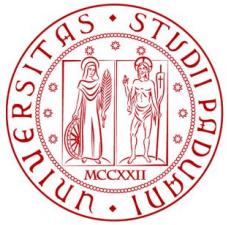
Computer and Networks Security

MSc Degree in Computer Science
2018-2019

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

Teaching Assistant
Giuseppe Bernieri
bernieri@math.unipd.it
Eleonora Losiouk
elosiouk@math.unipd.it



UNIVERSITÀ DEGLI STUDI DI PADOVA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

DIPARTIMENTO MATEMATICA


20
GGIO

WARNING

Basic Information

Language: 

Credits: 6 ECTS (CFU)

Schedule: MSc I year, **I semester**

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

Course website:
http://www.math.unipd.it/~conti/teaching/CNS1819/index.html

Course Group/Mailing List:

Google Group "CNS_1819_UNIPD"

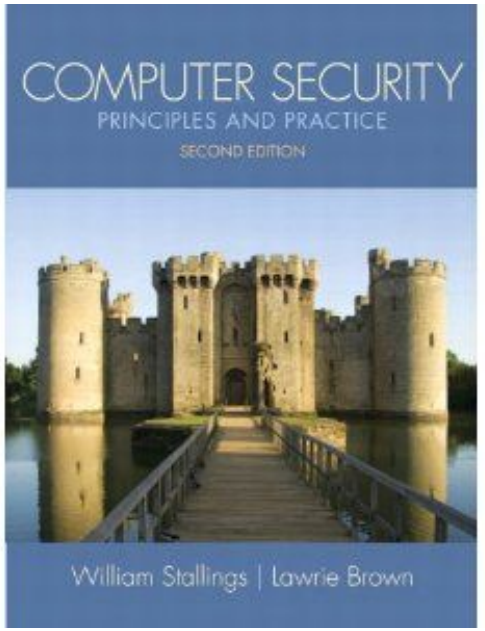
Course Content

Part I: Security Principles and Practice

- Computer Security Technology and Principles
  - Overview, Crypto Tools, User Authentication, Access Control, DB security, Malicious Software, DoS, Intrusic Detection, Firewall and Intrusion Prevention
- Software Security and Trusted Systems
  - Buffer Overflow, Software Security, OS security, Trusted Computing
- (Management Issues)
  - IT Security Mgmt and Risk Assessment, IT Security Controls/Plans/Procedures, Physical Security, HR Security, Auditing, Legal and Ethical Aspects.

Material:

- Book (chapters 1-13):
  - Computer Security – Principles and Practice 2ed *W. Stallings, L. Brown*
  - Slides will be available on course/group page



Course Content

Part II: Advanced Topics

- Recent and relevant security issues in traditional and novel technologies (botnet, DoS, smartphone security, RFID, social networks, novel authentication techniques, future Internet ...)
- To acquire the ability to apply security principles to new/unseen/complex scenarios
- Each student will present one topic in class

Course Content

The **second part** of the course takes the form of seminars based on a selection of scientific papers (that either have had a strong impact on security today, or explore novel ideas that may be important in the future). The list of topics can be found **HERE**.
For each topic will be indicated one primary paper, and possibly other additional papers. All the students are required to read all primary papers and be able to competently discuss the material in class. Each student will be responsible for presenting one lecture (based on one of the primary paper including as much relevant related work as necessary to distill the work presented in the paper). The speaker will have a finite time (20 minutes) to present the papers. The presentation will be followed by 10 minutes of interactive discussion in the class. 48 hours before each lecture each student must submit (via email, to both the lecturer and the teaching assistant) at least two thought-provoking questions for each on the main papers covered in the lecture. These questions should critically evaluate the papers (e.g., questioning the assumptions, criticize the methodology, compare with other solutions, propose alternative solutions, etc.).

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

Topic 22: P2P BotNet Detection

Primary:

- Shishir Nagaraja, Prateek Mittal, Chi-Yao Hong, Matthew Caesar, and Nikita Borisov BotGrep: Finding P2P Bots with Structured Graph Analysis Usenix Security 2010.

Secondary:

- Su Chang and Thomas E. Daniels P2P botnet detection using behavior clustering and statistical tests. Proceedings of the 2nd ACM workshop on Security and artificial intelligence (2009).
- M\E1rk Jelasity and Vilmos Bilicki, Towards Automated Detection of Peer-to-Peer Botnets: On the Limits of Local Approaches Usenix LEET 2009.
- Jian Kang, Jun-Yao Zhang, Qiang Li, Zhuo Li Detecting New P2P Botnet with Multi-chart CUSUM 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing.

Course Content

Part III:

Guest lectures by

Prof Radha Poovendran
(University of Washington, Seattle)

"Tackling Control Plane Saturation Attacks"

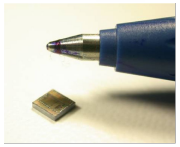
Grading Criteria

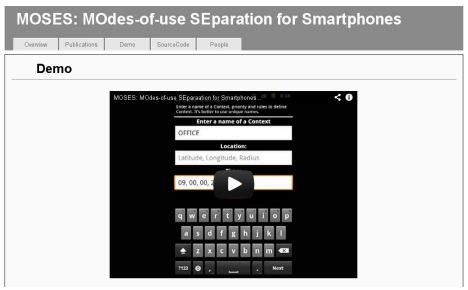
- ***(25%) presentation (during the second part of the course)***
  - *(15%) Layout and Graphics*
  - *(30%) Content*
  - *(20%) Organization*
  - *(20%) Presentation*
  - *(15%) Q&A*
- ***(25%) participation in the discussions in the class (during the second and third part of the course)***
- ***(25%) content and quality of the 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).***

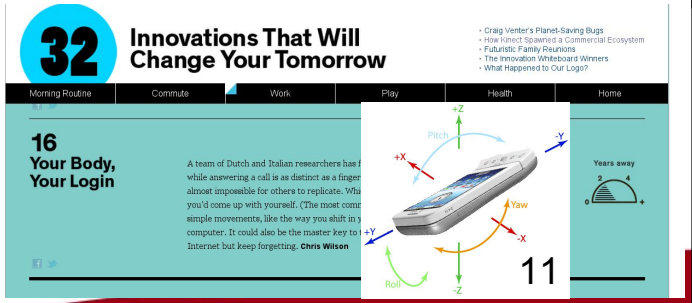
Research/Essay/(Thesis) Topics

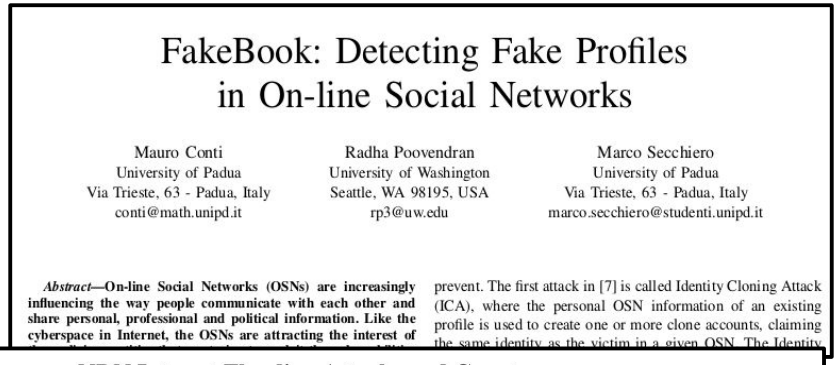
Università degli Studi di Padova

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





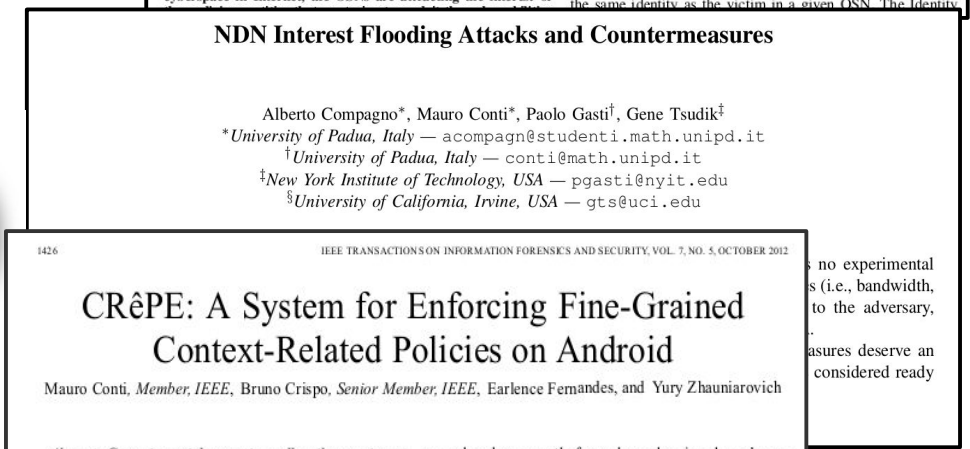



FakeBook: Detecting Fake Profiles in On-line Social Networks

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

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*

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

CAPTCHaStar

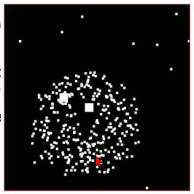
Survey

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. 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!



Agostino Sturato (Interconnected networks) -IEEE ICNC 2016)

… and several on-going works:

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

Schedule

			Lecture Schedule	Talks
Wednesday	3	October	Course Introduction	
Thursday	4	October	Ch10_Buffer Overlow Attacks	
Wednesday	10	October	Ch1. Overview - Ch2. Crypto - Ch6_Malware	"Android Malware" (Eleonora Losiouk, University of Padova)
Thursday	11	October	Ch3_User Authentication - Ch4_Access Control	"GAN based Privacy Attacks on Decentralized Deep Learning" (Briland Hitaj, University of Rome Sapienza)
Wednesday	17	October	Ch 7_Denial of Service	Talk by Giuseppe Bernieri, University of Padova
Thursday	18	October	Ch12. OS Security	"Security and privacy of medical devices" (Eduard Marin, KU Leuven, Belgium)
Wednesday	24	October	Ch 8_Intrusion Detection - Ch9_Firewall and IPS	Talk by Luca Calderoni, University of Bologna
Thursday	25	October	Ch13_Trusted Computing and Multilevel Security	Talk by Eleonora Losiouk, University of Padova
Wednesday	31	October	Ch5.Database Security	Talk by Ankit Gangwal, University of Padova

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...

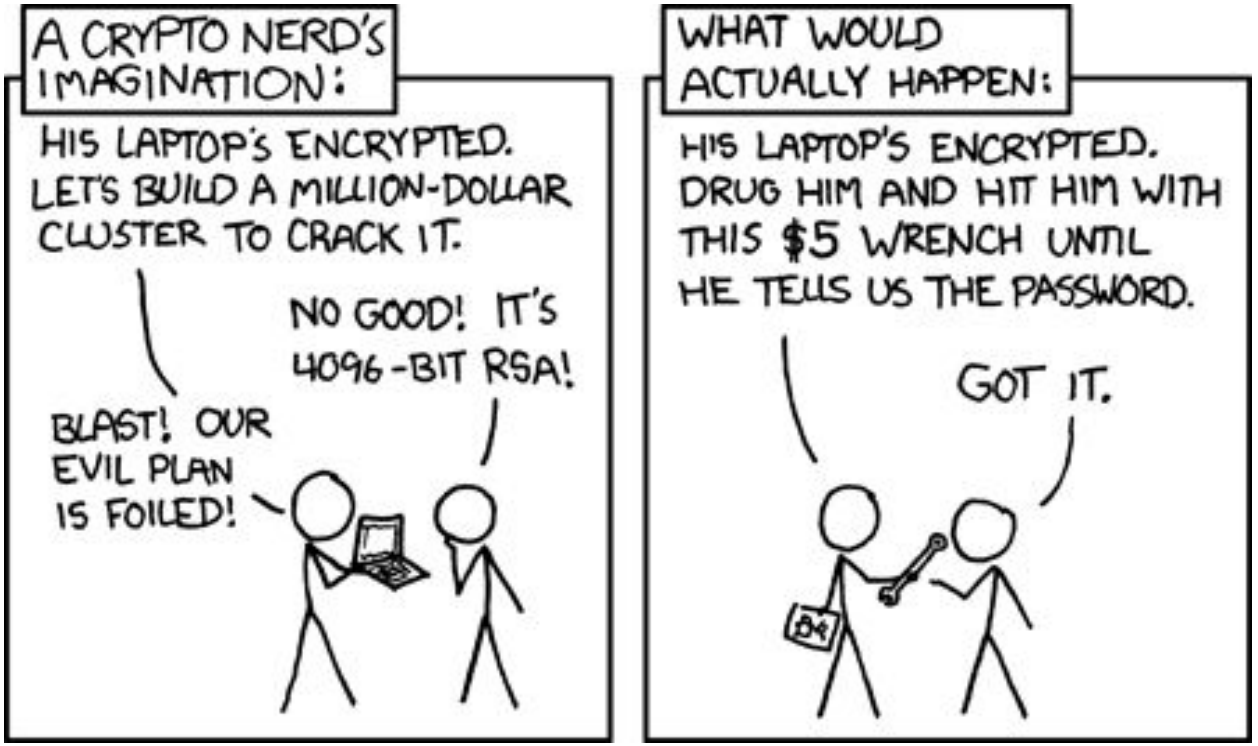
3) The security of a system is equivalent to the security of its less secure component (rule of the weakest link)

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"

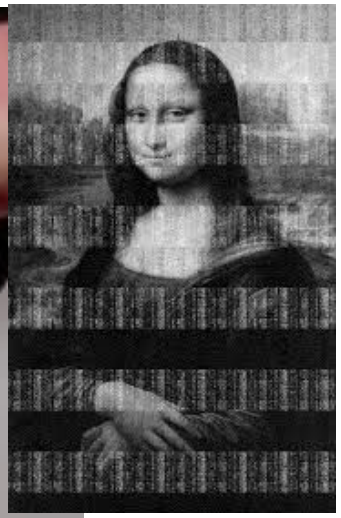
Bill Neugent

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"

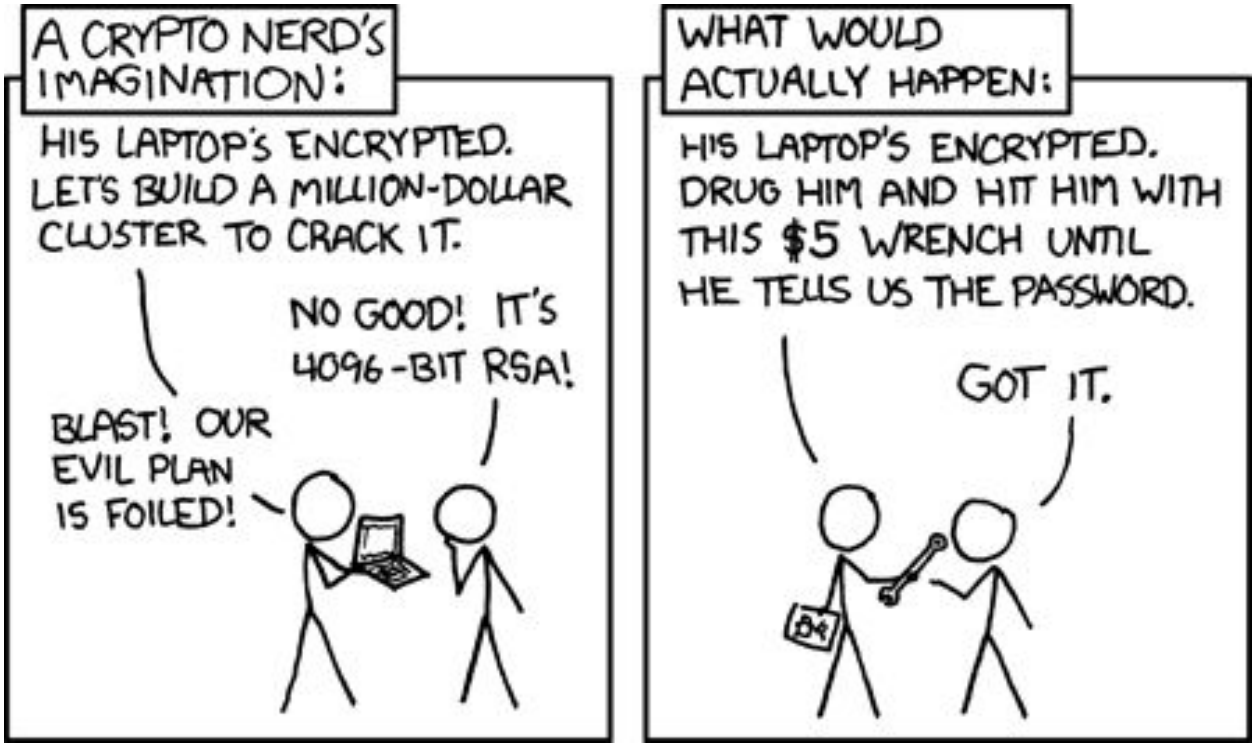
Bill Neugent

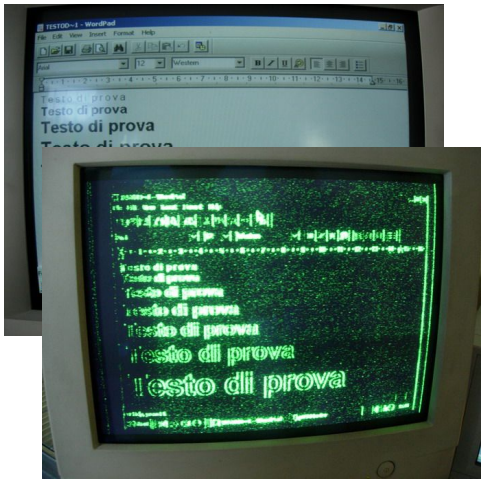
Some key concepts to start

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

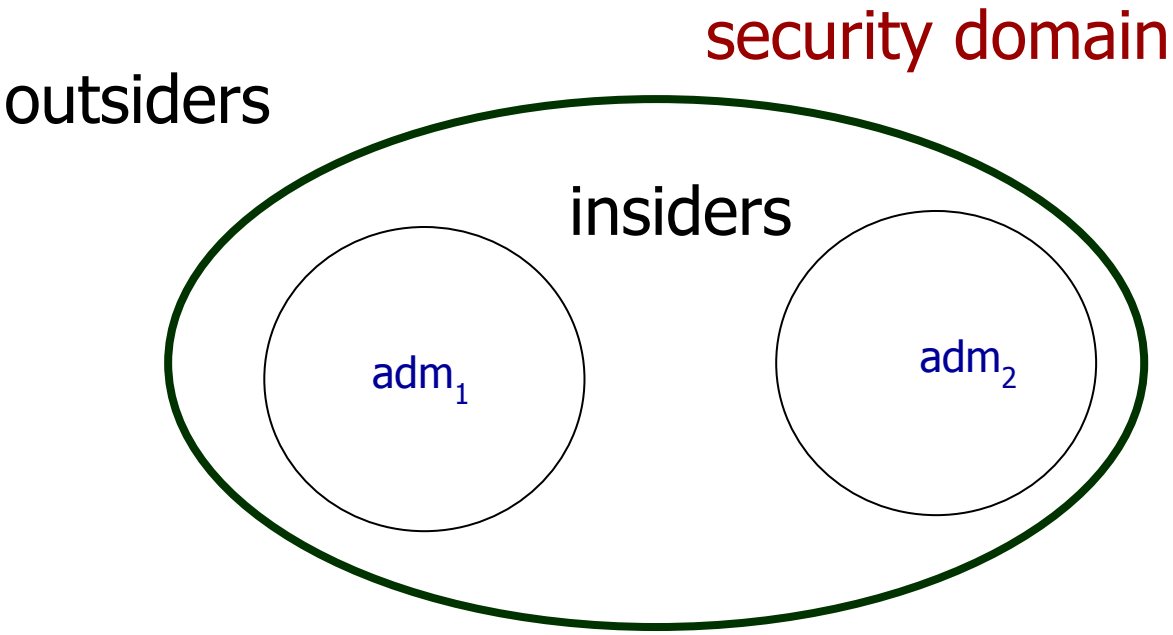
Auxiliary security properties

- 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

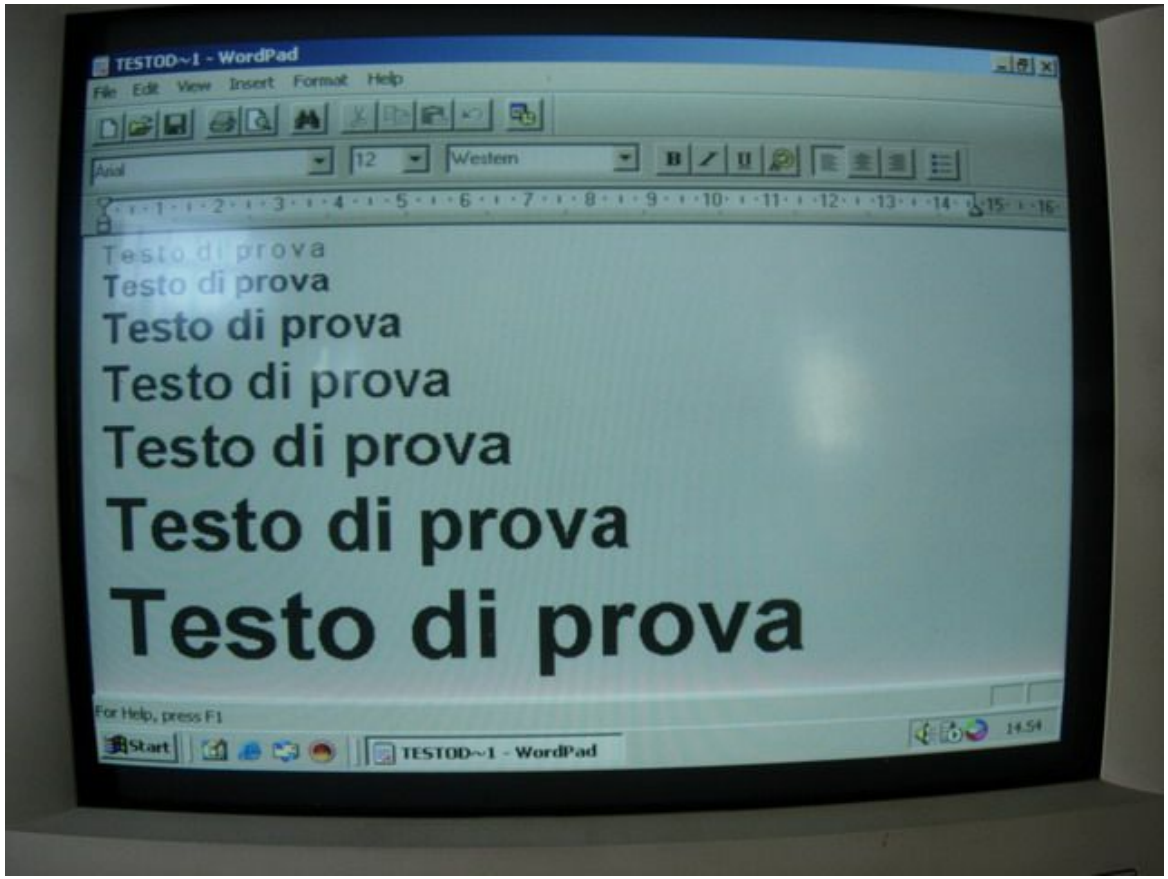


security domain and admin domain may differ

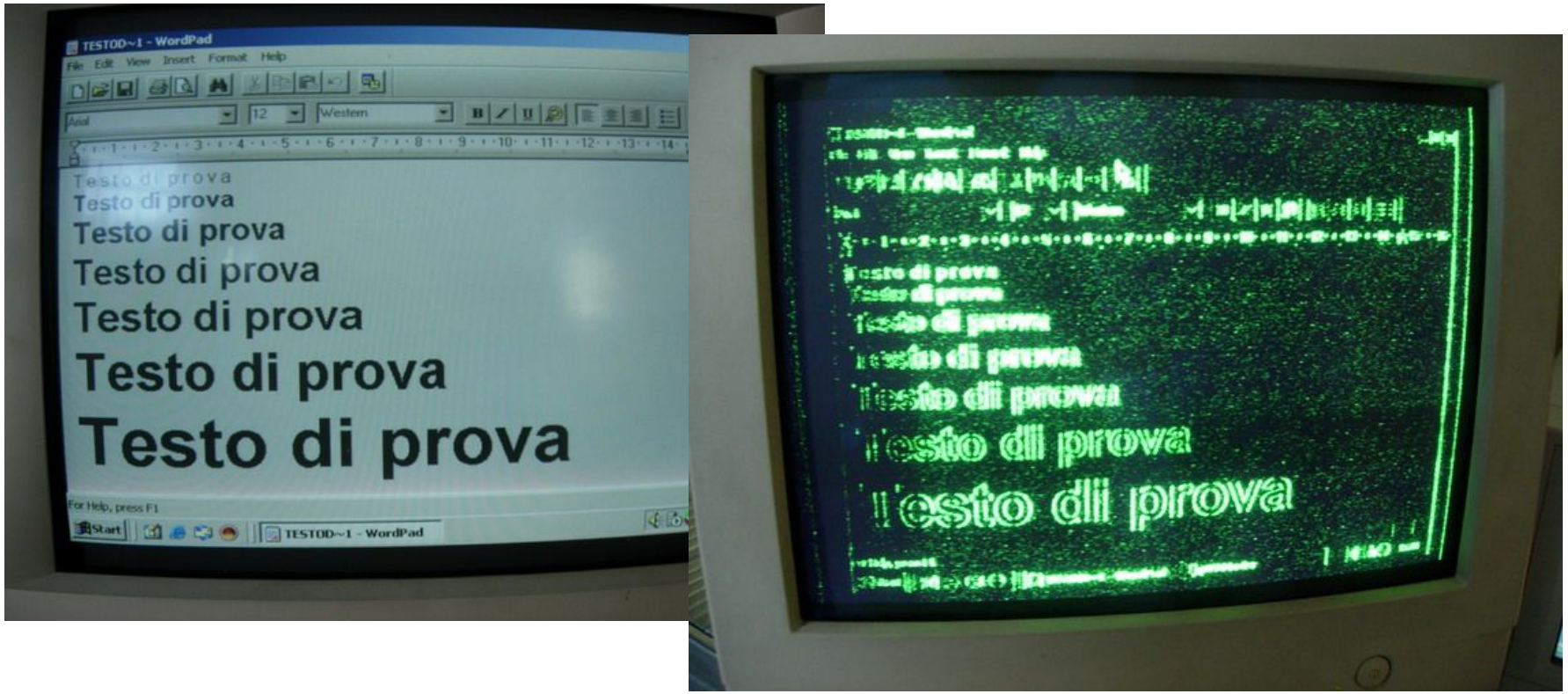
Types of attack

- 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?

http://www.math.unipd.it/~conti/teaching/CNS1819/index.html

conti@math.unipd.it

bernieri@math.unipd.it, elosiouk@math.unipd.it