

WEBINAR



Effective protection of Critical Infrastructures against cyber threats

29 October 2020 - 11:00 CET

in collaboration with



CYBERWISER.eu
Cyber Range & Capacity Building in Cybersecurity



Reactively Defending Against Advanced CyberSecurity Threats: The ReAct project

Webinar | 29 October 2020

Evangelos Markatos
FORTH and ReAct

Funded by the European Commission
Horizon 2020 – Grant # 740129



Critical Infrastructures Webinar 29.10.2020 | www.cyberwatching.eu | [@cyberwatching.eu](https://twitter.com/cyberwatching.eu)

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 786669. The content of this talk reflects reflect the views only of their author. The European Commission/ Research Executive Agency are not responsible for any use that may be made of the information it contains.

Roadmap

- ◆ CyberSecurity
 - ◆ Then and Now
- ◆ The heart of the problem
- ◆ The solution
- ◆ Who
- ◆ Summary



Roadmap

● CyberSecurity

● Then and Now

● The heart of the problem

● The solution

● Who

● Summary



CyberSecurity: Old or New?

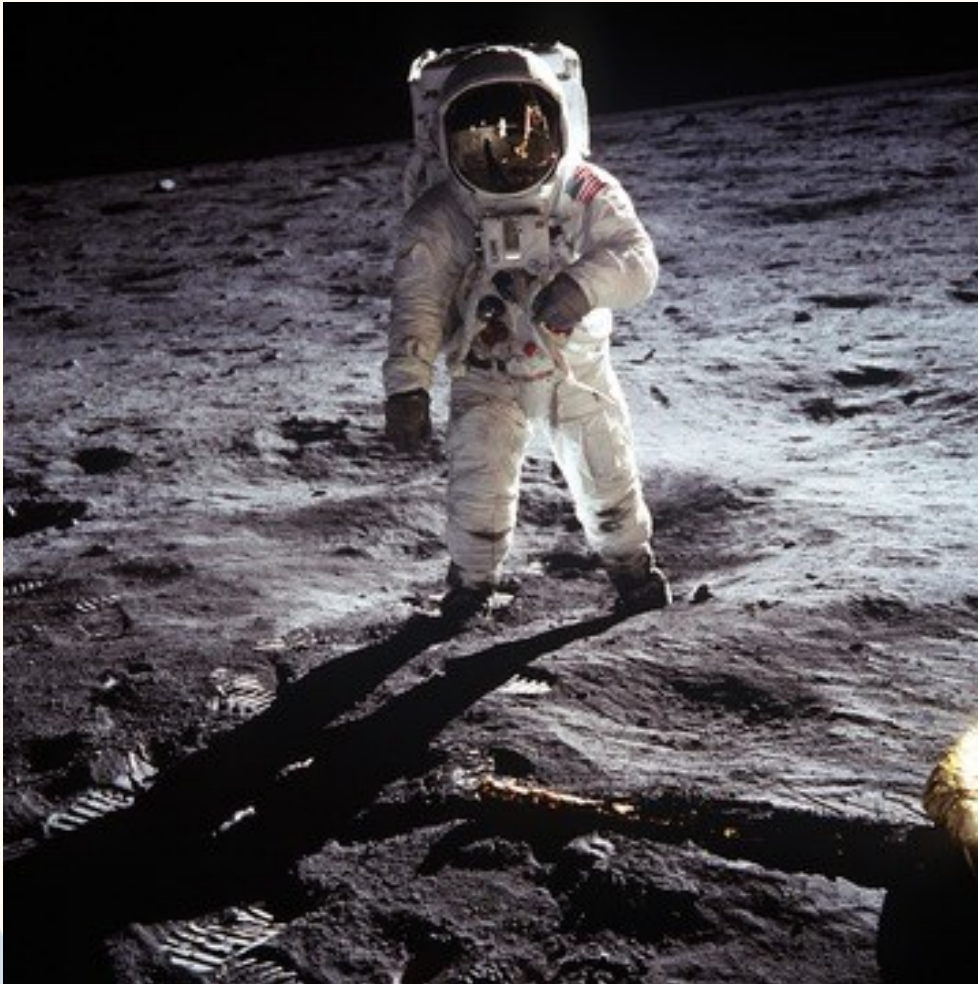
- ◆ Why are we talking about cybersecurity?
- ◆ Is this a new problem?
- ◆ Didn't we have this problem
 - ◆ 20 years ago?
 - ◆ 30 years ago?
 - ◆ 40 years ago?
 - ◆ 50 years ago?



A trip down Memory Lane: 1969

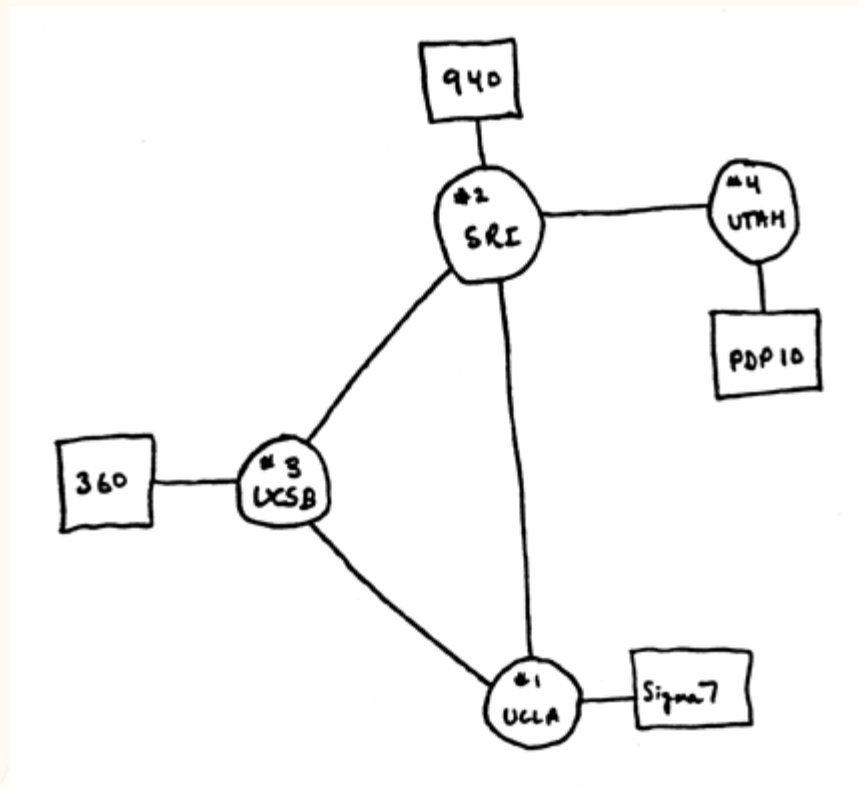


1969: Man Landed on the Moon



1969: The Internet (ARPANET) was invented

◆ The Internet (ARPANET) in Dec 1969:



So, in 1969

- ◆ We had **computers**
 - ◆ They landed the man on the moon
- ◆ We had the **Internet**
 - ◆ It was called ARPANET, but still...
- ◆ We had **software**
- ◆ **Did we have any cybersecurity issues?**



Cyber Security Problems in 1969

◆ CyberSecurity in 1969

- ◆ Existed but
- ◆ Not a major problem

◆ Because:

◆ **Closed Community**

- ◆ mostly academics had access

◆ **Boring applications**

- ◆ mostly numerical analysis

◆ Computers **did not have a lot of value**

- ◆ No data
- ◆ No financial value

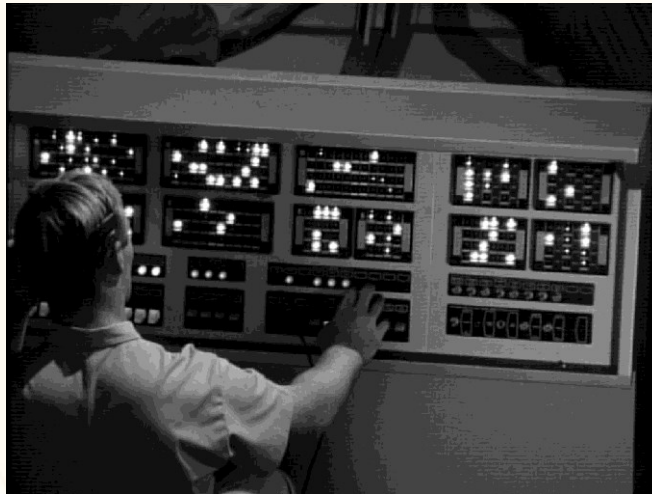
◆ **Small scale:**

- ◆ just four nodes



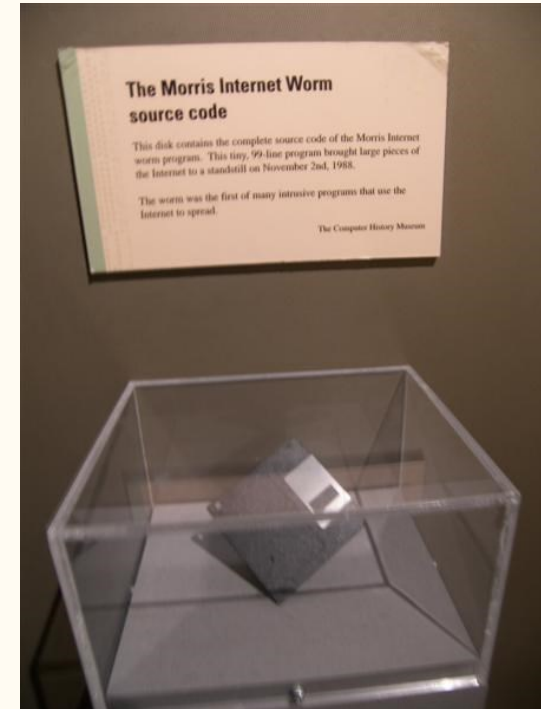
The end result

- ◆ So, because cybersecurity was not a major issue in 1969
- ◆ **The Internet was not designed with security in mind**
 - ◆ Small Academic community
 - ◆ Restricted physical (and virtual) access



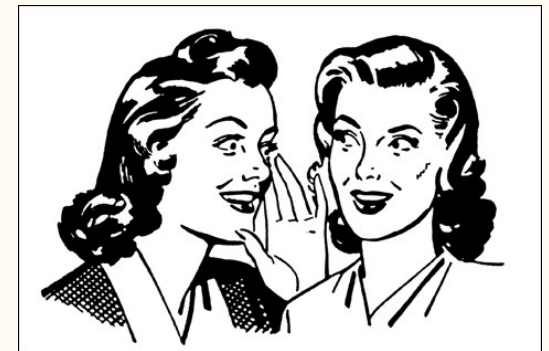
The situation did not change

- For 25 years computers
- Internet kept on being
 - **Boring**
 - Mostly numerical analysis
 - **Closed Community**
 - Mostly academics had access
- There was an occasional cyberattack
 - But people (out there) did not take notice...
 - They did not have an Internet connection
 - They did not have a facebook account...
 - They did not have a smartphone...



And then... in mid 90's

- ◆ Something changed!
- ◆ People started connecting to the Internet
 - ◆ The **ISPs** started offering Internet Connections
- ◆ People of all realms – not only academics
- ◆ Computers **started storing data**
 - ◆ Lots of data!
 - ◆ **Interesting data!**
 - ◆ **Personal Data:** Email - Gossip!
 - ◆ **Financial data:** Credit card numbers!



And then...

- ◆ Things changed even more!
- ◆ Computers started **doing** things
 - ◆ In the **physical world**
- ◆ Such as
 - ◆ Controlling appliances (**refrigerators**, etc.)
 - ◆ Controlling **machinery**
 - ◆ Running factories
 - ◆ Controlling Medical equipment
 - ◆ **Self-Driving cars!**



THE Question

Now it is time to pose THE Question:

How **valuable** is a computer to a cyberattacker?



Computers started to have value for attackers!

- ◆ **Compromising a computer in the 70's**
 - ◆ **had little value**
- ◆ What could an attacker do with it?
- ◆ Solve equations?
- ◆ Do numerical analysis?
 - ◆ So what?



Computers started to have value!

- Compromising a computer today
 - has a lot value!
- Cyberattackers can **monetize** it in several ways:
 - **Steal** the personal/professional stored **data**
 - Ask for **ransom**
 - Send **SPAM**
 - **Host illegal** markets
 - Mine **Cryptocurrencies**
 - Host illegal services (fake DNS, etc.)
 - Industrial espionage
 - ...



Major Damage

- Compromised computers can now do major damage

MIT Technology Review Topics Mag:

CAMILO JIMENEZ ON UNSPLASH

[Computing / Cybersecurity](#)

A patient has died after ransomware hackers hit a German hospital

This is the first ever case of a fatality being linked to a cyberattack.

Roadmap

- ◆ CyberSecurity
 - ◆ Then and Now
- ◆ The heart of the problem
- ◆ The solution
- ◆ Who
- ◆ Summary



What is the problem? I

◆ We have lots of cyberattacks because:

◆ Computers are vulnerable

◆ They contain **mistakes (bugs)**!

◆ Software **bugs** (overflows etc.)

◆ Hardware **bugs** (rowhammer, etc.)

◆ Bugs are **programming mistakes**

◆ **Human errors**

◆ Left in a computer program



What is the problem? II

● **Hackers** are using these **bugs** (human mistakes)

● to **compromise** computers

● **How?**

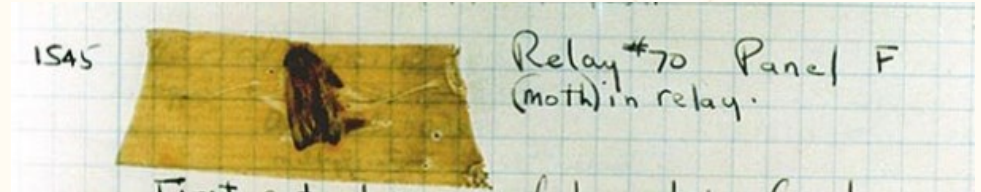
● Hackers search for bugs

● If they find a bug

● **They keep it secret**

● **Why?**

● So that no one fixes it... ☹️



What is the problem? III

● Hackers find a way to **turn the mistake into an attack!**

● e.g.

● If they know that the key is under the mat

● They wait for the house to be empty, they wait for the night to fall, and they open with the key!

● Once they have the attack they choose a day to do it

● And then they ATTACK! (**ZERO day**)

● compromise all vulnerable computers

● After that companies create a **software patch**

● That **removes the bug**

● Users apply the PATCH (**PATCH day**)



Roadmap

- ◆ CyberSecurity
 - ◆ Then and Now
- ◆ The heart of the problem
- ◆ The solution
- ◆ Who
- ◆ Summary



The ReAct approach

- The solution lies in
- a **fundamental change of our mindset**

We should

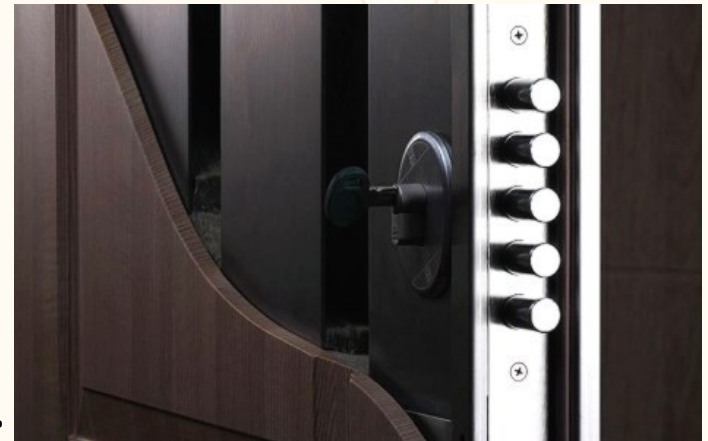
change the way we think about cybersecurity

An example: securing your home

- ◆ Suppose that you have just bought a new home and
- ◆ You would like to make your new home more secure.

◆ You think:

- ◆ More **secure front door**
- ◆ **Better alarm, stronger fence**, etc.



◆ We say:

- ◆ No! Before securing your home **try to break into it!**
- ◆ Do not purchase a new front door before you break into it!
- ◆ In your effort to break into your new home consider the following:

Breaking into your house

- ◆ Did you consider the **back door**?
- ◆ How about the **skylight on the roof**?
- ◆ Or the **stone** under which you store the **spare key**?
- ◆ Or the **garage door** that opens with a **remote**?
- ◆ Or the **digital assistant** that you can ask to
 - ◆ “open the front door”?
- ◆ Or that **loose board** in the fence that you can remove and squeeze through?
- ◆ Did you know that people can “saw” their way in?
 - ◆ By “**cutting**” through your **lightweight walls**?



Breaking and Fixing

● OK!

● Now that **you know how to break in**

● You can **make your home more secure**

● In ReAct we do exactly the same:

● We break into systems

● In order to know how to fix them

Our approach

- **Do not rush into protecting systems**
 - Before you know how to break them
- **Do not purchase a more secure front door**
 - Before you know how to break in your house
- **Do not try to secure your system**
 - Before you know how to break it
- This is ReAct's approach:
 - **Break things first**, and then try to fix them

What does this mean in the digital word?

- Try to “break” programs
- Try to **make systems fail**
- Once you break them
 - Try to understand why they failed
- And finally,
- Try to fix them



How do we break things?

◆ Fuzzing

- ◆ Run the program
 - ◆ with **every possible input**
 - ◆ **every possible combination of values**
 - ◆ every possible “unexpected” thing you can think of
- ◆ See if it crashes...
 - ◆ If it does this is **good news!**
- ◆ But... all possible inputs take exponential time
 - ◆ Needs guidance from algorithms to do it in reasonable time



How do we break things? II

Manual Analysis

- Hack the system
- Needs ingenuity...
- And lots of hardware...



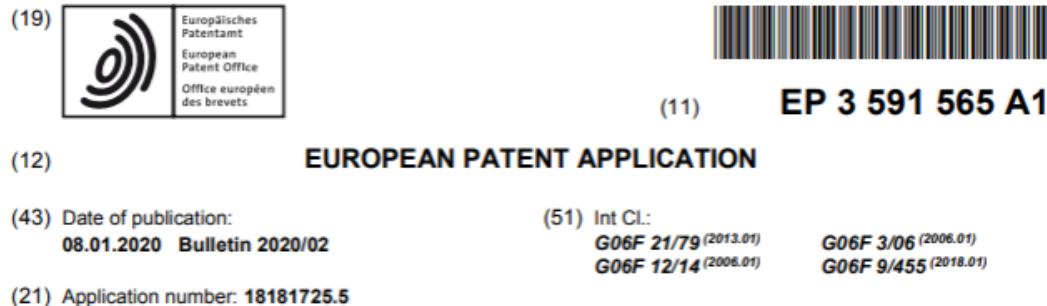
Did we find any bugs?

- YES!
- A bug in INTEL's processors:
 - CrossTalk
 - They leak sensitive data!
- What happened?
 - VUA (the finders) notified INTEL
 - Intel issued a **microcode update**
 - **June 2020**
 - Intel gave the VUA a **bug bounty award!**
- For more info see:
 - <https://www.vusec.net/projects/crosstalk/>
- Same thing for cache side-channel attacks with NETCAT!
 - <https://www.vusec.net/projects/netcat/>



Any other bugs?

- Rowhammer
- When you read memory too fast
 - Some bit in another application's address space changes
- VUA disclosed the bug and developed a solution:
 - ZebRAM
- The solution has been patented!



Any more bugs?

◆ Lots of CVEs from (RUB):

- ◆ CVE-2018-10191
- ◆ CVE-2018-10199
- ◆ CVE-2018-11743
- ◆ CVE-2018-12247
- ◆ CVE-2018-12248
- ◆ CVE-2018-12249



To summarize: ReAct's innovation:

Change your way of thinking about cybersecurity:

Break things first!

Before you try to protect them

● ReAct has applied this approach and:

- Discovered two **major hardware bugs**
- Discovered several software bugs
- Received **several bug bounty awards**
- Filled a **patent application**
- was assigned several CVEs

Roadmap

- ◆ CyberSecurity
 - ◆ Then and Now
- ◆ The heart of the problem
- ◆ The solution
- ◆ Who
- ◆ Summary



React - Who

◆ FORTH



◆ Vrije Universiteit



◆ U of Cyprus



◆ EURECOM



◆ RUHR UNIVERSITÄT BOCHUM



◆ NortonLifeLock



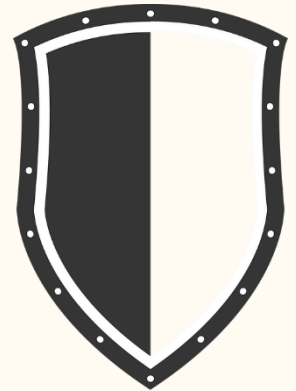
Roadmap

- ◆ CyberSecurity
 - ◆ Then and Now
- ◆ The heart of the problem
- ◆ The solution
- ◆ Who
- ◆ Summary



Summary

- ◆ The Internet was **not designed with security in mind**
- ◆ Systems contain bugs/vulnerabilities
- ◆ ReAct's approach is:
 - ◆ **Break** the system
 - ◆ Before
 - ◆ You try to fix it
- ◆ ReAct develops mechanisms to **protect computers** from attackers and cyberattacks



Acks

Photos from

Wikimedia

<https://creativecommons.org/licenses/by/3.0/>

Pixabay

<https://pixabay.com/service/license/>

Flicker

<https://creativecommons.org/licenses/by-sa/2.0/>

Picpedia, Pxhere, technofaq, stackexchange

Nicepic, blogspot.com

Thank-you

Evangelos Markatos, markatos@ics.forth.gr
FORTH and ReAct

<https://react-h2020.eu/>

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 786669. The content of this talk reflects reflect the views only of their author. The European Commission/ Research Executive Agency are not responsible for any use that may be made of the information it contains.



www.cyberwatching.eu
[@cyberwatching.eu](https://twitter.com/cyberwatching.eu)
info@cyberwatching.eu

What's next? A glimpse into the future

◆ Ransomware

◆ In 2017 Wannacry attacked thousands of computers

◆ Encrypted the files

◆ Asked owners for money

◆ What's next?

◆ Lock us out of our car?

◆ Lock us out of our home?

◆ Disable our car's breaks?

◆ What?

◆ Attackers will just follow the computers....





Thank-you

Evangelos Markatos, markatos@ics.forth.gr
FORTH-ICS and ReAct

<https://react-h2020.eu/>

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement No. 786669. The content of this talk reflects reflect the views only of their author. The European Commission/ Research Executive Agency are not responsible for any use that may be made of the information it contains.