Computer & Network Security

team:BIANCHI-8039933-COMPUTER_AND_NETWORK_SECURITY_1

Giuseppe Bianchi

Giuseppe.bianchi@uniroma2.it

Università di Roma Tor Vergata

2021

Course goals

- ➔**Understand basic crypto primitives**
  - ⇨And learn how to use (and how to… mis-use!)

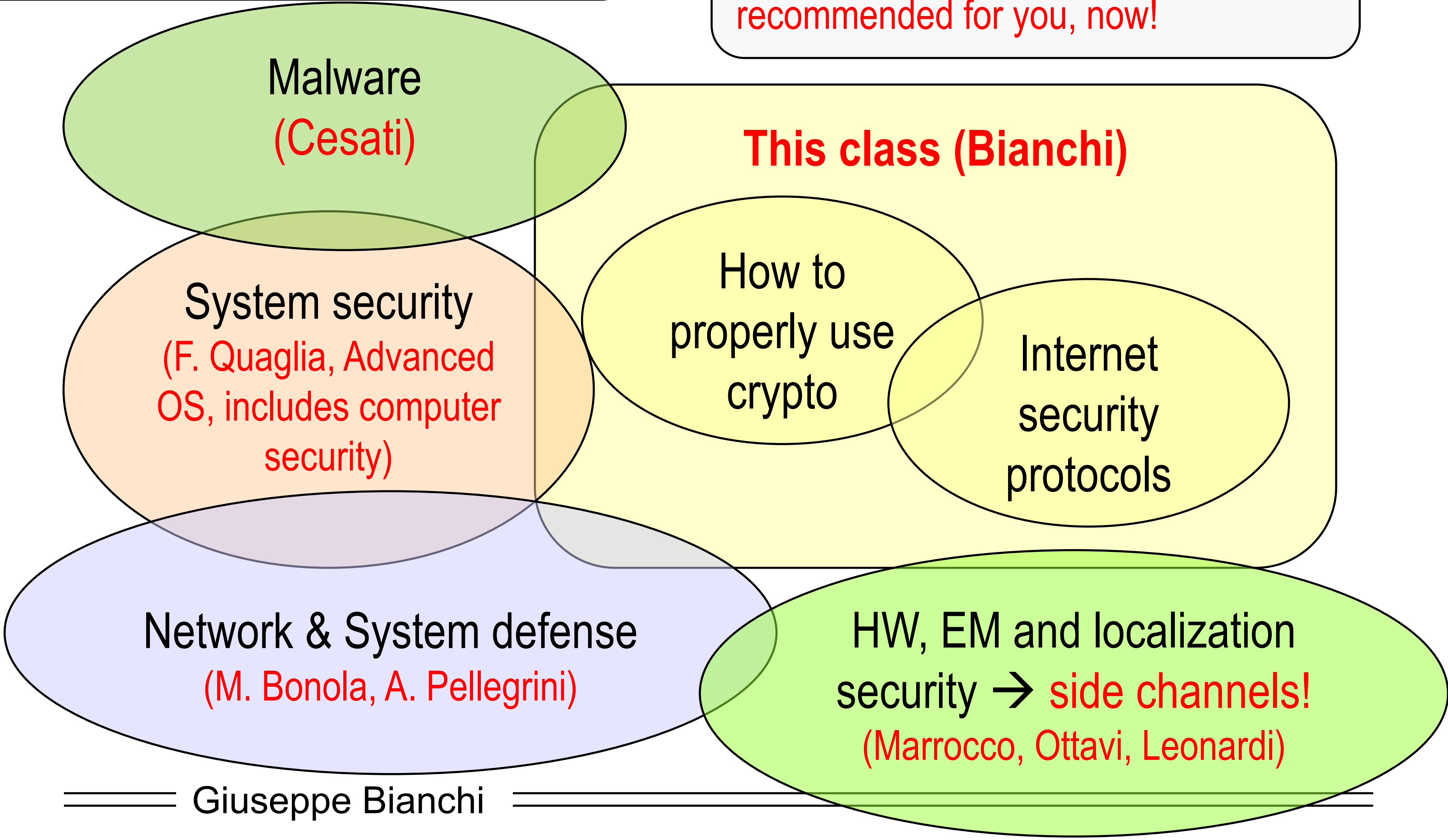
- ➔**Understand Internet Security protocols**

- ➔**Extra**
  - ⇨modern tools and their exploitation

Course positioning @ rm2

Vulnerability (→ ethical hacking)
bachelor, lab, Caponi & Bernardinetti

ICT infrastructure security
bachelor, VERY basic, Bianchi++, NOT recommended for you, now!



Malware
(Cesati)

This class (Bianchi)

How to properly use crypto

Internet security protocols

System security
(F. Quaglia, Advanced OS, includes computer security)

Network & System defense
(M. Bonola, A. Pellegrini)

HW, EM and localization security → side channels!
(Marrocco, Ottavi, Leonardi)

Our major take-home messages

- ➔**Good crypto can be badly used**
  - ⇨Most breaches exploit poor protocol constructions and/or vulnerabilities
  - ⇨Some "warm-up" examples
    - →with review of a few basic concepts

- ➔**Designing good security protocol**
  - ⇨Focus: revisit TLS (and IPsec)
  - ⇨Understand their specific choices
    - →why they did what

Our major take-home messages

- ➔ **Good crypto can be badly used**
  - ⇨ Most breaches exploit poor protocol constructions and/or vulnerabilities
  - ⇨ Some "warm-up" examples
    - → with review of a few basic concepts
- ➔ **Designing good security protocol**
  - ⇨ Focus: revisit TLS (and IPsec)
  - ⇨ Understand their specific choices
    - → why they did what

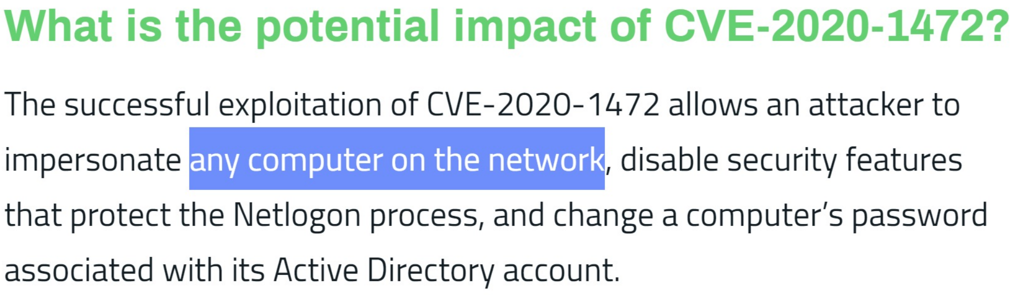
A real world story

Hello, what’s your level of security?

No worries. military grade AES encryption

Are you kidding?
When did this happen?
WiFi WEP 1998?
2G 1999 disaster?
ZeroLogon attack,
Last oct 2020!

Ooops, but you «forgot»
IV = 000000000



What is the potential impact of CVE-2020-1472?

The successful exploitation of CVE-2020-1472 allows an attacker to impersonate any computer on the network, disable security features that protect the Netlogon process, and change a computer’s password associated with its Active Directory account.

Our major take-home messages

- ➔**Good crypto can be badly used**
  - ⇨Most breaches exploit poor protocol constructions and/or vulnerabilities
  - ⇨Some "warm-up" examples
    - →with review of a few basic concepts

- ➔**Designing good security protocol**
  - ⇨Focus: revisit TLS (and IPsec)
  - ⇨Understand their specific choices
    - →why they did what

Course syllabus / 1

- ➔ **Basic crypto (≈ 1.5 CFU)**
  - ⇨ attacks, countermeasures, security services, basic cryptographic constructions (stream ciphers, block ciphers and modes, hash functions, Merkle-Damgard Construction, NMAC and HMAC, pseudo random functions, key management, public key algorithms, digital signatures, etc);
  - ⇨ Not necessarily at the beginning (we'll do this when needed)
  - ⇨ Partially overlaps with ICT infrastructure security (but better hear twice than never…)

Course syllabus / 2

- ➔**Authentication and network protocol support (≈ 1.5 CFU)**
  - ⇨basics, PPP PAP and CHAP and relevant extensions, one time passwords, EAP, authentication in 3/4/5G, RADIUS and relevant vulnerabilities; DIAMETER, Public Key Infrastructure;

Course syllabus / 3

➔in-depth analysis of TLS and Ipsec (≈ 3 CFU)

- ⇨ basics, handshake, key management with RSA, anonymous/fixed/ephemeral Diffie-Hellman and integration in TLS; perfect forward secrecy; TLS record; MAC and encryption composition (and vulnerabilities); attacks to TLS with CBC (BEAST); attacks to TLS messaging (padding oracle, side channel attacks); attacks to TLS compression (CRIME), attacks to TLS session integrity (truncation attack), attacks to TLS handshake (renegotiation attack), attacks to TLS RSA key transport (Bleickenbacker's Oracle and recent implementation attacks such as ROBOT); key derivation hierarchy and PRFs, KDFs; Brief introduction to TLSv1.3 and differences with respect to v1.2. Comparative analysis of TLS vs IPsec, VPN with IPsec, IKE.

Course syllabus / 4

- ➔**advanced crypto (≈ 3 CFU)**
  - ⇨trivial secret sharing, Shamir' secret sharing, commitments and verificable secret sharing (Feldman, Pedersen); Secure Multiparty Computation based on secret sharing; Pedersen's distributed key generation; linear secret sharing and access control matrices; threshold cryptography; threshold signatures and issues with threshold RSA (why Shoup's construction); basics of elliptic curve cryptography; ECDH; ECDSA; bilinear maps (pairing based cryptography) and example constructions (Joux 3-way DH, Boneh/Franklin Identity Based Encryption, brief intro to Attribute Based Encryption).

Course syllabus / 5

- ➔**Extras (if time permits)**
  - ⇨TESLA, Merkel Trees and their applications, Blockchain basics, selected security topics in storage, wireless, etc.
  - ⇨Further topics may be optionally addressed in dedicated talks by invited experts, depending on the year

Course modes

- ➔**6 CFU mode:**
  - ⇨Just stop up to TLS/Ipsec (incuded)
  - ⇨First 2/3 of the lectures
- ➔**9 CFU mode:**
  - ⇨Complete program

Exams

- ➔ **Last year:**
  - ⇨3 written midterm
  - ⇨Oral (or mixed written-oral) for all others
- ➔ **This year:**
  - ⇨Same, though we may reduce to two midterm…

Materiale didattico

- **Worth to have…**
  - Jean Philippe Aumasson, "***Serious Cryptography***", no-starch press, 2018
    - Very good practical treatment of crypto!
  - Nadjid Nakhjini, Mahsa Nakhjini "***AAA and Network Security for Mobile Access***", Wiley, 2005
    - Plenty of material on protocols: PPP, Radius, Diameter, EAP, IPsec, PKI, etc.
  - Stephen Thomas, "***SSL and TLS Essentials***", Wiley, 2000
    - Monography on TLS/SSL – very old (we will do much more) but very nice
- **Best ever online reference (but not for beginners)**
  - Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, "Handbook of applied cryptography", 2001,
    - http://www.cacr.math.uwaterloo.ca/hac/
- **Various extra material – will give you when needed**

Mailing list

- iss@lists.uniroma2.it
- Register at:
- https://lists.uniroma2.it/index.html/info/iss

- (though I’ll probably mainly use teams, so make sure you are in the team)