TÉCNICO LISBOA

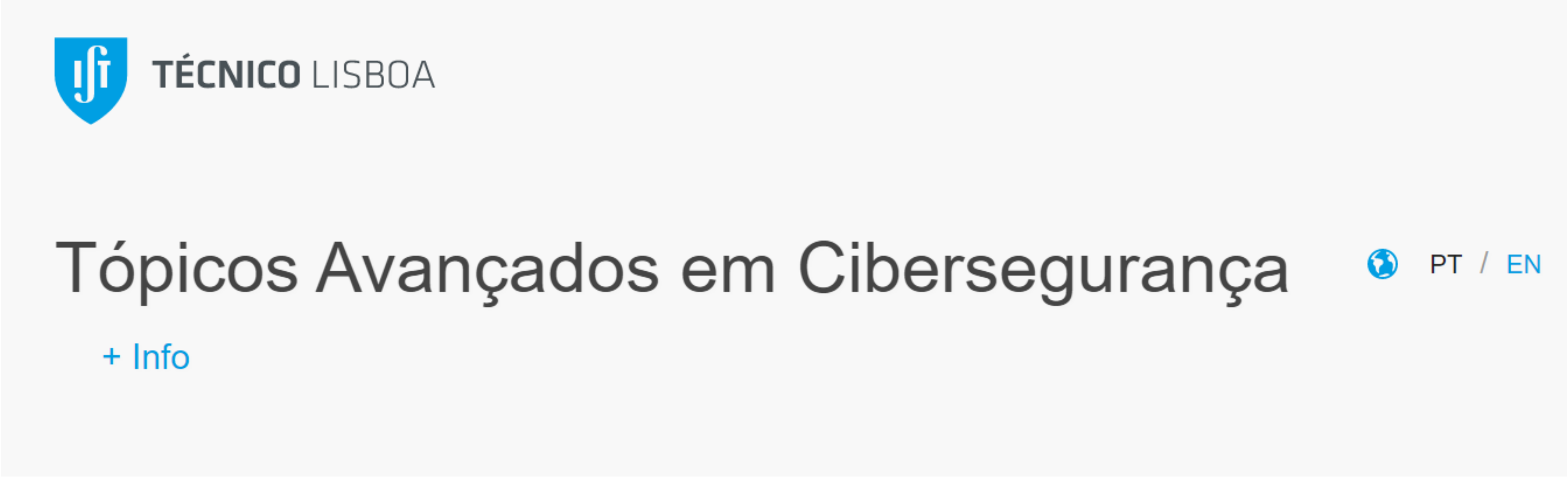
Advanced Topics in Cybersecurity

Prof. Miguel L. Pardal

Miguel.Pardal@tecnico.ulisboa.pt

Friday, April 9th, 2021

Official TACib Page: Fénix



Tópicos Avançados em Cibersegurança

https://fenix.tecnico.ulisboa.pt/disciplinas/TACib46/2020-2021/2-semestre

- All information in this presentation can be superseded by what is in Fénix

Agenda

- Course context and objectives
- Work methodology
- Evaluation
- Work plan

Course context and objectives

Advanced Topics in Cybersecurity

Cybersecurity

“the prevention of damage to, unauthorized use of, exploitation of, and the restoration of electronic information and communications ***systems****, and the* ***information*** *they contain, in order to strengthen the confidentiality, integrity and availability of these systems.”*

Definition by **NIST**
(U.S. National Institute of Standards and Technology)

CIA properties

- **C**onfidentiality
  - Absence of disclosure of data by non-authorized parties
- **I**ntegrity
  - Absence of invalid system or data modifications by non-authorized parties
- **A**vailability
  - Readiness of the system to provide its service

Extended properties

- CIA properties:
  - Confidentiality
  - Integrity
  - Availability
- TIU properties:
  - Transparency
  - Intervenability
  - Unlinkability

Digital Citizenship

TIU properties

- **T**ransparency
  - Control with whom data is shared, how long it is held, how it is audited
  - Define the privacy risks
- **I**ntervenability
  - The right to access, change, correct, block, revoke consent, and delete personal data
- **U**nlinkability
  - Allow the separation of informational contexts, such as work, personal, family, citizen, and social

Research topics

- Hardware security
- Software security
- Network security
- Cryptography
- Security protocols
- Authentication & Authorization

Course objectives

- Study some of the latest advancements in Cybersecurity, through a reading group
    - Read scientific papers
    - Take notes
    - Present
    - Discuss
- Learn from the best researchers
    - Gain insight for your own work

Work methodology

Advanced Topics in Cybersecurity

Research: *standing on the shoulders of giants*

- Our research is only possible because of the work of others before us
  - Actual People, Labs, Universities

OSDI 2014

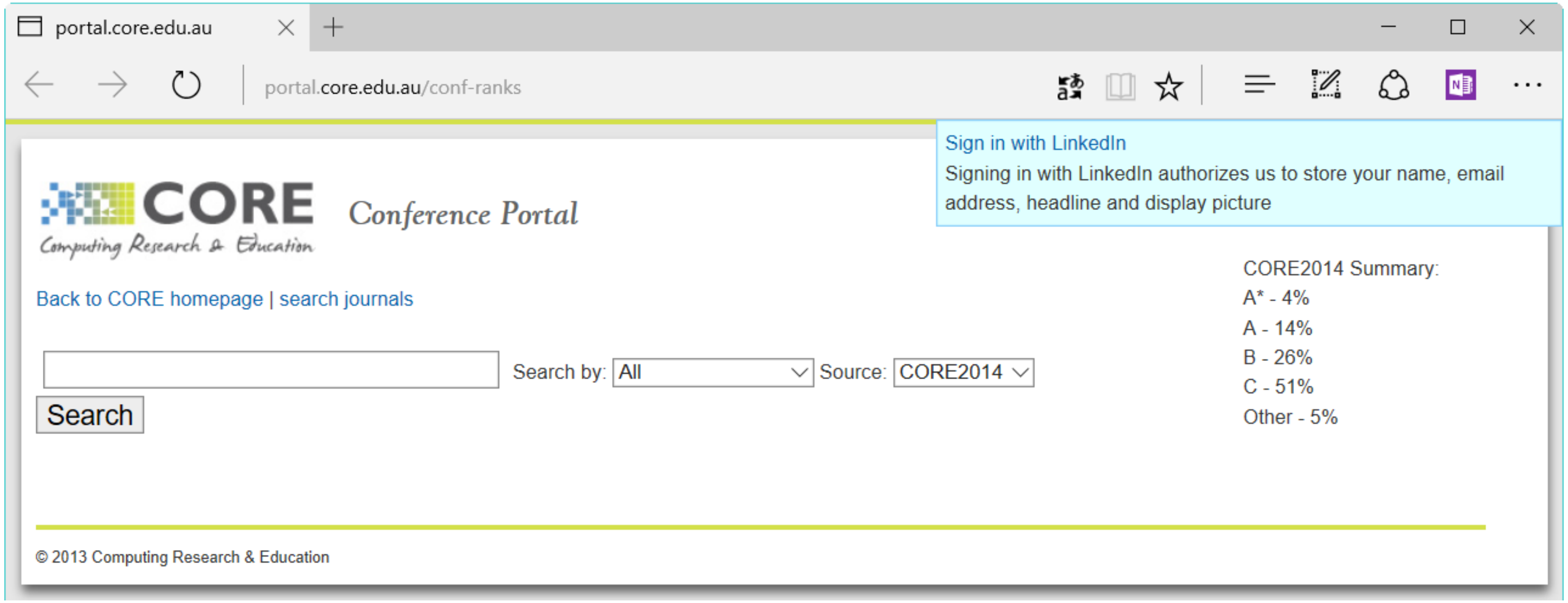
Different types of publications

- Technical report
- Workshop paper
- Conference paper
- Book chapter
- Journal article
- Book

Maturity of published work

- First promising results
  - Workshop
- Ongoing work with evaluation
  - Conference
- **Fully developed and innovative findings**
  - **Top conference**
- Extended and completed work
  - Journal

Conference rankings



Sign in with LinkedIn

Signing in with LinkedIn authorizes us to store your name, email address, headline and display picture

Conference Portal

Back to CORE homepage | search journals

Search by: All Source: CORE2014

CORE2014 Summary:
A* - 4%
A - 14%
B - 26%
C - 51%
Other - 5%

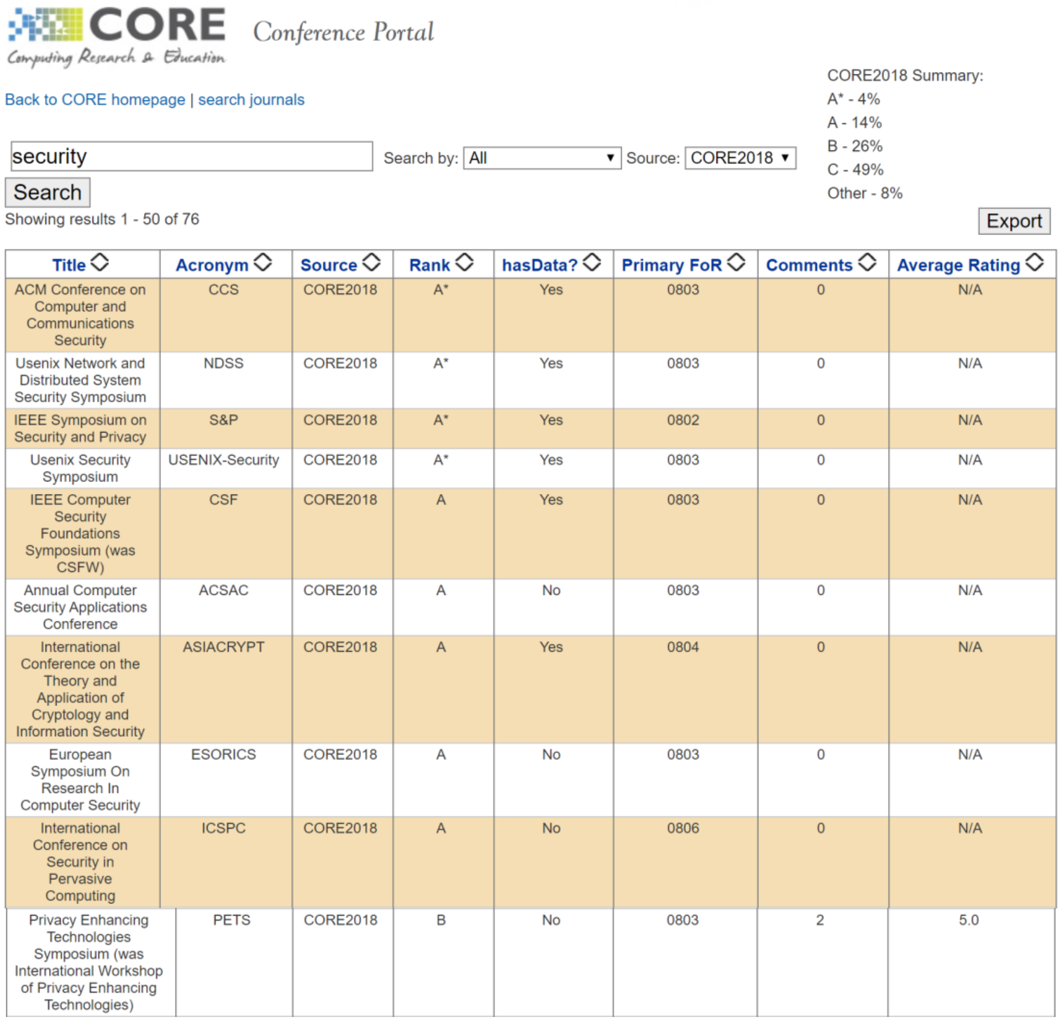
© 2013 Computing Research & Education

http://portal.core.edu.au/conf-ranks/

Top security conferences (CORE A*)

CCS acm SIGSAC

IEEE S&P



CORE Computing Research & Education Conference Portal

Back to CORE homepage | search journals

CORE2018 Summary:
A* - 4%
A - 14%
B - 26%
C - 49%
Other - 8%

security Search by: All Source: CORE2018

Search

Showing results 1 - 50 of 76

Export

Title	Acronym	Source	Rank	hasData?	Primary FoR	Comments	Average Rating
ACM Conference on Computer and Communications Security	CCS	CORE2018	A*	Yes	0803	0	N/A
Usenix Network and Distributed System Security Symposium	NDSS	CORE2018	A*	Yes	0803	0	N/A
IEEE Symposium on Security and Privacy	S&P	CORE2018	A*	Yes	0802	0	N/A
Usenix Security Symposium	USENIX-Security	CORE2018	A*	Yes	0803	0	N/A
IEEE Computer Security Foundations Symposium (was CSFW)	CSF	CORE2018	A	Yes	0803	0	N/A
Annual Computer Security Applications Conference	ACSAC	CORE2018	A	No	0803	0	N/A
International Conference on the Theory and Application of Cryptology and Information Security	ASIACRYPT	CORE2018	A	Yes	0804	0	N/A
European Symposium On Research In Computer Security	ESORICS	CORE2018	A	No	0803	0	N/A
International Conference on Security in Pervasive Computing	ICSPC	CORE2018	A	No	0806	0	N/A
Privacy Enhancing Technologies Symposium (was International Workshop of Privacy Enhancing Technologies)	PETS	CORE2018	B	No	0803	2	5.0

NDSS

USENIX SECURITY SYMPOSIUM

http://portal.core.edu.au/conf-ranks/?search=security&by=all&source=CORE2018&sort=arank&page=1

ACM CCS topics

- Attacks
- Biometric Security
- Blockchain
- Certificates
- Cloud Security
- Cryptographic Primitives
- Cyber Threat
- Cyberphysical Security
- Encryption (Searchable, Updatable, Homomorphic, etc.)
- Fingerprinting
- Forensics
- Formal Analysis
- Fuzzing: Methods and Applications
- Internet Security
- Internet of Things
- Language Security
- ML (Machine Learning) for Security
- Mobile Security
- Passwords and Accounts
- Privacy
- Privacy-Preserving Techniques
- Protocols
- SDN (Software Defined Network) Security
- Secret Sharing
- Secure Computing
- Side Channels
- Signatures
- Software Security
- TEE (Trusted Execution Environment)
- User Study
- Web Censorship and Auditing
- Web Security
- Zero-Knowledge Proofs

Usenix NDSS

- Anti-malware techniques: detection, analysis, and prevention
- Cyber-crime defense and forensics (e.g., anti-phishing, anti-blackmailing, anti-fraud techniques)
- Security for future Internet architectures and designs (e.g., Software-Defined Networking)
- Implementation, deployment and management of network security policies
- Integrating security in network protocols (e.g., routing, naming, and management)
- Cyber attack (e.g., APTs, botnets, DDoS) prevention, detection, investigation, and response
- Software/firmware analysis, customization, and transformation for systems security
- Privacy and anonymity in networks and distributed systems
- Security and privacy for blockchains and cryptocurrencies
- Public key infrastructures, key management, certification, and revocation
- Security for cloud/edge computing
- Security and privacy of mobile/smartphone platforms
- Security for cyber-physical systems (e.g., autonomous vehicles, industrial control systems)
- Security for emerging networks (e.g., home networks, IoT, body-area networks, VANETs)
- Security for large-scale, critical infrastructures (e.g., electronic voting, smart grid)
- Security and privacy of systems based on machine learning and AI
- Security of Web-based applications and services (e.g., social networking, crowd-sourcing)
- Special problems and case studies: e.g., tradeoffs between security and efficiency, usability, cost, and ethics
- Usable security and privacy
- Trustworthy Computing software and hardware to secure networks and systems

IEEE S&P CFP topics

- Access control and authorization
- Accountability
- Anonymity
- Application security
- Attacks and defenses
- Authentication
- Censorship resistance
- Cloud security
- Distributed systems security
- Economics of security and privacy
- Embedded systems security
- Forensics
- Hardware security
- Intrusion detection and prevention
- Malware and unwanted software
- Mobile and Web security and privacy
- Language-based security
- Network and systems security
- Privacy technologies and mechanisms
- Protocol security
- Secure information flow
- Security and privacy for the Internet of Things
- Security and privacy metrics
- Security and privacy policies
- Security architectures
- Usable security and privacy

Usenix Security topics overview

USENIX
SECURITY SYMPOSIUM

- System security
- Network security
- Security analysis
- Data-driven security and measurement studies
- Privacy-enhancing technologies and anonymity
- Usable security and privacy
- Language-based security
- Hardware security
- Research on surveillance and censorship
- Social issues and security
- Applications of cryptography

Latest proceedings

- ACM CCS 2020 https://dl.acm.org/doi/proceedings/10.1145/3372297
- Usenix NDSS 2020 https://www.ndss-symposium.org/ndss-program/2020-program/
- IEEE Security & Privacy 2020 https://www.computer.org/csdl/proceedings/sp/2020/1dAAQaOrrva
- Usenix Security 2020 https://www.usenix.org/conference/usenixsecurity20/technical-sessions

Evaluation

Advanced Topics in Cybersecurity

Evaluation methodology

- Paper presentation (50%)
- Paper notes (30%)
- Participation (20%)

Evaluation methodology in detail

- Paper presentation (50%)
  - 2 papers for each student
  - Prepare slides, present paper
  - Answer detailed questions about paper
- Paper notes (30%)
  - Write and submit notes for each paper not presented
  - Notes are graded
  - Grade is calculated from the average
- Participation (20%)
  - Class discussion
  - Questions asked

Paper presentation

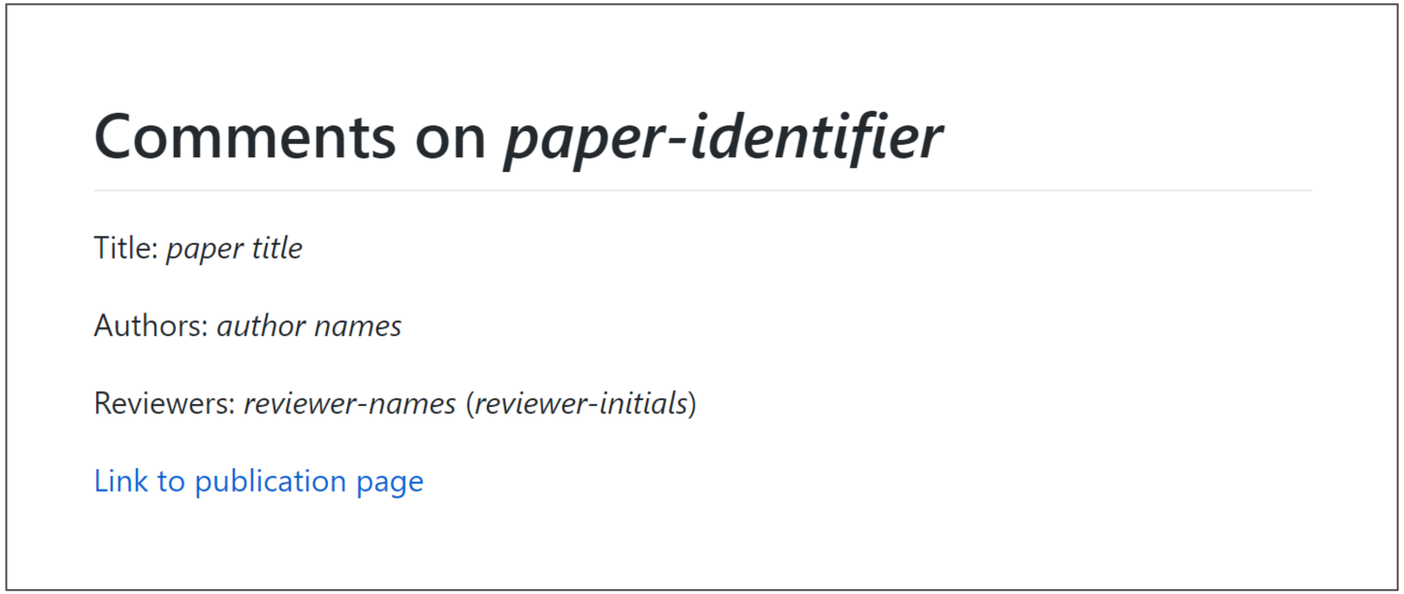
- Objective
  - Present very clearly the **main idea** (problem and solution) of the paper and give some interesting **insights**
  - 20 minutes presentation, followed by discussion
- Mandatory: use slides
  - E.g., PowerPoint
- Grading criteria:
  - Does the audience understand the idea/insights?
  - What is the problem? How does the paper solve it?
  - Present the most interesting but not all experimental results?
  - Slides illustrate and support the talk? Are they well organized? Are there diagrams to help convey difficult ideas?
  - Is the presentation fluid? With good time management?
  - Is the presenter able to answer (hard) questions about the paper?

Paper notes

- Title, Authors
- **Reviewer**: name and initials
- Link to publication page
- **Contribution**
  - What are the major issues addressed in this publication?
  - What are the main contributions (as stated by the authors)?
- **Strengths**
- **Weaknesses**

- Points of interest
  - System characteristics, assumptions
  - Examples or scenarios
  - Evaluation data sets
  - (something else that may be useful)
- See also
  - link to related publications
- Comparison
  - Is this work relevant for your work?
  - How is your work distinct from this work?

Template for scientific paper notes



Comments on *paper-identifier*

Title: *paper title*

Authors: *author names*

Reviewers: *reviewer-names* (*reviewer-initials*)

Link to publication page

Min: 300 words
Max: 600 words

Template in MarkDown format:
https://gist.github.com/miguelpardal/6e0d5bb94171765db79476e41aafff7d

Work plan

Advanced Topics in Cybersecurity

To-Do

- Pick class timeslot
- For each student presentation:
  - Pick a date
  - Select candidate papers to present
  - Prepare slides and present
  - Answer questions about paper
- Paper selection is made one week in advance, for each paper
- Also, on the other weeks:
  - Read paper of the week and write notes using template
  - Submit notes
  - Participate in discussion
    - Ask questions

Deadlines

- Pick class timeslot – **today**
- Pick presentation dates – **today**
- Select paper to present – **until Monday, April 12th**
    - Send 3 candidate papers, sorted by preference (favorite first)
    - I will select one to assure topic diversity
- Prepare slides – **until lecture**
    - I can provide feedback, if requested until **one working day before class**
- Paper notes – **until one working day before class**
    - If lectures are on Mondays, this means **Friday** before the lecture, **14:00**

Presentation schedule

See latest version at:
https://tinyurl.com/tacib21-2

Date	Presenter initials	Paper
April 9th	MP	(introduction)
April 16th	GB	(announced on April 12th)
April 23rd	JG	(announced on April 19th)
April 30th	GB	(announced on April 26th)
May 7th	JG	(announced on May 3rd)

Final Information

- Theoretical lectures chair:
  - Prof. Miguel Pardal

- To ask questions, send notes, and slides:
  - ➢ Email: Miguel.Pardal@tecnico.ulisboa.pt
  - ➢ Subject prefix: [TACib] …

- Coursework:
  Presentation + Paper Notes + Participation