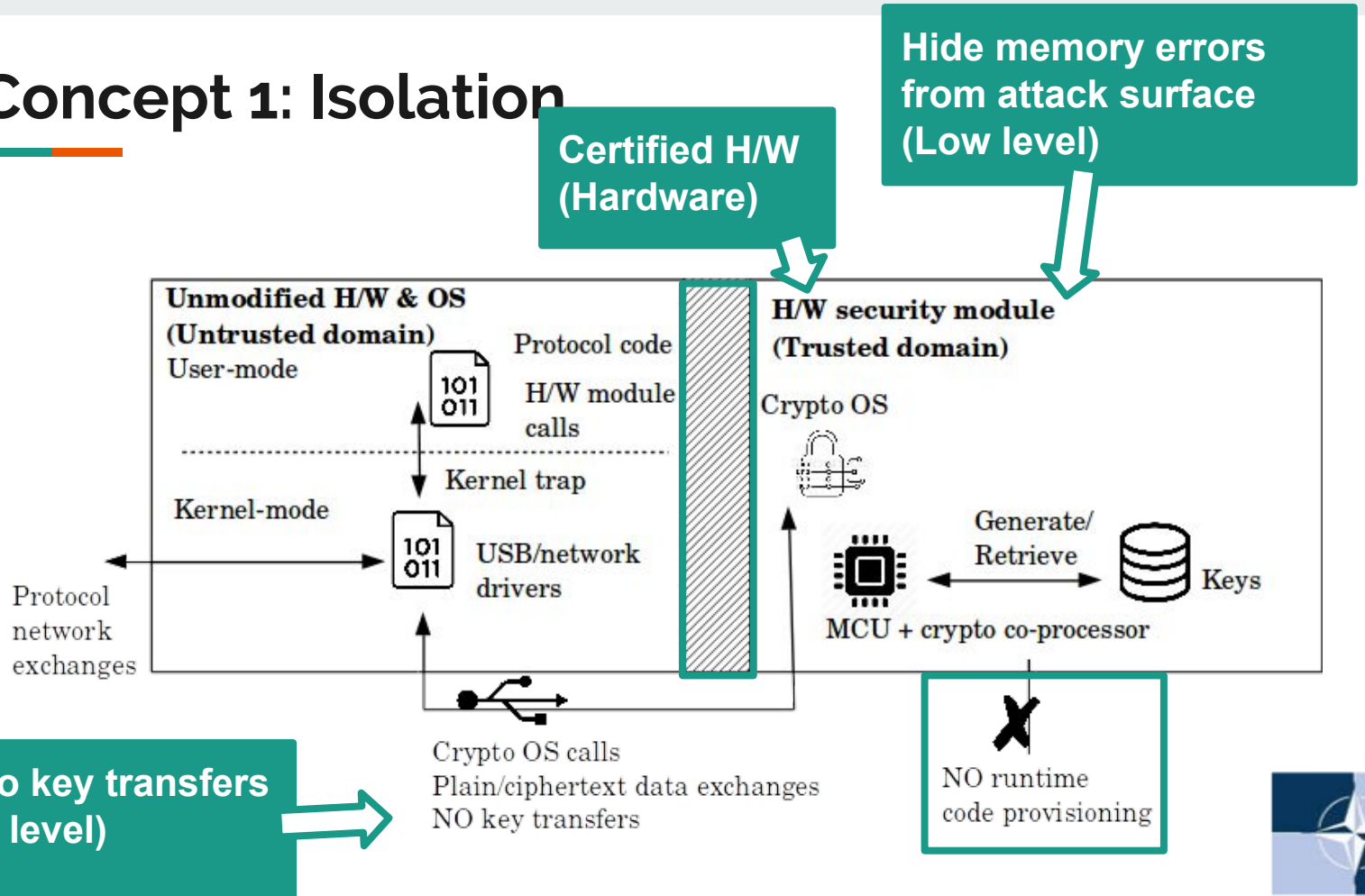
Concept 1: Isolation



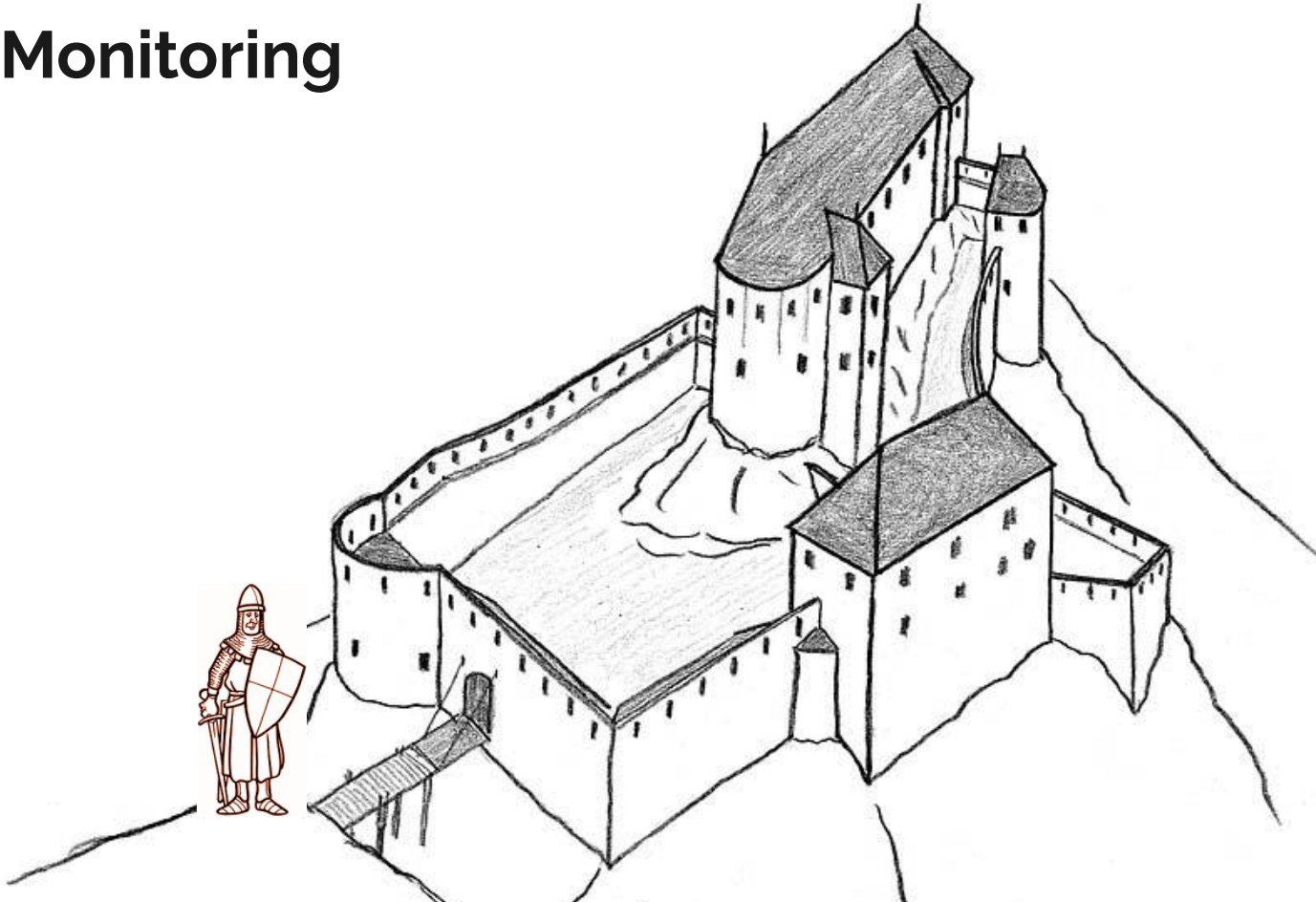
L-Università ta' Malta

NATO OTAN

Concept 1: Isolation



Concept 2: Monitoring



L-Università ta' Malta

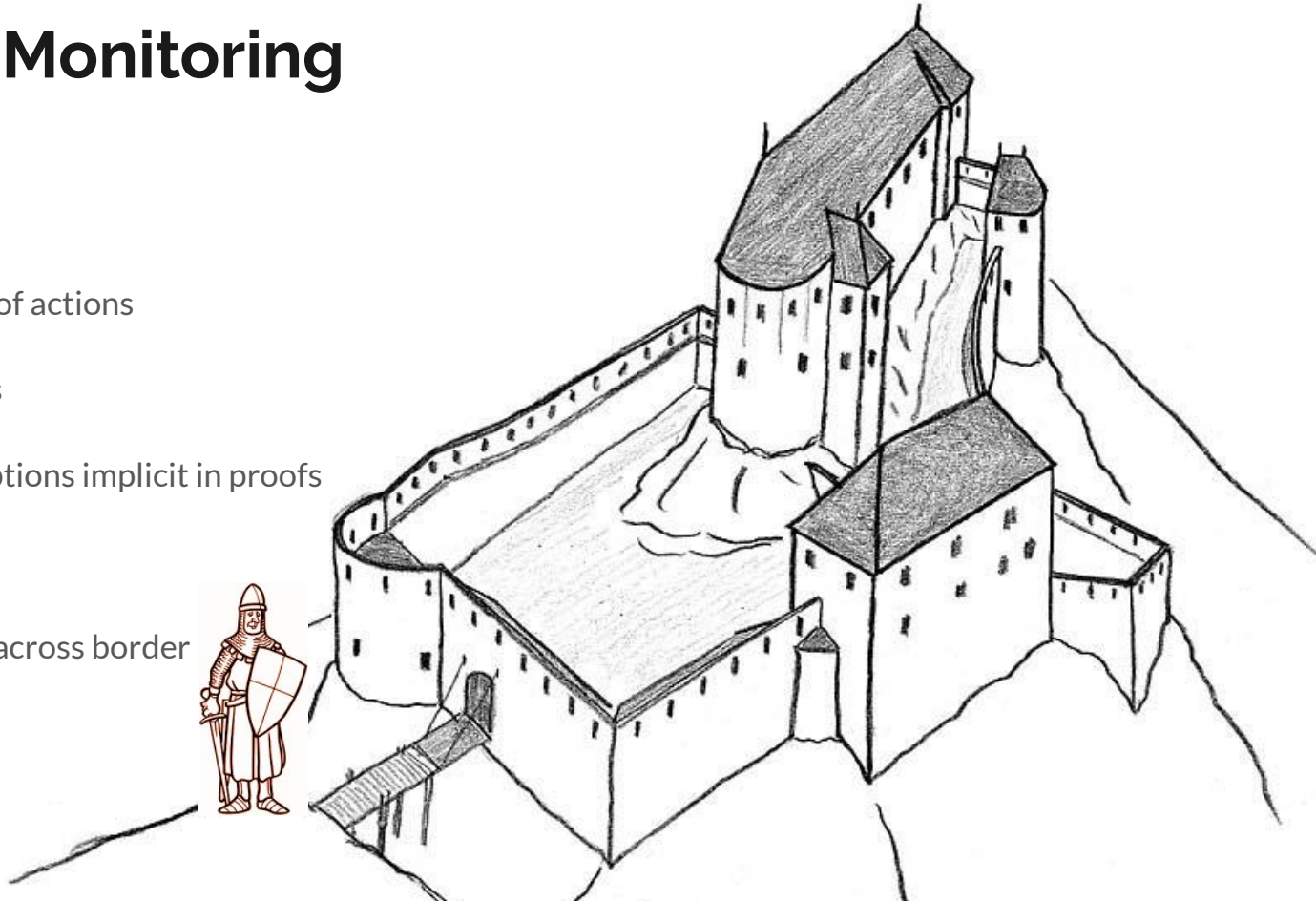
Concept 2: Monitoring

High level

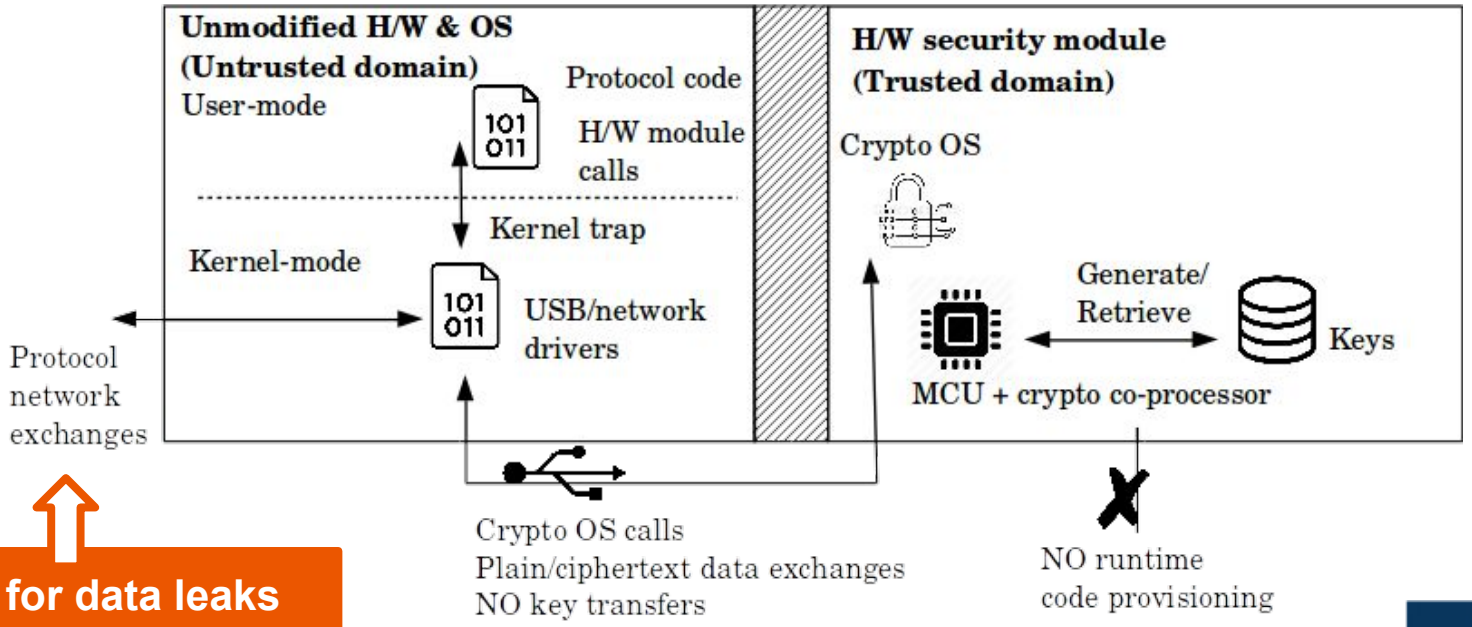
- Check sequences of actions
- Check parameters
- Check any assumptions implicit in proofs

Low level

- Plaintext leakage across border

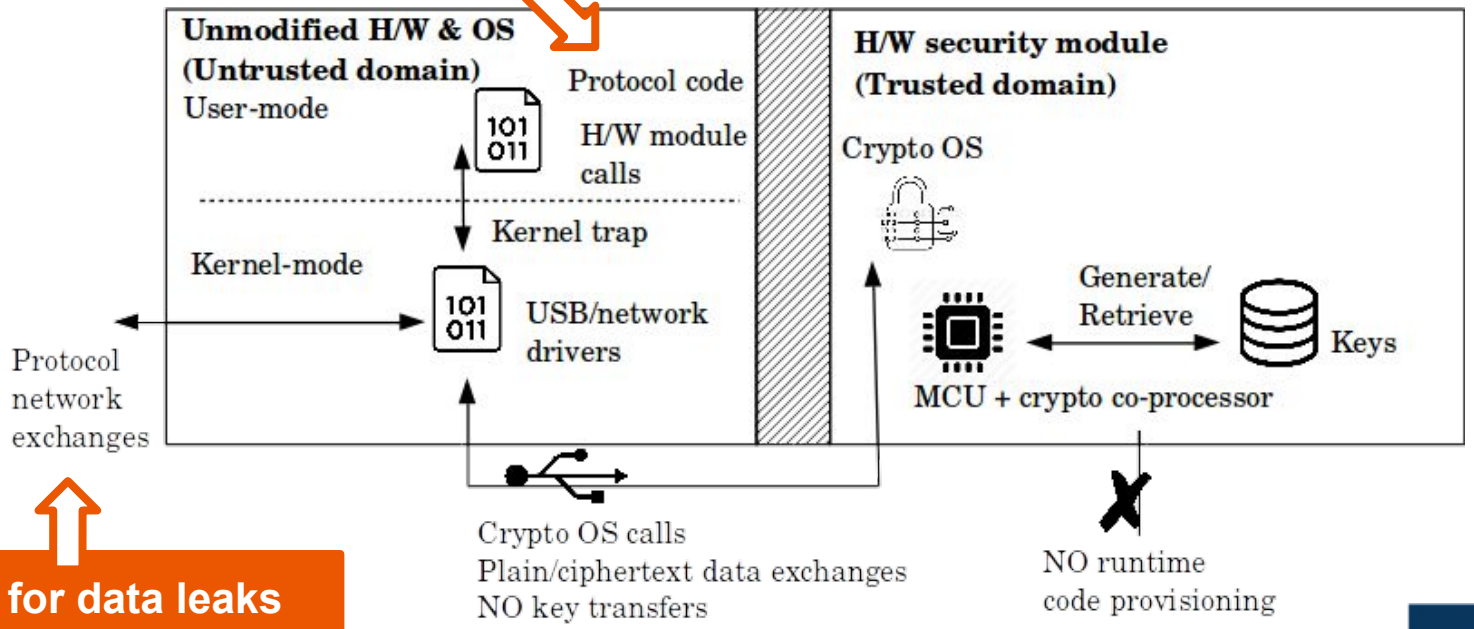


L-Università ta' Malta



Monitor for data leaks (Medium level)

Monitor code while executing (High level)

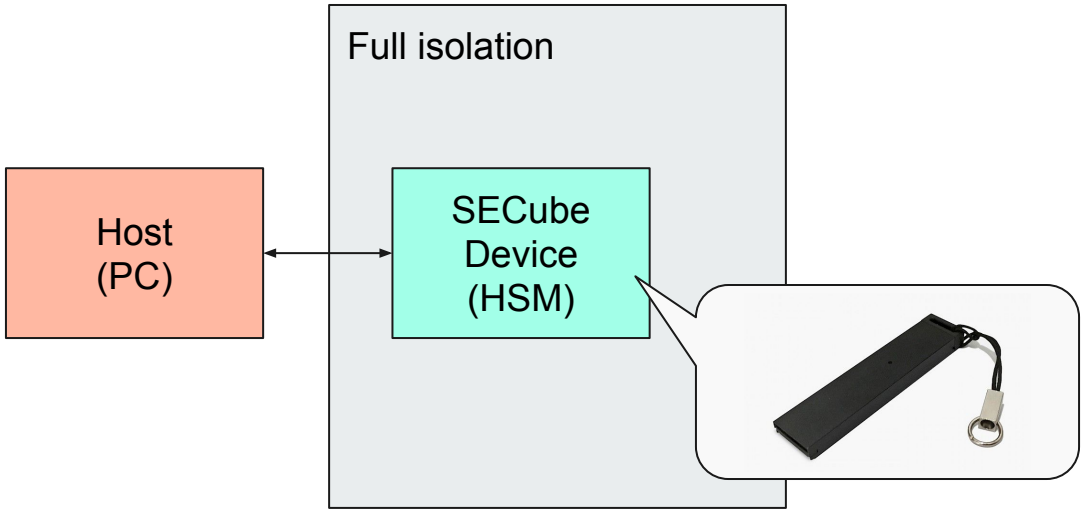


Monitor for data leaks (Medium level)

NATO OTAN

How does it look in practice?

Hardware Security Module



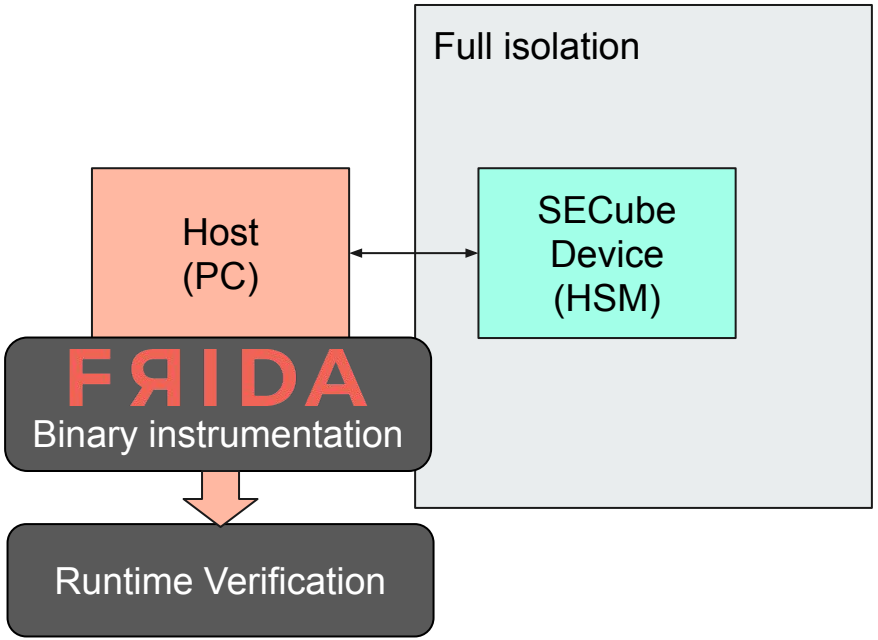
Hardware Security Module

SECube-deployed code

- No service backdoors
- No automatic software updates
- Even if somehow an attack is successful, isolation makes it hard to smuggle the information out

NATO-cleared hardware

Architecture



Why Runtime Verification?

It works at runtime and

- Logically separate from the rest of the system code
- Automatically synthesised from mathematical description
- Attempts to keep overheads to a minimum

High level monitors

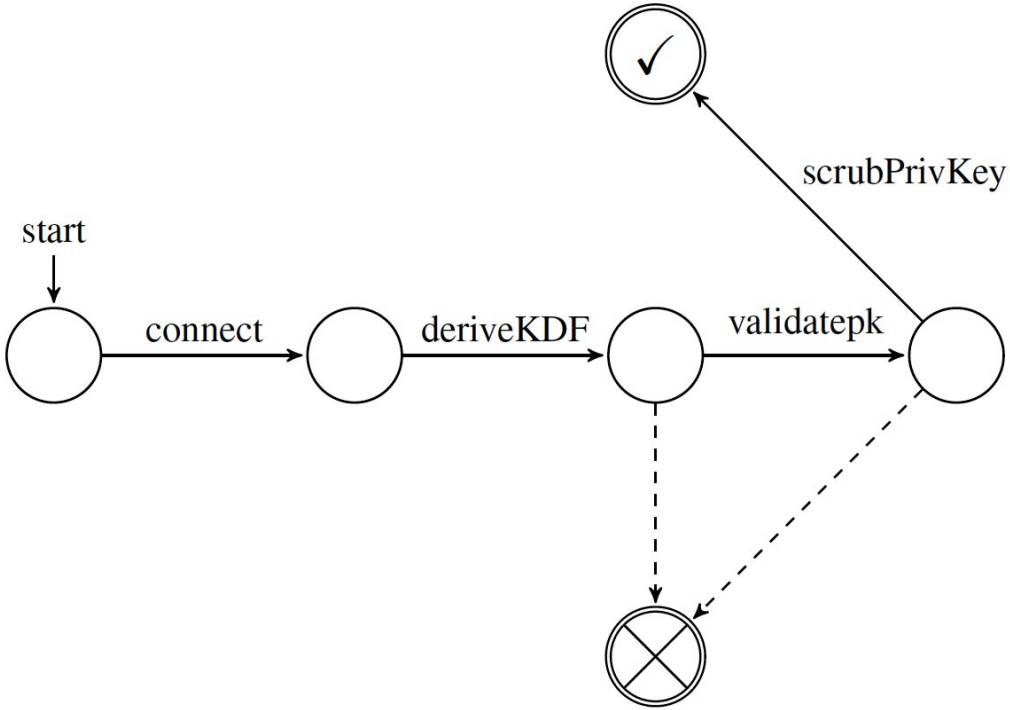
Sequence of actions (according to protocol design)

Valid parameters

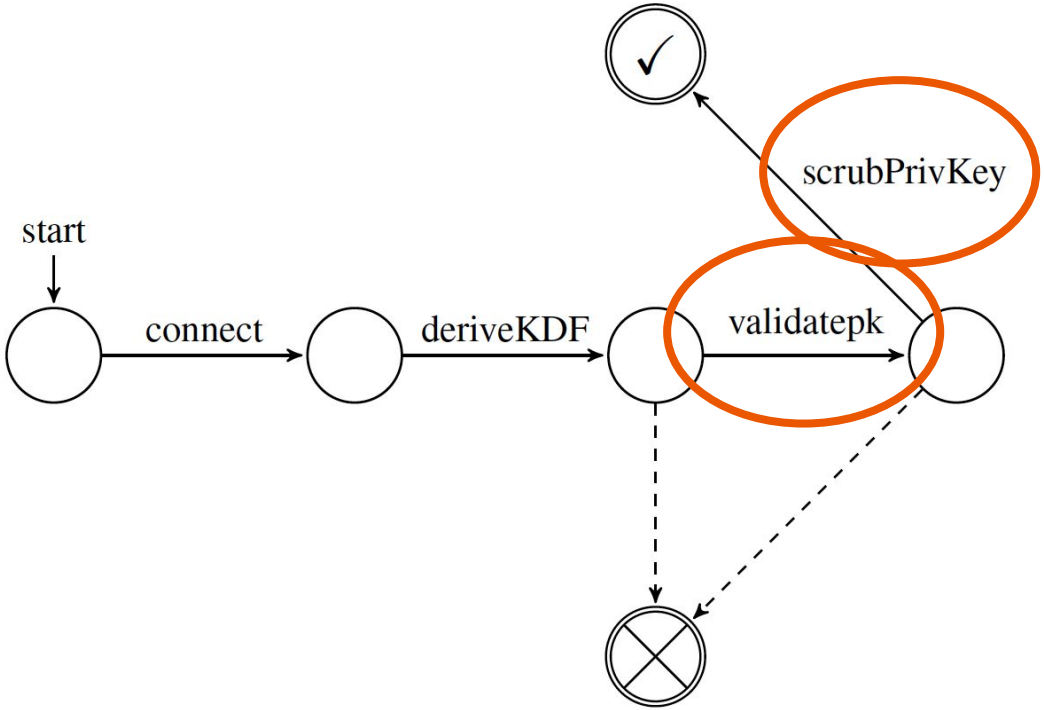
Valid returns values

Data is wiped after use

Monitoring language and experiments



Monitoring language and experiments



Data Leaks Monitors

Successfully detected plaintext from the USB communication

Simulated malware attack trying to smuggle plaintext out

Checking all outflows for any leaks of the plaintext

Data Leaks Monitors

Successfully detected plaintext from the USB communication

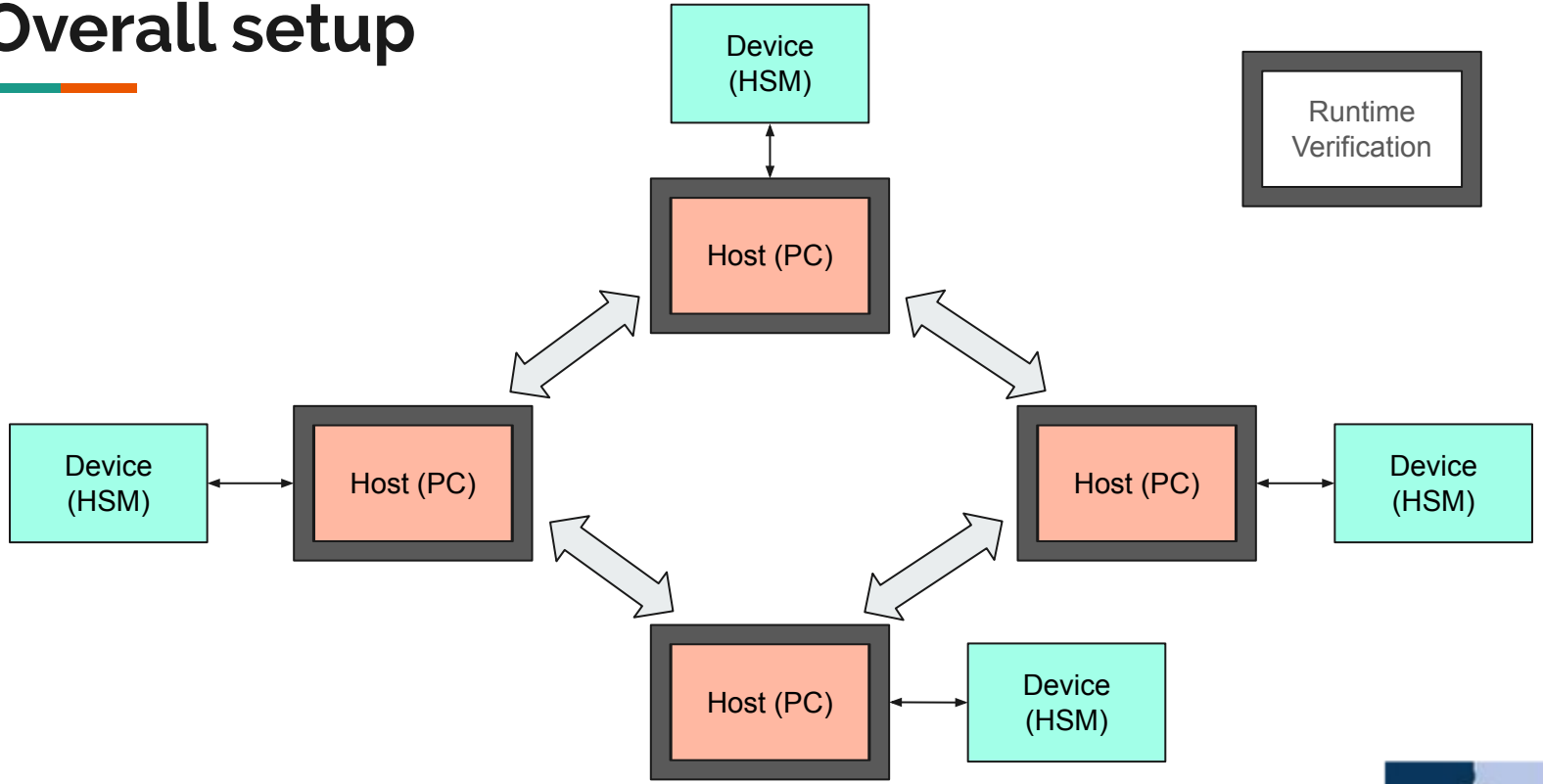
Simulated malware attack trying to smuggle plaintext out

Checking all outflows for any leaks of the plaintext

L-Università ta' Malta

NATO OTAN

Overall setup



L-Università ta' Malta

NATO OTAN

Updates on Dissemination and other activities

New Additions to our Research Team

Christian Colombo

Mark Vella

Robert Abela

Jennifer Bellizzi

Yonas Leguesse

L-Università ta' Malta

NATO OTAN

Visits

Peter Špaček 4-month visit in Malta

Slovak team visit to Malta for 1 week

More details in following presentations

L-Università ta' Malta

NATO OTAN

Publications and Presentations

COLOMBO, C. - VELLA, M.: **Towards a Comprehensive Solution for Secure Cryptographic Protocol Execution based on Runtime Verification**. In: 4th International Workshop on FORmal methods for Security Engineering (FORSE), Valletta, Malta, 2020.

COLOMBO, C. - VELLA, M.: **Secure Cryptographic Protocol Execution based on Runtime Verification.** Talk at Cybersecurity Conference, ESkills Foundation, Malta, February 2020.

ŠPAČEK, P. - COLOMBO, C. - VELLA, M.: **Using TEE and RV in PQ-TLS Communication**. Computer Science Annual Workshop. Department of Computer Science. University of Malta. 2019.

Other Dissemination

Christian Colombo on **radio programme in Maltese** focusing on online security, featured on Radio Mocha Malta.

ŠPAČEK, P. - COLOMBO, C. - VELLA, M.: **Combining HSM and RV to secure communication.** Talk at the Department of Computer Science. University of Malta. 2019.

Video production in progress to explain the concepts to the general public.