

# CyberSecurity: Principle and Practice

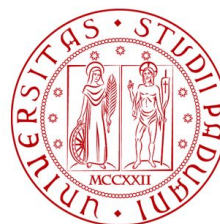
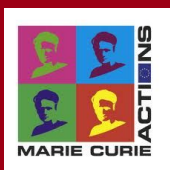
*BSc Degree in Computer Science  
2023-2024*

**Prof. Mauro Conti**

Department of Mathematics  
University of Padua  
conti@math.unipd.it  
<http://www.math.unipd.it/~conti/>

**Teaching Assistants**

Tommaso Bianchi  
tommaso.bianchi@phd.unipd.it  
Riccardo Preatoni  
riccardo.preatoni@studenti.unipd.it



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA



SPRITZ  
SECURITY & PRIVACY  
RESEARCH GROUP



DIPARTIMENTO  
**MATEMATICA**

Language:



Credits: 6 ECTS (CFU)

Schedule: BSc II year, **I semester**

A day-by-day schedule will be available on course or group page

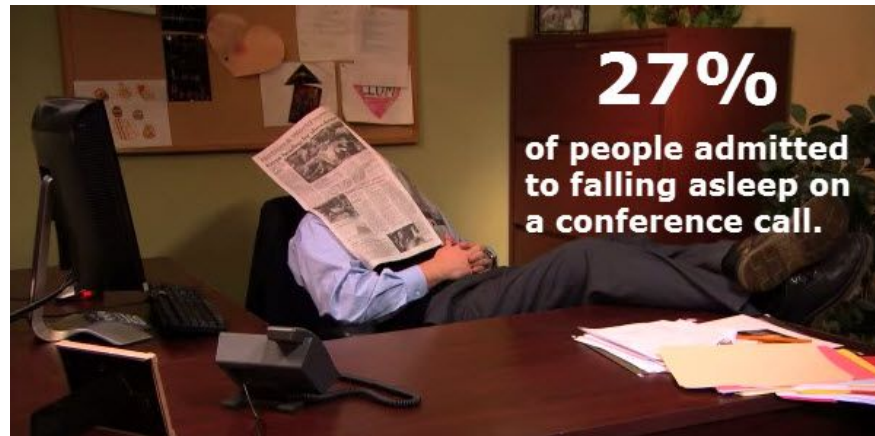
Course website:

<https://www.math.unipd.it/~conti/teaching/CPP2324>

You can attend the course in presence at the University, but for exceptional cases (e.g. Covid or Visa problem) the class can be followed online.

Lectures will be also recorded 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.
- *Pwning*
  - 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 choose one

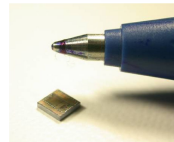
- **Final Exam:**
  - set of exercises covering the course topics
- **Three practical exercises:**
  - to be solved only during the semester course
- **A research project:**
  - possibly interacting also with security researcher ([SPRITZ group](#))

# Spritz Group Project Topic



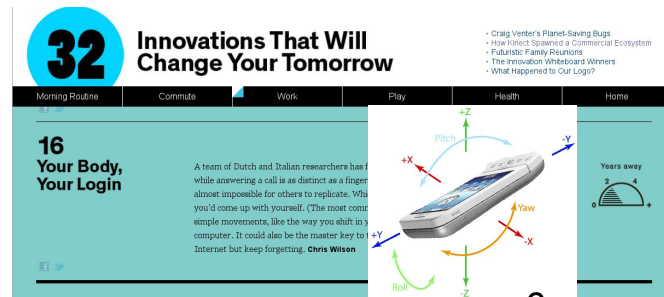
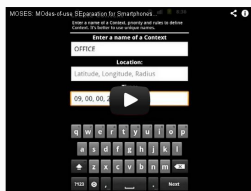
UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

Security/privacy in: wired/wireless networks, smartphones, social networks, distributed systems, sensor networks, RFID, cloud computing, content centric networking, vehicular networks, location based services, ...



## MOSES: MODES-of-use SEparation for Smartphones

Demo



## FakeBook: Detecting Fake Profiles in On-line Social Networks

Mauro Conti  
University of Padua  
Via Trieste, 63 - Padua, Italy  
conti@math.unipd.it

Radha Poovendran  
University of Washington  
Seattle, WA 98195, USA  
rp3@uw.edu

Marco Secchiero  
University of Padua  
Via Trieste, 63 - Padua, Italy  
marco.secchiero@studenti.unipd.it

**Abstract**—On-line Social Networks (OSNs) are increasingly influencing the way people communicate with each other and share personal, professional and political information. Like the cyberspace in Internet, the OSNs are attracting the interest of

prevent. The first attack in [7] is called Identity Cloning Attack (ICA), where the personal OSN information of an existing profile is used to create one or more clone accounts, claiming the same identity as the victim in a given OSN. The Identity

## NDN Interest Flooding Attacks and Countermeasures

Alberto Compagno\*, Mauro Conti\*, Paolo Gasti†, Gene Tsudik‡  
\*University of Padua, Italy — acompagn@studenti.math.unipd.it  
†University of Padua, Italy — conti@math.unipd.it  
‡New York Institute of Technology, USA — pgasti@nyit.edu  
§University of California, Irvine, USA — gts@uci.edu

1426

IEEE TRANSACTION ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 5, OCTOBER 2012

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

Mauro Conti, Member, IEEE, Bruno Crispo, Senior Member, IEEE, Earlene Fernandes, and Yury Zhauniarovich

**Abstract**—Current smartphone systems allow the user to use only marginally contextual information to specify the behavior of the applications: this hinders the wide adoption of this technology to its full potential. In this paper, we fill this gap by proposing CRêPE, a fine-grained Context-Related Policy Enforcement

researchers have recently focused on enhancing phones' security models and their usability.

One significant challenge in the security of smartphones is to control the behavior of applications.

no experimental  
s (i.e., bandwidth,  
to the adversary,  
asures deserve an  
considered ready



# 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).



# Some key concepts to start with...



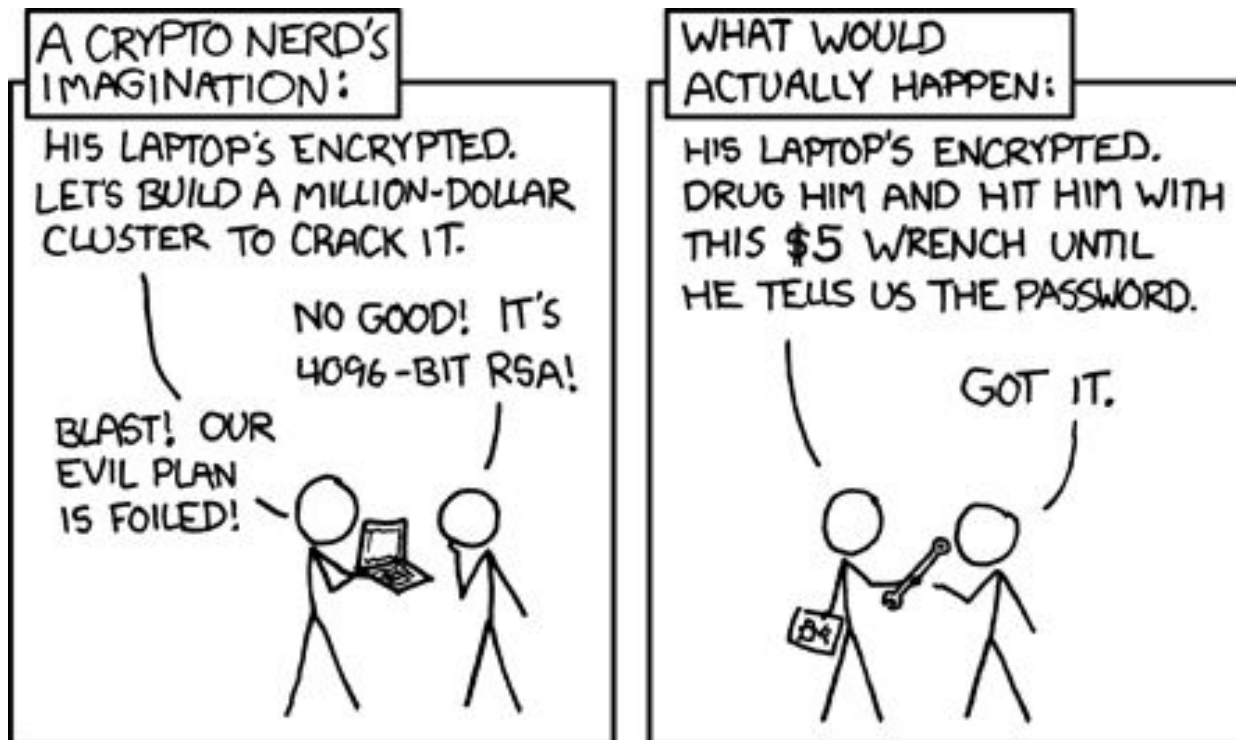
3) The security of a system is equivalent to the security of its less secure component  
(rule of the weakest link)



# Some key concepts to start with...



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



# Some key concepts to start with...



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



# Some key concepts to start with...



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

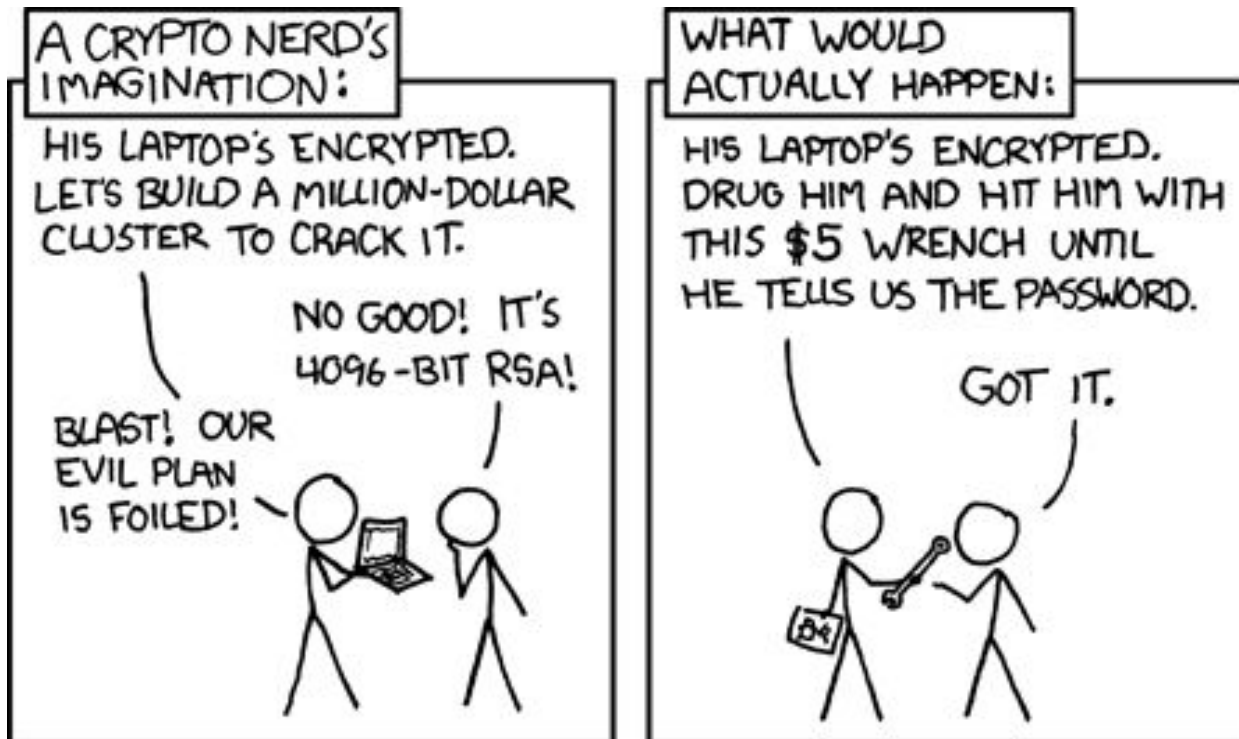




# Some key concepts to start with...



- 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...





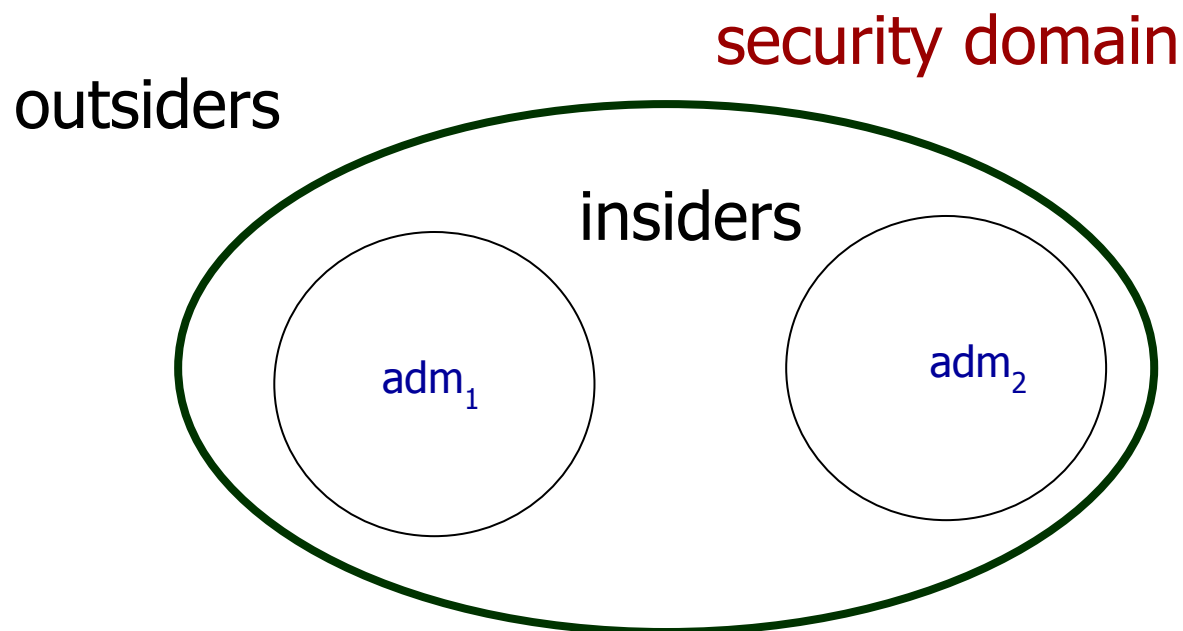
- **Confidentiality:** to prevent unauthorised disclosure of the information
- **Integrity:** to prevent unauthorised modification of the information
- **Availability:** to guarantee access to information
- **Authentication:** to prove the claimed identity can be Data or Entity authentication



- **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**

- 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



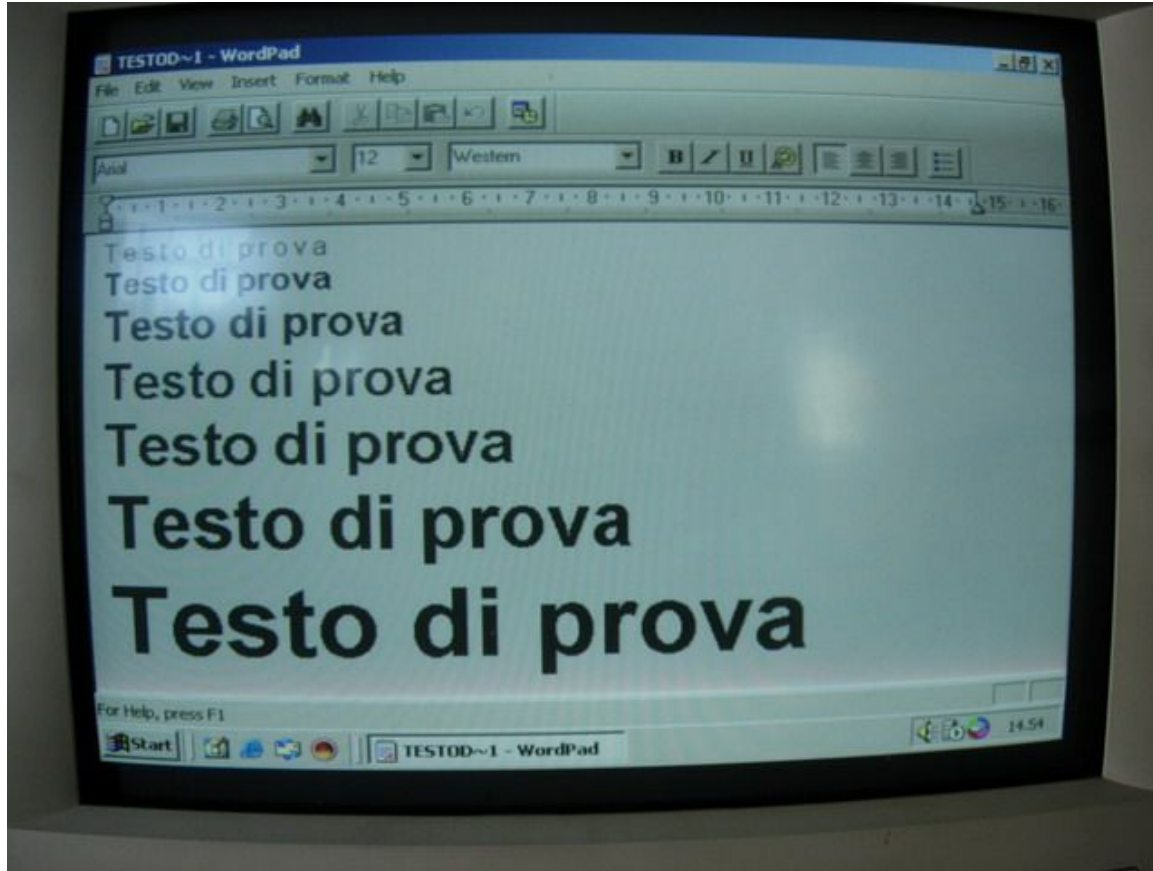


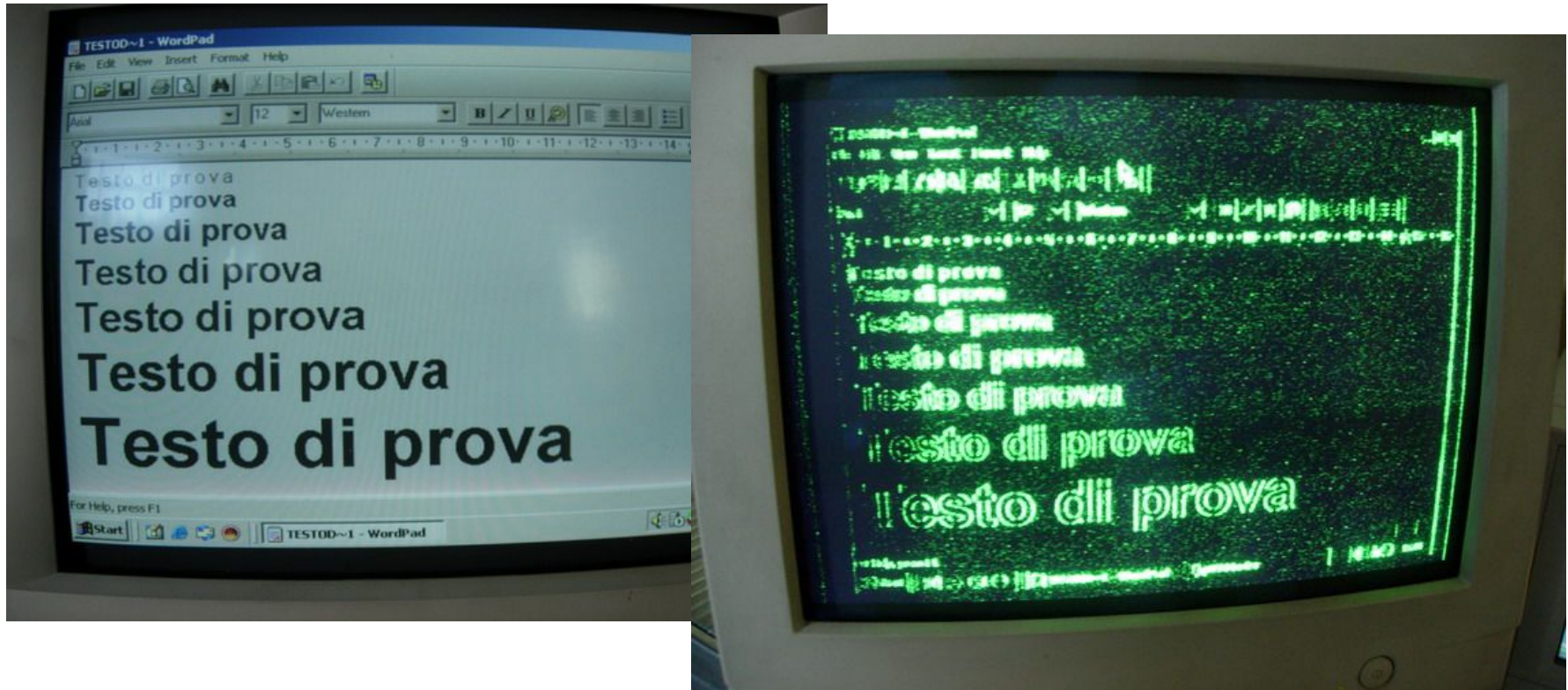
security domain and admin domain may differ

- **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

# Questions? Feedback? Suggestions?



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA

