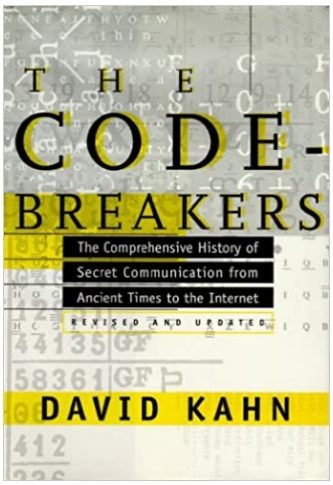
Introductory notes

Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
gianluca.dini@unipi.it
Version: 2022-03-02

1

Historical perspective



2

Don't invent your own crypto, but use well-established ones

Applied Cryptography

secret writing

3

Why are secrets so important?

- Because they are everywhere
  - Secure communication
    - Web traffic: HTTPS
    - Wireless traffic: 802.11i WPA2, GSM, Bluetooth
  - Encrypting files on disks
    - EFS, TrueCrypt
  - Content protection
    - DVD (CSS); Blu-ray (AACS)
  - User authentication
    - Pwd, 2FA,…
  - …and much more

4

Why “applied” cryptography?

- Don’t invent your own crypto-but use well-established ones
- *“Anyone who tries to create his or her own cryptographic primitive is either a genius or a fool. Given the genius/fool ratio of our species, the odds aren't very good.”* — Bruce Schneier, Secrets and Lies: Digital Security in a Networked World

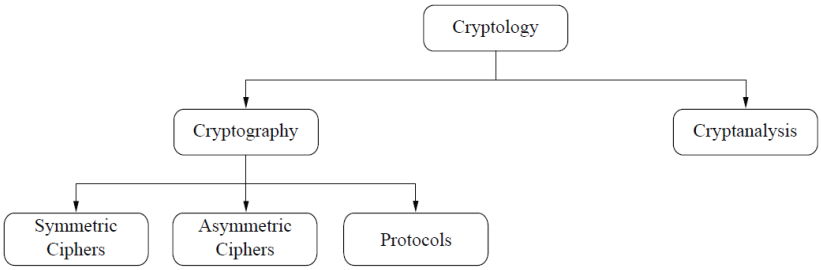
5

Why “applied” cryptography?

- Use cryptography as a building block
- We will learn to
  - Understand and use crypto-primitives
    - Ciphers, hash functions, digital signatures, key exchange
  - Reason about security
    - Whether and why primitives and protocols are secure
  - Analyze, design and implement protocols
    - Authentication protocols
    - Key management protocols
    - Crypto-protocols in general

6

Cryptology



7

The adversary

- There is an *intelligent* adversary, with an *objective, resources* and *abilities*

8

A security engineer thinks differently

- Unfair competition against the adversary
- Security vs. performance and usability
- What's the ROI?
- Devil hides in details

9

What does "security" mean?

- Many very smart, highly motivated people tried to break it but couldn't **3**
- There are 834 quadrillions possible keys so it must be secure **4**
- Here is a mathematical proof, accepted by experts, that shows it is secure **1**
- Here is a strong argument why breaking it is as hard as solving a problem we believe is hard **2**

11

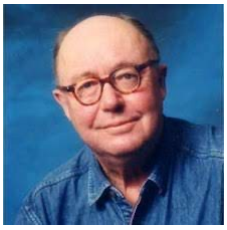
Things to remember

- Cryptography is
  - a very useful tool
  - the basis for many mechanisms
- Cryptography is not
  - "the silver bullet" for all security problems
    - Software bugs, social engineering
  - reliable if not designed, implemented and used properly
    - WEP, Heartbleed,…
  - Something you should try to invent yourself

12

Cryptography isn't the silver bullet

- "*Whoever thinks his problem can be solved using cryptography, doesn't understand his problem and doesn't understand cryptography*." – Attributed by Roger Needham and Butler Lampson to each other

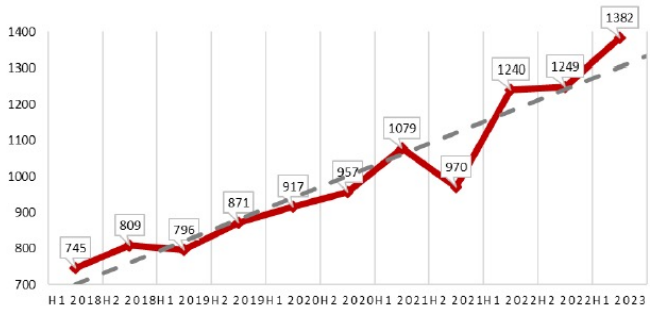


13

The Clusit Report

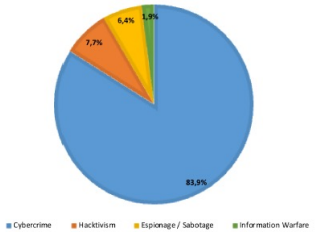
14

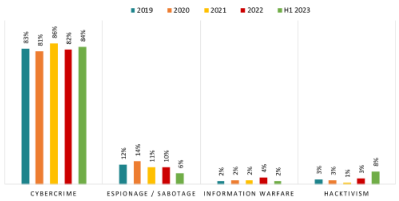
Number of attacks 2018 – 2024



15

Who are the adversaries?

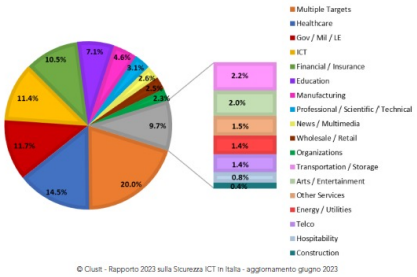




84% is cybercrime, i.e., attackers for money

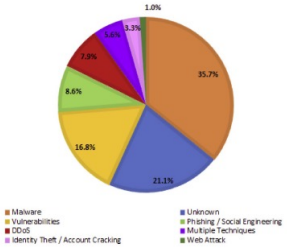
16

Who are the victims?



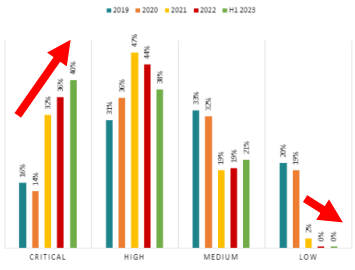
17

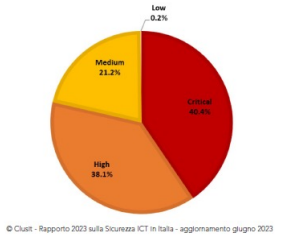
What are the attack techniques?



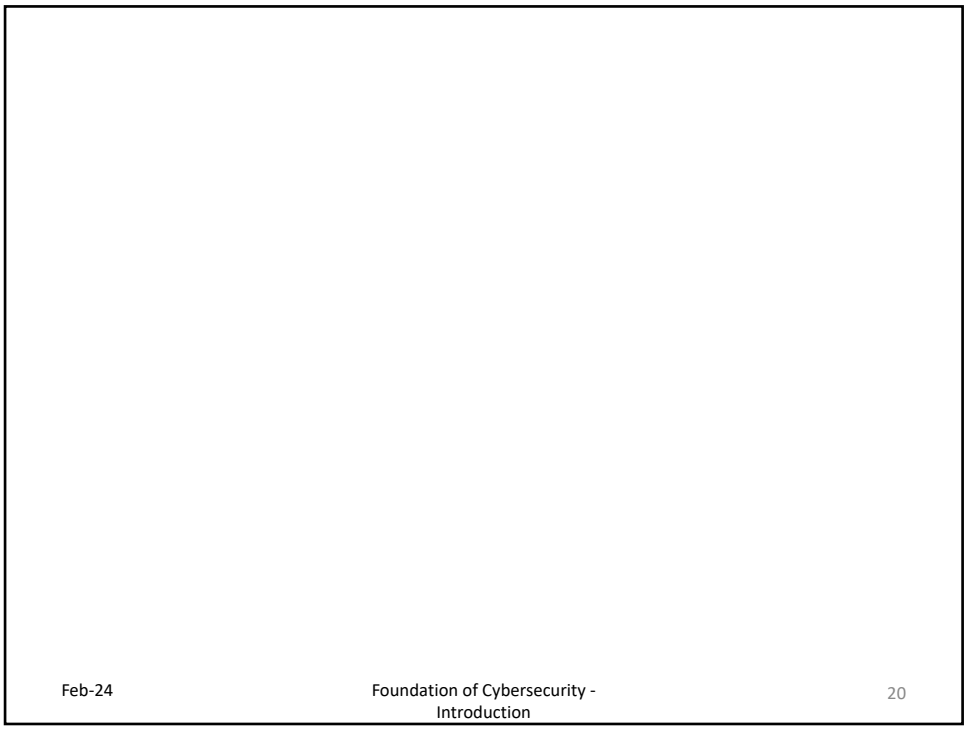
18

What is the severity of attacks?





19



20