CyberSecurity: Principle and Practice
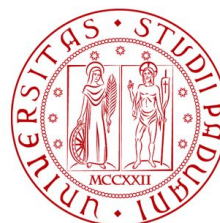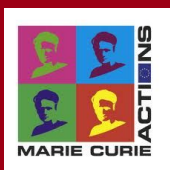
BSc Degree in Computer Science
2020-2021

Prof. Mauro Conti
Department of Mathematics
University of Padua
conti@math.unipd.it
http://www.math.unipd.it/~conti/

Teaching Assistants
Luca Pajola
pajola@math.unipd.it.
Pier Paolo Tricomi
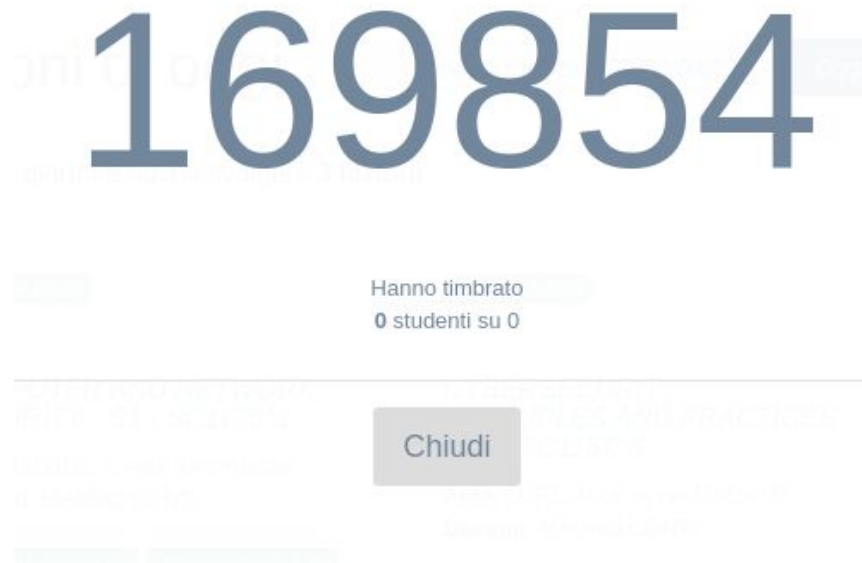pierpaolo.tricomi@phd.unipd.it

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Before Anything Else!

https://gestionedidattica.unipd.it

169854

Hanno timbrato
0 studenti su 0

Chiudi

No matter the hat...

No matter the hat...

but wear a mask!

Language:

Credits: 6 ECTS (CFU)

Schedule: BSc III year, **I semester**
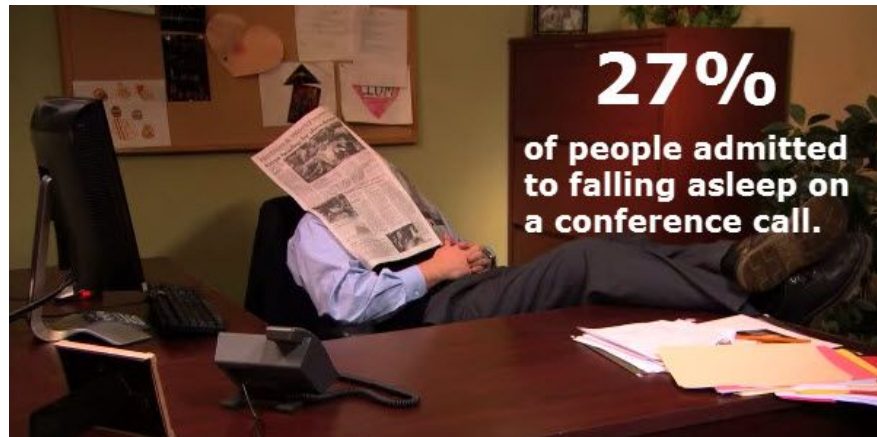   A day-by-day schedule will be available on course or
   group page

Course website:
https://www.math.unipd.it/~conti/teaching/CPP2021

You can attend the course <u>either at the University or online</u>.
<u>Lectures will be also recorded</u> and available in the Moodle platform.

Sleeping during the class is optional, but not recommended.

Cyber security areas:
- *Cryptography*
  - Ciphers; hash functions; symmetric/asymmetric encryption
- *Web Vulnerabilities*
  - Bad programming practices; injections; language vulnerabilities.
- *Reverse Engineering*
  - Reversing techniques; patching; anti-debug.
- *Pawning*
  - Buffer overflow; defenses; Return Oriented Programming; Global Offset Table.

Each lesson consists in ~30' of theory and ~60' of exercises

The final exam has three different formats, among which students can <u>choose one</u>

- **Final Exam**:
  - set of exercises covering the course topics
- **Three practical exercises:**
  - to be solved only during the semester course
- **A research project:**
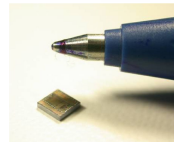 - possibly interacting also with security researcher (<u>SPRITZ group</u>)
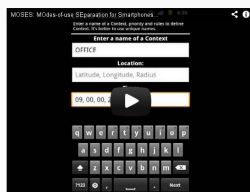
Security/privacy in: wired/wireless networks, smartphones, social networks, distributed systems, sensor networks, RFID, cloud computing, content centric networking, vehicular networks, location based services, ...

FakeBook: Detecting Fake Profiles in On-line Social Networks

NDN Interest Flooding Attacks and Countermeasures

CRêPE: A System for Enforcing Fine-Grained Context-Related Policies on Android

MOSES: MOdes-of-use SEparation for Smartphones

32 Innovations That Will Change Your Tomorrow

16 Your Body, Your Login

The New York Times

SMART TEETH

9

What "secure" means?

Some key concepts to start with...

1) Security is not just "a product" (e.g. a firewall); it is rather a "process", which needs to be managed properly

2) Nothing is 100% secure
   (do we need it? How much it would cost?)
   Example: credit cards

"The three golden rules for ensuring computer security: do not own a computer; do not power it on; and do not use it."
– Robert (Bob) Morris (Former NSA Chief Scientist).

3) The security of a
system is equivalent to the
security of its less secure
component
(rule of the weakest link)

4) Security by obscurity never works
5) Cryptography is a powerful tool but...
   it is not enough!

4) Security by obscurity never works
5) Cryptography is a powerful tool but…
    it is not enough!

4) Security by obscurity never works
5) Cryptography is a powerful tool but…
   it is not enough!

4) Security by obscurity never works
5) Cryptography is a powerful tool but...
   it is not enough!

6) Do not rely on users!

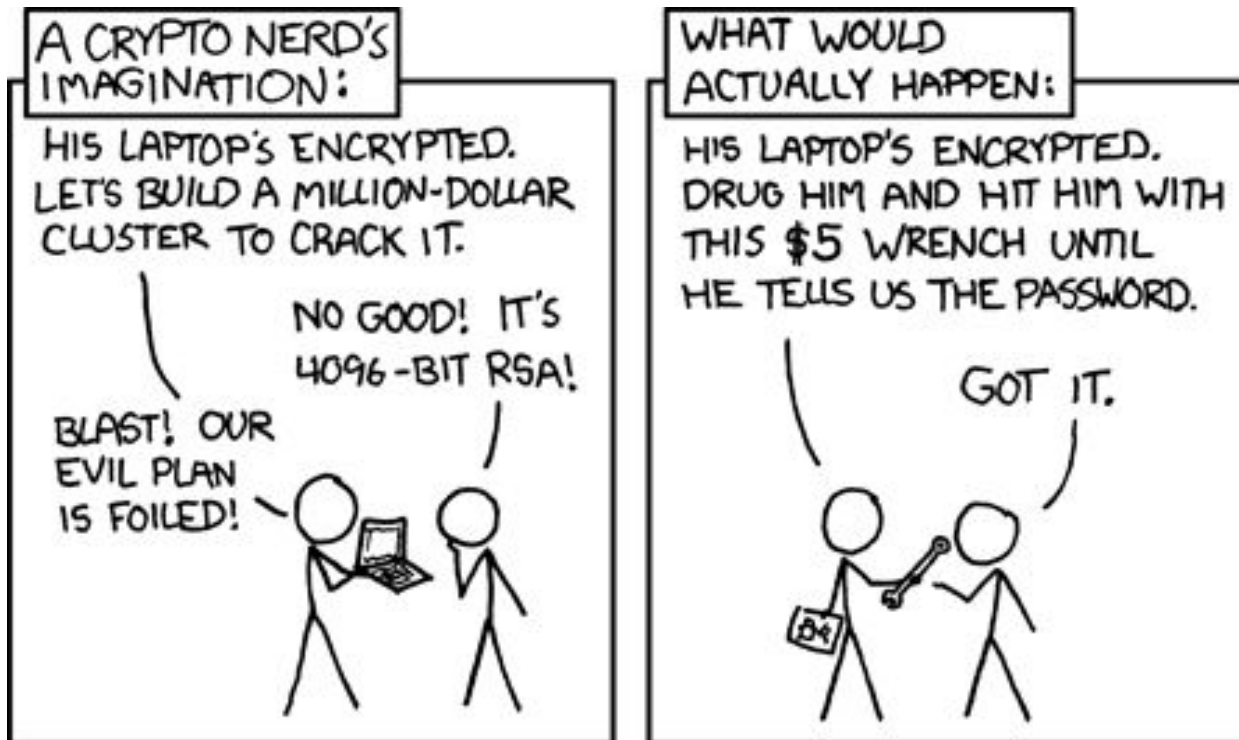*"Given a choice between dancing pigs and security, users will pick dancing pigs everytime."*
- Prof. Ed Felten (Princeton University)

*"If the computer prompts him with a warning screen like: "**The applet DANCING PIGS could contain malicious code that might do permanent damage to your computer, steal your life's savings, and impair your ability to have children**," he'll click OK without even reading it. Thirty seconds later he won't even remember that the warning screen even existed"*
- Bruce Schneier

So, what "secure" means?
A network/system is secure when…

Basic security properties

- Confidentiality: to prevent unauthorised disclosure of the information

- Integrity: to prevent unauthorised modification of the information

- Availability: to guarantee access to information

- Authentication: to prove the claimed identity can be Data or Entity authentication

- Non repudiation: to prevent false denial of performed actions
- Authorisation: "What Alice can do"
- Auditing: to securely record evidence of performed actions
- Attack-tolerance: ability to provide some degree of service after failures or attacks
- Disaster Recovery: ability to recover a safe state
- Key-recovery, key-escrow, ...
- Digital Forensics

Security mechanisms

- Random Numbers (e.g. for Initialization Vectors)
- Pseudo Random Numbers
- Encryption/Decryption
- Hash functions
- Hash chain (inverted)
- Message integrity code (MIC)
- Message authentication code (MAC and HMAC)
- Digital signatures
  - Non repudiation
- Key exchange (establishment) protocols
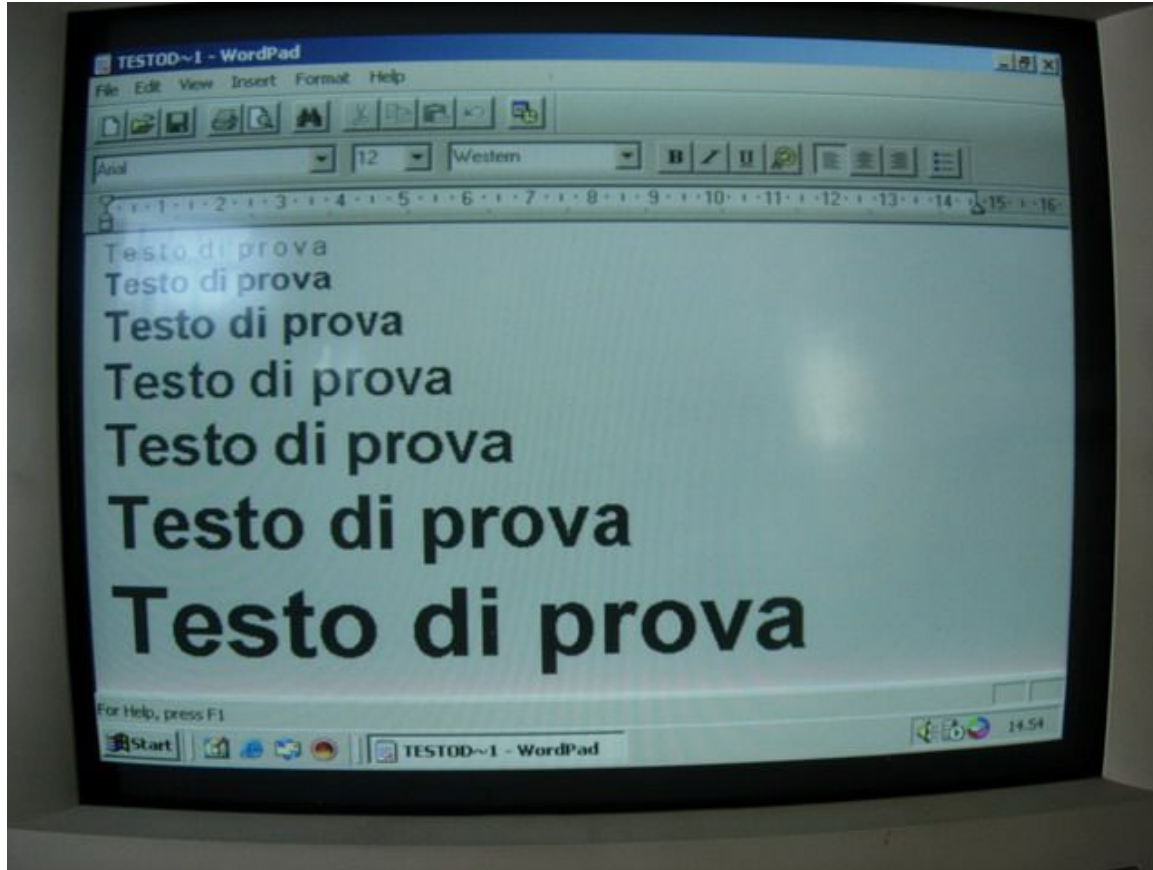- Key distribution protocols
- Time stamping

security domain

outsiders

insiders

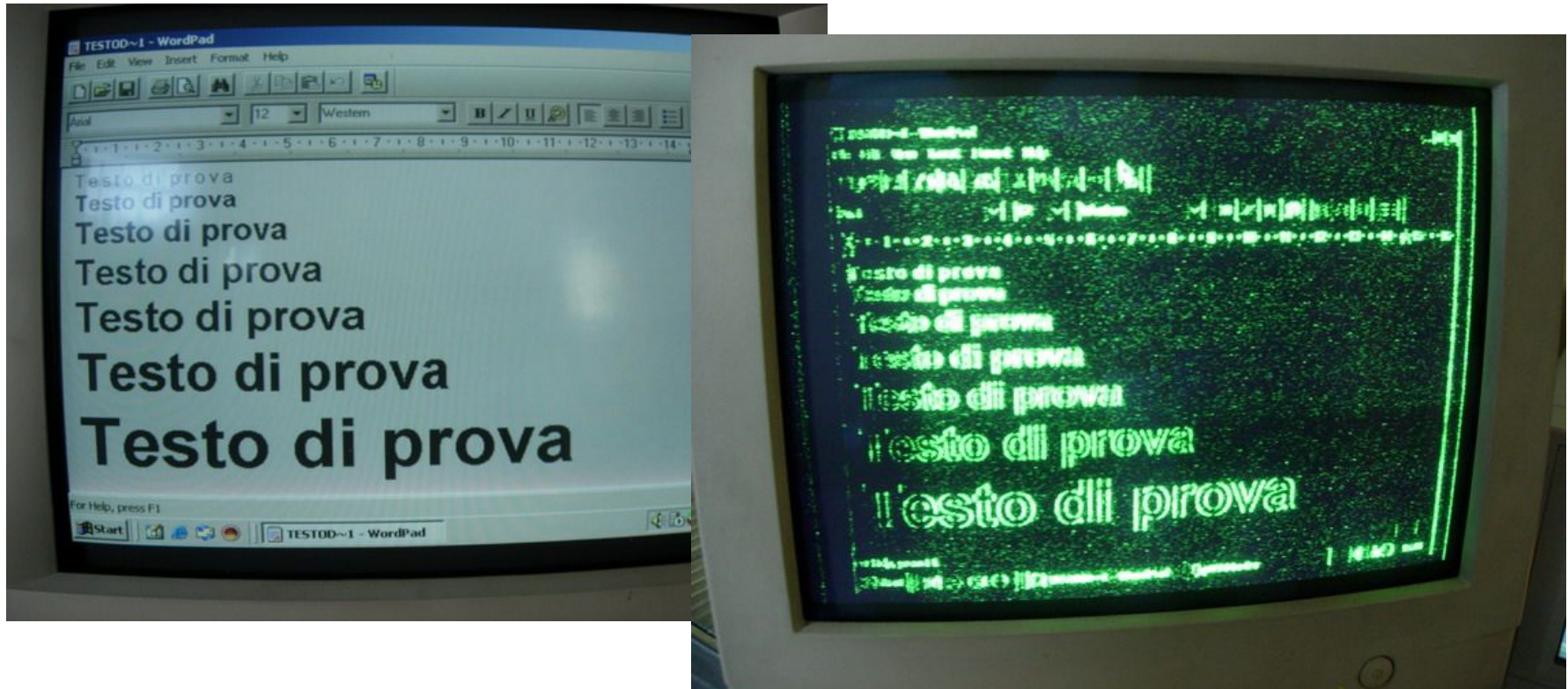adm$_1$

adm$_2$
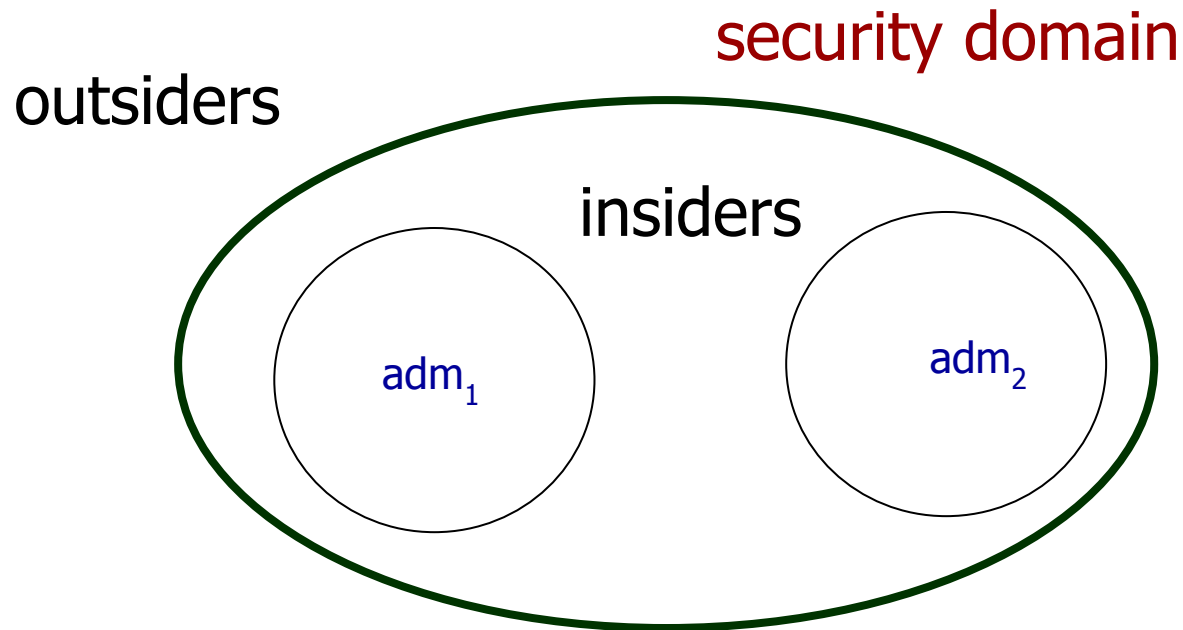
security domain and admin domain may differ

- Passive: the attacker can only read any information
  - Tempest (signal intelligence)
  - Packet Sniffing

- Active: the attacker can read, modify, generate, destroy any information

- More recent attack approaches
  Big Data => User profiling