Cybersecurity Challenges

What are researchers doing to help?

Christian Colombo   Mark Vella

Science in the City 2021

A technology-centric life
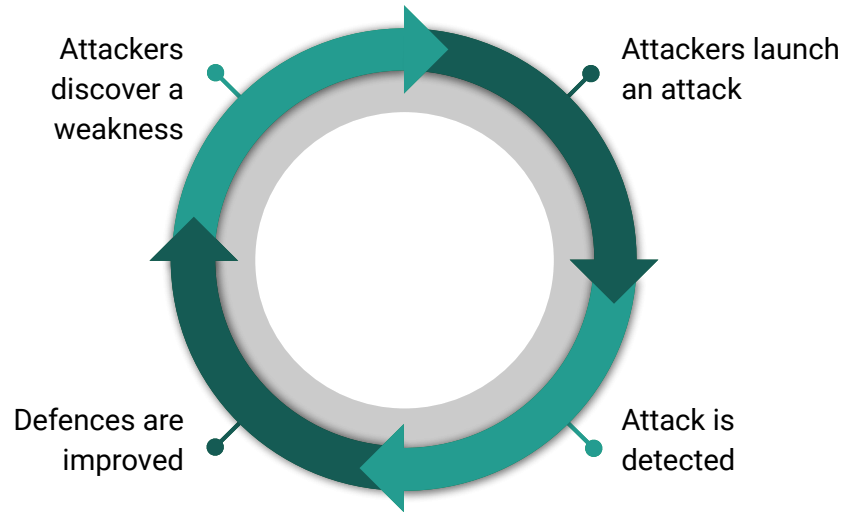
Attackers have a great opportunity!

Security - A game of cat and mouse

Attackers discover a weakness
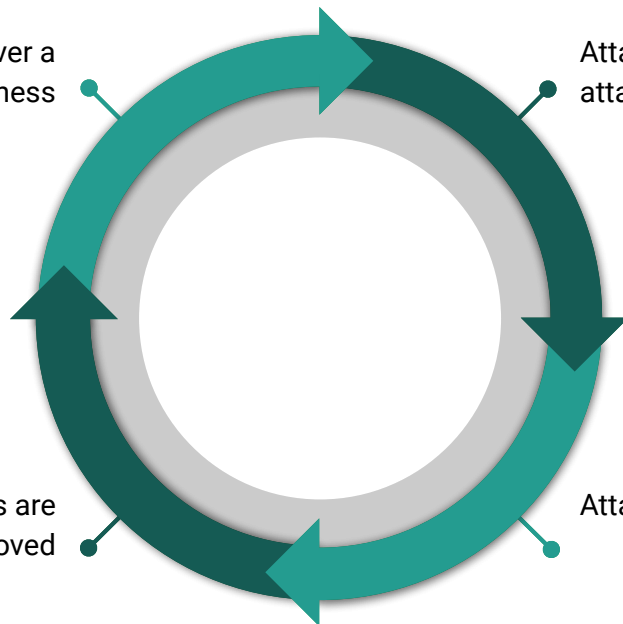
Attackers launch an attack

Defences are improved

Attack is detected
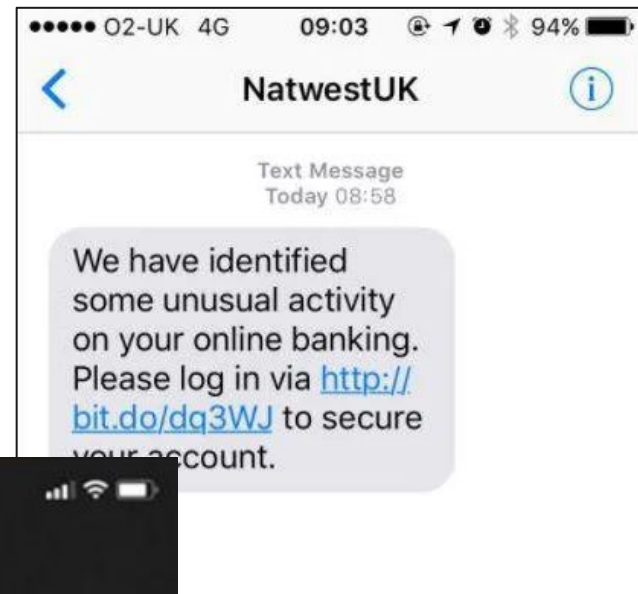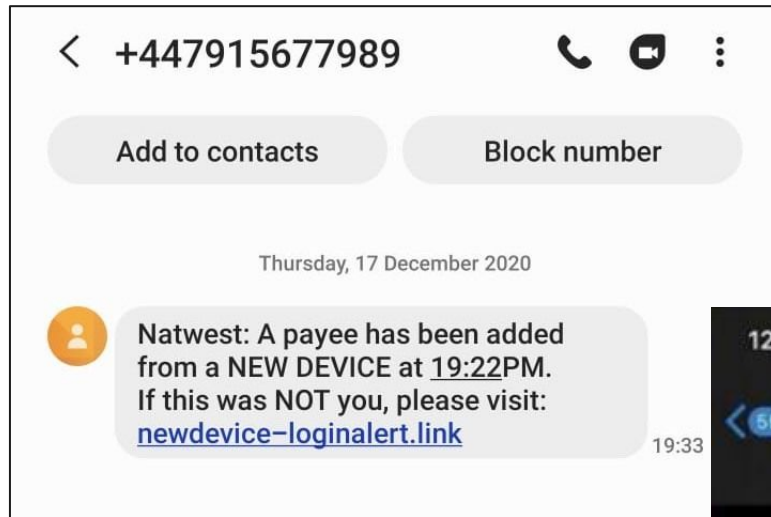
Attackers discover a weakness

Attackers launch an attack

Attack is detected

Defences are improved

Part 1 - Detecting Attacks

Phishing attacks

+447915677989

Add to contacts   Block number

Thursday, 17 December 2020

Natwest: A payee has been added from a NEW DEVICE at 19:22PM. If this was NOT you, please visit: newdevice−loginalert.link
19:33

●●●●● O2-UK 4G   09:03   @ ◀ ☀ ✳ 94% ▬

NatwestUK   (i)

Text Message
Today 08:58

We have identified some unusual activity on your online banking. Please log in via http://bit.do/dq3WJ to secure your account.

12:24   ⏽ 🛜 ▬

55

DHL ›

Text Message
Today 12:23

hello Claire Il-pakkett tieghek qed jistenna l-kunsinna jekk joghgbok ikkonferma l-hlas (1.99 EUR) fil-link li gejja : https://bit.ly/DHL-Malta1

L-Università
ta' Malta

Phishing attacks

TIMES OF MALTA

Latest   National   World   Opinion   Community   Sp[...]

How BOV hackers got away with €13 million

Phishing e-mails did the job... and bank still doesn't know how long hackers had access
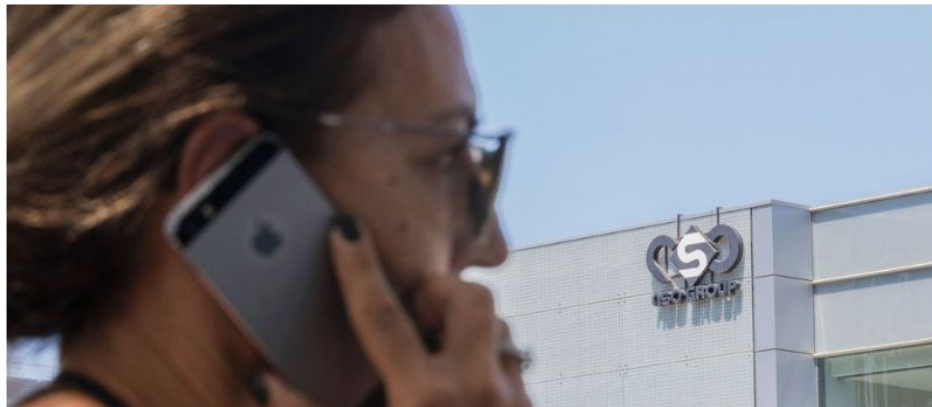
L-Università ta' Malta

Tech

Pegasus: Spyware sold to governments 'targets activists'

🕐 19 July

How does it work?

O2-UK 4G 09:03 94%

NatwestUK

Text Message
Today 08:58

We have identified some unusual activity on your online banking. Please log in via http://bit.do/dq3WJ to secure your account.

Click + Social Engineering →

Phone infected by malware

L-Università ta' Malta

You got infected through phishing... now what?

Click + Social Engineering

Phone infected by malware

L-Università ta' Malta

What are we doing about this?

Detecting attacks - Current Situation
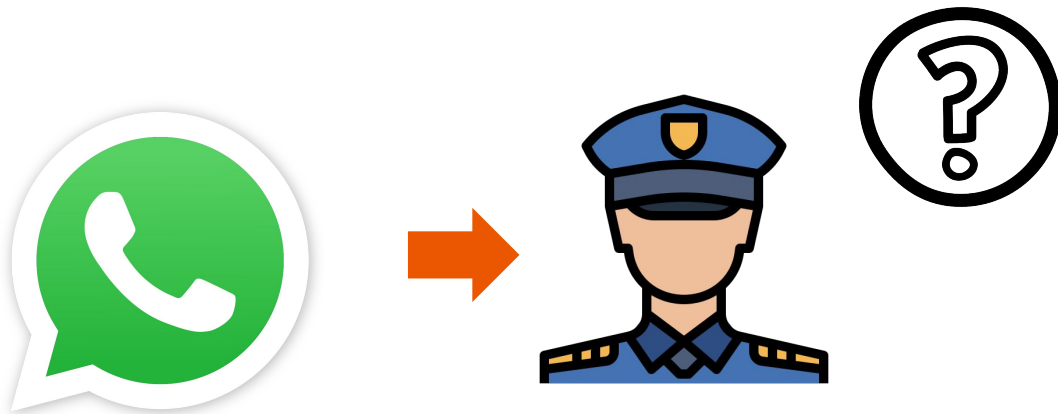
Compromised Whatsapp?

Could it be sending messaging without me knowing it?

Detecting attacks - Current Situation

Compromised Whatsapp?

Could it be sending messaging without me knowing it?

Detecting attacks - MobFor Tool

Detecting attacks - MobFor Tool

Detecting attacks - MobFor Tool
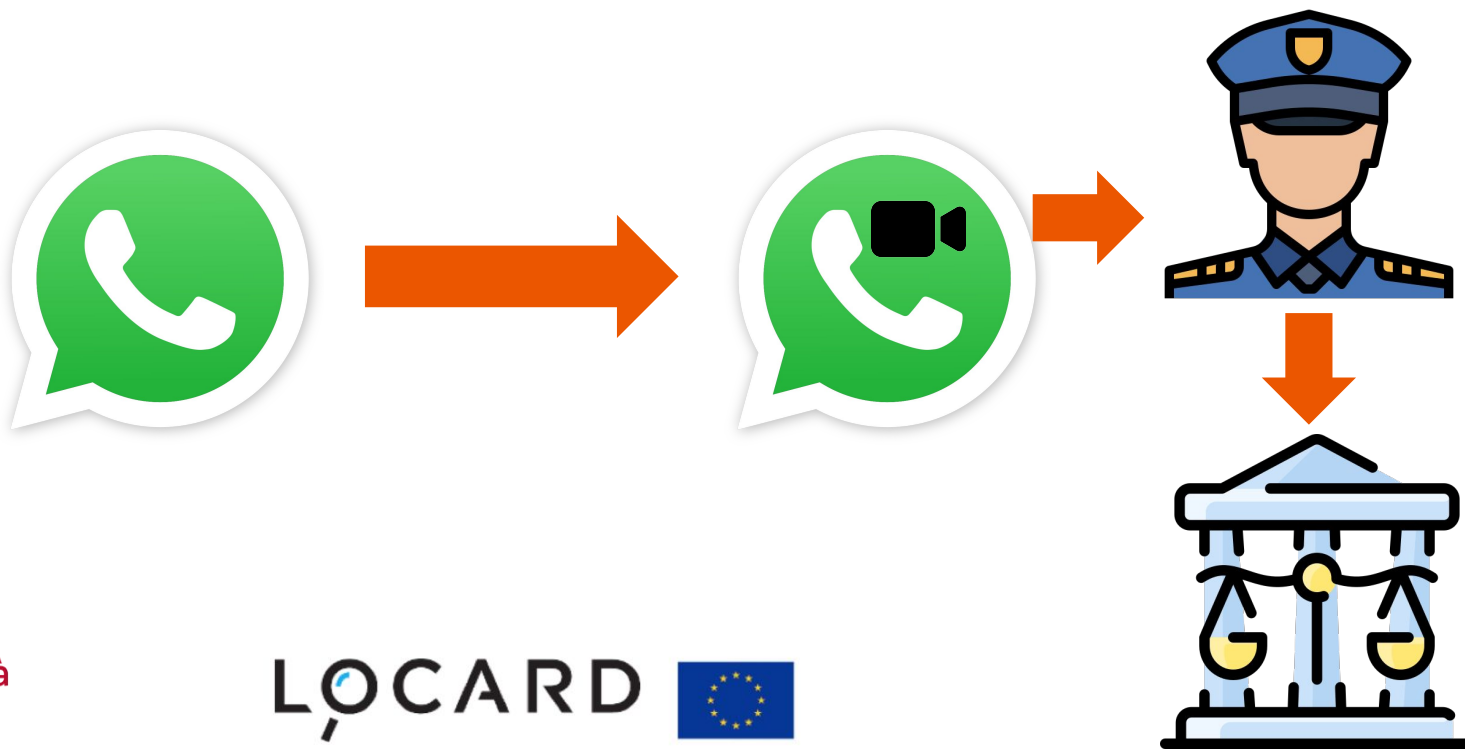
Signal, Telegram and others too

Part 2 - Communication Security and Privacy

L-Università ta' Malta

Communication on the Internet

Everytime you load a webpage!
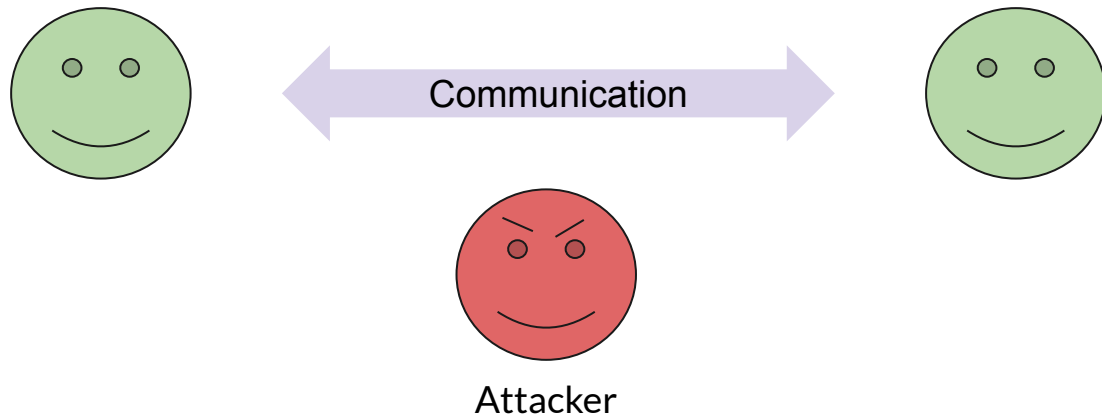
Every chat!

Every message!

Communication on the Internet

Everytime you load a webpage!

Every chat!

Every message!

Communication
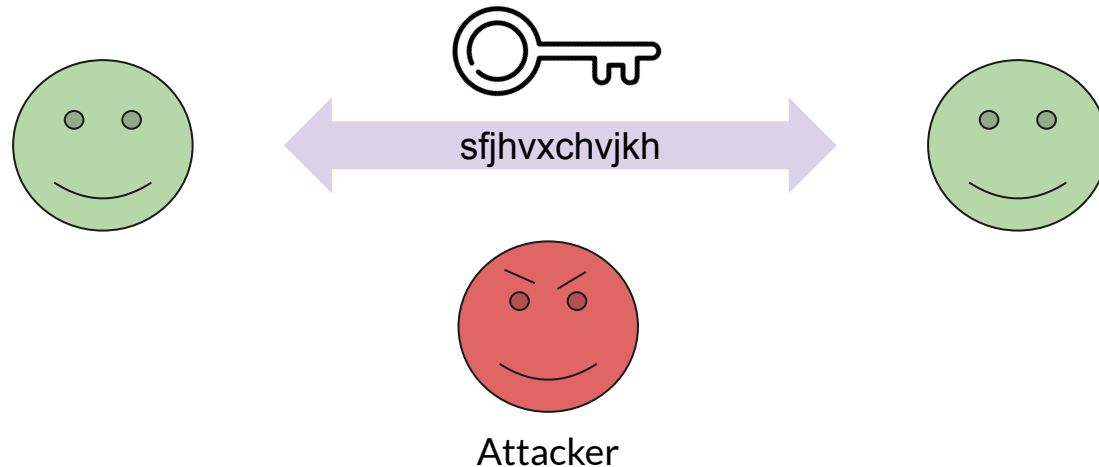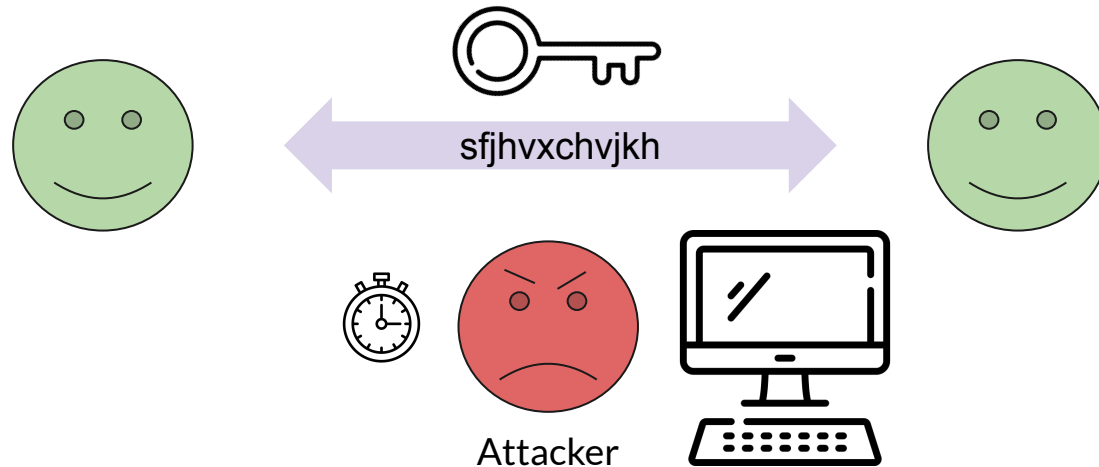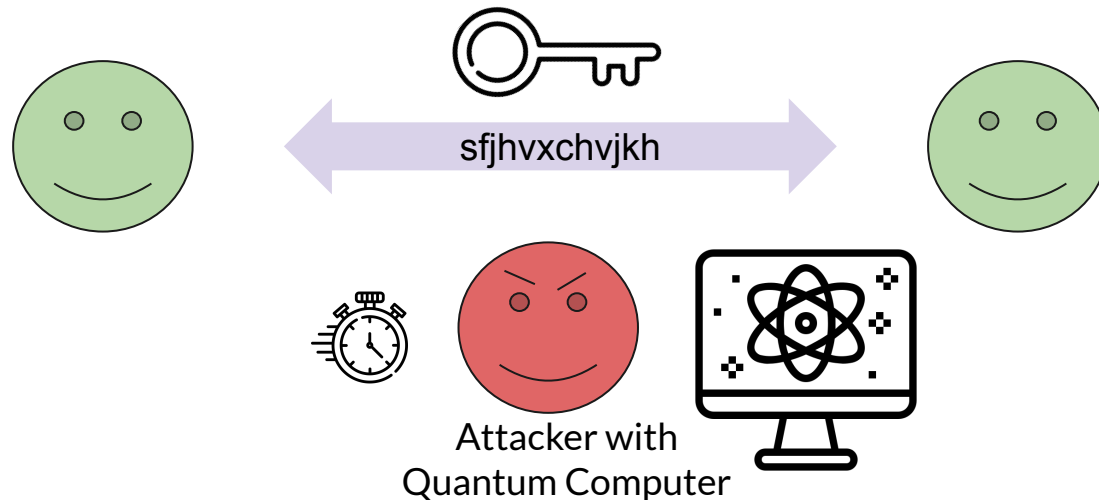
Attacker

Communication on the Internet

Everytime you load a webpage!

Every chat!

Every message!

sfjhvxchvjkh

Attacker

L-Università ta' Malta

Cracking Encryption is Hard Work!

A classical computer might take billions of years to crack one!

sfjhvxchvjkh

Attacker

Cracking Encryption with Quantum Computer

A classical computer might take billions of years to crack one!

But, a **Quantum Computer** (when it becomes available) could reduce that number considerably!

sfjhvxchvjkh

Attacker with
Quantum Computer

L-Università
ta' Malta

Quantum-Safe Protocol - Stronger encryption

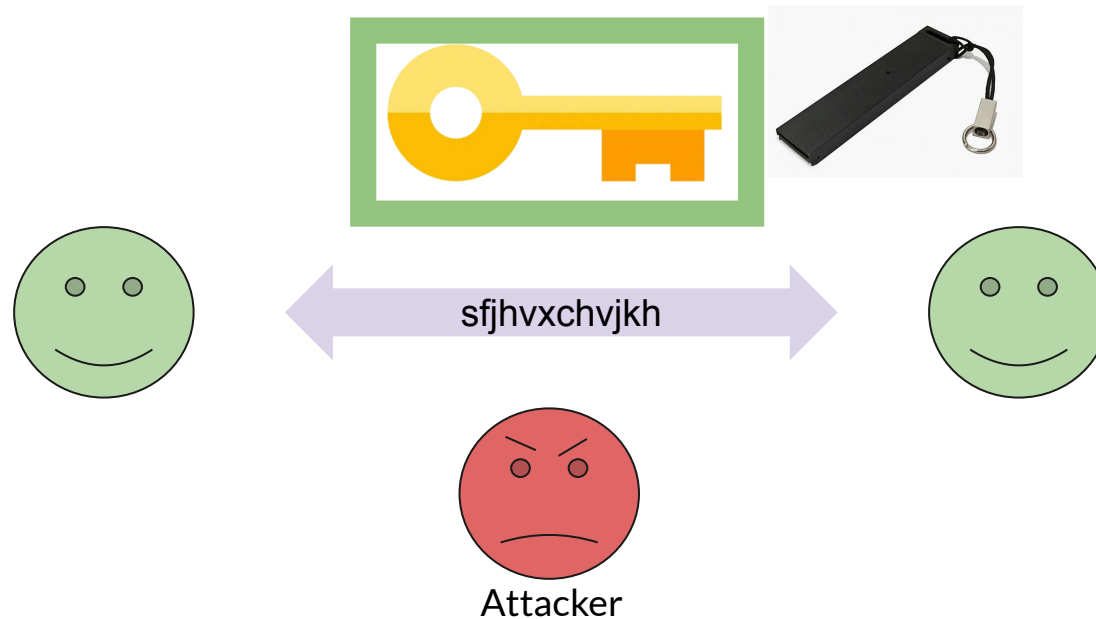sfjhvxchvjkh

Attacker with
Quantum Computer
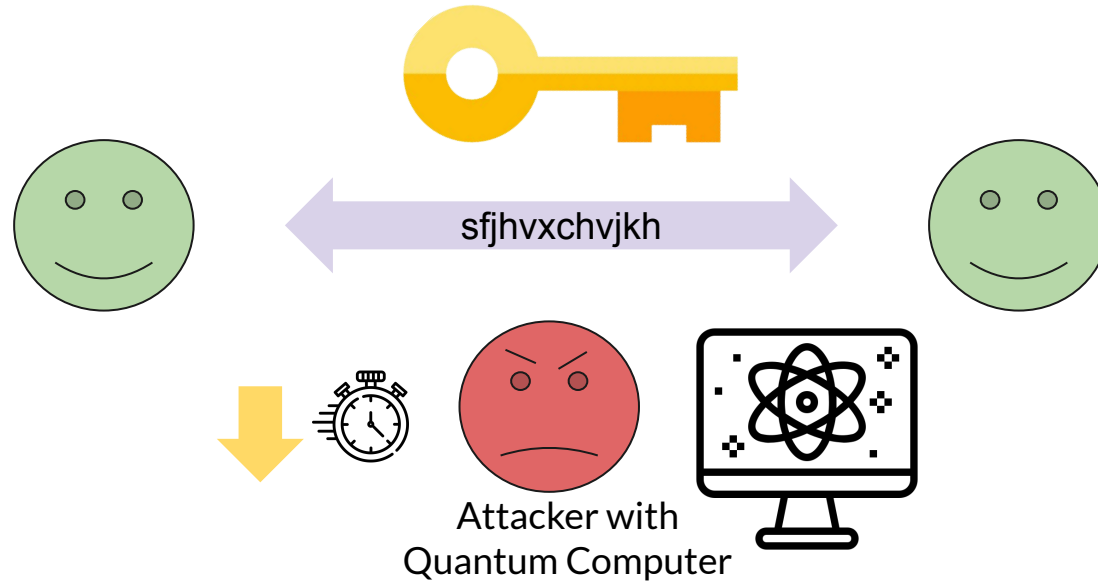
Quantum-Safe Protocol Implementation

sfjhvxchvjkh
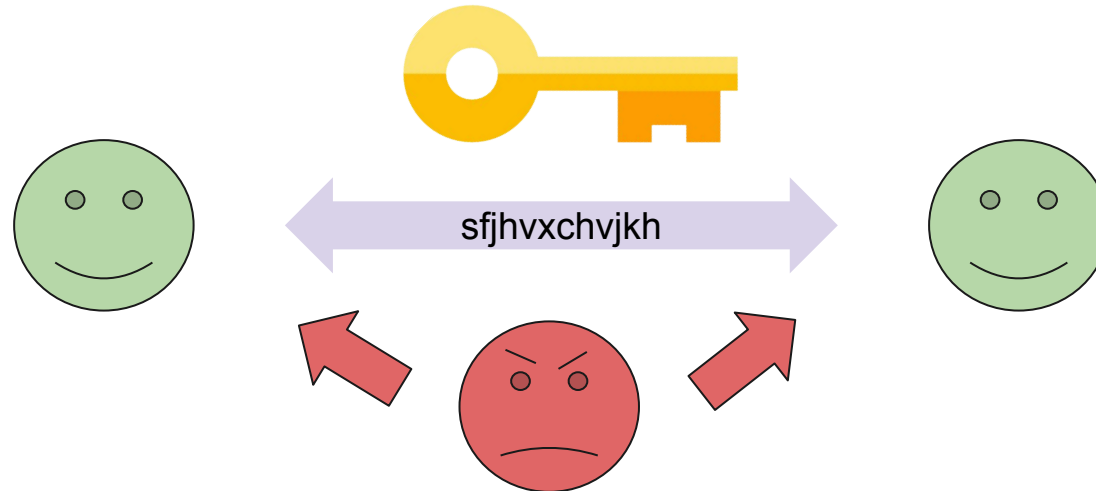
Attacker can try to steal key
or decrypted message!

Key is isolated on special device for protection

sfjhvxchvjkh

Attacker

Communication process is monitored

sfjhvxchvjkh

Attacker
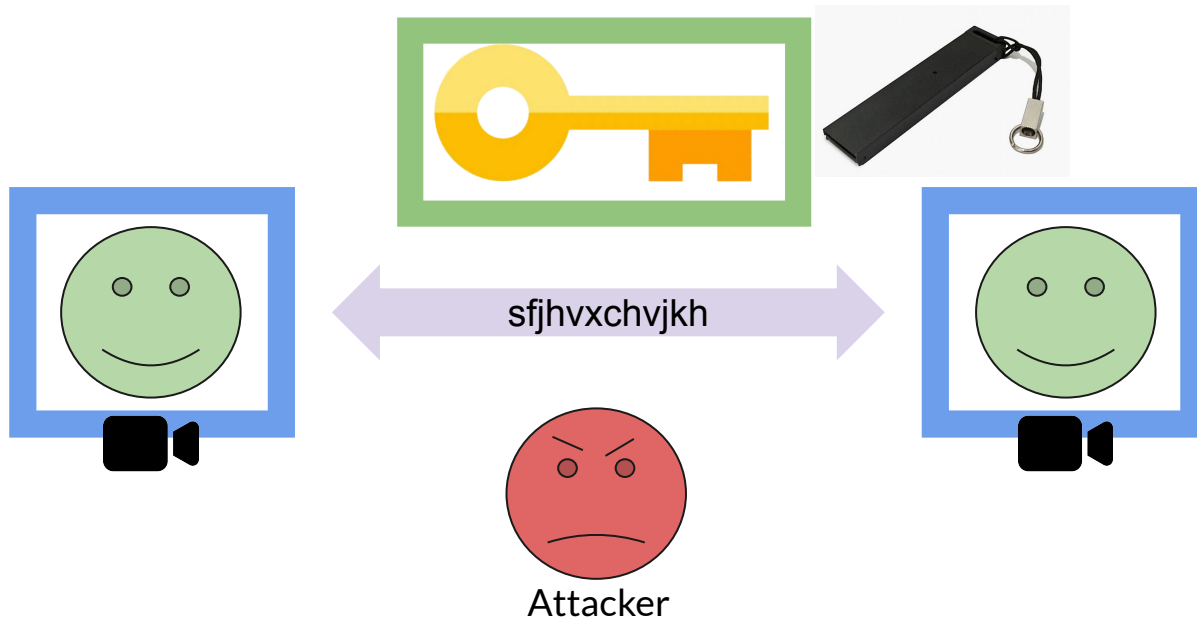
Data leaving the safe areas is monitored

sfjhvxchvjkh

Attacker
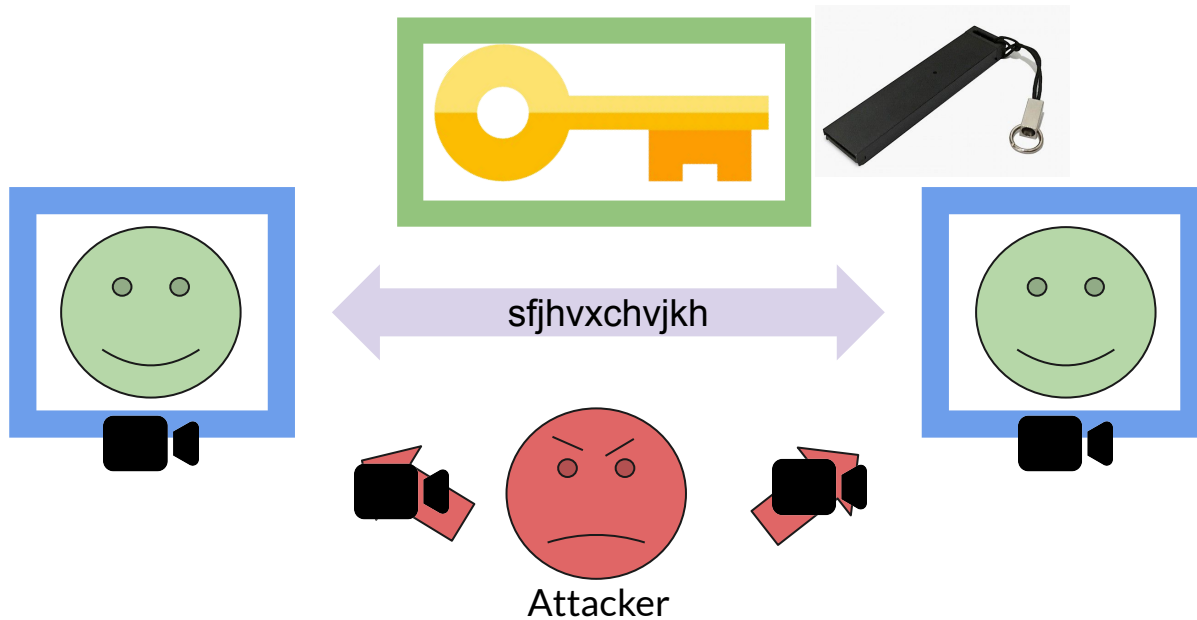
Q&A

Questions?

Comments?

Christian.Colombo@um.edu.mt

Mark.Vella@um.edu.mt

LOCARD

NATO OTAN

L-Università ta' Malta