The Cyber Research Domain: From Threat, to Tool, to Training

University of Malta
MCAST

Introduction

Threats | Tools | Training

Introduction

Threats → Tools → Training

Ransomware attack vectors

Uptake in Phishing

- In recent years, especially post-Covid, we saw an uptake in phishing attempts.
- Locally several campaigns targeted clients of couriers, banks, telecom companies, airlines, etc. with some even making headline news.
- In June, a Malta Police press release stated that "Scammers conned €50,000 from 40 people in one day".

Ħlas tat-tbaħħir mhux imħallas, Biex thallas dan issa żur: https://bit.ly/3xrrkfd jekk ma thallasx dan il-pakkett tieghek jiġi rritornat lil min jibgħat

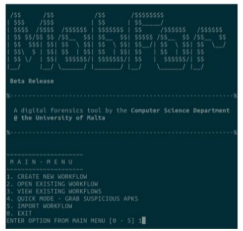
INFO
Ikseb kitts ta 'trazzin b'xejn kontra l-epidemija COVID-19 mill-Ministeru tas-Sahha https://bit.ly/covid09-MT

RV-TEE - NATO Project

MobFor (i)

MobFor is a tool, developed by the University of Malta, to assist investigators in gathering evidence related to possible unlawful interception attacks via popular messaging apps e.g. Whatsapp, Telegram, Signal and PushBullet.

https://mobfor.gitlab.io/mobfor-pages/



This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

NATO OTAN

Introduction

Threats → Tools → Training

Ransomware attack vectors

Uptake in Phishing

- In recent years, especially post-Covid, we saw an uptake in phishing attempts.
- Locally several campaigns targeted clients of couriers, banks, telecom companies, airlines, etc. with some even making headline news.
- In June, a Malta Police press release stated that "Scammers conned €50,000 from 40 people in one day".

Ħlas tat-tbaħħir mhux imħallas, Biex thallas dan issa żur: https://bit.ly/3xrrkfd jekk ma thallasx dan il-pakkett tieghek jiġi rritornat lil min jibgħat

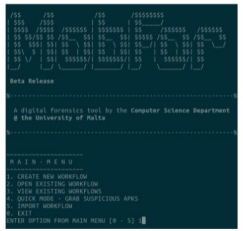
INFO
Ikseb kitts ta 'trazzin b'xejn kontra l-epidemija COVID-19 mill-Ministeru tas-Sahha
https://bit.ly/covid09-MT

RV-TEE - NATO Project

MobFor (i)

MobFor is a tool, developed by the University of Malta, to assist investigators in gathering evidence related to possible unlawful interception attacks via popular messaging apps e.g. Whatsapp, Telegram, Signal and PushBullet.

https://mobfor.gitlab.io/mobfor-pages/



This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

Getting into Cybersecurity

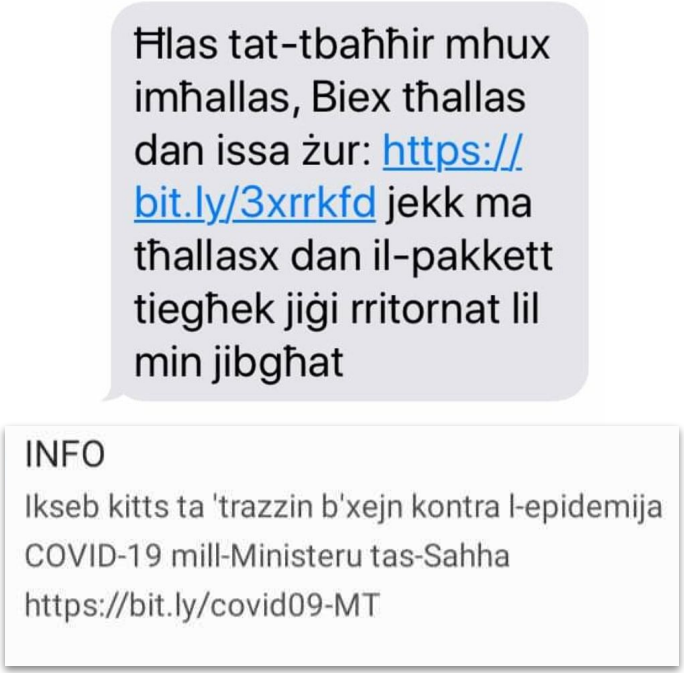
MCAST HackSpace

MCAST HackSpace

https://hackspace.mcast.edu.mt

Uptake in Phishing

- In recent years, especially post-Covid, we saw an uptake in phishing attempts.
- Locally several campaigns targeted clients of couriers, banks, telecom companies, airlines, etc. with some even making headline news.
- In June, a Malta Police press release stated that “Scammers conned €50,000 from 40 people in one day”.



Phishing: Related projects

Ongoing research at MCAST IICT into the ability to recognise and deal with email phishing produced interesting results:

60%

Clicked links in phishing emails

< 40%

Use a password manager for most accounts

50%

Use 2FA when available

https://

Common misconceptions

Target: Automated system that runs phishing simulations, tracks user interaction and builds short training material **specifically for each user**.

Dataset: Malta phishing attempts

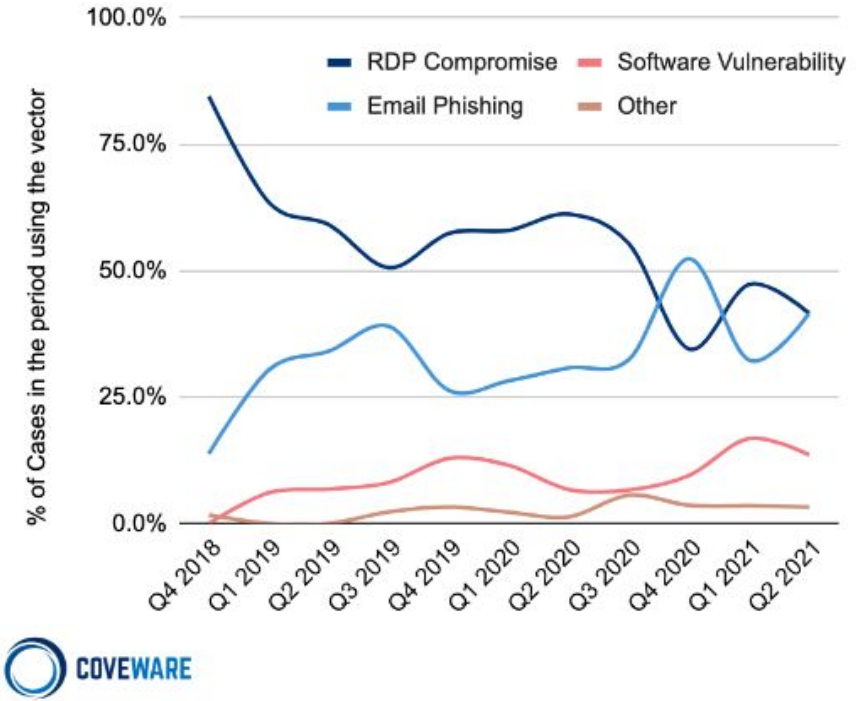
Public collection of samples targeting Malta from Q2 2021 onward. Data includes:

- type - msg | email | social
- source - Official | Media | MCAST | SocialMedia
- link - shortened | lookalike | other | unknown
- motivation - delivery | change | lockout | financial | 2facode | win | opportunity
- lang - en | mt
- personalised - yes | no
- entity - e.g. BOV or MaltaPost (or None)
- description - short description of phishing attempt
- many have transcript, screenshots and other information.

Ransomware attack vectors

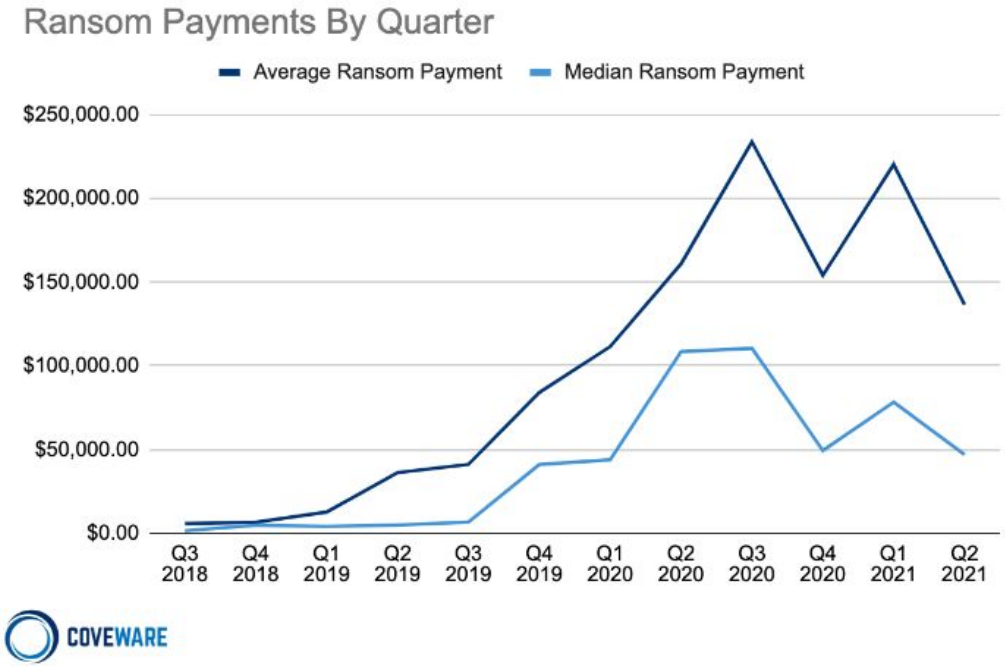
- Ransomware often in the news, especially after high-profile attacks in the USA (Colonial Pipeline, JBS, DC Police) and elsewhere (CD Projekt Red, Kia, Acer, Ireland's HSE, Kaseya, Accenture).

- Analysis show that **phishing** and **RDP attacks** are the most popular entry points for ransomware attacks … low-cost yet effective.



Ransomware payments

- Suspected ransomware payments in H1 2021 reached $600 million. (US Dept. of Treasury)
- That is more than the 2020 total.
- Payment values are also rising.



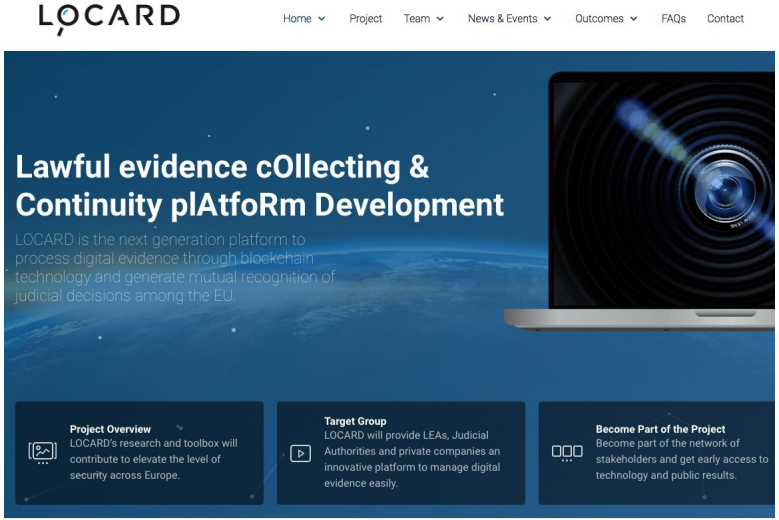
Ransomware awareness

There is no 100% protection, but it's possible to ward off opportunistic attackers.

With our students we make sure to cover the basics:

- Always change change default passwords
- Never reuse passwords, use password managers
- Enable 2FA whenever possible
- Keep software updated
- Design solid backup strategies, and test them.

LOCARD Project



This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

MobFor (i)

MobFor is a tool, developed by the University of Malta, to assist investigators in gathering evidence related to possible unlawful interception attacks via popular messaging apps e.g. Whatsapp, Telegram, Signal and PushBullet.

https://mobfor.gitlab.io/mobfor-pages/

This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

MobFor (ii)

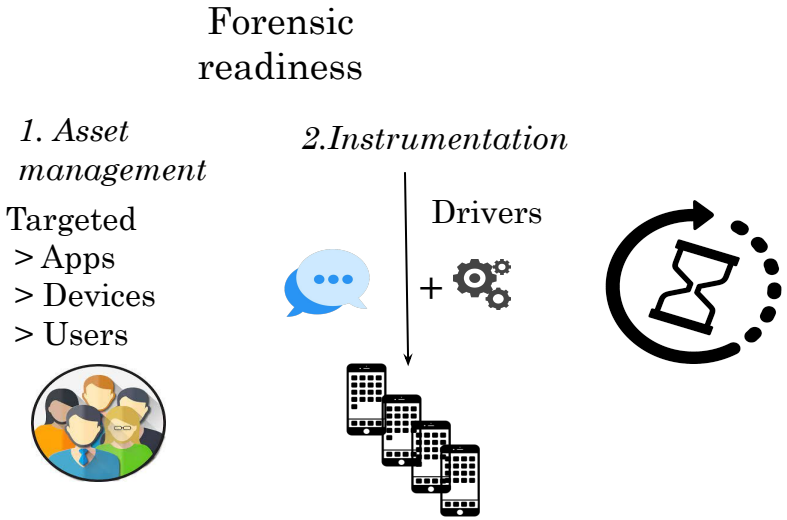
Forensic readiness

1. Asset management

Targeted
> Apps
> Devices
> Users

This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

MobFor (ii)



This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

MobFor (ii)

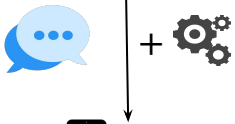
Forensic readiness

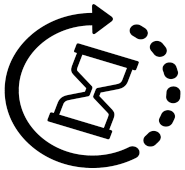
1. Asset management

Targeted
> Apps
> Devices
> Users

2.Instrumentation

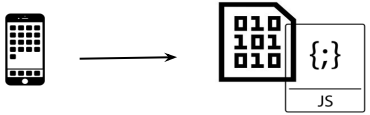
Drivers





Forensic acquisition

3.Event-triggered memory dumps



This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

MobFor (ii)

Forensic readiness

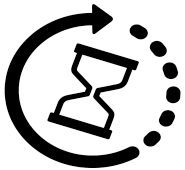
1. Asset management

Targeted
> Apps
> Devices
> Users

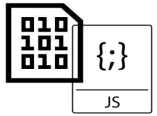
2.Instrumentation

Drivers

Forensic acquisition



3.Event-triggered memory dumps

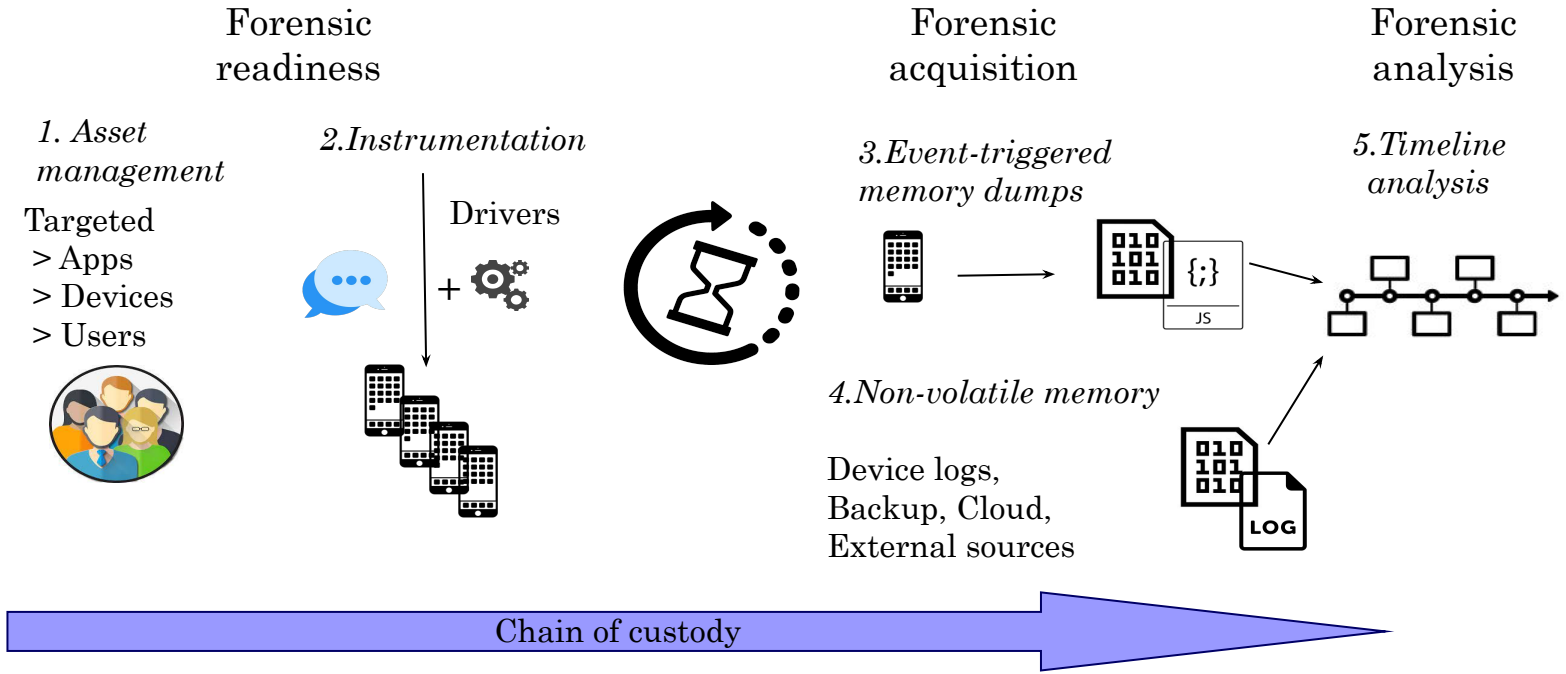


4.Non-volatile memory

Device logs,
Backup, Cloud,
External sources

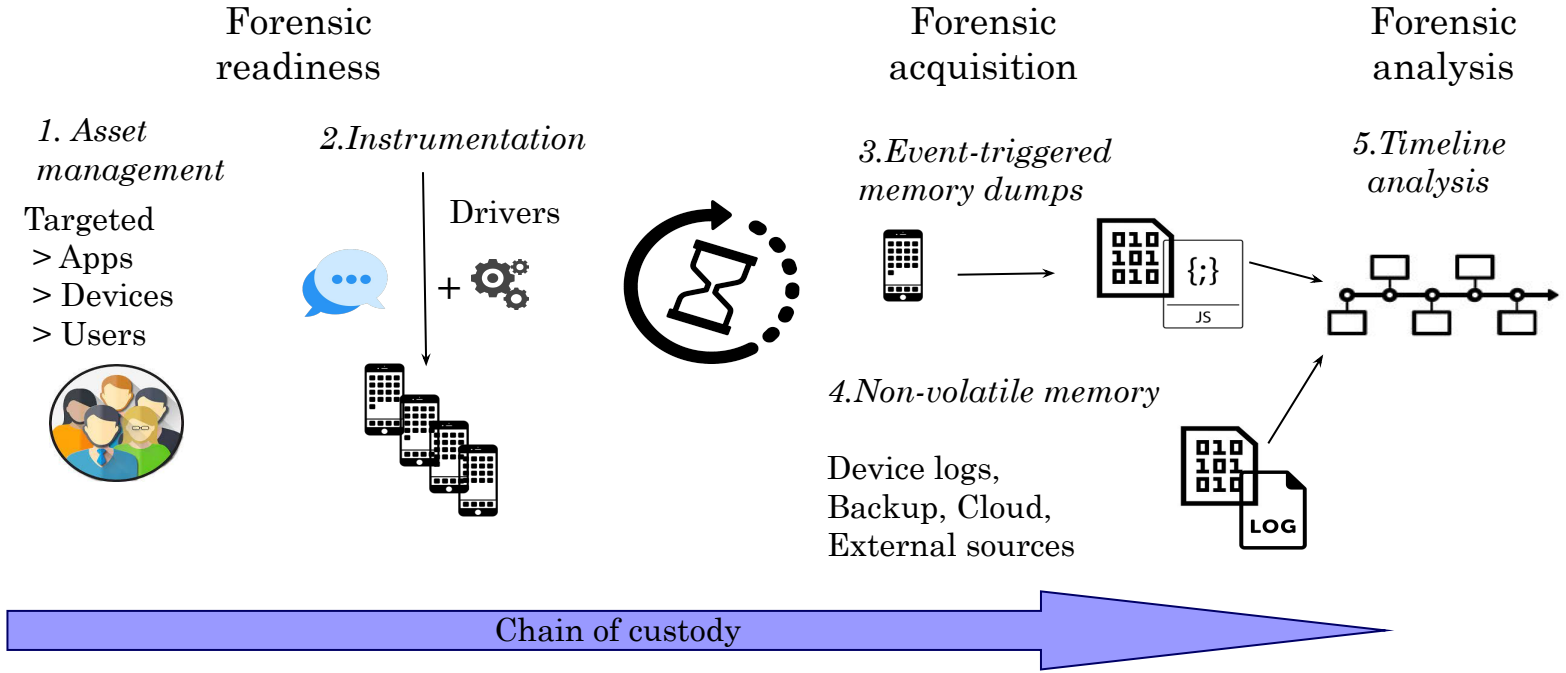
This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

MobFor (ii)



This project has received financial support from the European Union Horizon 2020 Programme under grant agreement no. 832735.

Technologies



Technologies

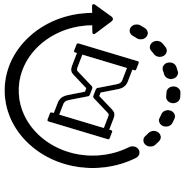
Forensic readiness

1. Asset management

Targeted
> Apps
> Devices
> Users

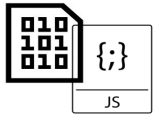
2.Instrumentation

Drivers



Forensic acquisition

3.Event-triggered memory dumps

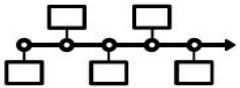


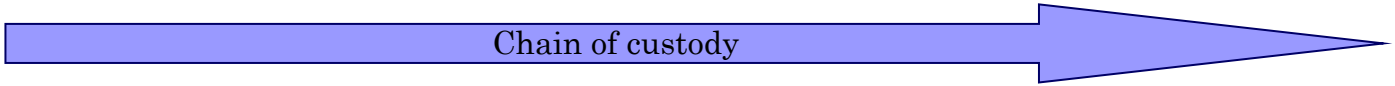
4.Non-volatile memory

Device logs,
Backup, Cloud,
External sources

Forensic analysis

5.Timeline analysis





RV-TEE - NATO Project

Quantum-Safe Communication Protocol

RV-TEE - NATO Project

How do we ensure security from bugs, attacks, vulnerabilities?

Quantum-Safe Communication Protocol

RV-TEE - NATO Project

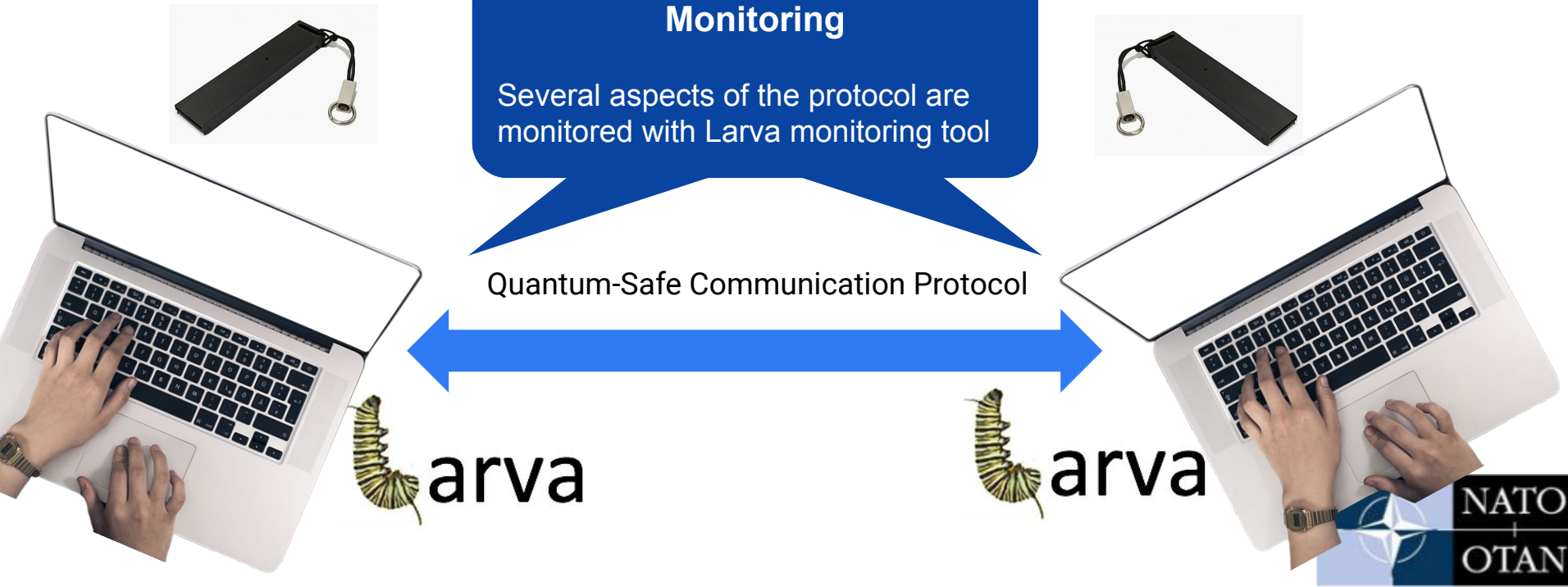
Isolation

Sensitive operations and data (keys) kept separate on a USB Token

Quantum-Safe Communication Protocol

NATO OTAN

RV-TEE - NATO Project



RV-TEE - NATO Project

Isolation

Sensitive operations and data (keys) are kept separate

Monitoring

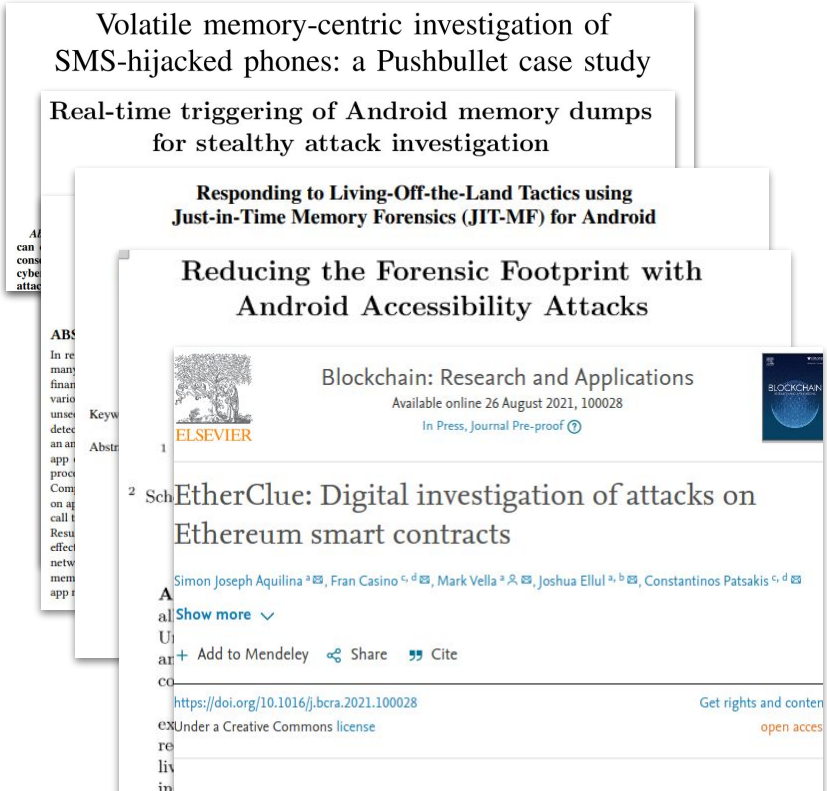
Several aspects of the protocol are monitored with Larva monitoring tool

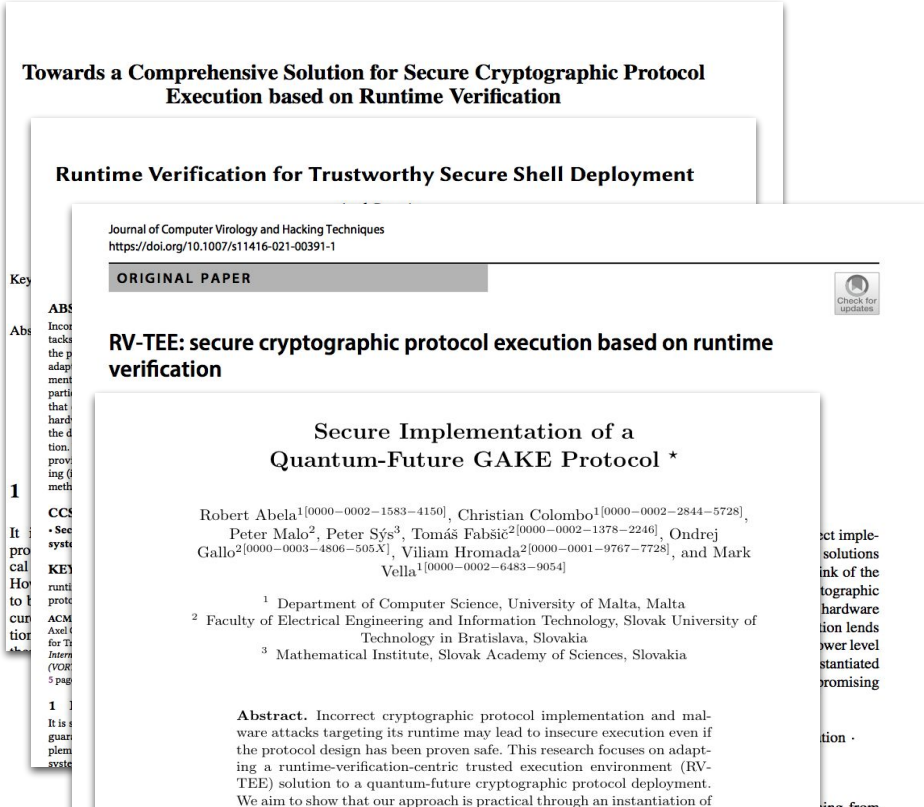
Secure Communication

- From bugs
- From attackers
- From vulnerabilities

NATO OTAN

Our Contributions





Getting into Cybersecurity

- You cannot learn to protect your infrastructure just by reading guidelines and standards.
- We try to instill the culture of Security by Design.
- We want our students to convince their future employers that information security is vital and does not come for free.

Our Approach

- Understand the underlying technical principles.
- Know what an offender might be up to...otherwise you cannot protect yourself.
- Implement protection measures.
- Know how to respond to incidents.

Cyber Research - What does it take?

- Solid programming skills.
- Understanding of the inner-workings of hardware and operating systems.
- Understanding of computer networks and the various protocols that enable communication between machines.
- Perseverance.

University of Malta and MCAST offer full-time and part-time courses that will help you start the journey!

MCAST HackSpace

https://hackspace.mcast.edu.mt

MCAST **Hack**Space

- A new initiative we are starting this year at MCAST's Institute of Information and Communication Technology.
- An informal space where students, academics and industry partners can discuss emerging information security related topics.
- Some of the planned sessions:
  - Hands-on Security Fundamentals with Real-Life Challenges
  - Hardware Hacking
  - Cyber Attack Simulation
  - Dark Web & Tor
  - Digital Forensics: Challenges and Opportunities.

Thank you

christian.colombo@um.edu.mt

jennifer.bellizzi@um.edu.mt

robert.abela@mcast.edu.mt

chris.f.farrugia@mcast.edu.mt

L-Università ta' Malta

MCAST