UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

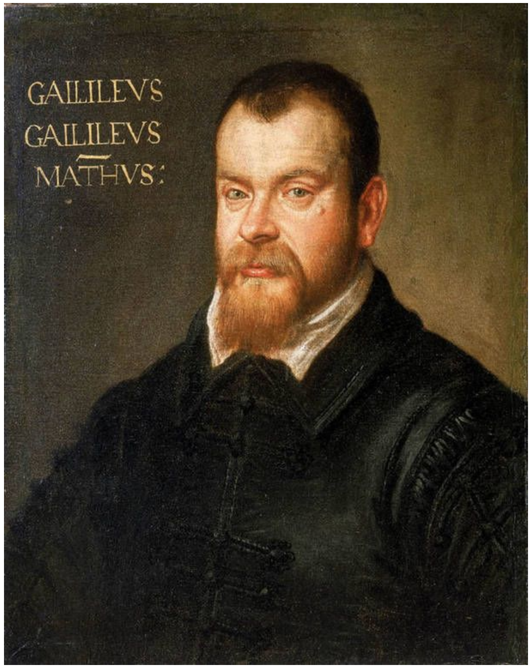
DIPARTIMENTO MATEMATICA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

Cybersecurity Research

Prof. Mauro Conti
conti@math.unipd.it

Research Process

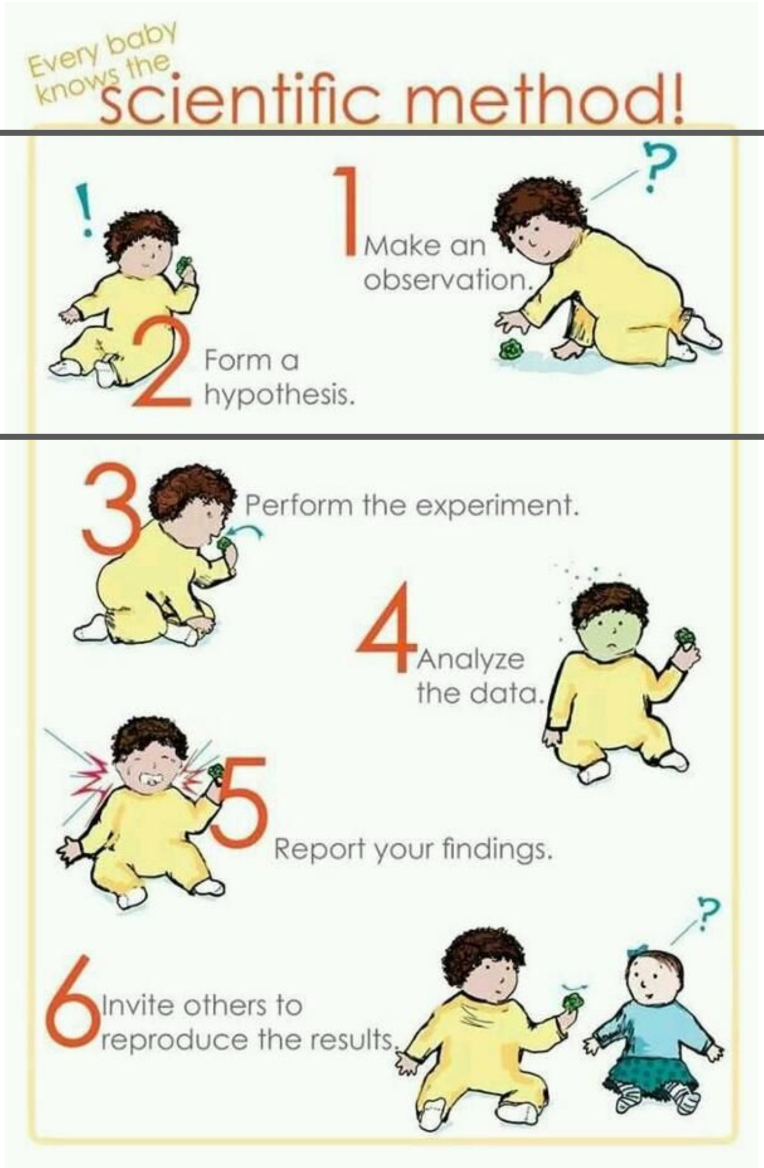


Research Process

Research Process

Playing,
Reading Papers,
Attending Talks,
Thinking,
Discussing,
Criticizing,
Questioning

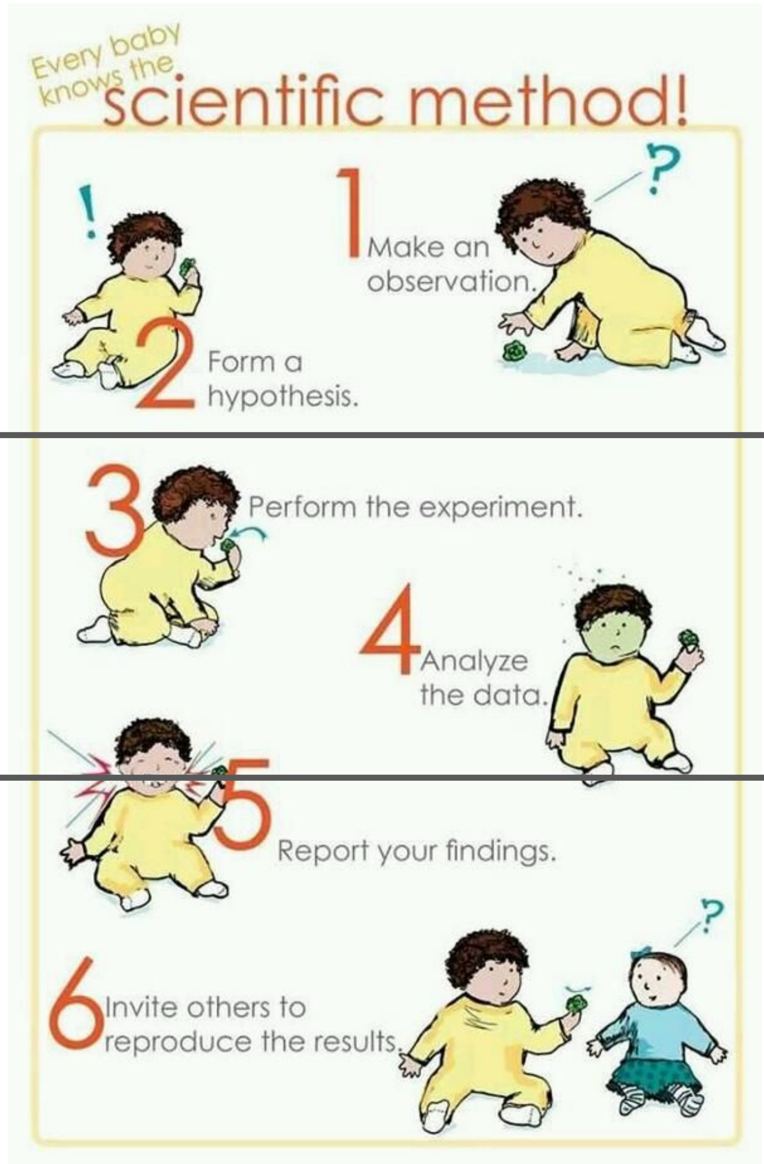
Research Process



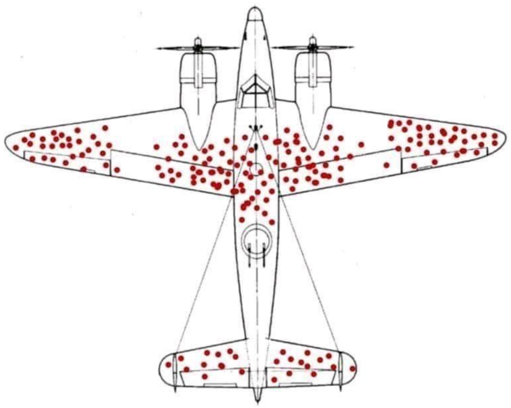
Playing,
Reading Papers,
Attending Talks,
Thinking,
Discussing,
Criticizing,
Questioning

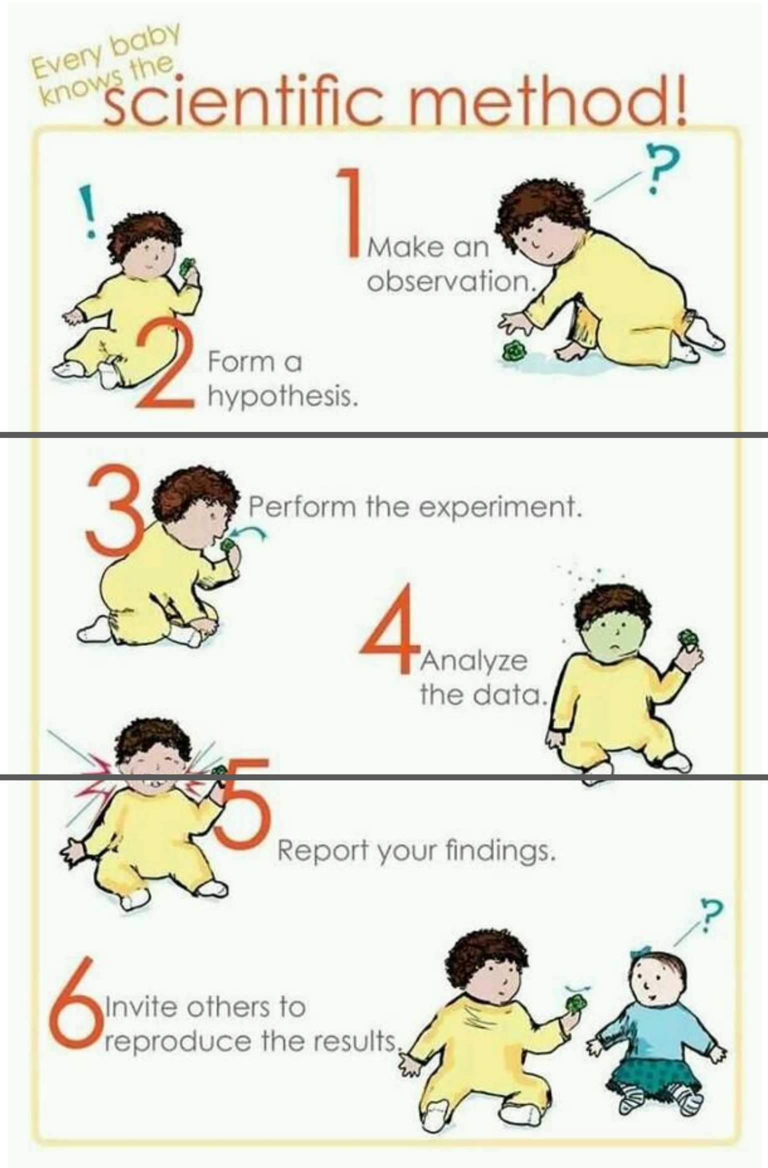
Research Process

Designing **Sound Experiments**, Looking at Data, Criticizing, Questioning



Research Process

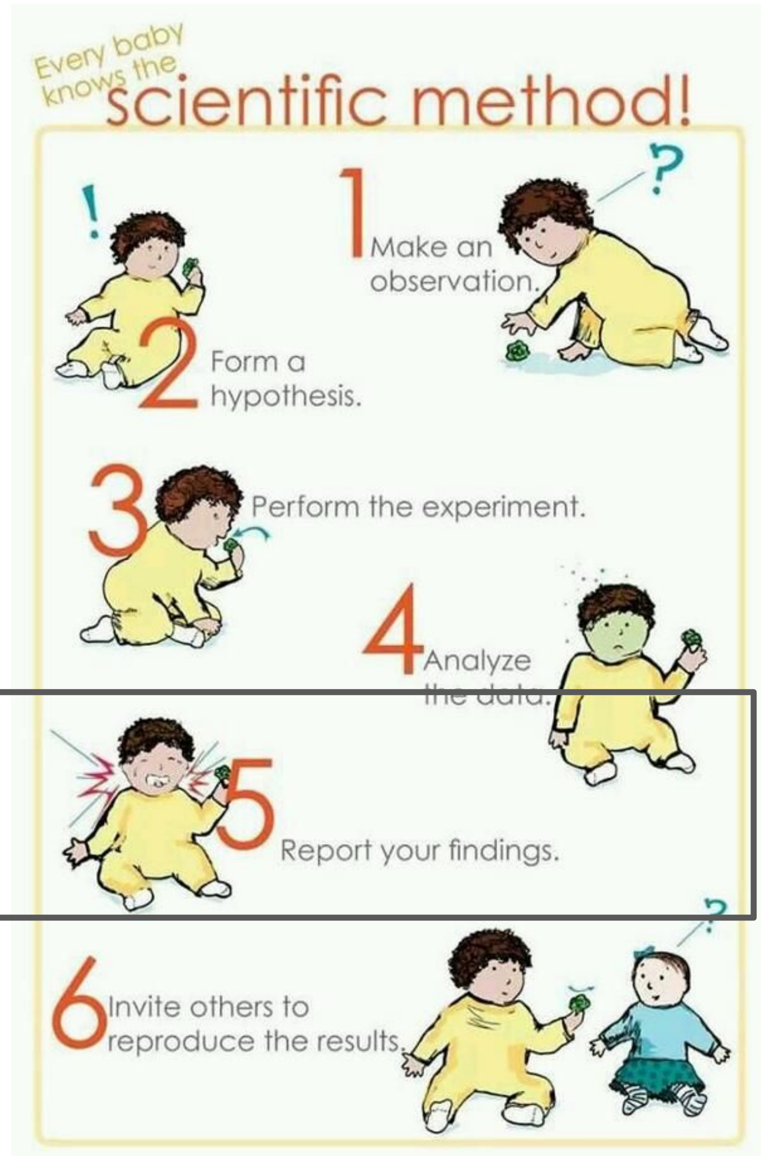




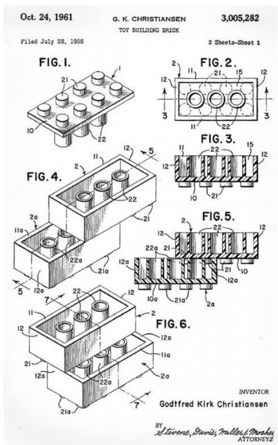
Designing **Sound Experiments**, Looking at Data, Criticizing, Questioning

Research Process

Writing...
Papers
(Reports,
blogs...)
Presenting
Results



Research Process



Writing...
Papers
(Reports,
blogs...)
Presenting
Results

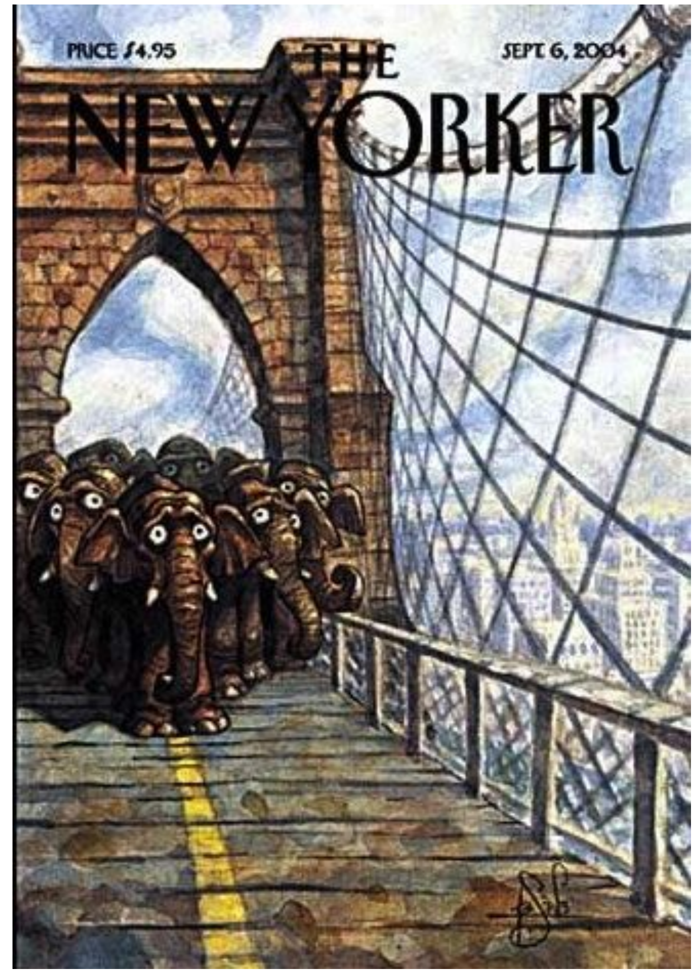
Research Process

Writing...
Papers
(Reports,
blogs...)
Presenting
Results

And Particularly for Cybersecurity…

And Particularly for Cybersecurity...

Expect (imagine) the unexpected



A paper

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 System for Android. While the concept of context-related access control is not new, this is the first work that brings this concept into the smartphone environment. In particular, in our work, a context can be defined by: the status of variables sensed by physical (low level) sensors, like time and location; additional processing on these data via software (high level) sensors; or particular interactions with the users or third parties. CRêPE allows context-related policies to be set (even at runtime) by both the user and authorized third parties locally (via an application) or remotely (via SMS, MMS, Bluetooth, and QR-code). A thorough set of experiments shows that our full implementation of CRêPE has a negligible overhead in terms of energy consumption, time, and storage, making our system ready for a production environment.**

***Index Terms*—Android security, context policy, smartphone security.**

I. Introduction

IN the world, there is an average of almost one mobile telephone per human being (with small differences between developed and developing countries). The computational capabilities of mobile phones have increased significantly in the last years, leading to so called smartphones. These devices (just "phones" in this paper) can actually run applications in such a way that is similar to desktop computers. However, because of the specific characteristics of smartphones (user mobility and communication features among others), the security and privacy of these devices is particularly exposed [1]. These challenges reduce the users' confidence and make it more difficult to adopt this technology to its full potential. To alleviate this problem, 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 applications and services (e.g. WiFi or Bluetooth). In several smartphone systems the behavior of the applications is completely under the control of a centralized entity (e.g. once an application is installed, the user cannot control its behavior). For example, Apple has complete control on the applications installed on iPhone devices. In fact, the only way to install applications onto a (non rooted) iPhone is by downloading them from the Apple App Store. And in turn, in order to appear in the App Store, an application has to pass an Apple vetting procedure.

However, even in systems where the user can control the behavior of the applications, this is still mostly based on policies per application (non system-wide), and policies are set only at installation time. For instance, in the J2ME platform each MIDlet suite uses a JAD (Java Application Descriptor) file to provide the device at installation time with access control information. Similarly, in Android [2] an application developer declares in a manifest file all the permissions that the application must have, in order for it to access protected parts of the API and to interact with other applications. At installation time, these permissions are granted to the application based on its signature and interaction with the user [3]. While Android gives more flexibility than J2ME or other systems (the user is at least notified about the resources that the application uses), granting permissions all-at-once and only at installation time is still a coarse-grained control: the user has no ability to govern how the permissions are exercised after the installation. As an example, Android does not allow policies that grant access to a resource only for a fixed number of times, or only under some particular circumstances. Meanwhile, to protect users' privacy, the current security models restrict trusted third parties' control over mobile phones. Typically, only the device manufacturer and the network provider have control over the smartphone. There are no mechanisms to allow other authorized parties (e.g. a company that provides a smartphone to its employee or the private owner) to have full control over the behavior of the phone.

Hence, there is a need for a system that will help the user to enforce the policies she defines, and help her to comply with the policies specified by authorized third parties. The following examples can be scenarios for which having a practical solution might extend the usability of the phone:

- A user might want her Bluetooth interface to be discovered when she is at home or in her office, not otherwise.
- A user might lend her phone to a friend, while the user does not want her friend to be able to use some applications or to have certain data available (e.g. SMSs).

Manuscript received July 10, 2011; revised March 25, 2012; accepted May 08, 2012. Date of publication June 11, 2012; date of current version September 07, 2012. This work was supported in part by the project S-MOBILE, funded by STW-Sentinels, NL. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Elisa Bertino.

M. Conti was with Vrije Universiteit Amsterdam, Amsterdam 1081 HV, The Netherlands. He is now with the University of Padua, Padua, 35131, Italy (e-mail: conti@math.unipd.it).

B. Crispo and Y. Zhauniarovich are with Università di Trento, Trento, 38123, Italy (e-mail: crispo@disi.unitn.it; zhauniarovich@disi.unitn.it).

E. Fernandes was with Vrije Universiteit Amsterdam, Amsterdam 1081 HV, The Netherlands. He is now with the University of Michigan, Ann Arbor, MI 48109-2121 USA (e-mail: earlence@cs.vu.nl).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2012.2204249

A paper (inside)

- *Title*
- *Authors and Affiliations*

- *Abstract*
  - Brief description of the domain/context
    Need/Motivation!
  - Description of what is the work about / **Contribution**
    Summary of the results

- *Introduction*
  - Extended description of the history/domain
  - Identification of a problem and motivation
  - How the proposal solves the problem
  - Declaration of the scientific contribution
  - Organization of the paper

A paper (inside)

- *Related work*
  - Description of what has already been done
  - Compare with your work
    - Make your spot/niche
  - Highlight what your work does more than other papers

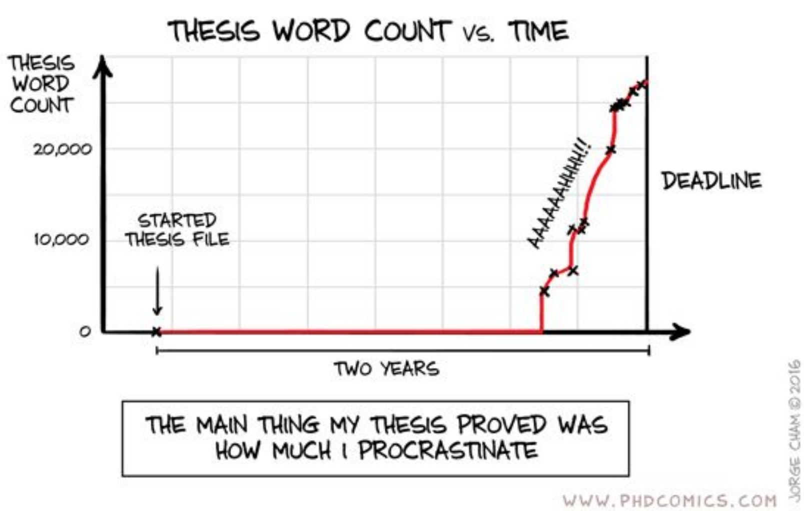
A paper (inside)

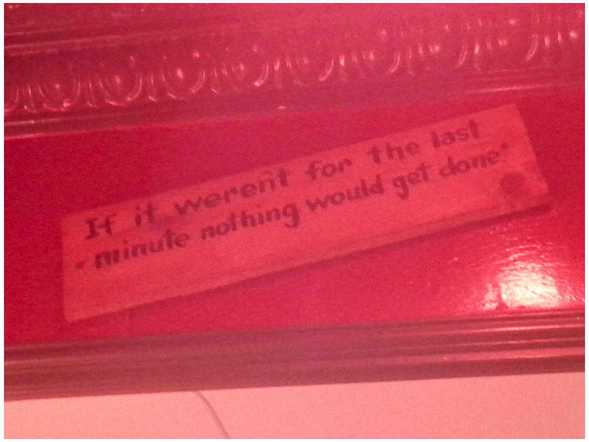
- *Description of the proposal*
  - Background knowledge
  - Formal definition of the problem (threat model)
  - Overview of the method
  - Detailed description of the components
- *Experimental evaluation*
  - Description of the tools used
  - Implementation of the experiment
  - Presentation of the results
  - Discussion and limitations
- *Conclusions*
  - Summarize of contribution and results
  - Possible future research directions

The Review Process

- Pick a venue (Journal / Conference ...)
    - Aim for top
  https://www.ted.com/talks/viktor_frankl_why_believe_in_others

- Submission (deadline!)





The Review Process

- Review
  - Journal: Editor in Chief / Associate Editor / Reviewers

IEEE TRANSACTIONS ON
INFORMATION FORENSICS AND SECURITY

Editor-in-Chief:
Mauro Conti
University of Padua, Italy
Email EiC
Email SPS Publications Office
Term Ends: 31 December 2024

Associate Editors:

Name	Affiliation
Frederik Armknecht	University Mannheim, Germany
Patrick Bas	CNRS - Lagis, France
Lejla Batina	Radboud University, The Netherlands
Marina Blanton	University at Buffalo-SUNY, USA
Matthieu R. Bloch	Georgia Institute of Technology, USA
Rainer Bohme	Universitat Innsbruck, Austria
Julien Bringer	SMART VALOR, Switzerland
Lorenzo Cavallaro	Royal Holloway, University of London, UK
Remi Cogranne	Troyes University of Technology, France
Dinu Coltuc	University of Tirgoviste, Romania
Pedro Comesana Alfaro	University of Vigo, Spain

  - Conference: Program Chair / Program Committee Members / Reviewers

Conference Organization

General Chairs:
- Emiliano Casalicchio (Sapienza University of Rome, Italy)
- Angelo Spognardi (Sapienza University of Rome, Italy)
- Giuseppe Bernieri (University of Padua, Italy)

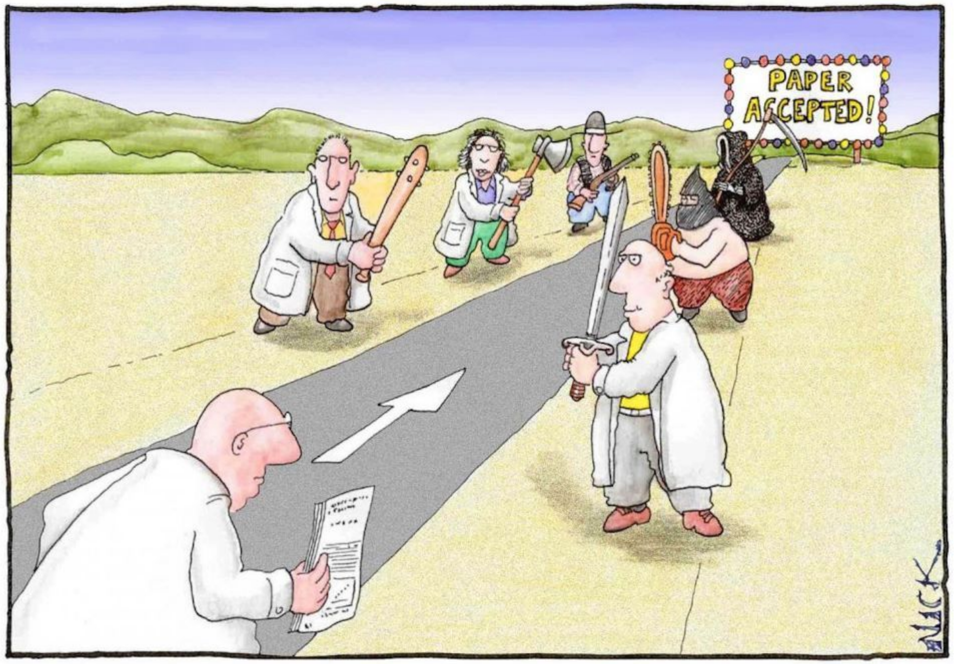
Program Chairs:
- Mauro Conti (University of Padua, Italy)
- Jianying Zhou (SUTD, Singapore)

Springer

The Review Process

Reviewer will judge:

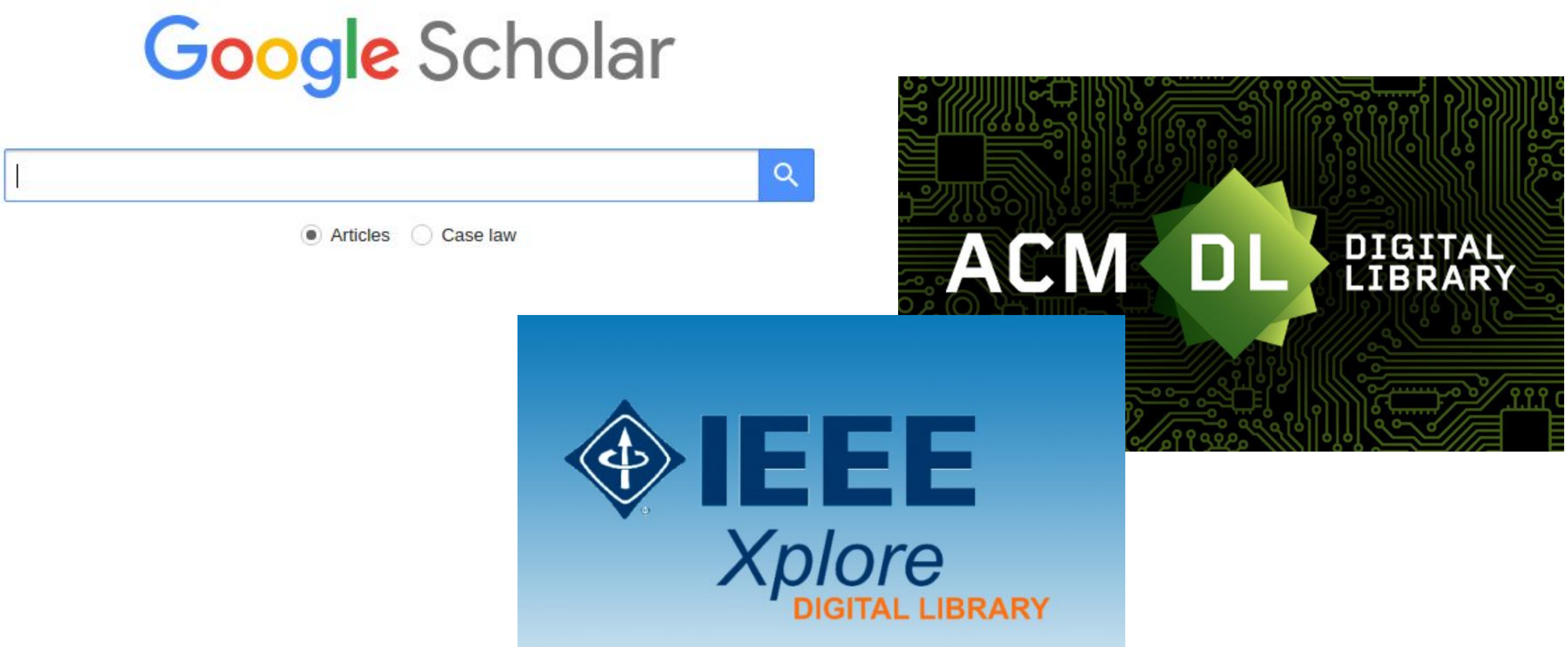
- Novelty of the idea
- Impact of the scientific contribution
- Solidity of the experimental design
- Quality of the presentation



Most scientists regarded the new streamlined peer-review process as "quite an improvement."

Reading Papers... where to go?

- By Topic



- Hint: Try to get the naming used already in the literature

Reading Papers... where to go?

- By Venue

A.R., I.F., and more...

Computer Security Conference Rank

Guofei Gu

Ranking

Note:

- How to judge how good a conference is? In my opinion, here are several criterias:
  - **Acceptance ratio:** definitely an important metric (maybe the easiest metric t
  - **Paper quality and impact:** how many classic papers are from this conferen conference have on the community? are they well cited and studied?
  - **Committee member quality:** what's the quality of TPC members? are they important factor because they will affect the quality of submission (good pap noted researchers in the committee), and control the quality of accepted pape
  - **Attendee/Paper number ratio:** another quantified metric. This somehow re community
  - **Location:** a beautiful place has some attraction. In addition, many researche other countries due to limited funding or time (or VISA problem...), so they j normally the conferences located in USA are better than in Europe, which is
  - **History:** a conference with a long history may have a good tradition and rep
  - **Industry connection:** this somehow reflects the impact on the industry. Non will attract more industry partners (so have more money to improve the qual
- This ranking list is only in my opinion. It is not official, nor accurate, only for refer
- For a general CS conference ranking list, please visit here.

Rank 1	S&P(Oakland)	IEEE Symposium on Security and Privacy
	CCS	ACM Conference on Computer and Communications Security
	Crypto	International Cryptology Conference
	Eurocrypt	European Cryptology Conference
	Security	Usenix Security Symposium
	NDSS	ISOC Network and Distributed System Security Symposium
Rank 2	ESORICS	European Symposium on Research in Computer Security
	RAID	International Symposium on Recent Advances in Intrusion Detection
	ACSAC	Annual Computer Security Applications Conference
	DSN	The International Conference on Dependable Systems and Networks
	CSFW	IEEE Computer Security Foundations Workshop
	Asiacrypt	International Conference on the Theory and Application of Cryptology and Information Security
	TCC	Theory of Cryptography Conference
	SecureComm	IEEE Communications Society/CreateNet Internation Conference on Security and Privacy for Emerging Areas in Communication Networks
	AsiaCCS	ACM Symposium on Information, Computer and Communications Security
	ACNS	International Conference on Applied Cryptography and Network Security

Google Scholar

Top publications

Categories > Engineering & Computer Science > Computer Security & Cryptography

	Publication	h5-index	h5-median
1.	ACM Symposium on Computer and Communications Security	82	123
2.	USENIX Security Symposium	81	116
3.	IEEE Transactions on Information Forensics and Security	78	106
4.	IEEE Symposium on Security and Privacy	72	128
5.	Network and Distributed System Secu		
6.	International Conference on Theory ar		
7.	International Cryptology Conference ((		
8.	Computers & Security		
9.	IEEE Transactions on Dependable and		
10.	International Conference on Financial		
11.	International Conference on The Theo (ASIACRYPT)		
12.	Theory of Cryptography		
13.	Workshop on Cryptographic Hardware		
14.	ACM on Asia Conference on Compute		
15.	Security and Communication Network:		
16.	Designs, Codes and Cryptography		
17.	IEEE Security & Privacy		
18.	European Conference on Research in		
19.	Computer Security Applications Confe		

Not secure | homepages.cs.ncl.ac.uk/changyu.dong/ranking.html

Security Conference Ranking

Rank	Name	Publication	Citation	Rate
1	S&P - IEEE Symposium on Security and Privacy	443	5728	12.93
2	CCS - Computer and Communications Security	484	4796	9.91
3	USENIX Security Symposium - USENIX Security Symposium	55	471	8.56
4	CRYPTO - CRYPTO	971	8281	8.53
5	CSFW - Computer Security Foundations Workshop	346	2836	8.20
6	NDSS - Network and Distributed System Security Symposium	172	1253	7.28
7	EUROCRYPT - Theory and Application of Cryptographic Techniques	947	6430	6.79
8	Information Hiding - Information Hiding	201	1044	5.19
9	ESORICS - European Symposium on Research in Computer Security	215	1030	4.79
10	FSE - Fast Software Encryption	307	1254	4.08
11	ASIACRYPT - ASIACRYPT	502	1949	3.88
12	Financial Cryptography - Financial Cryptography	235	861	3.66
13	Security Protocols Workshop - Security Protocols Workshop	207	758	3.66
14	RAID - Recent Advances in Intrusion Detection	127	421	3.31
15	CT-RSA - The Cryptographer's Track at RSA Conference	162	511	3.15
16	POLICY - IEEE International Workshop on Policies for Distributed Systems and Networks	136	414	3.04

Top Cyber Security Conferences Ranking (2019) [by year]

Here we define the Conference Impact Factor (CIF) as follows:

CIF = 1 / (AR+PR+CR), where
AR = No. accepted papers / No. of submissions
PR = No. accepted papers / No. of registered participants
CR = No. accepted papers / No. of citations (≈ 5 / h5-median)

Below is a CIF-based ranking of top cyber security conferences, for informal reference only. The CR data is from Google Scholar (h5-median). The ranking w be adjusted once a year. There is no intention to rank all cyber security conferences due to limited resources. However, if a conference that could be rank above the last one in the list is missing, please let me know (with the supporting data of at least past 5 years). Small conferences (with less than 20 accept papers or 60 participants on average) are excluded.

Conference	CIF (2019)	AR (2010-2019)	PR (2010-2019)	CR (2019)
1. IEEE S&P	3.80	**12.6%** = 50.4 / 398.5	**9.8%** = 50.4 / 516	**3.9%** (128)
2. Usenix Sec	3.15	**16.6%** = 65.6 / 396.3	**10.8%** = 65.6 / 606	**4.3%** (116)
3. ACM CCS	2.65	**17.5%** = 111.3 / 635.6	16.2% = 111.3 / 685.4	**4.1%** (123)
4. NDSS	2.46	**17.3%** = 53.9 / 312.2	18.9% = 53.9 / 285	**4.5%** (112)
5. Eurocrypt	2.42	22.3% = 51.5 / 230.5	**13.3%** = 51.5 / 386.3	**5.7%** (88)
6. CHES	2.36	25.1% = 34 / 135.7	**8.6%** = 34 / 396.6	8.6% (58)
7. Crypto	2.33	23.3% = 62.6 / 269.2	**14.0%** = 62.6 / 447.6	5.7% (87)
8. ACSAC	2.06	20.1% = 46.6 / 231.6	17.9% = 46.6 / 260.3	10.6% (47)
9. PETS	1.98	21.4% = 30.4 / 142.1	18.9% = 30.4 / 160.8	10.2% (49)
10. Asiacrypt	1.88	22.2% = 56 / 252.2	22.5% = 56 / 248.6	8.5% (59)
11. RAID	1.77	24.5% = 24.5 / 100.1	19.7% = 24.5 / 124.6	12.2% (41)
12. FC	1.77	26.4% = 31.8 / 120.6	23.3% = 31.8 / 136.7	6.8% (74)
13. ESORICS	1.53	**20.0%** = 52.5 / 262.3	33.8% = 52.5 / 155.1	11.4% (44)
14. ACM AsiaCCS	1.49	23.1% = 59.2 / 255.9	35.1% = 59.2 / 168.7	8.9% (56)
15. PKC	1.47	24.8% = 36.1 / 145.7	30.3% = 36.1 / 119	12.8% (39)
16. CT-RSA	1.47	29.7% = 25.6 / 86.2	25.7% = 25.6 / 99.6	12.5% (40)
17. ACM WiSec	1.42	29.0% = 23.9 / 82.3	28.1% = 23.9 / 85	13.2% (38)
18. FSE	1.36	30.8% = 32 / 103.8	21.9% = 32 / 146.2	20.8% (24)
19. ACNS	1.35	20.5% = 33.1 / 161.2	35.2% = 33.1 / 94	18.5% (27)
20. IEEE CSF	1.32	31.3% = 27 / 86.3	28.6% = 27 / 94.4	15.6% (32)
21. TCC	1.30	33.7% = 42.3 / 125.4	34.3% = 42.3 / 123.5	8.9% (56)

Reading Papers... where to go?

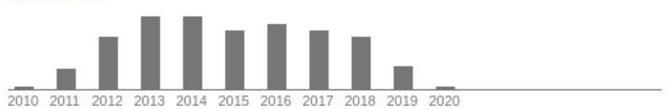
- By Venue
  - Some TOP ones:
    - Conferences:
      - ACM CCS, IEEE S&P, Usenix Security, NDSS...
    - Journals
      - ACM TOPS, IEEE TDSC, IEEE TIFS

Assessing a Paper

- **(Read it!)**
- Venue
- Authors (Name, Impact, Reputation)
- Impact / Citations
- ...

Crepe: Context-related policy enforcement for android

Autori	Mauro Conti, Vu Thien Nga Nguyen, Bruno Crispo
Data pubblicazione	2010/10/25
Conferenza	International Conference on Information Security
Pagine	331-345
Editore	Springer, Berlin, Heidelberg
Descrizione	Most of the research work for enforcing security policies on smartphones considered coarse-grained policies, e.g. either to allow an application to run or not. In this paper we present CRePE, the first system that is able to enforce fine-grained policies, e.g. that vary while an application is running, that also depend on the context of the smartphone. A context can be defined by the status of some variables (e.g. location, time, temperature, noise, and light), the presence of other devices, a particular interaction between the user and the smartphone, or a combination of these. CRePE allows context-related policies to be defined either by the user or by trusted third parties. Depending on the authorization, third parties can set a policy on a smartphone at any moment or just when the phone is within a particular context, e.g. within a building, or a plane.
Citazioni totali	Citato da 315

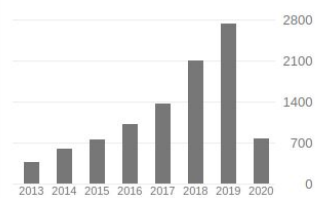


Articoli in Scholar: Crepe: Context-related policy enforcement for android
M Conti, VTN Nguyen, B Crispo - International Conference on Information Security, 2010
Citato da 315 Articoli correlati Tutte e 15 le versioni

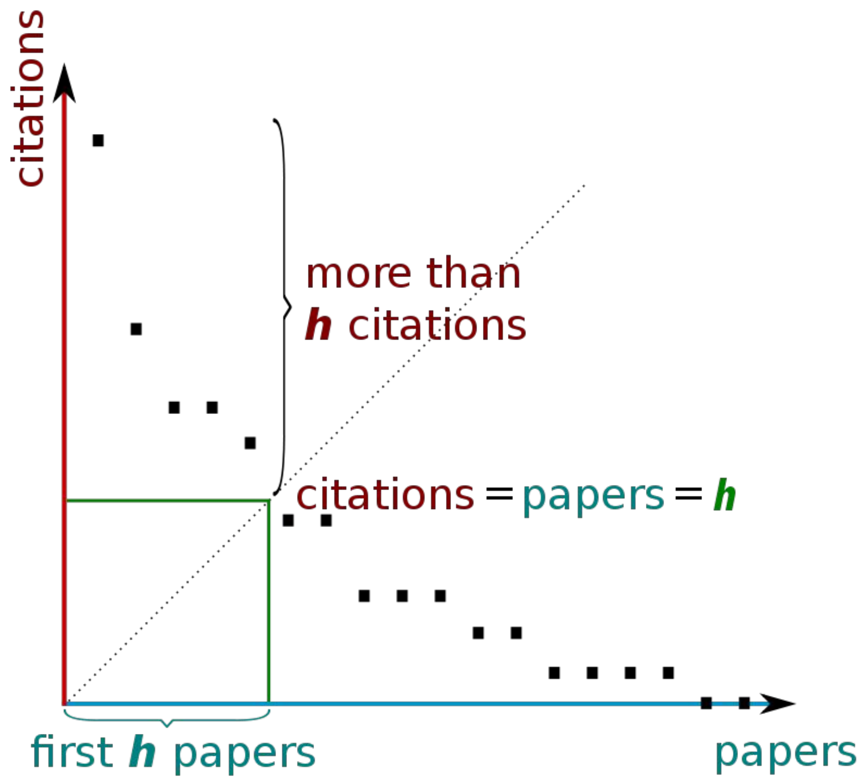
Assessing a Researcher (even more complex): Cit., H-index and more...

Citata da VISUALIZZA TUTTO

	Tutte	Dal 2015
Citazioni	11154	8813
Indice H	51	47
i10-index	179	156



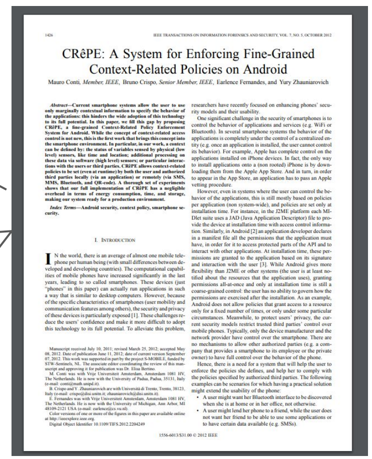
Reading Papers... where to go?



Citation Graph

References

1. Android-Developers. Android dev phones, http://developer.android.com/guide/developing/device.html (retrieved June 30, 2010)
2. Android Project. Android, http://www.android.com (retrieved June 30, 2010)
3. Andromaly Project. Andromaly anomaly detection in android platform. http://andromaly.wordpress.com/ (retrieved June 30, 2010)
4. Becher, M., Hund, R.: Kernel-level interception and applications on windows mobile devices. Technical Report TR-2008-003, Department for Mathematics and Computer Science, University of Mannheim, Germany (2008)
   Google Scholar
5. Steel, R.C., Nagappan, R.: Core Security Patterns: Best Practices and Stategies for J2EE, Web Services, and Identity Management. Prentice Hall, Englewood Cliffs (2005)
   Google Scholar
6. Damiani, M.L., Bertino, E., Catania, B., Perlasca, P.: Geo-rbac: A spatially aware rbac. ACM Trans. Inf. Syst. Secur. 10(1) (2007)
   Google Scholar
7. Dashti, M.T., Nair, S.K., Jonker, H.: Nuovo DRM paradiso: Designing a secure, verified, fair exchange drm scheme. Fundam. Inf. 89(4), 393–417 (2009)
   MathSciNet zbMATH Google Scholar
8. Desmet, L., Joosen, W., Massacci, F., Naliuka, K., Philippaerts, P., Piessens, F., Vanoverberghe, D.: A flexible security architecture to support third-party applications on mobile devices. In: CSAW 2007, pp. 19–28 (2007)
   Google Scholar
9. Djuknic, G.M., Richton, R.E.: Geolocation and assisted gps. Computer 34(2), 123–125 (2001)
   CrossRef Google Scholar
10. Enck, W., Ongtang, M., McDaniel, P.: On lightweight mobile phone application certification. In: CCS 2009, pp. 235–245 (2009)
    Google Scholar
11. Enck, W., Ongtang, M., McDaniel, P.: Understanding android security. IEEE Security and Privacy 7(1), 50–57 (2009)
    CrossRef Google Scholar



Crepe: Context-related policy enforcement for android

Cerca tra gli articoli con citazioni

TaintDroid: an information-flow tracking system for realtime privacy monitoring on smartphones
W Enck, P Gilbert, S Han, V Tendulkar - ACM Transactions on …, 2014 - dl.acm.org
Today's smartphone operating systems frequently fail to provide users with visibility into how third-party applications collect and share their private data. We address these shortcomings with TaintDroid, an efficient, system-wide dynamic taint tracking and analysis system …
Citato da 3672 Articoli correlati Tutte e 75 le versioni

Aurasium: Practical policy enforcement for android applications
R Xu, H Saidi, R Anderson - Presented as part of the 21st {USENIX} …, 2012 - usenix.org
The increasing popularity of Google's mobile platform Android makes it the prime target of the latest surge in mobile malware. Most research on enhancing the platform's security and privacy controls requires extensive modification to the operating system, which has …
Citato da 508 Articoli correlati Tutte e 11 le versioni

[PDF] Towards Taming Privilege-Escalation Attacks on Android.
S Bugiel, L Davi, A Dmitrienko, T Fischer, AR Sadeghi - NDSS, 2012 - Citeseer
Android's security framework has been an appealing subject of research in the last few years. Android has been shown to be vulnerable to application-level privilege escalation attacks, such as confused deputy attacks, and more recently, attacks by colluding …
Citato da 460 Articoli correlati Tutte e 12 le versioni

[PDF] Quire: Lightweight provenance for smart phone operating systems
M Dietz, S Shekhar, Y Pisetsky, A Shu - USENIX security …, 2011 - usenix.org
Smartphone apps are often granted to privilege to run with access to the network and sensitive local resources. This makes it difficult for remote endpoints to place any trust in the provenance of network connections originating from a user's device. Even on the phone …
Citato da 455 Articoli correlati Tutte e 19 le versioni

[PDF] Xmandroid: A new android evolution to mitigate privilege escalation attacks
S Bugiel, L Davi, A Dmitrienko - … Report TR-2011 …, 2011 - download.hrz.tu-darmstadt.de
Google Android has become a popular mobile operating system which is increasingly deployed by mobile device manufactures for various platforms. Recent attacks show that Android's permission framework is vulnerable to applicationlevel privilege escalation …
Citato da 330 Articoli correlati Tutte e 7 le versioni