Computer and Networks Security: Advanced Topics

MSc Degrees in
CyberSecurity / Computer Science / Data Science
Academic Year 2023-2024

Course Introduction

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

Teaching Assistants
Francesco Marchiori
francesco.marchiori@math.unipd.it
Alessandro Lotto
alessandro.lotto@phd.unipd.it

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

DIPARTIMENTO MATEMATICA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

UNIVERSITÀ DEGLI STUDI DI PADOVA

Before Anything Else!

https://gestionedidattica.unipd.it

No matter the hat...

No matter the hat...

but wear a mask!

Basic Information

Language: 

Credits: 6 ECTS (CFU) / 48 hours

Schedule:

- Wed 8.30 to 10.30 Room: 2C (Via del Pescarotto, 8)
- Thu 8.30 to 10.30 Room: 2C (Via del Pescarotto, 8)

Course reference websites:

- https://stem.elearning.unipd.it/course/view.php?id=7309
- https://www.math.unipd.it/~conti/teaching/CNS2324/

Basic Information

The attendance of the course is in person. Students which are abroad for problems with VISA can attend using the Zoom link.

Lectures will be also recorded and available in the Moodle platform. Alternatively, slides will be made available.

A day-by-day lecture content will be available on course websites.

Basic Information

This is intended to be an interactive class: class participation is strongly recommended (and will play a role in the grading criteria).

Basic Information

This is intended to be an interactive class: class participation is strongly recommended (and will play a role in the grading criteria).

Sleeping during the class is optional, but not recommended.

Course Content

Learning Objectives:
This course is about learning to study, analize, discuss, criticize and work on advanced topics (and research) in cybersecurity.

The goal is to acquire the ability to apply security principles to new/unseen/complex scenarios.

This will be done by being exposed to actual research topics and scientific papers and discussing things together.

Course structure:
The course is divided in two main parts (as follows).

Course Content

Part I: Advanced Topics

- We will cover, through lectures and also talks from invited speaker, recent and relevant security issues in traditional and novel technologies, such as:
  - IoT and Cyber-Physical System
  - (Adversarial) Machine Learning for Security
  - Blockchain
  - Advanced Cryptography Applications
  - User Authentication

Course Content

Part II: Students Presentations

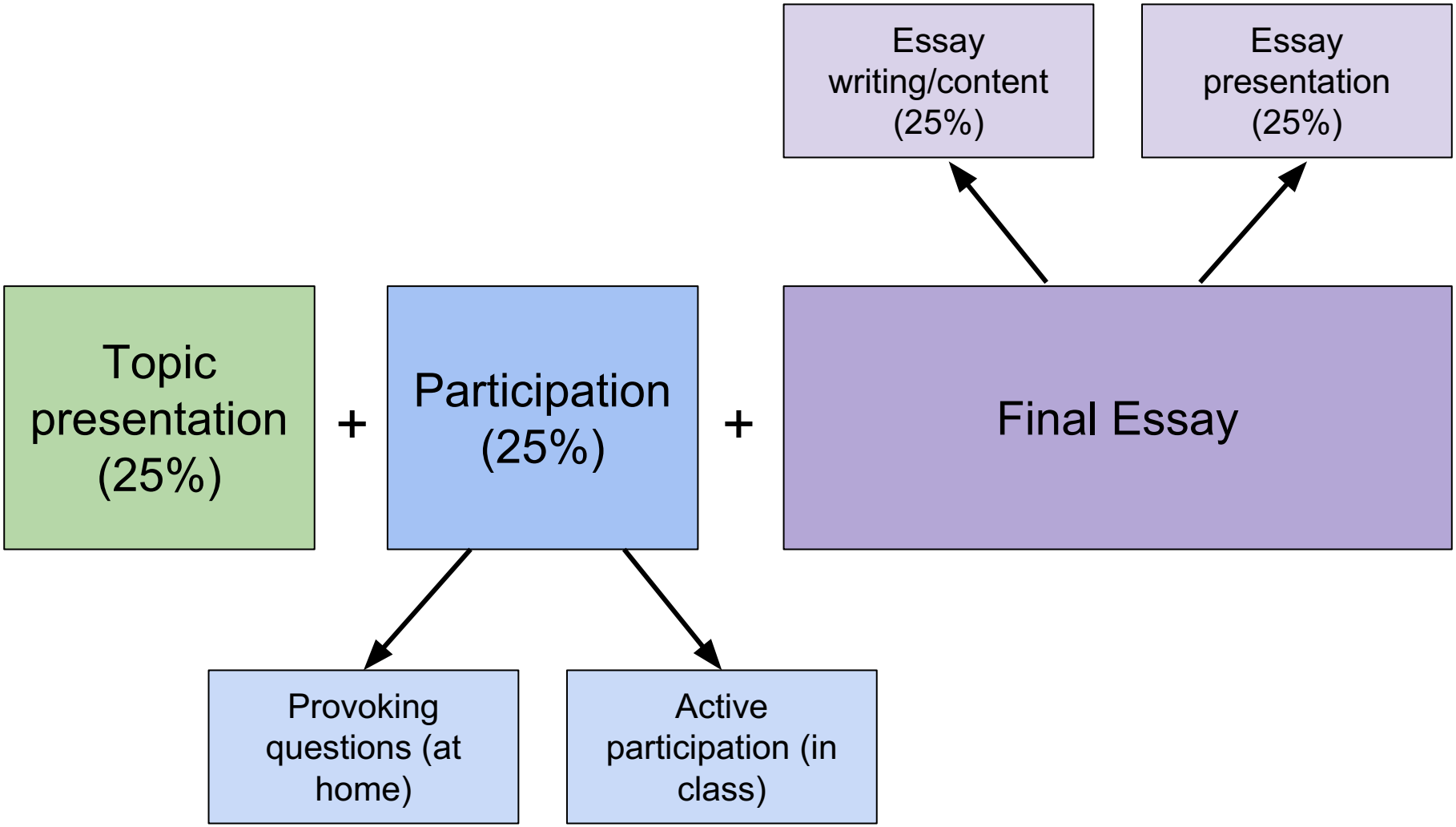
- Students present to the class a given topic
  - Group of *about* 3 students
  - The topics are assigned (from a list available on course website) through a bidding phase, at the end of the *Part I*
  - Topics are similar to the one presented in Part I

- Students are also required to:
  - Send provoking questions regarding the topics presented by other groups
  - Interact with the presenting group during the lecture

Exam

- Each group (as identified in *Part II*) is evaluated through a final project
  - The goal is identify *improvement directions* of a state-of-the-art problem
  - The topic should be “close” to the one presented in *Part II* (topic shall be identified together with the lecturer)
  - The work should be supported by experiments
  - Essay (about 10 pages) + presentation of the project

Grading Criteria



Grading Criteria

- **(25%) presentation (during the second part of the course)**
  - (15%) Layout and Graphics
  - (30%) Content
  - (20%) Organization
  - (20%) Presentation
  - (15%) Q&A
- **(25%) participation in the discussions in the class (during the second part of the course)**
- **(25%) content and quality of the project/essay**
  - (30%) Style
  - (20%) Originality
  - (50%) Organization (Clarity in your argumentation, Coherence between assumptions and conclusions, Logical organization, Evidence to support claims
- **(25%) oral discussion of the essay (during which the student can also be asked questions on the first part of the course).**

Project presentations for final essay

Projects can be:

- Proposed by the group and discussed with the teaching team to evaluate the feasibility
- Selected through a list of proposals presented by SPRITZ group members. There will be a project presentations in early december

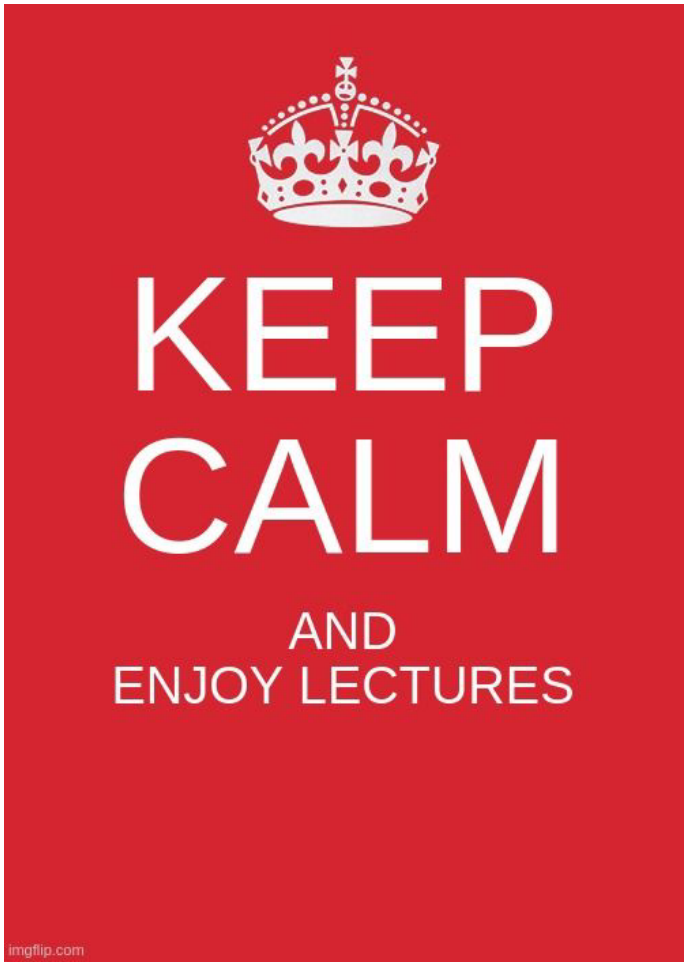
Attendance Questionnaire

In order to help us in organizing the course, please fill the attendance questionnaire on Moodle as soon as possible!

Grading Criteria

A lot of information!

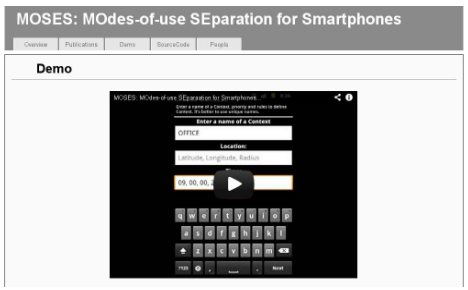
TAs will remind you all the deadlines through the course!

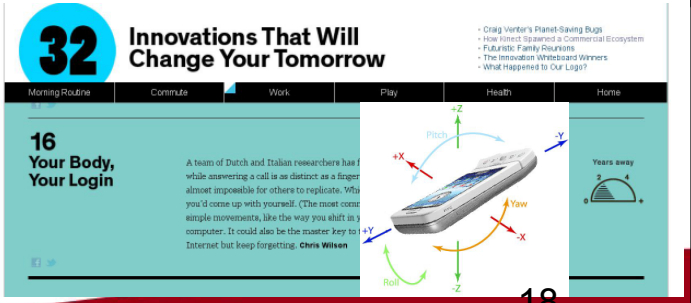


Spritz Group Project Topic

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*





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 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

Sapienza Univ. Rome, Italy ~2000


WARNING

“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*

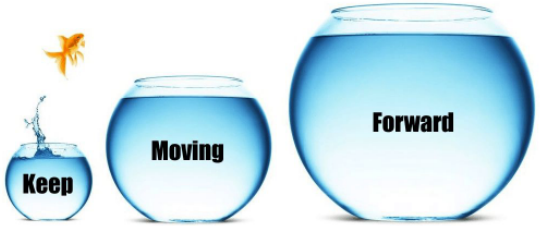
Università degli Studi di Padova — SPRITZ Security & Privacy Research Group

CAPTCHaStar

Survey

What is a CAPTCHA? PATENTED

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
the
distorted text (e.g. padosa) 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!



Questions? Feedback? Suggestions?

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

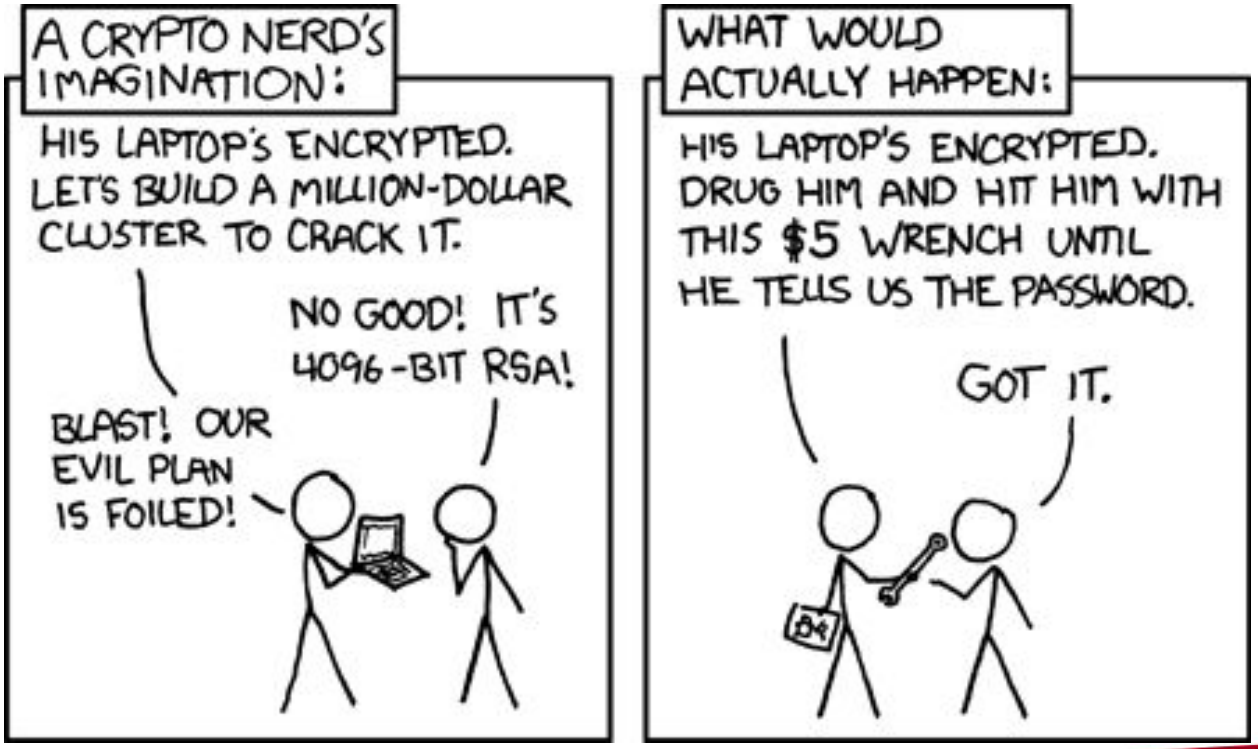
“The three golden rules for ensuring computer security: do not own a computer; do not power it on; and do not use it.”
– Robert (Bob) Morris (Former NSA Chief Scientist).

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)

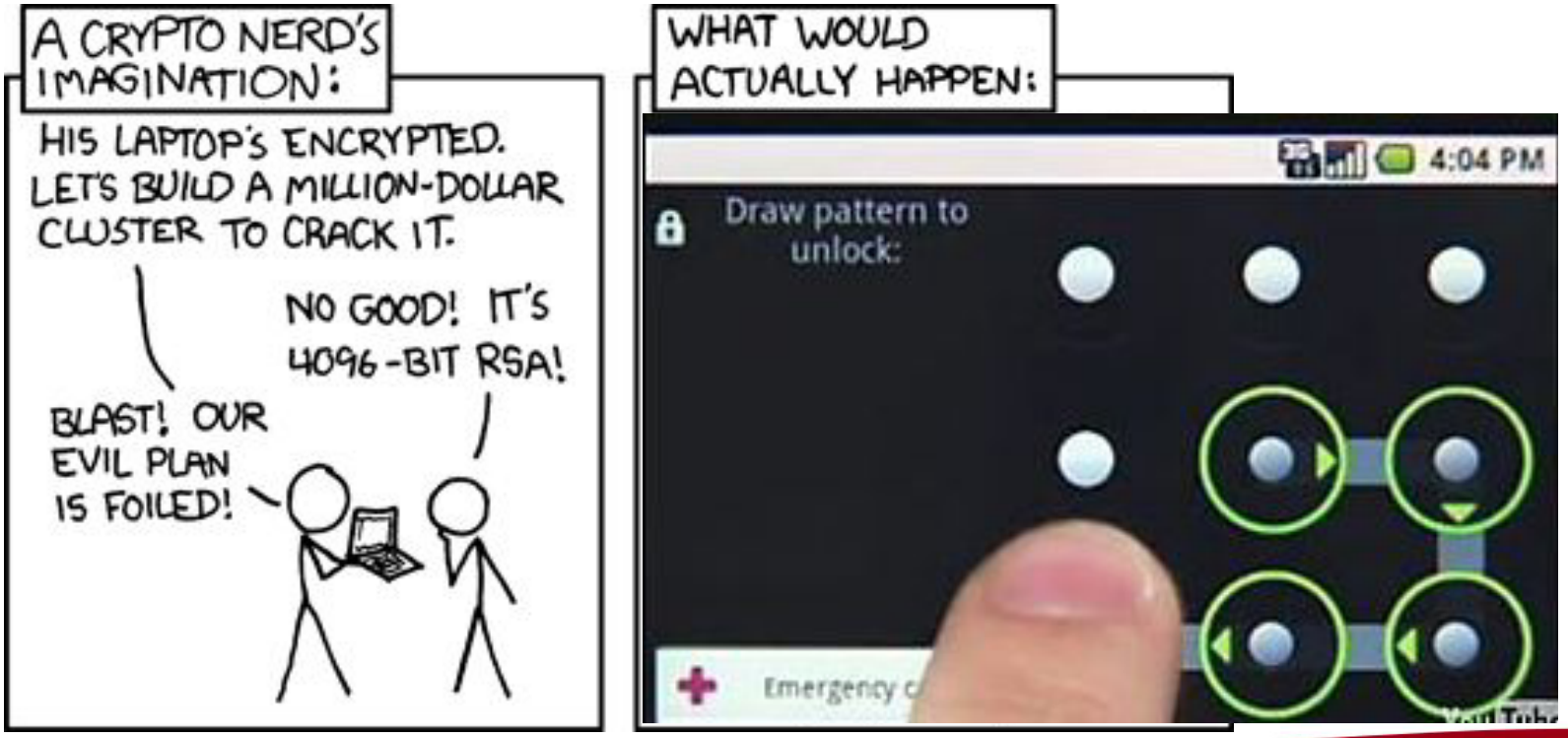
Some key concepts to start with...

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



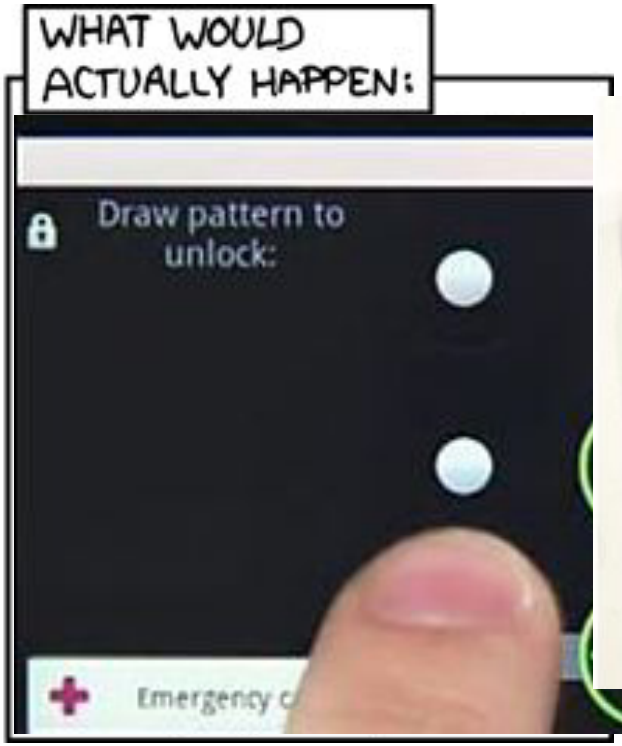
Some key concepts to start with...

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



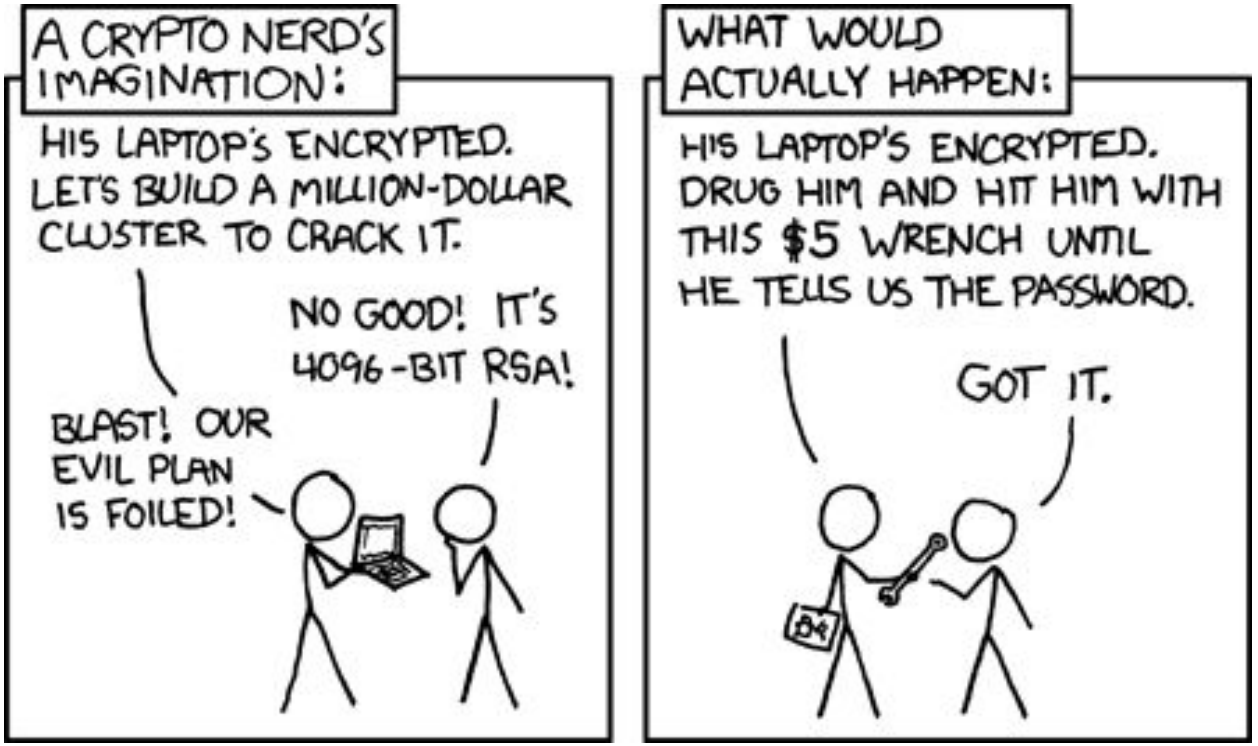
Some key concepts to start with...

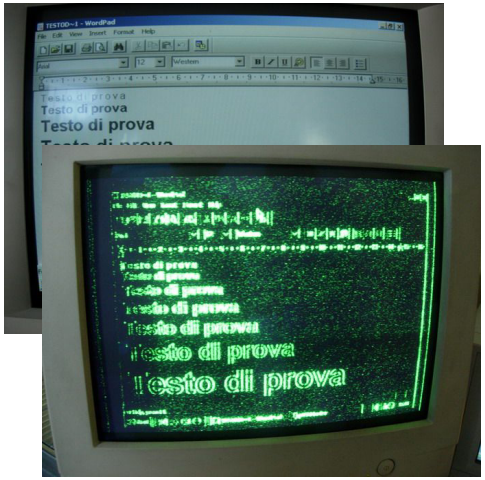
4) Security by obscurity never works
5) Cryptography is a powerful tool but...
   it is not enough!



Some key concepts to start with...

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





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

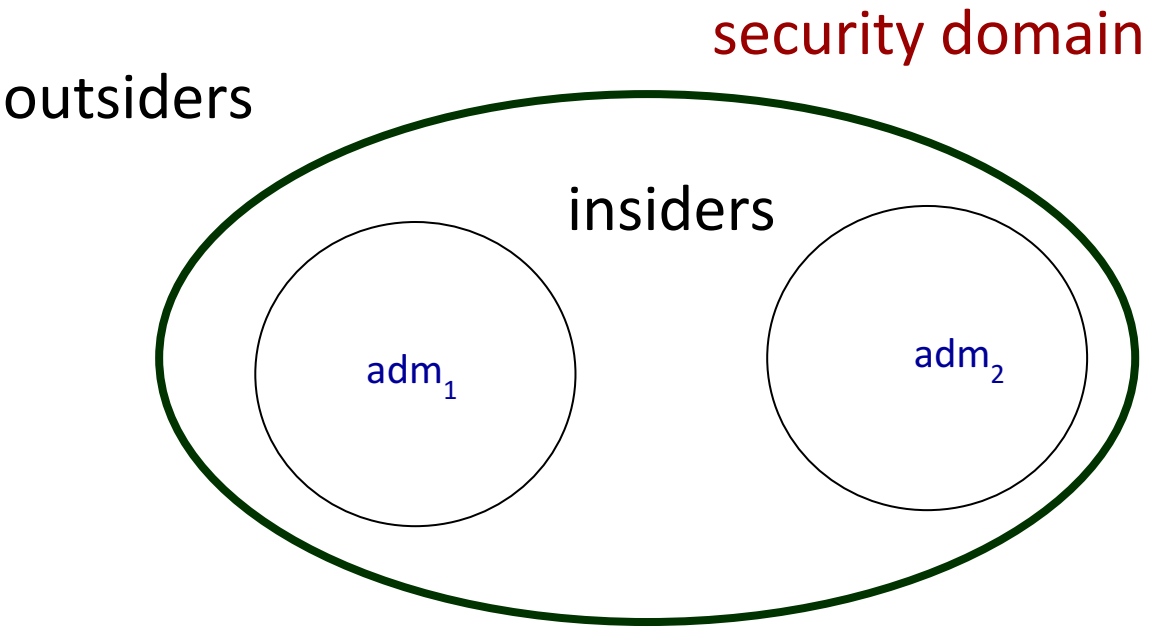
Auxiliary security properties

- 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

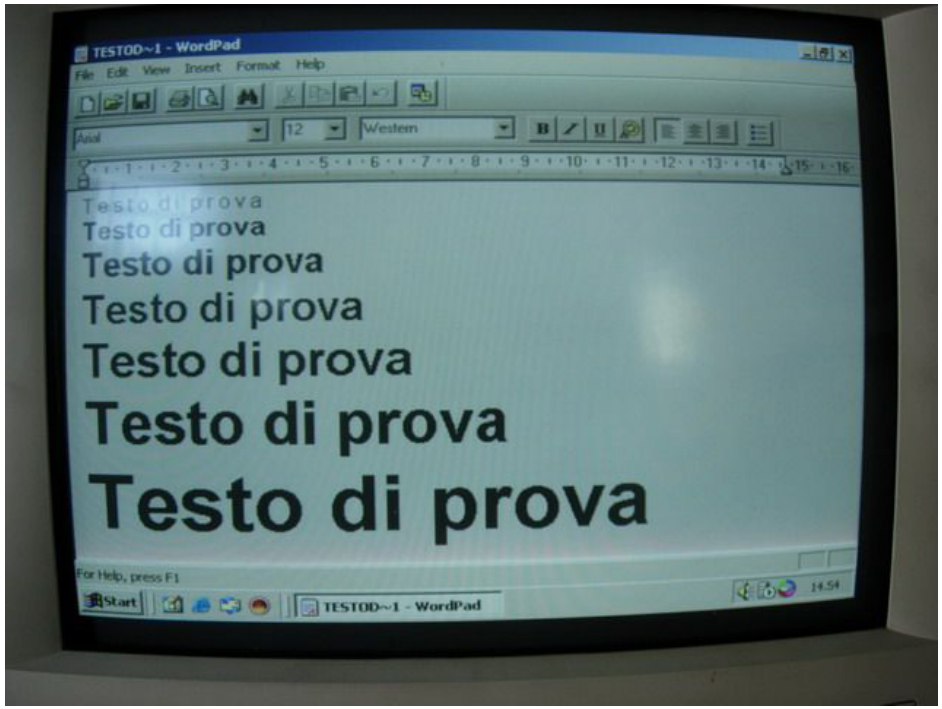


security domain and admin domain may differ

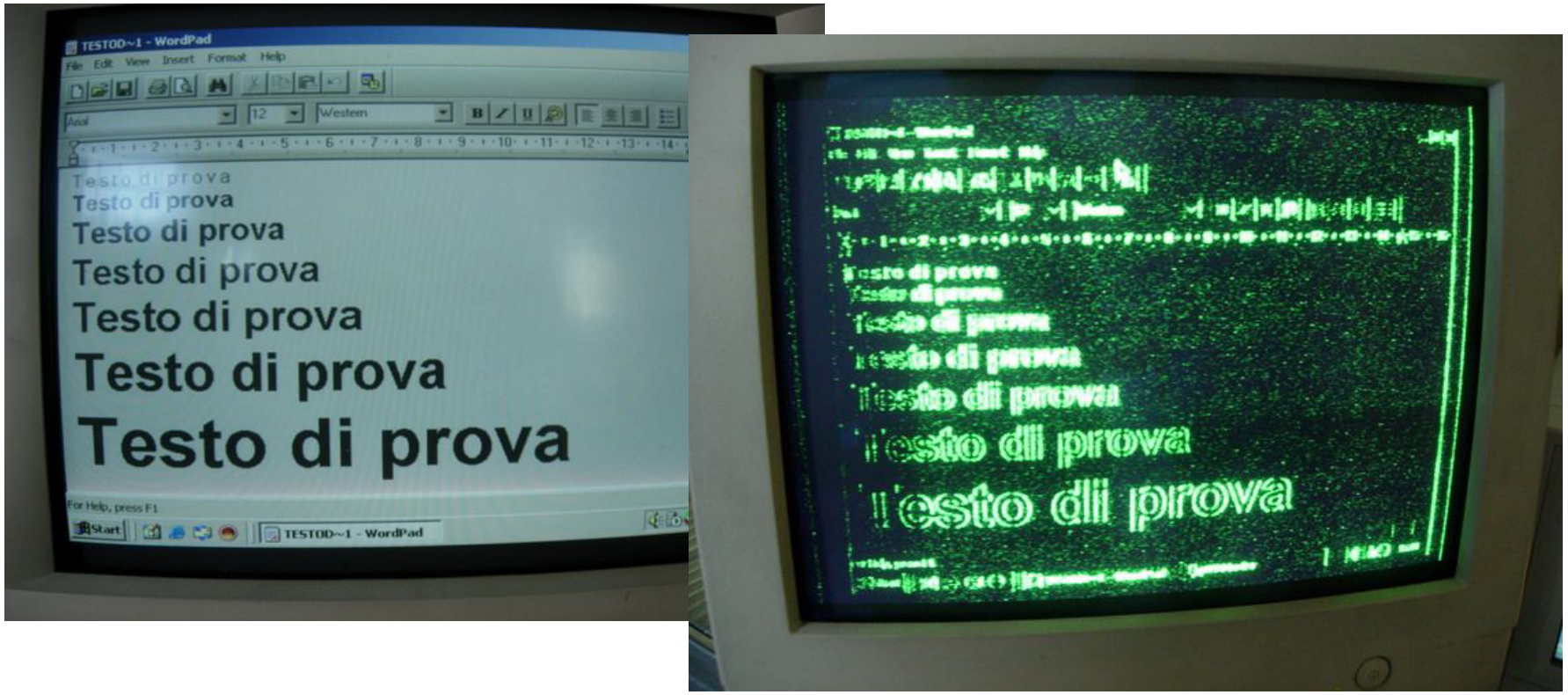
Types of attack

- 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