# CyberSecurity: Principle and Practice

*BSc Degree in Computer Science*
*2019-2020*


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

Teaching Assistants
Luca Pajola
luca.pajola@phd.unipd.it.
Eleonora Losiouk
elosiouk@math.unipd.it


MARIE CURIE ACTIONS

UNIVERSITÀ DEGLI STUDI DI PADOVA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

DIPARTIMENTO MATEMATICA

# Basic Information

Università degli Studi di Padova

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/CPP1920/index.html

Course Group/Mailing List:

Google Group "CPP_1920_UNIPD"

# Course Content



**Topics**

- Cryptography
- User authentication
- Access control
- Database security
- Malware
- Denial of service
- Intrusion detection
- Buffer overflow attacks
- Software/hardware security
- Operating system security
- Trusted computing and multilevel security

For each topic there will be a theoretical and a practical lesson.

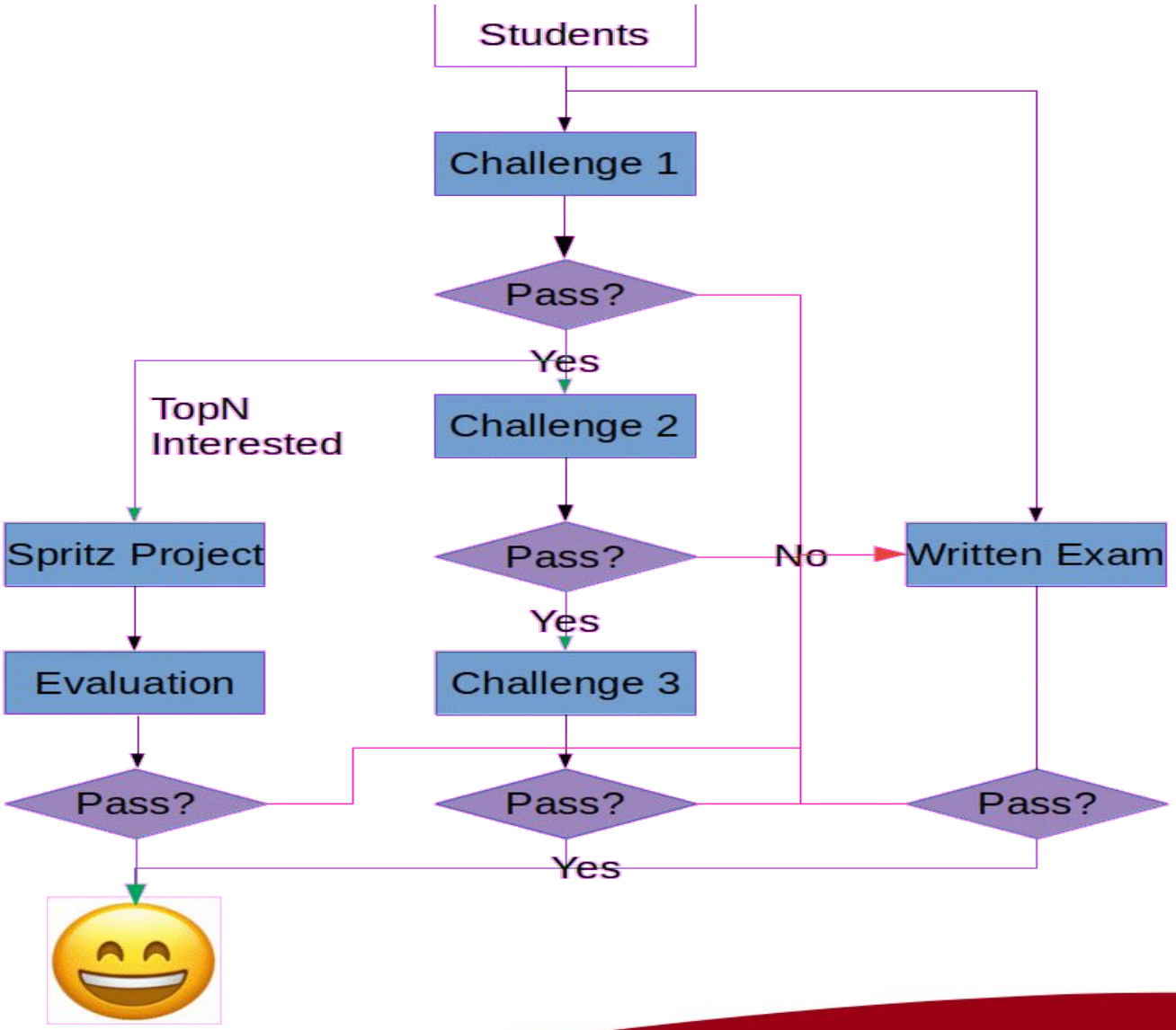
# Grading criteria



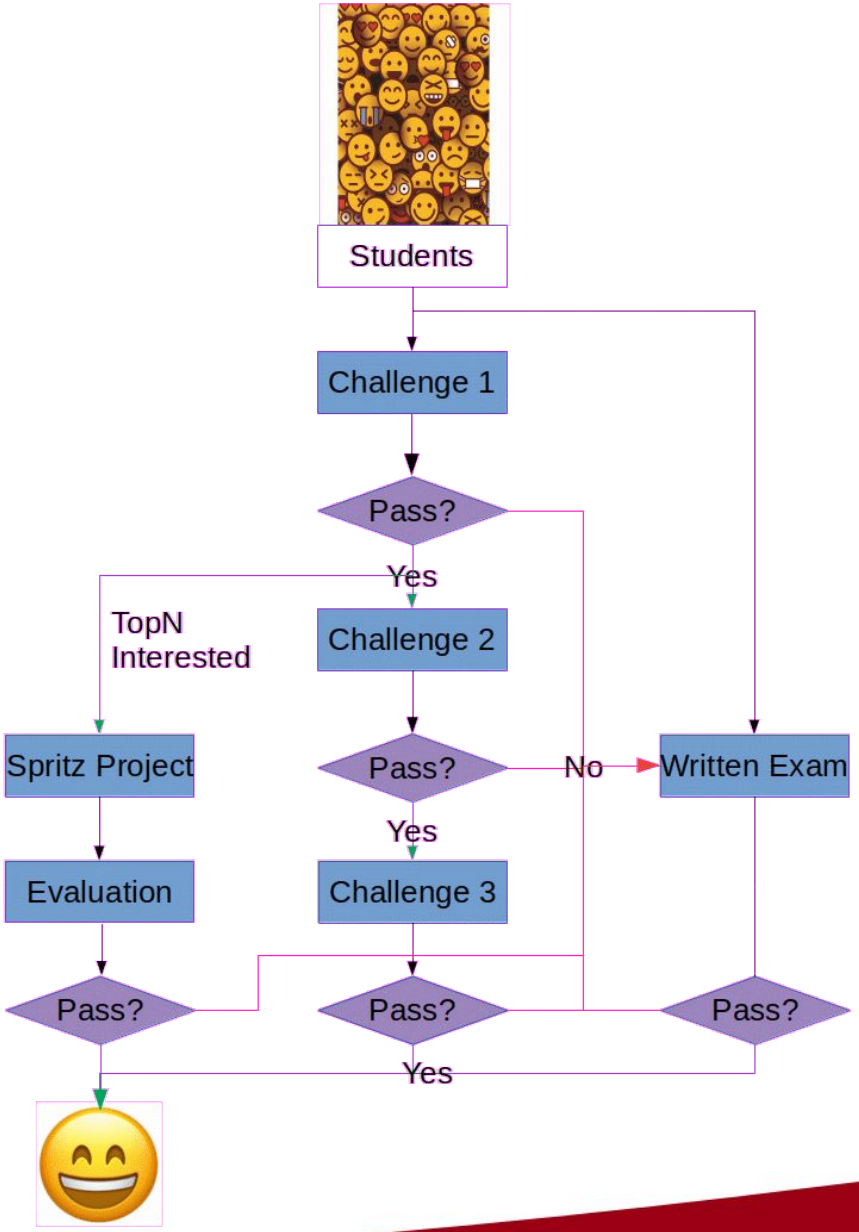
The final exam has three different formats, among which students can choose one:

- **Three practical exercises** (i.e., Challenge 1, Challenge 2 and Challenge 3) to be solved only during the semester course
- **A research project** to be done under the supervision of a member of the SPRITZ group - students that choose this option will be selected either through the first Challenge or through an interview with the lecturer and the teaching assistants
- **Written exam** - students are required to be confident with all the concepts introduced during the course in order to answer to the 30 questions of the written exam. For each question the score is:
  - +1 if the answer is correct
  - -1 if the answer is wrong
  - 0 otherwise

# Grading criteria



# Grading criteria



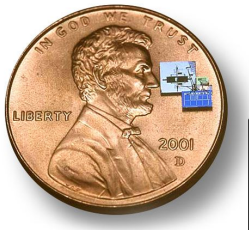

Additional info:

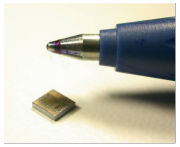
- **All students** can apply for a Spritz Group project and not only the *topN* candidates that pass the first challenge. However, the acceptance of such students is made by the lecturer and the assistants after an interview
- A Spritz project could evolve into a **thesis project**
- The challenges can be done **only** during the course

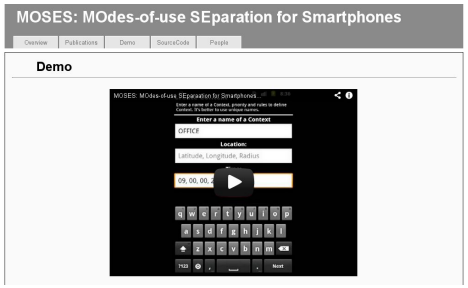
# Spritz Group Project Topic

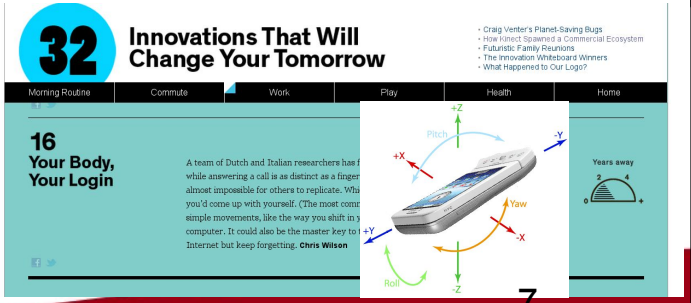


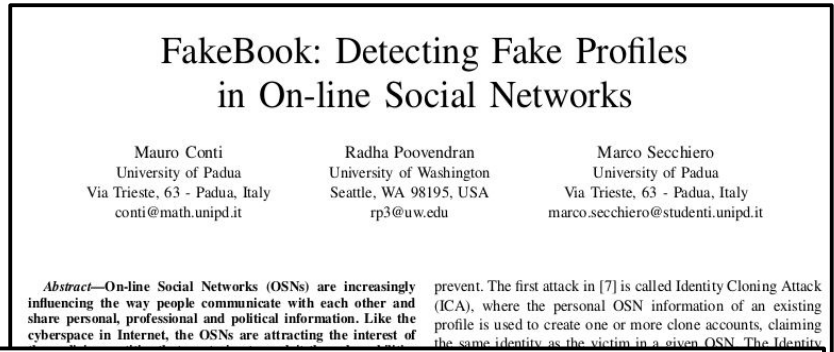
Security/privacy *in: wired/wireless networks, smartphones, social networks, distributed systems, sensor networks, RFID, cloud computing, content centric networking, vehicular networks, location based services, ...*



FakeBook: Detecting Fake Profiles in On-line Social Networks

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

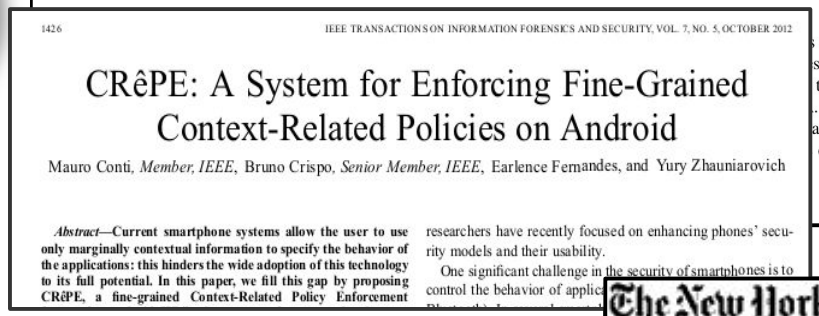
*Abstract*—On-line Social Networks (OSNs) are increasingly influencing the way people communicate with each other and share personal, professional and political information. Like the cyberspace in Internet, the OSNs are attracting the interest of

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

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

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



1426 IEEE TRANSACTIONS 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*, Earlence 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 applic

# CNS course “Hall of fame”

Università degli Studi di Padova

## Can’t you hear me knocking: Identification of user actions on Android apps via traffic analysis

ACM CODASPY (a.r. 21%)


Mauro Conti, University of Padua, Padua, Italy, conti@math.unipd.it
Luigi V. Mancini, Sapienza University of Rome, Rome, Italy, lv.mancini@di.uniroma1.it
Riccardo Spolaor, University of Padua, Padua, Italy, spolaor.riccado@gmail.com


## OASIS: Operational Access Sandboxes for Information Security

ACM CCS SPSM 2014


Mauro Conti *, Università di Padova, Padova, Italy, conti@math.unipd.it
Earlence Fernandes, University of Michigan, Ann Arbor, Michigan, USA, earlence@umich.edu
Justin Paupore, University of Michigan, Ann Arbor, Michigan, USA, jpaupore@umich.edu
Atul Prakash, University of Michigan, Ann Arbor, Michigan, USA, aprakash@umich.edu
Daniel Simionato, Università di Padova, Padova, Italy, daniel.simionato@gmail.com


## LineSwitch: Efficiently Managing Switch Flow in Software-Defined Networking while Effectively Tackling DoS Attacks

ACM ASIACCS 2015 (a.r. 20%)


Moreno Ambrosin, Mauro Conti, Fabio De Gaspari, University of Padua, Italy, {surname}@math.unipd.it, fabio.degaspari@studenti.unipd.it
Radha Poovendran, University of Washington, USA, rp3@uw.edu


## Boten ELISA: A Novel Approach for Botnet C&C in Online Social Networks

IEEE CNS 2015 (a.r. 28%)


Alberto Compagno*, Mauro Conti†, Daniele Lain†, Giulio Lovisotto† and Luigi Vincenzo Mancini*
*Department of Computer Science, Sapienza University of Rome. Via Salaria 113, 00198 Rome, Italy
Email: {compagno, mancini}@di.uniroma1.it
†Department of Mathematics, University of Padua. Via Trieste 63, 35121 Padua, Italy


## Losing Control: On the Effectiveness of Control-Flow Integrity under Stack Attacks

ACM CCS 2015 (a.r. 19.81%)


Mauro Conti*, Stephen Crane‡, Lucas Davi†, Michael Franz‡, Per Larsen‡, Christopher Liebchen†, Marco Negro†, Mohaned Qunaibit†, Ahmad-Reza Sadeghi†
†CASED, Technische Universität Darmstadt, Germany
‡University of California, Irvine
*University of Padua, Italy



IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 4, APRIL 2016 665


## Security Vulnerabilities and Countermeasures for Target Localization in Bio-NanoThings Communication Networks

IEEE TIFS (i.F. 2.408)


Alberto Giaretta, Sasitharan Balasubramaniam, *Senior Member, IEEE*, and Mauro Conti, *Senior Member, IEEE*


## CAPTCHaStar

Università degli Studi di Padova — SPRITZ Security & Privacy Research Group

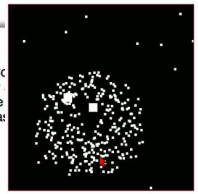
**Survey**

PATENT PENDING

**What is a CAPTCHA?**

CAPTCHA is an acronym that stands for Completely Automated Public Turing test to tell Co
practice, a CAPTCHA is a test used to check whether a computer system is being used by
automated program). CAPTCHAs are useful to avoid the abuse of online services by some
registration of e-mail addresses to send spam. The most common CAPTCHA is the text bas

distorted text (e.g. ) in a text-box.
We are working to design a novel CAPTCHA that we named **CAPTCHaStar**.
By taking part in this survey you will help us to provide a better CAPTCHA.
The survey will take only few minutes (some 10 minutes) and you might enjoy it.
Thanks for your help!



Agostino Sturato (Interconnected networks) -IEEE ICNC 2016)

… and several on-going works:

- Marco Ulgelmo (Name Data Networking)
- Daniele Lain (Keystroke)
- Giulio Lovisotto (De-authentication)

# 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)

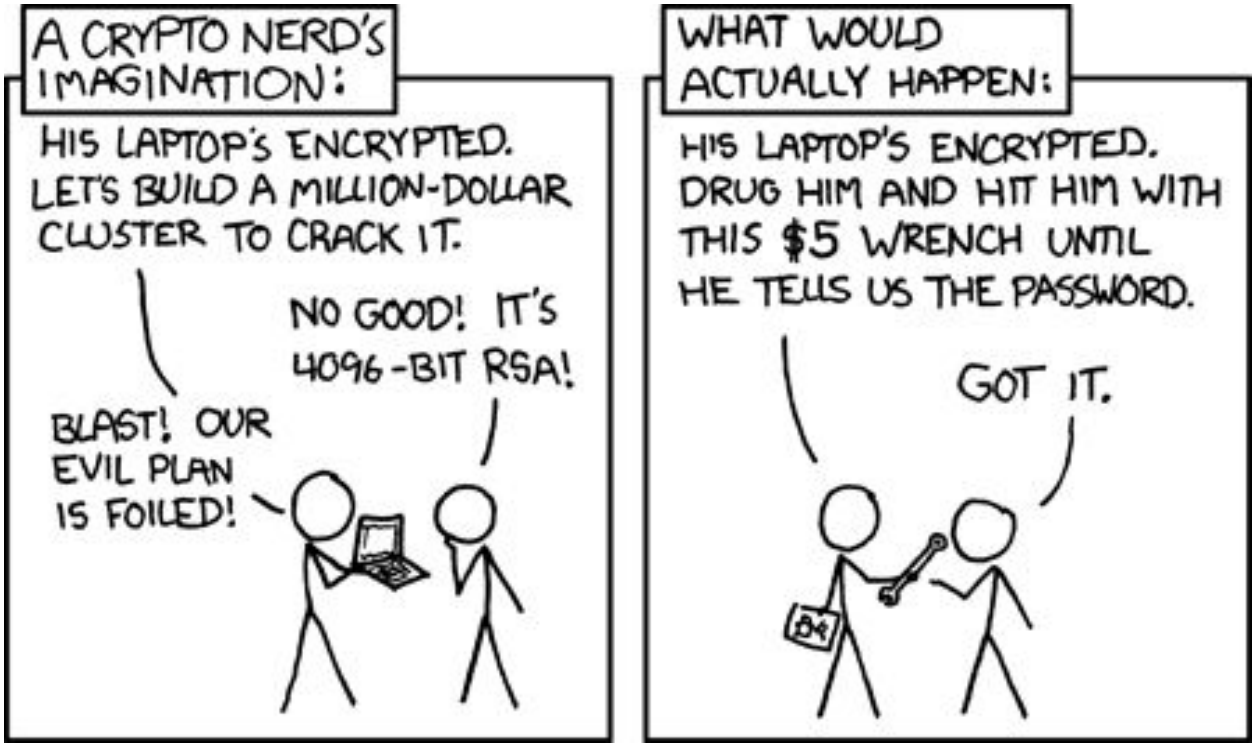
# Some key concepts to start with...



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

*"The protection provided by encryption is based on the fact that most people would rather eat liver than do mathematics"*

*Bill Neugent*



# Some key concepts to start with...



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

*"The protection provided by encryption is based on the fact that most people would rather eat liver than do mathematics"*

*Bill Neugent*


# Some key concepts to start with...

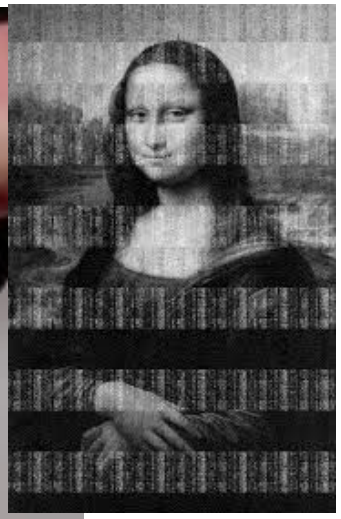


4) Security by obscurity never works
5) Cryptography is a powerful tool but...
it is not enough!

*"The protection provided by encryption is based on the fact that most people would rather eat liver than do mathematics"*

*Bill Neugent*





# Some key concepts to start with...



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

*"The protection provided by encryption is based on the fact that most people would rather eat liver than do mathematics"*

*Bill Neugent*


# Some key concepts to start with...



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

*"The protection provided by encryption is based on the fact that most people would rather eat liver than do mathematics"*

*Bill Neugent*



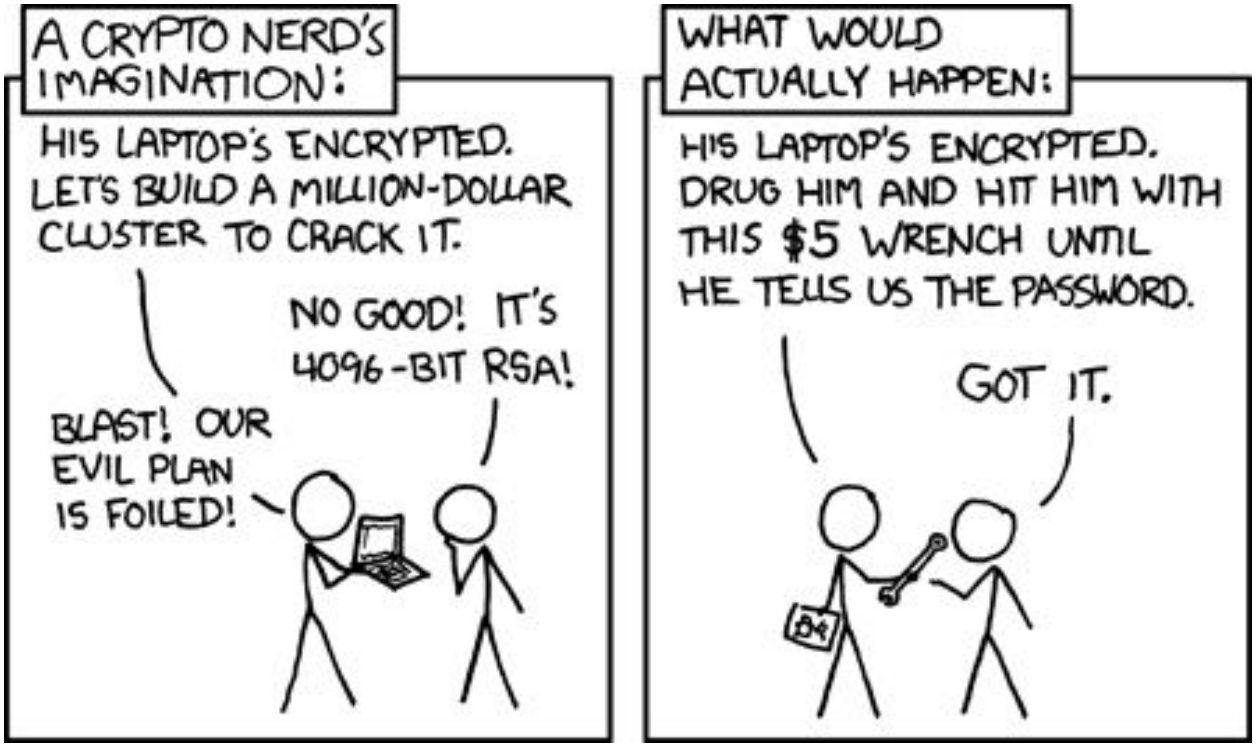
# Some key concepts to start with...



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

*"The protection provided by encryption is based on the fact that most people would rather eat liver than do mathematics"*

*Bill Neugent*




# Some key concepts to start with...



## 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

# Auxiliary security properties



- 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

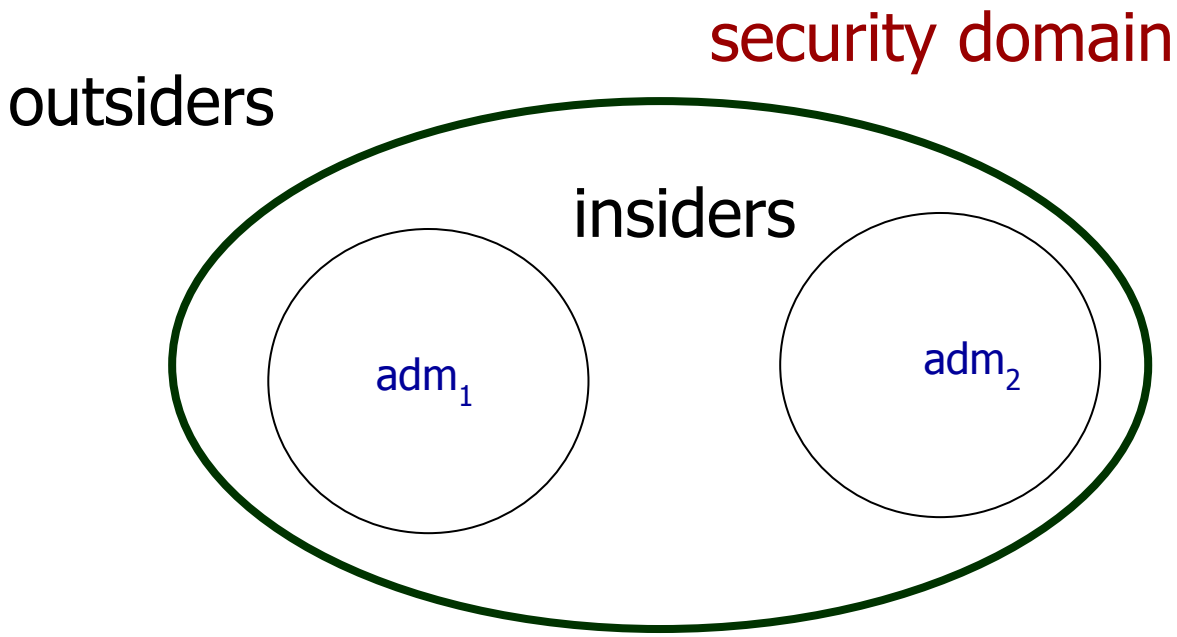
# Security mechanisms



- 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

# Types of attacker






security domain and admin domain may differ

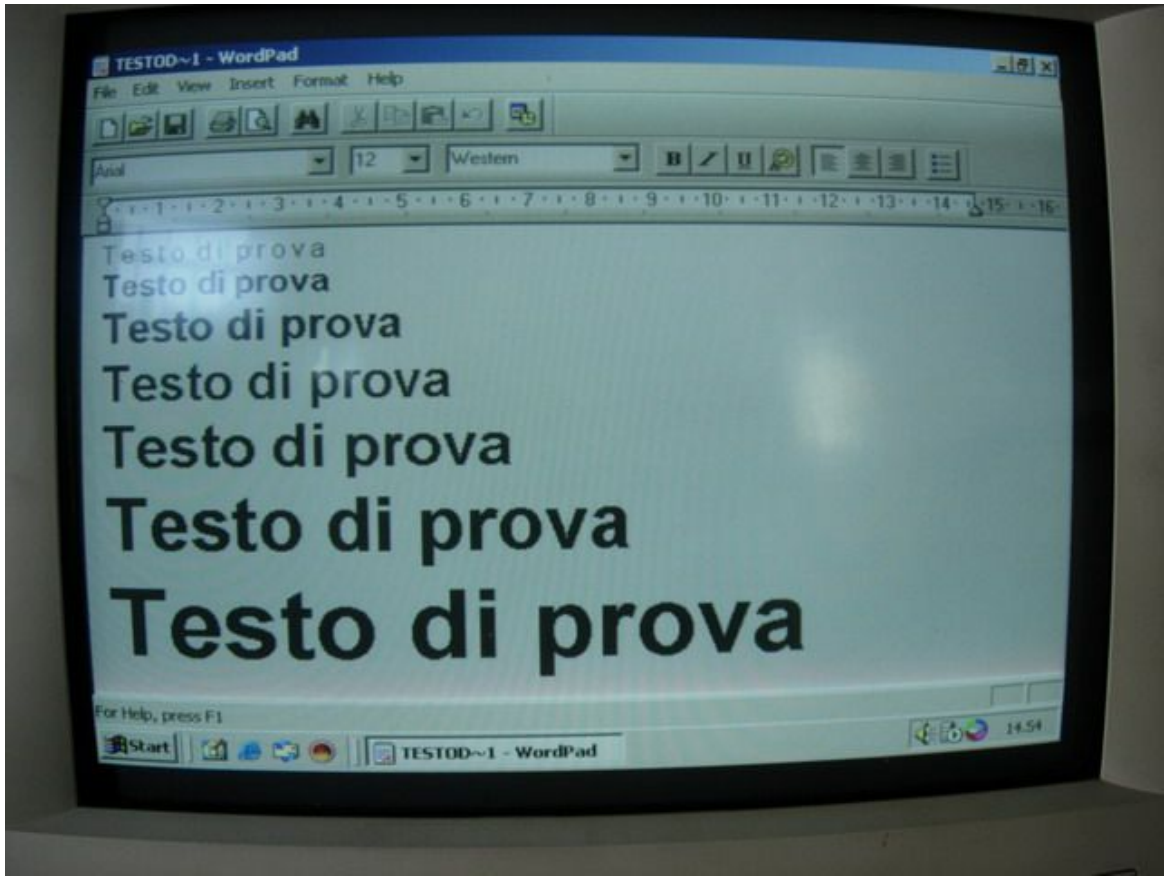
# Types of attack



- Passive: the attacker can only read any information
  - Tempest (signal intelligence)
  - Packet Sniffing
- Active: the attacker can read, modify, generate, destroy any information

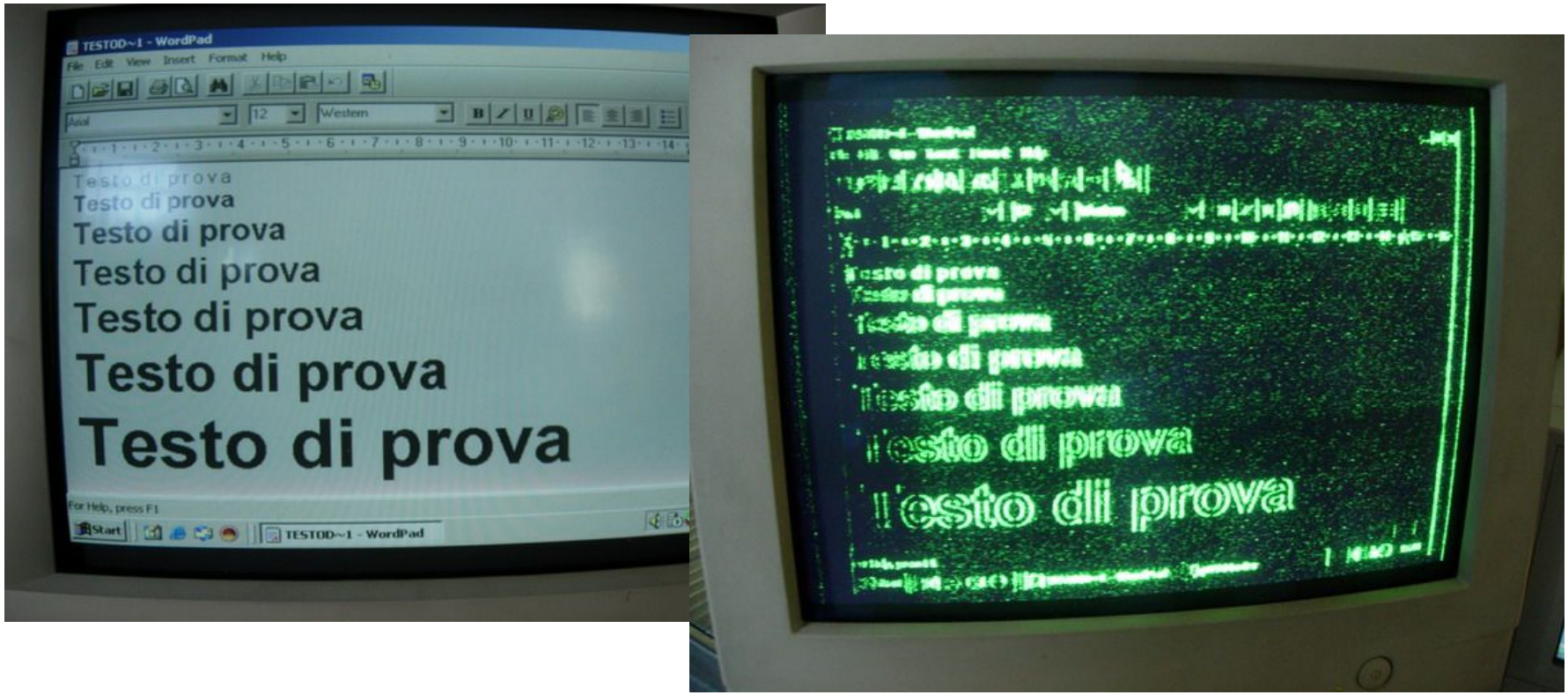
# TEMPEST




TESTOD~1 - WordPad
File Edit View Insert Format Help
Arial
12
Western
Testo di prova
Testo di prova
Testo di prova
Testo di prova
Testo di prova
Testo di prova
Testo di prova
For Help, press F1
Start
TESTOD~1 - WordPad
14:54

# TEMPEST






- More recent attack approaches

  Big Data => User profiling

# Questions? Feedback? Suggestions?