Introduction to Information Security

Riccardo Spolaor, Ph.D rspolaor@sdu.edu.cn

Shandong University, School of Computer Science and Technology

Basic Information

Language: 

Teacher: Riccardo Spolaor
email: rspolaor [AT] sdu [DOT] edu [DOT] cn

64 hours: 32 lesson, ~32 laboratory

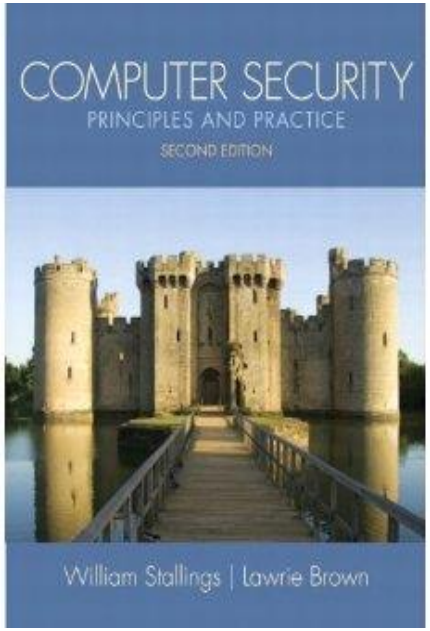
Schedule: **II semester**

Teacher website: www.spolaor.com

Course Wechat Group

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, Intrusion 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 Wechat 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

Presentation (second part)

- Seminars based on the selection of scientific papers on security.
- We will provide the list of topics and papers later in the course.

Speaker (The student giving the presentation)**:**

- A student selects a topic for the presentation.
- For each topic, we select a primary paper and one or more secondary papers.
- The speaker presentation has a time limit of 20 minutes to present the papers
  - The main focus is on the primary
  - Briefly introduce and compare with the secondary papers

Audience (All other students):

- Read the primary papers (and be able to competently discuss it in class)
- Participate to the discussion after the presentation (10 minutes)
- Submit an email with two thought-provoking questions (48 hours before the presentation day)
- Such questions should critically evaluate the paper (e.g., assumptions methodology, other solutions, etc.)

Purpose:

- This class is going to be interactive
- Stimulate discussion
- The participation to the discussion is strongly recommended (part of the grading criteria)
- Better to not sleep during the class

Presentation (second part)

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.

Grading Criteria

- ***(25%) presentations (during the second and third part of the course)***
  - *(15%) Layout and Graphics*
  - *(30%) Content*
  - *(20%) Organization*
  - *(20%) Presentation*
  - *(15%) Q&A*

- ***(10%) participation in the discussions in the class (during the second and third part of the course)***

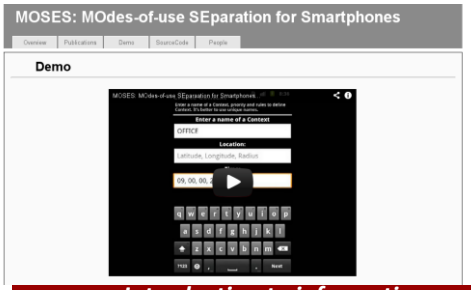
- ***(25%) content and quality of the essay***
  - *(30%) Style*
  - *(20%) Originality*
  - *(50%) Organization (Clarity in your argumentation, Coherence between assumptions and conclusions, Logical organization, Evidence to support claims)*

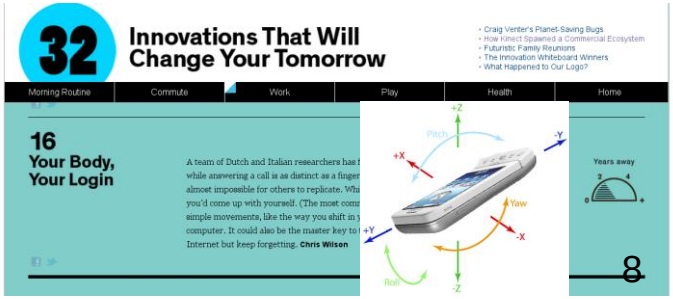
- ***(25%) oral discussion of the essay (during which the student can also be asked questions on the first part of the course).***

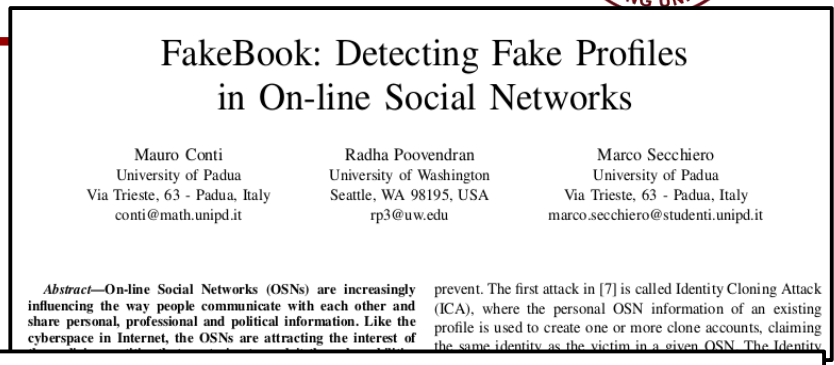
- ***(15%) Laboratory tasks***

Research/Essay/(Thesis) Topics

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

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”

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

ACM CODASPY (a.r. 21%)
IEEE TIFS

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

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

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

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*

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

ACM CCS 2015 (a.r. 19.8%)

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

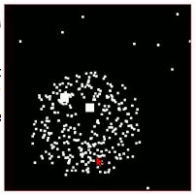
CAPTCHaStar

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

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 ba
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!




this page
intentionally
left blank

Riccardo Spolaor, Ph.D.
Short-Bio

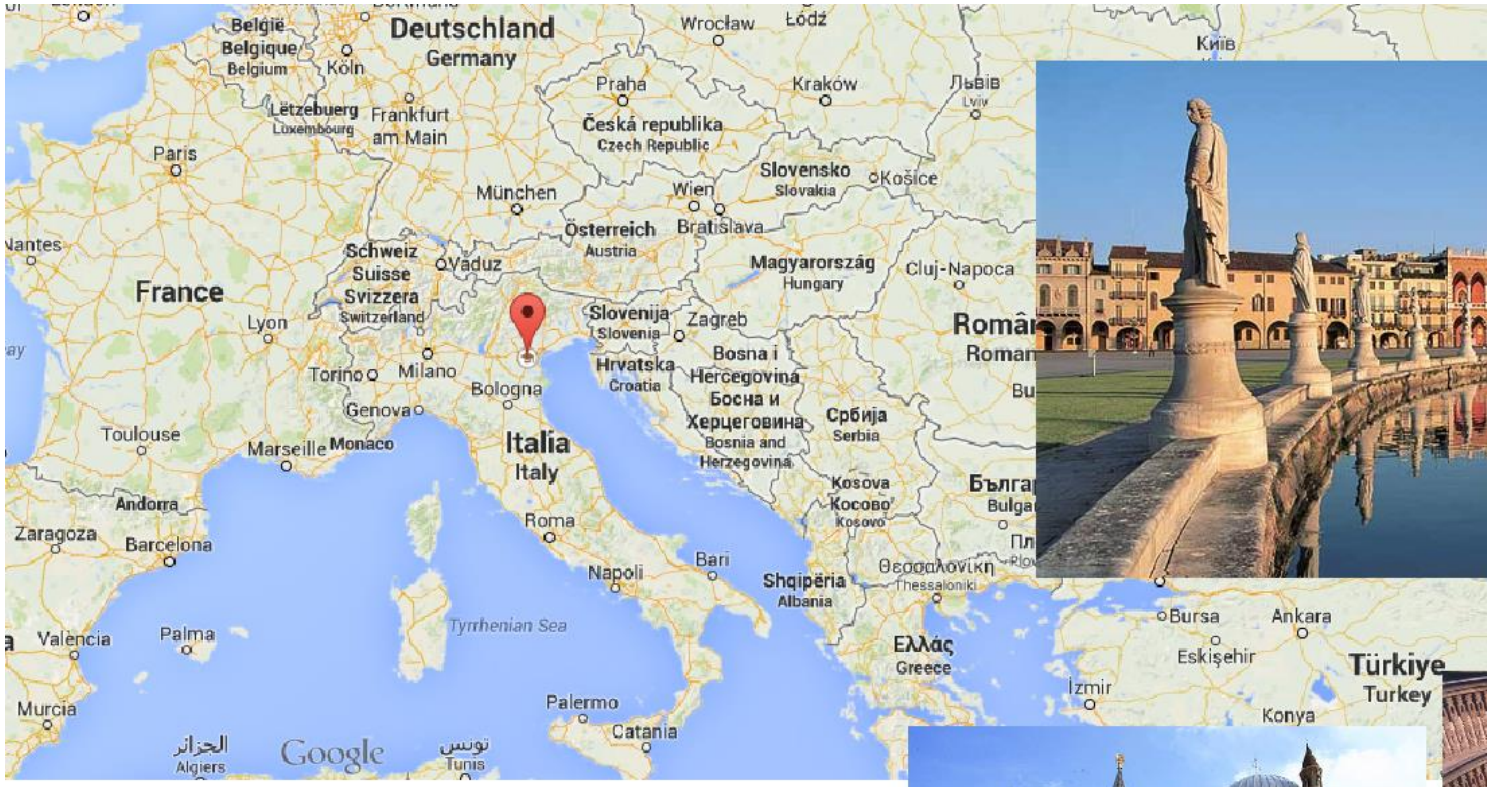
Education and Employment:

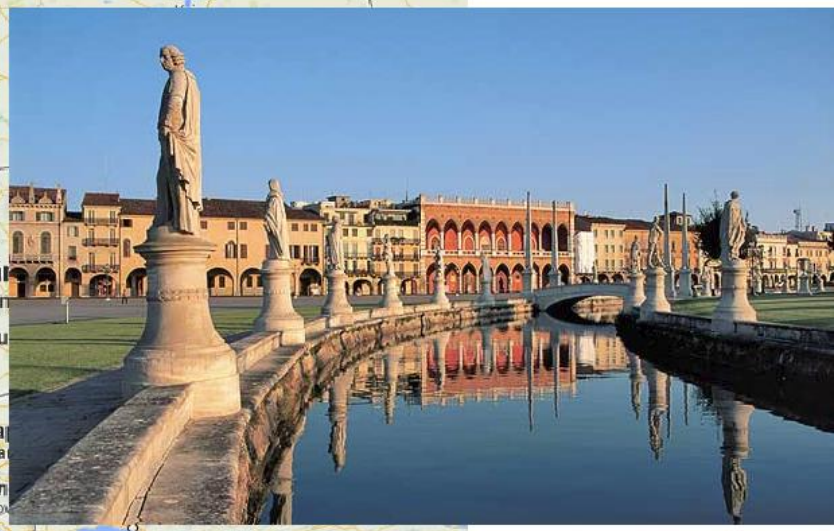
- BSc, MSc, PhD: University of Padua (Italy)
- Post-Doc: University of Oxford (UK)

My contacts:

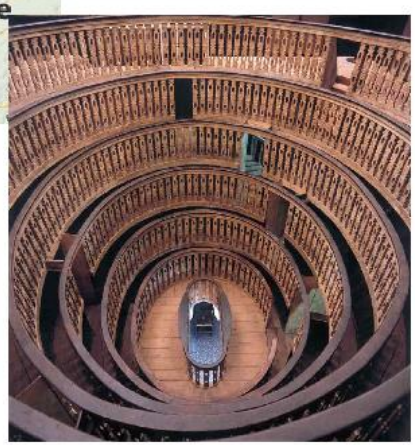
- Email: rspolaor [AT] sdu [DOT] edu [DOT] cn
- WeChat: riccardo_spolaor
- Website: www [DOT] spolaor [DOT] com
- Skype ID: riccardo.spolaor
- Office: N3-302

Riccardo Spolaor, Ph.D.
University of Padua (Alma Mater)





- Padua is the second-oldest university in Italy and the world's fifth-oldest surviving university
- 4th best Italian university and ranked the world's 116th



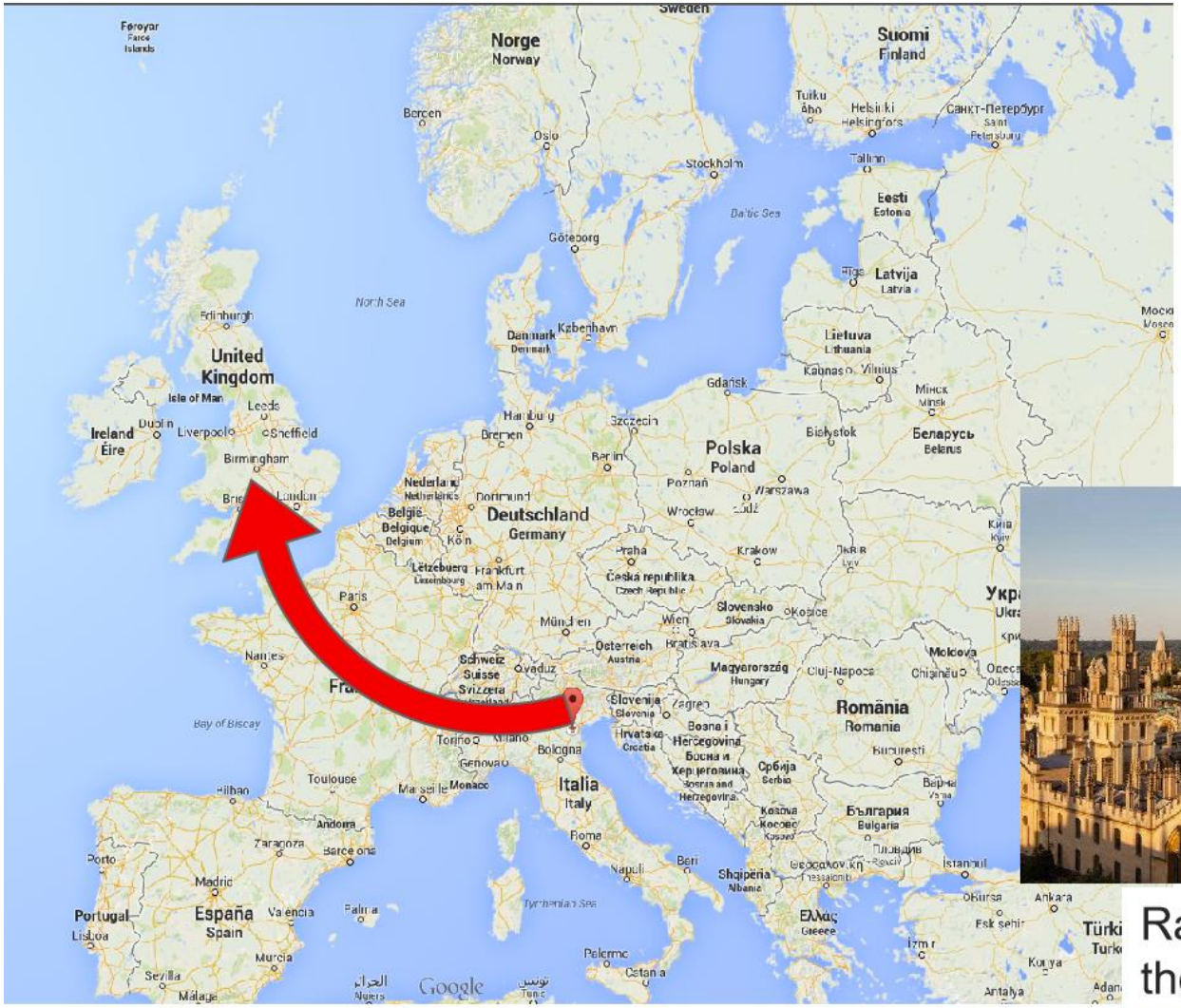
SPRITZ Research group, University of Padua (Alma Mater)

Security and Privacy Research Group…
(**S**ecurity and **PRI**vacy…**T**hrough **Z**eal)
http://spritz.math.unipd.it/

Mauro Conti
Full Professor, University of Padua, Italy
Affiliate Professor, University of Washington, USA
Head of SPRITZ Security and Privacy Research Group
Director of UniPD node of CINI Cybersecurity National Lab
EU Marie Curie Fellow Alumni
CEO and co-funder of CHISITO
Co-funder of DYALOGHI

Contact:
University of Padua - Dep. of Mathematics and HIT Center
Via Trieste, 63 - 35131, Padua, Italy
Room 528 - Phone +39 049 827 1488 - Fax +39 049 827 1479
conti@math.unipd.it

SPRITZ Research group, University of Oxford (UK) (Former affiliation)



Ranked 1st in the world in the Times Higher Education World University Rankings

System Security Lab, University of Oxford (UK) (Former affiliation)

Ivan Martinovic

Professor Ivan Martinovic

Professor of Computer Science

Governing Body Fellow, Kellogg College

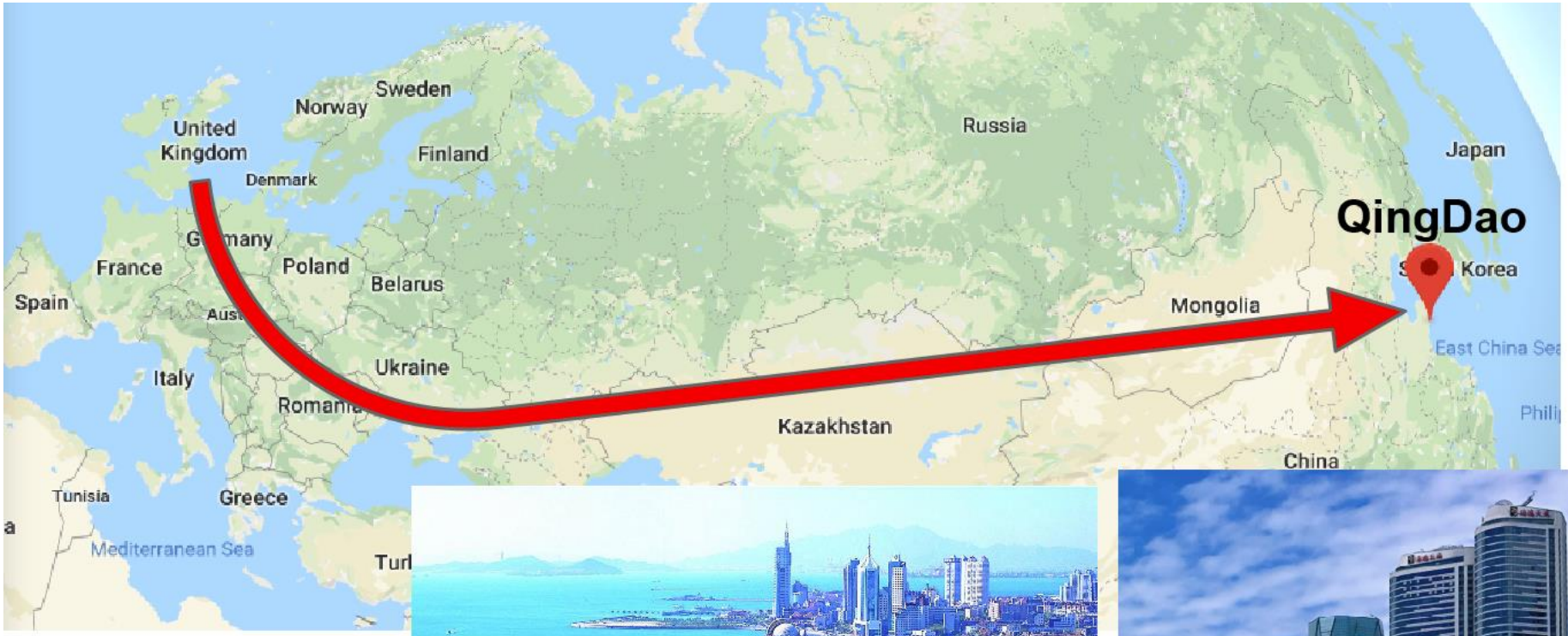
E: firstname.lastname@cs.ox.ac.uk
T: +44 (0)1865 6-10745

Department of Computer Science,
Robert Hooke Building, Room 117,
Parks Road, Oxford OX1 3QD
United Kingdom

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

Riccardo Spolaor, Ph.D.
Shandong University (Current affiliation)



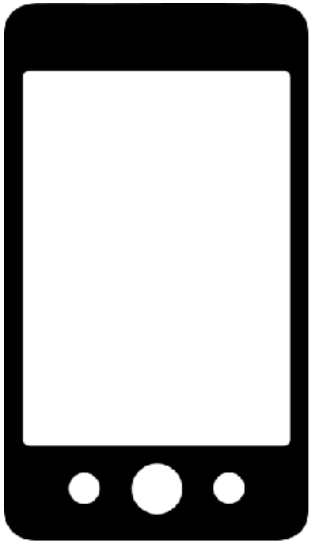
Institute of Intelligence Computing Shandong University (China) (Current Affiliation)

Riccardo Spolaor, Ph.D.
Short-Bio

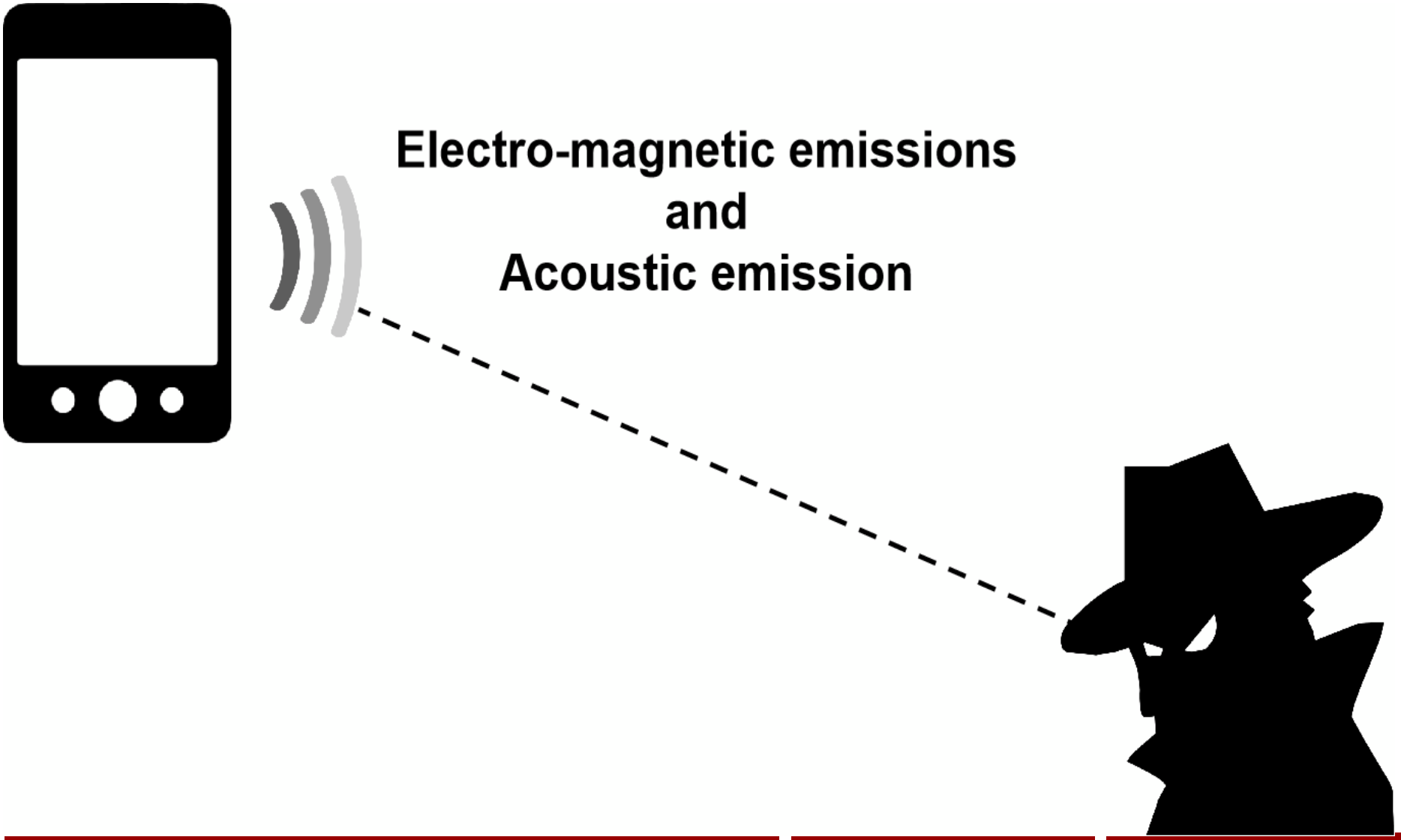
My Main Research Interests are:

- Privacy and security issues on mobile devices
- Application of machine learning techniques to infer user information
- Network traffic analysis and SDN
- Energy consumption analysis
- Malware behavioral analysis
- Edge computing and IoT applied security

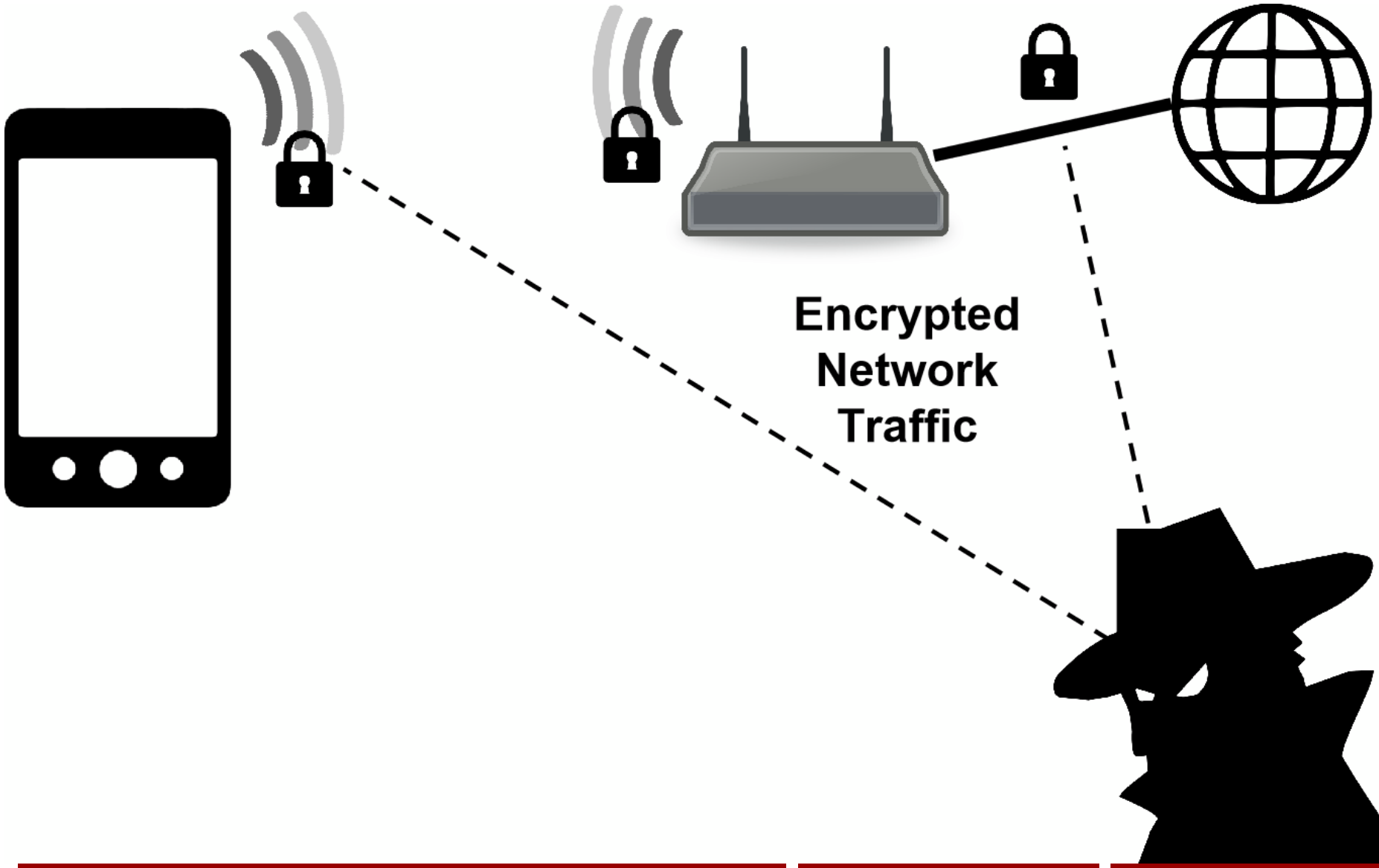
What are the Side-Channels on a Mobile System?



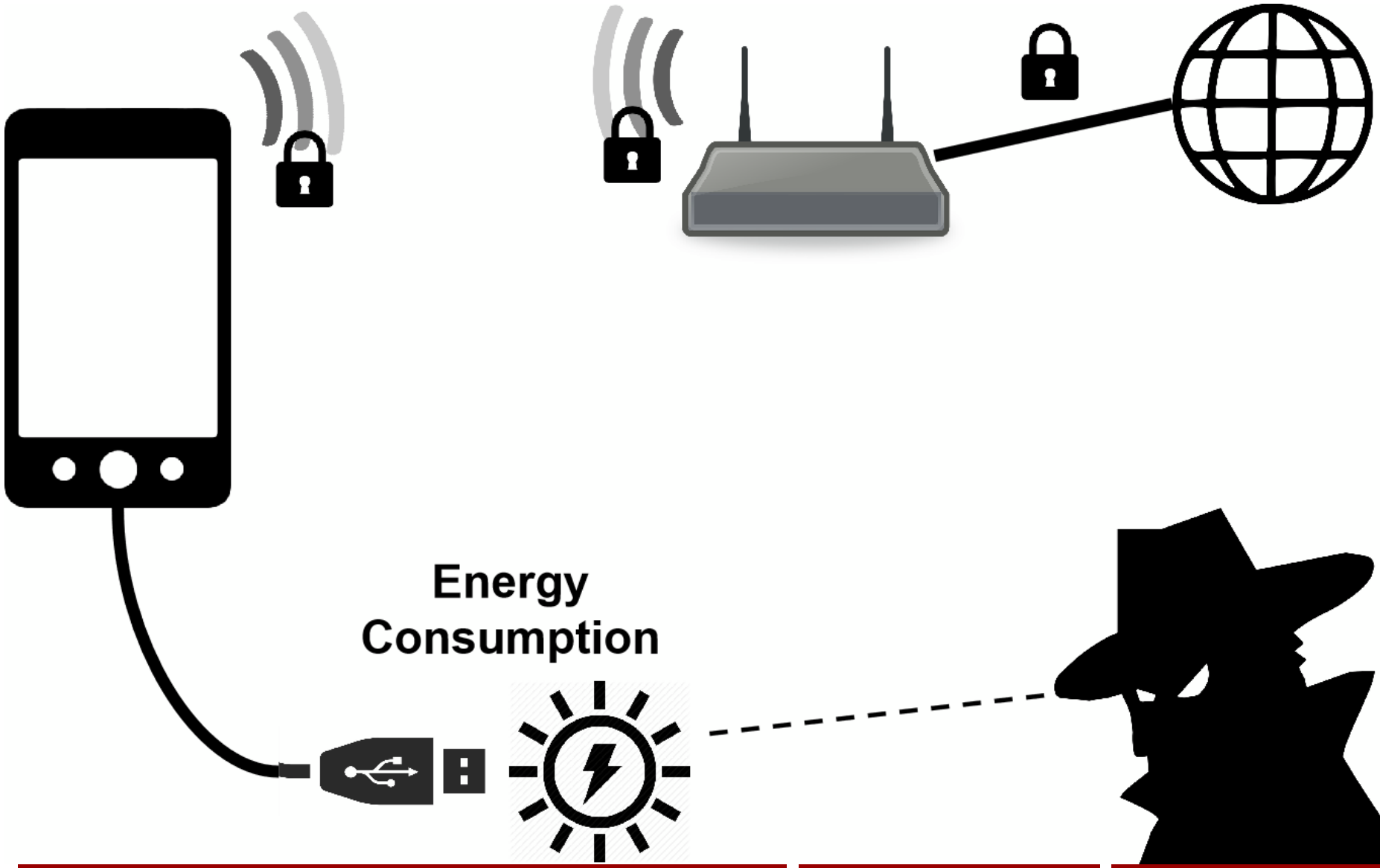
What are the Side-Channels on a Mobile System?



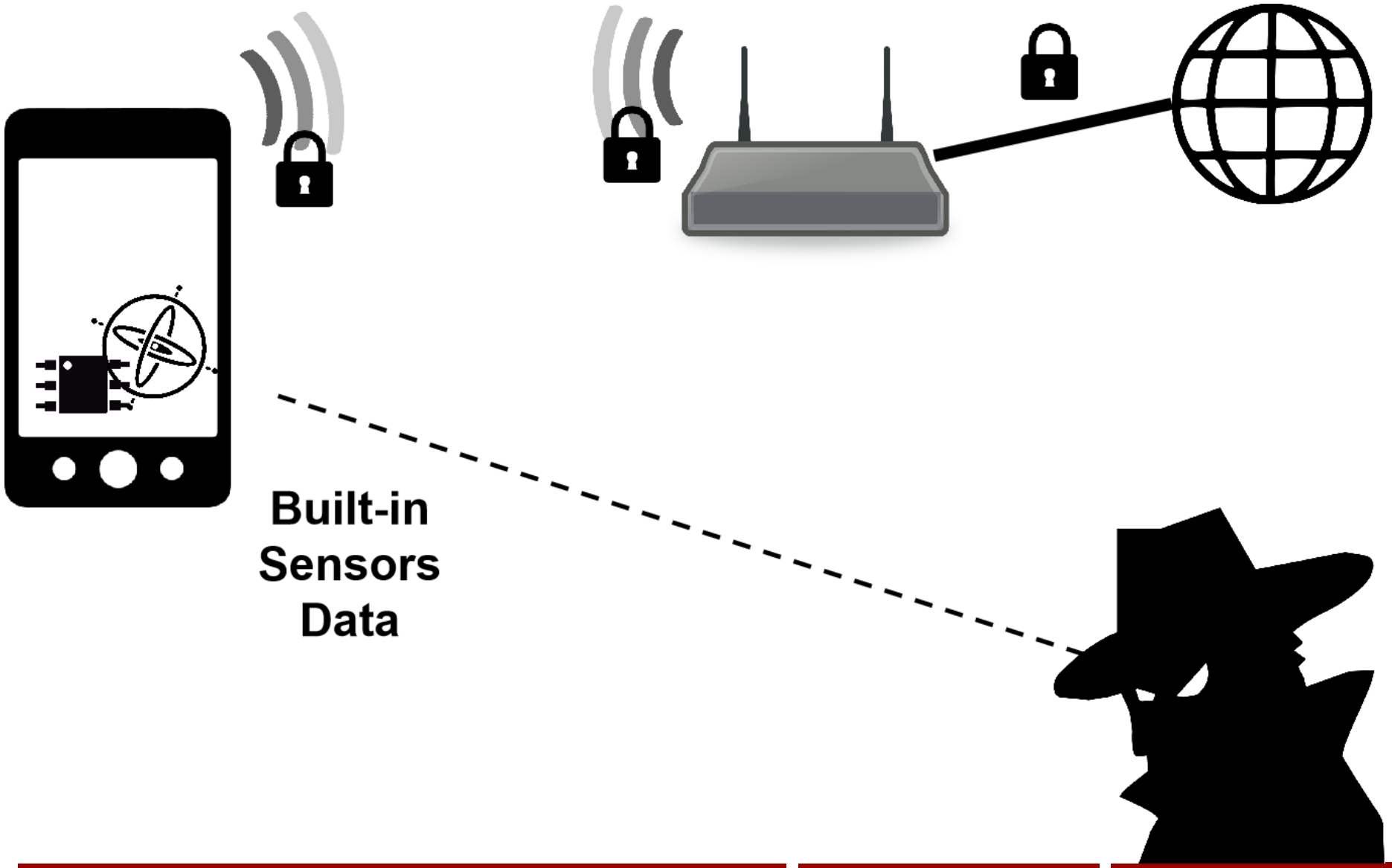
What are the Side-Channels on a Mobile System?



What are the Side-Channels on a Mobile System?



What are the Side-Channels on a Mobile System?



What are the Side-Channels on a Mobile System?

Sound-induced vibrations

Recent works

mmEcho: A mmWave-based Acoustic Eavesdropping Method

To appear at IEEE SP 2023 (CCF A)

Pengfei Hu, Wenhao Li, Riccardo Spolaor*, Xiuzhen Cheng
School of Computer Science and Technology, Shandong University, Qingdao, China
Email: {phu, rspolaor, xzcheng}@sdu.edu.cn, li_wenhao@mail.sdu.edu.cn

AccEar: Accelerometer Acoustic Eavesdropping with Unconstrained Vocabulary

Published at IEEE SP 2022 (CCF A)

Pengfei Hu*, Hui Zhuang*, Panneer Selvam Santhalingam†, Riccardo Spolaor*, Parth Pathak†, Guoming Zhang*, Xiuzhen Cheng*
* Shandong University, China
† George Mason University, USA
Email: {phu, rspolaor, guomingzhang, xzcheng}@sdu.edu.cn, {psanthal, phpathak}@gmu.edu, {zhuanghui303}@gmail.com

Plug and Power: Fingerprinting USB Powered Peripherals via Power Side-channel

To appear at INFOCOM 2023 (CCF A)

Riccardo Spolaor*, Hao Liu*, Federico Turrin†, Mauro Conti†‡, Xiuzhen Cheng*
* School of Computer Science and Technology, Shandong University, Qingdao, China.
† Department of Mathematics, University of Padua, Padua, Italy.
‡ Delft University of Technology, Delft, Netherlands.

BLEWhisperer: Exploiting BLE Advertisements for Data Exfiltration

Published at ESORICS 2022 (CCF B)

Ankit Gangwal[1], Shubham Singh[1], Riccardo Spolaor[2,*], and Abhijeet Srivastava[1]

[1] International Institute of Information Technology, Hyderabad, India
gangwal@iiit.ac.in,
{shubham.singh, abhijeet.srivastava}@students.iiit.ac.in
[2] Shandong University, Qingdao Campus, China
rspolaor@sdu.edu.cn
* Corresponding author

Survivalism: Systematic Analysis of Windows Malware Living-Off-The-Land

Published at IEEE SP 2021 (CCF A)

Frederick Barr-Smith, Oxford University; Xabier Ugarte-Pedrero, Cisco Systems; Mariano Graziano, Cisco Systems; Riccardo Spolaor, Oxford University; Ivan Martinovic, Oxford University

HiPo: Detecting Fake News via Historical and Multi-Modal Analyses of Social Media Posts

Submitted at IWQoS 2023 (CCF B)

Tianshu Xiao, Sichang Guo, Jingcheng Huang, Riccardo Spolaor*, Xiuzhen Cheng
School of Computer Science and Technology, Shandong University, Qingdao, China.
Email: xy727118@163.com, 201900140039@mail.sdu.edu.cn, max.hjc@outlook.com, {rspolaor, xzcheng}@sdu.edu.cn

Robust Network Intrusion Detection via Semi-Supervised Deep Reinforcement Learning

Submitted at ESORICS 2023 (CCF B)

Riccardo Spolaor, Tianhao Chen, Pengfei Hu*, and Xiuzhen Cheng

School of Computer Science and Technology, Shandong University, Qingdao, China
{rspolaor, phu, xzc}@sdu.edu.cn, cth@mail.sdu.edu.cn
* Corresponding author


this page
intentionally
left blank

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…

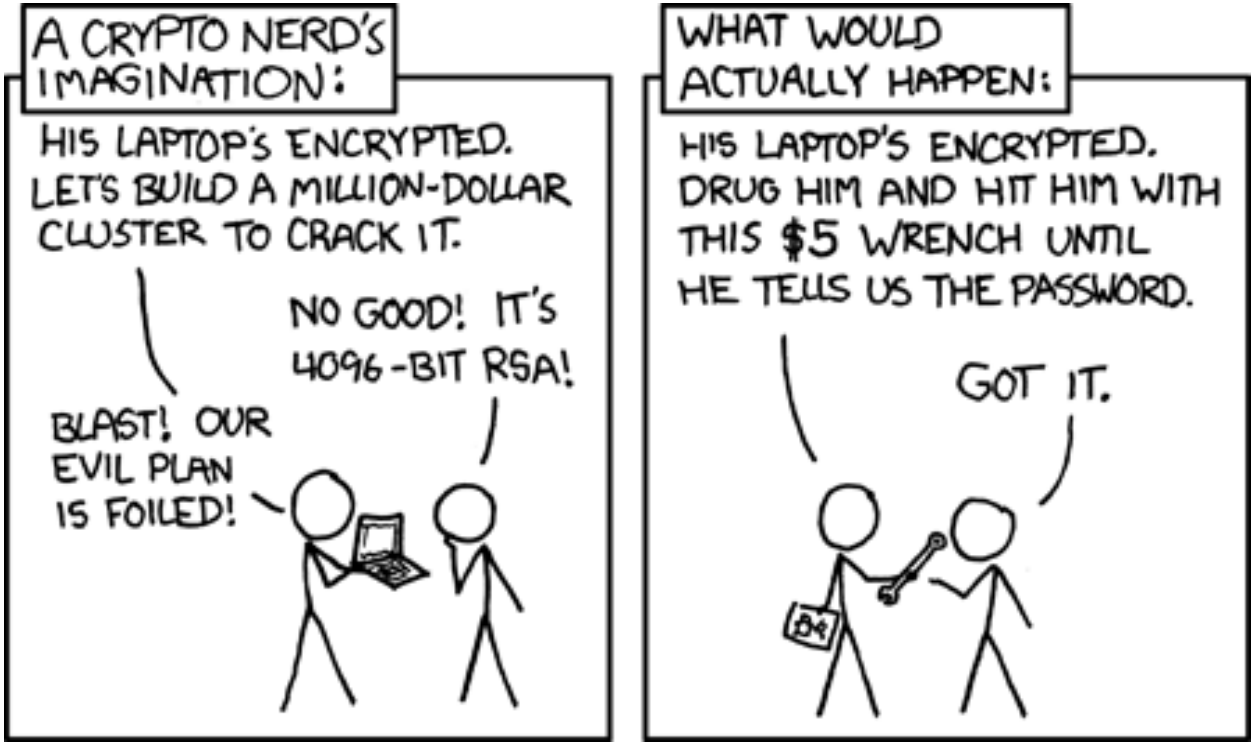
3) The security of a system is equivalent to the security of its less secure component (rule of the **weakest link**)

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

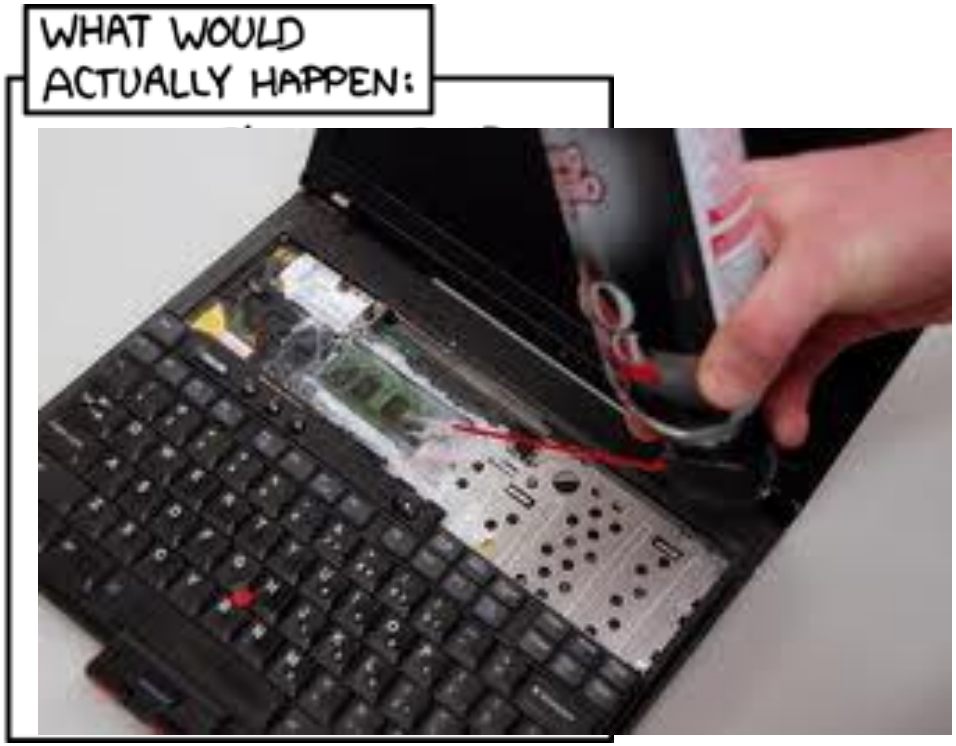


Some key concepts to start with...

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

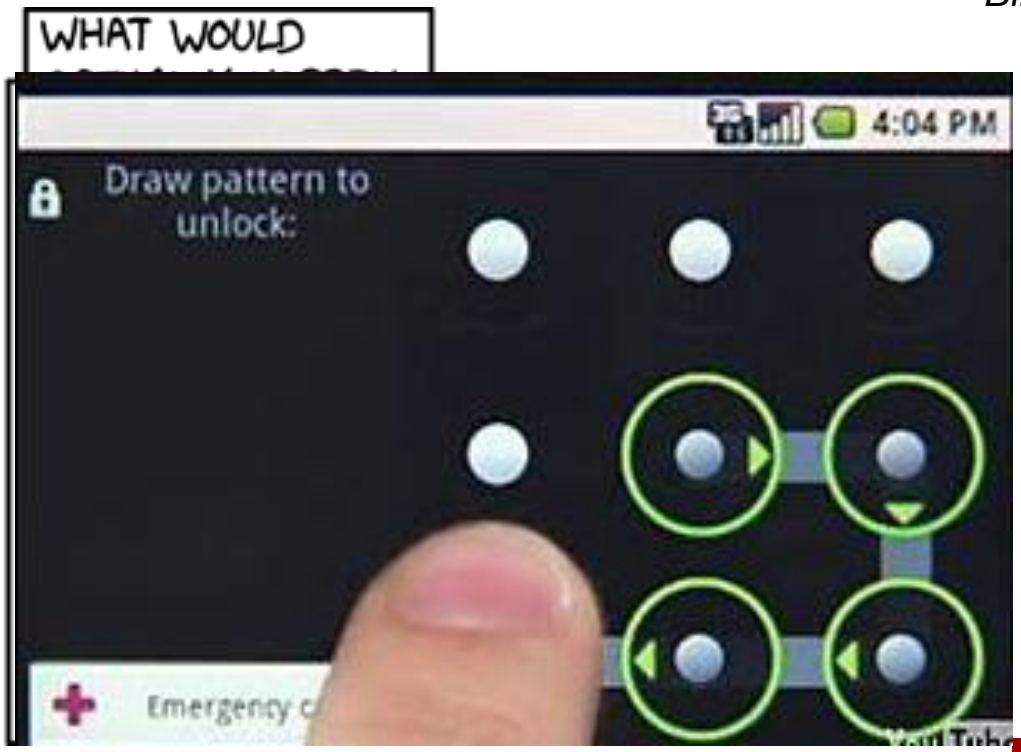


Some key concepts to start with...

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...

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…

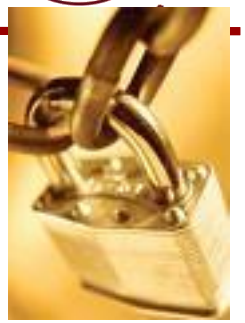
Basic security properties

- 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

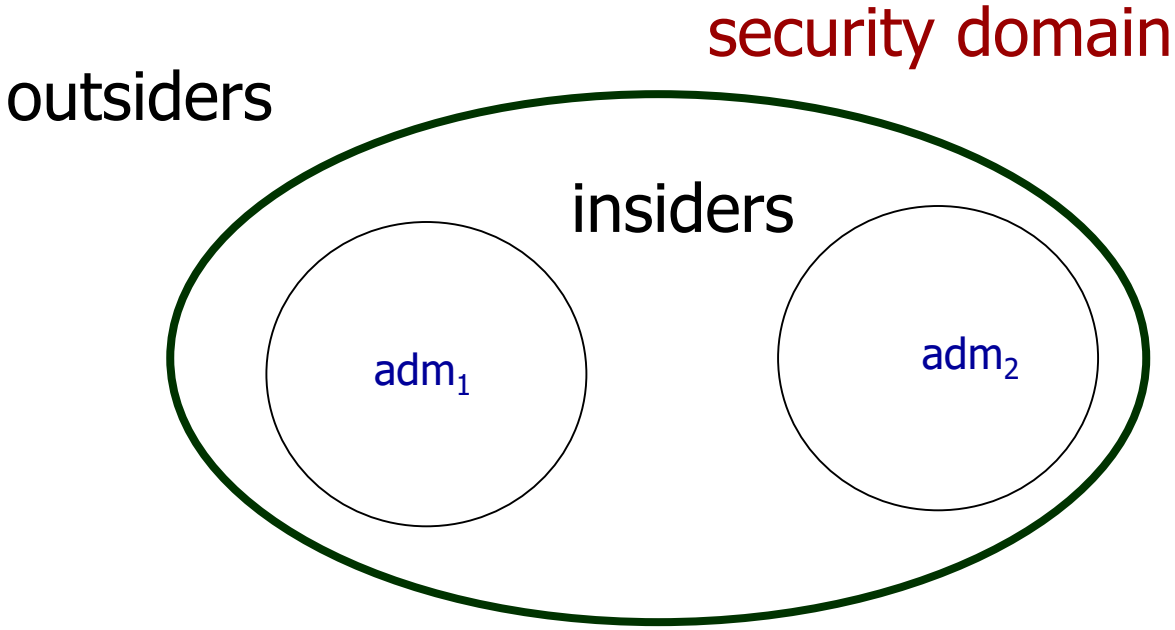
- Non repudiation: to prevent false denial of performed actions
- Authorisation: ”What Alice can do”
- Auditing: to securely record evidence of performed actions
- Attack-tolerance: ability to provide some degree of service after failures or attacks
- Disaster Recovery: ability to recover a safe state
- 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



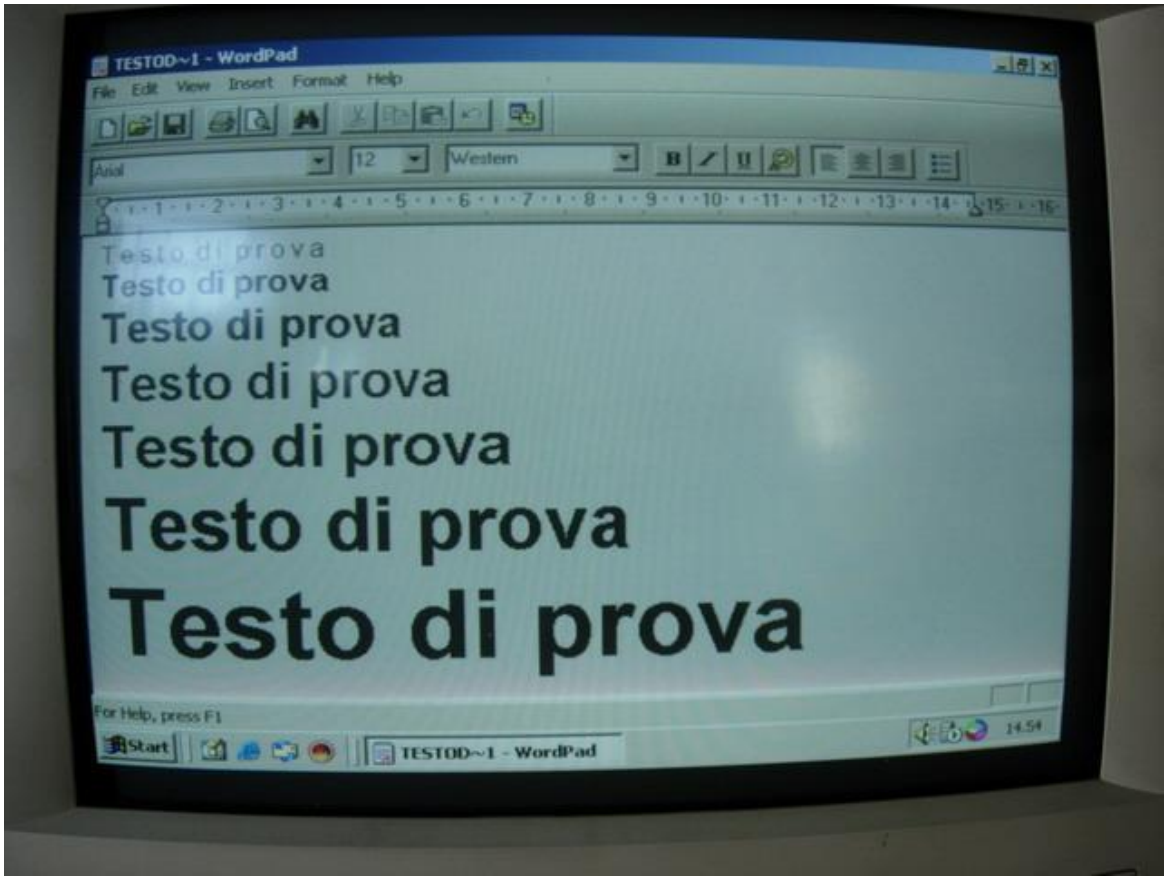
security domain and admin domain may differ

Types of attack

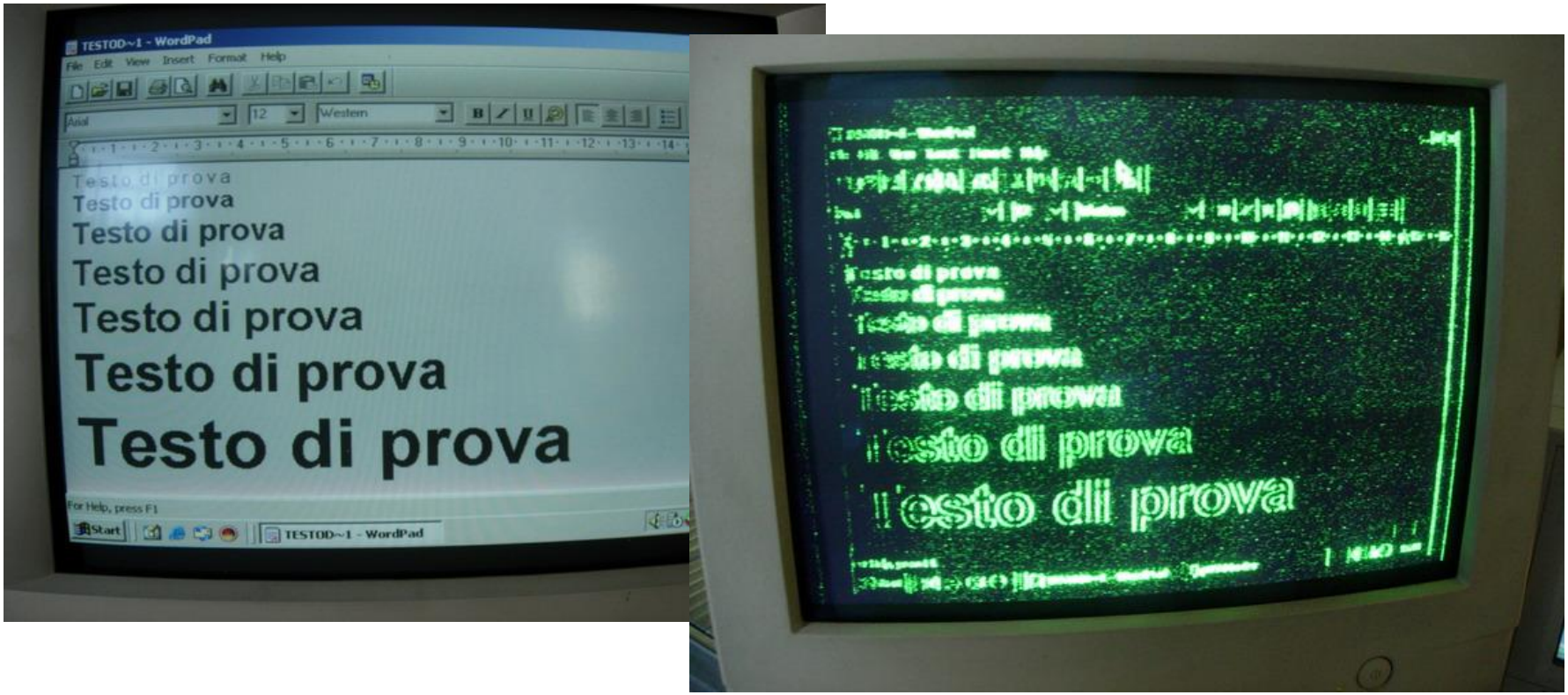
- Passive: the attacker can only read any information
  - Tempest (signal intelligence)
  - Packet Sniffing

- 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

TEMPEST on HDMI

Questions? Feedback? Suggestions?

Group: [SDU BSc 23] infosec

Valid until 3/3 and will update upon joining group

www.spolaor.com

rspolaor@sdu.edu.cn

The TA of this course is Feng Ning (2978539712@qq.com)