

AP Cyber Security

DIITET

AP Cyber Security

1. Cyber-Physical Systems (CPS) Security
2. Network Security
3. Intrusion Detection and Protection
4. Privacy
5. Information Sharing and Analytics
6. Cyber-intelligence on Social Media
7. Secure Software Engineering
8. Access Control and Trust Management
9. Cryptography
10. Cloud Security
11. Cyber insurance
12. Conclusions

Cyber-Physical Systems (CPS) Security

contact: Luca Durante - IEIIT

CPSs have functional and performance requirements (real-time scheduling and communications) not allowing the automatic enforcement of high level access control policies , thus a system level approach is needed:

Who can do what on what is computed starting from the formal model of the real system and from the security policies. The two sets of triples are compared.

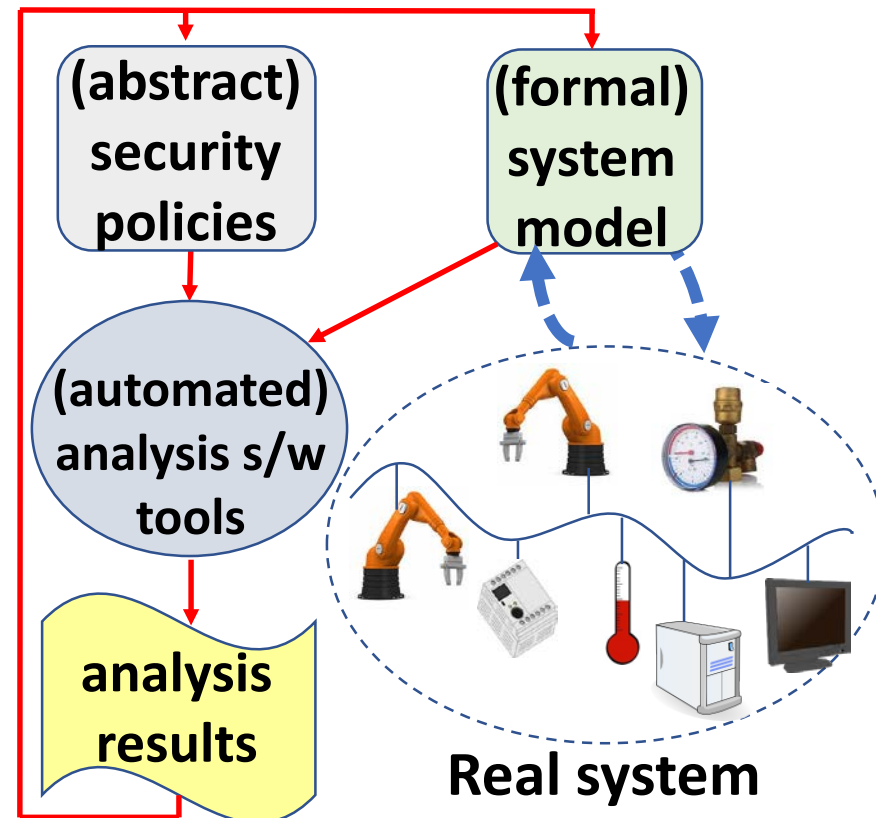
The system model and/or the set of policies are updated until the comparison of the sets of triples is satisfactory.

The real system is updated accordingly to the changes of the system model.

Further activities:

Modelling industrial firewall performance

Leveraging new network management paradigms as SDN and NFV to implement security mechanisms



Network Security

contact: Maurizio Aiello – IEIIT

Slow DoS Attacks Development

Focus

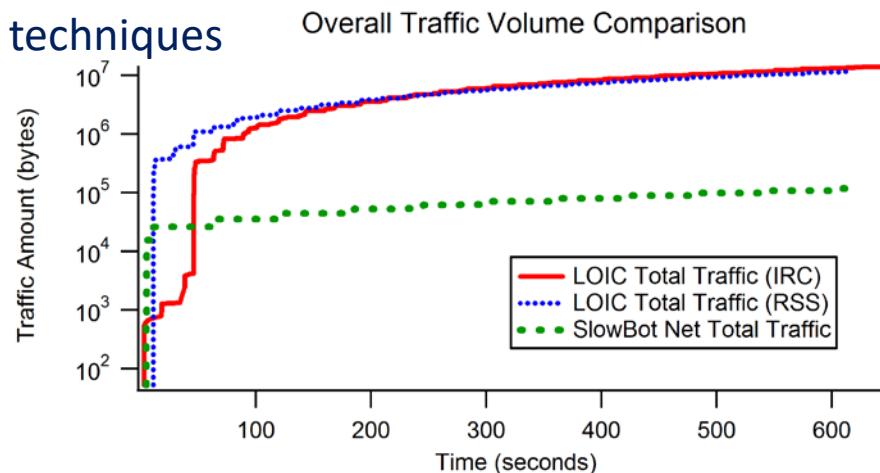
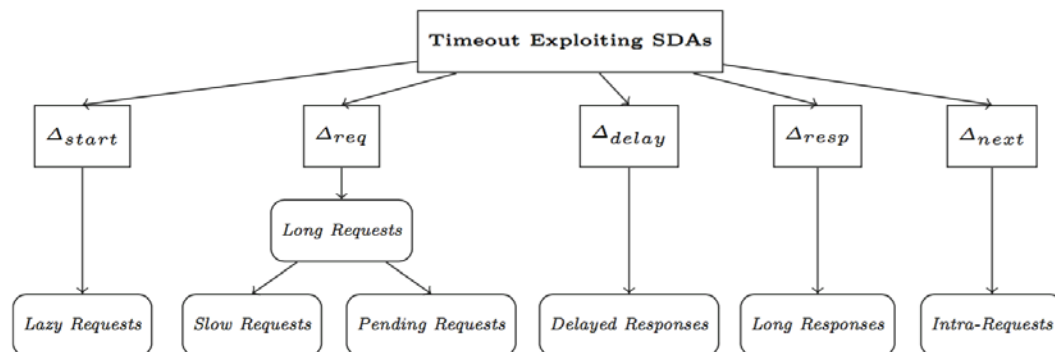
- Innovative cyber-attacks
- Threats apparently behaving legitimately
- Emerging scenarios

Activities

- Vulnerability assessment and penetration testing
- Deep study of emerging Denial of Service attacks
- Deep study of Internet of Things devices and networks
- Deep study of covert channels and data exfiltration techniques
- Deep study of darknets and Tor environments

Results

- Development of innovative offensive tools
- Pioneers of the “slow” DoS context



Network Security

contact: Maurizio Aiello – IEIIT

Innovative protection methodologies

Focus

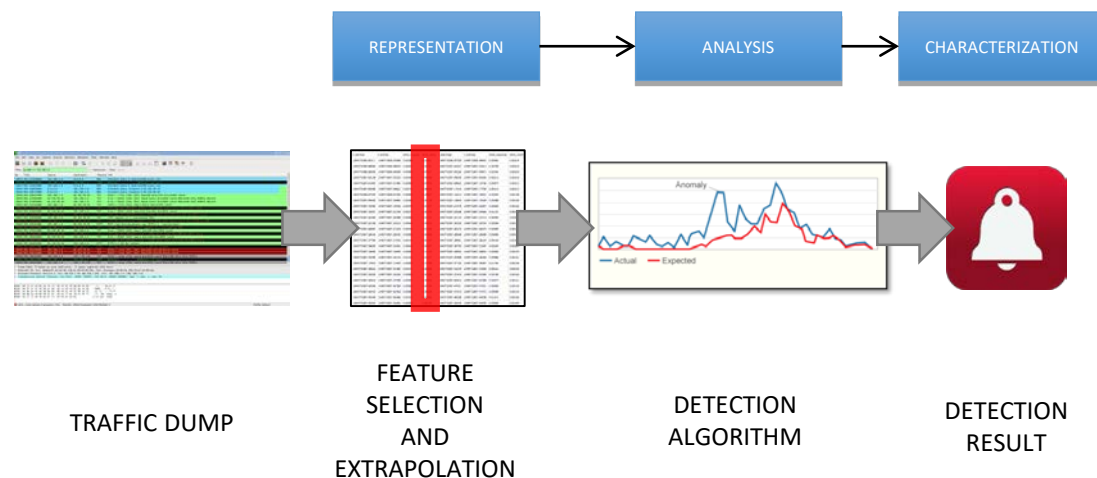
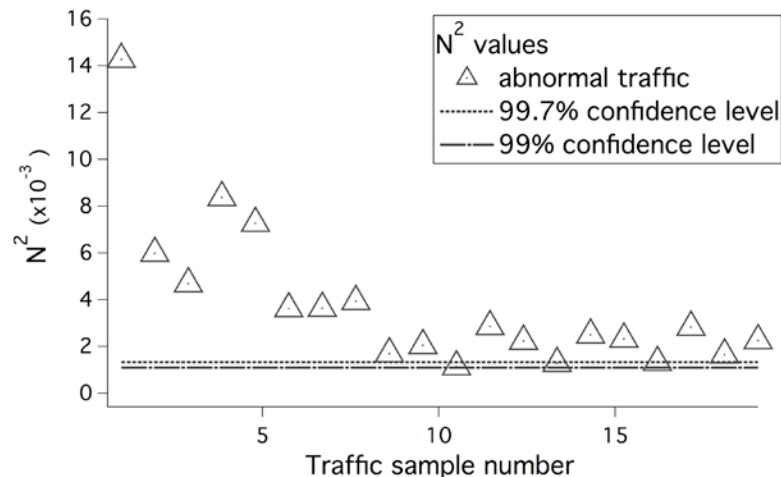
- Last generation threats
- Threats difficult to counter
- Innovative cyber-attacks internally implemented

Activities

- Design and development of Intrusion Detection Systems
- Adoption of statistics, machine learning, neural networks methods

Results

- First, identification of innovative threats
- Then, efficient threats protection (almost in real-time)



Network Security

contact: Flavio Lombardi - IAC

TOR Web

The exploration and analysis has flourished in the recent past on Web graphs, but not on the TOR network.

Little information is available about the topology of the TOR WEB graph and its relation with content semantics.

IAC, as part of the EU-ISEC IANCIS project has contributed to improve knowledge on TOR Dark Web, providing:

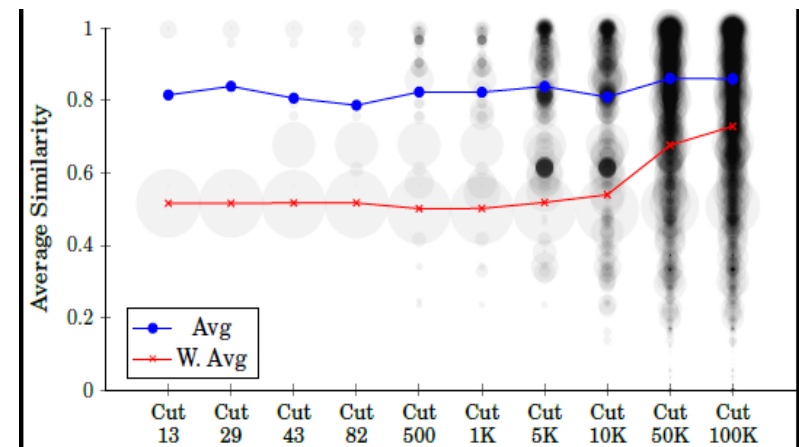
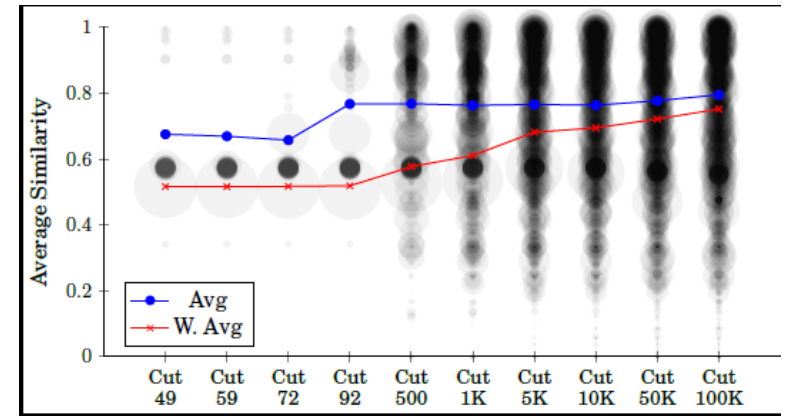
- a study on automatic TOR exploration;
- novel representative metrics for evaluating TOR data;
- a novel in-depth analysis of the hidden services graph correlating hidden services' semantics and topology.

A better knowledge of the TOR topology and semantics, allowing for more effective Police investigations

Challenges include:

- dealing with an ever changing TOR graph and content;
- analyzing content in many different languages and slangs;
- exploring a larger portion of the network;
- leveraging additional analysis techniques.

We are extending and improving results based on past achievements and new tools.



Intrusion Detection and Protection

contact: Luca Caviglione- IMATI

Intrusion Detection and Protection of mobile devices deals with the investigation of security hazards targeting modern mobile devices, including smartphones, wireless sensors, as well as IoT nodes.

In particular, three main themes have been investigated:

- **Steganographic Channels:** methods and techniques to create covert channels for the exfiltration of data or to allow malware to behave stealthy.
- **Energy-aware Security:** understand the energetic footprint of security to perform optimizations and to develop new detection techniques independent of the attack or the used hardware.
- **Application and OS Security:** offline and runtime check of security performances of applications, the guest OS or virtualized resources.

Privacy

contact: Anna Monreale - ISTI



- **Privacy-by-design for big data publishing**

- designing of data transformations following the privacy-by-design principle for making data private while preserving data quality

- **Privacy-by-design for big data analytics and mining**

- designing data mining and big data analytics approaches which by-design guarantee privacy protection

- **Privacy-by-design for data mining outsourcing**

- designing privacy-by-design technologies that guarantee corporate privacy protection while outsourcing data mining tasks, i.e. the third party cannot infer sensitive information both from data and from extracted knowledge

- **Privacy enhancing technologies**

- development of technologies for privacy protection: from data usage control to privacy-aware secure multi-party computation

- **Privacy engineering**

- studying methodologies and tools for software engineering specific for privacy protection

- **Privacy risk assessment**

- studying methodologies for assessing the privacy risk level by considering different and realistic attack models that are particularly suitable for specific type of data

SoBigData Research Infrastructure



The Social Mining & Big Data Ecosystem: a research infrastructure (RI) for ethic-sensitive scientific discoveries and advanced applications of social data mining to the various dimensions of social life, as recorded by “big data”.

The **research community** will use the SoBigData RI facilities as a “secure digital wind-tunnel” for large-scale social data analysis and simulation experiments. SoBigData will serve the wide cross-disciplinary community of data scientists



Type of action: Research and Innovation action

Call: H2020-INFRAIA-2014-2015 (Research Infrastructure - Open Innovation and Open Science)

Grant n. 654024



PRO-RES

PROMoting integrity in the use of RESEARCH results

The objective of PRO-RES is to address the difficulties in delivering **responsible research and Innovation** (RRI) by producing a supported guidance framework that is comprehensive, flexible and durable, covers the spectrum of non-medical sciences.

It will balance the variety of political, institutional and professional constraints providing **practical solutions** for all stakeholders complying with the highest standards of research ethics and integrity.

List of participants

#	Participant Legal Name	Country
1	FONDATION EUROPEENNE DE LA SCIENCE	France
2	Academy of Social Sciences	United Kingdom
3	NATIONAL TECHNICAL UNIVERSITY OF ATHENS - NTUA	Greece
4	TARTU ULIKOOL	Estonia
5	Hrvatsko katoličko sveučilište	Croatia
6	INNOVATION IN RESEARCH & ENGINEERING SOLUTIONS	Belgium
7	European Alliance for Social Science and Humanities	France
8	INSTITUT DES HAUTES ETUDES ECONOMIQUES ET COMMERCIALES ASSOCIATION	France
9	CONOSCENZA E INNOVAZIONE SOCIETA A RESPONSABILITA LIMITATA SEMPLIFICATA	Italy
10	STERNBES 21 GMBH	Germany
11	DUBLIN CITY UNIVERSITY	Ireland
12	HELLENIC CENTRE FOR MARINE RESEARCH	Greece
13	CONSIGLIO NAZIONALE DELLE RICERCHE	Italy
14	EUROPEAN POLICY CENTRE	Belgium

Type of action: CSA (Coordinated and Support Action)
Call: H2020-SwafS-2016-17 (Science with and for Society)
Grant n. 788352

Information Sharing and Analytics

contact: Giuseppe Manco - ICAR

Objective

The design of machine learning, artificial intelligence and data analytics techniques able to make sense of large amounts of data

Approach

Study of **mathematical models** that allow to analyse, understand, and predict entity behavior within complex environments

Scalable data processing solutions able to deal with the *volume, variety* and *velocity* of complex data

Challenges

Behavioral profiling to detect malicious activities and devise models of trust

Information handling based on **theoretically guaranteed models of privacy**

Social sensing for prediction of sensitive information diffusion flows and secure information sharing

Attack prevention/response based on machine learning and AI to improve reaction to incidents

Impact

Automatically handle and **make sense** of complex data flows

Detect/Prevent attacks

Reduce/Mitigate/React to risks and effects of attacks

Safety, Security, Confidentiality

CyberSecurity District



A SERVICE CENTER FOR

- INDUSTRIAL RESEARCH
- DEVELOPMENT OF INDUSTRIAL PROTOTYPES
- TRAINING SECURITY SPECIALISTS



End-User Protection

An innovative Model for protection of the end-point

Securing internet services

Analysis of behavioral Risks and vulnerabilities

Securing mobile devices

Protection of Payment Systems

Protection of digital payment system

Process innovation

Deployment of new secure services

Analysis of System-level risks

Secure Dematerialization

Lifecycle of a digital document

Risk models and profiles

Models for access governance, security governance and trusted identity

Rights management

CYBERSECURITY
TRAINING MASTER PROGRAM



CyberSecurity District

Cosenza

- 30M€ investment
 - Initiative of the Italian Ministry for University and Research (MIUR) in the framework of National Operative Program – Research and Competitiveness 2007-2013.
- 200+ professionals involved for 4+ years
- Over 30 organizations including SMBE, LE, Research centers, Universities, Consulting agencies
- - Strategic in the core business of LE
 - Poste Italiane
 - NTT

CyberSecurity District Highlights

Attack Prevention/Response



Information sources: Web (Google Hacking) and Deep Web (Tor Network)

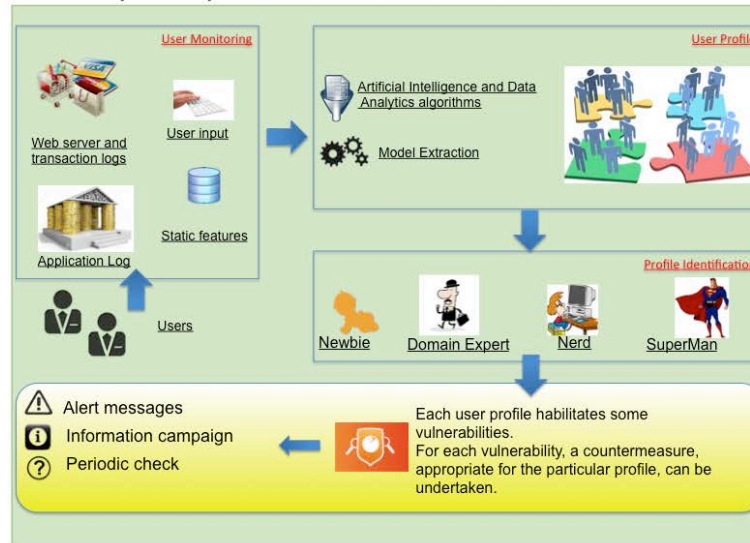
Data Gathering, Filtering, Cleaning and Manipulation

Ranking ensemble-based module and Deep Learning

Discovery of Alternative App Stores

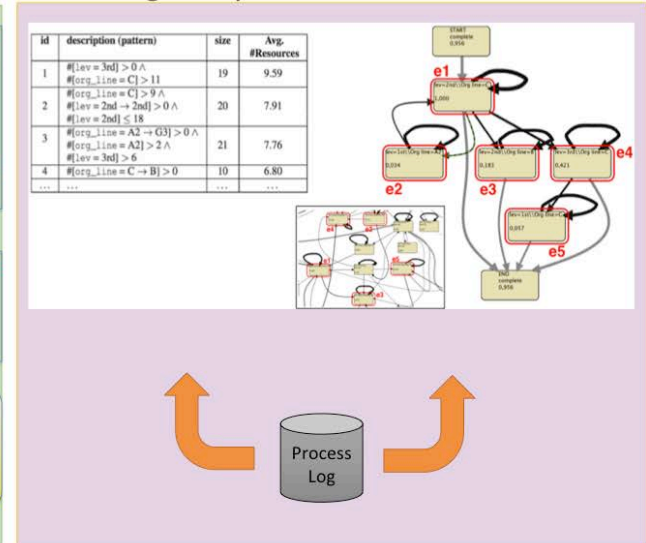
Reporting and monitoring unauthorized apps

Security Analytics



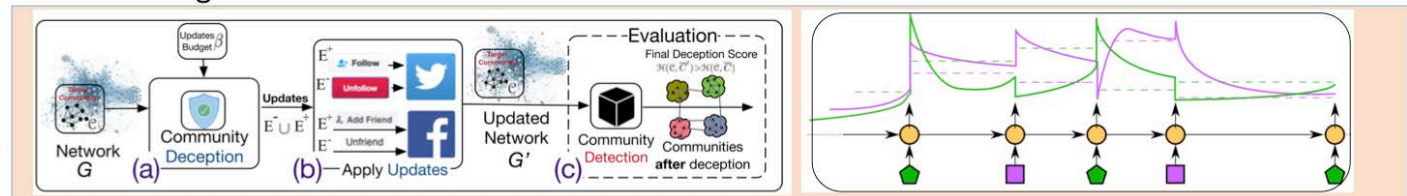
Event Log Analysis

id	description (pattern)	size	Avg. #Resources
1	#[lev = 3rd] > 0 \wedge #[org_line = C] > 11	19	9.59
2	#[org_line = C] > 9 \wedge #[lev = 2nd \rightarrow 2nd] > 0 \wedge #[lev = 2nd] \leq 18	20	7.91
3	#[org_line = A2 \rightarrow G3] > 0 \wedge #[org_line = A2] > 2 \wedge #[lev = 3rd] > 6	21	7.76
4	#[org_line = C \rightarrow B] > 0	10	6.80
...



Process Log

Social Sensing



Cyber-intelligence on Social Media

contact: Maurizio Tesconi - IIT

- **social media data gathering** for intelligence purposes, using both APIs and scraping techniques
- social media data analysis (using big data technologies):
 - **hate speech** detection, performing NLP analysis on user posts and comments
 - modeling behaviour in **user interactions** both in space and time
 - **malicious account** behaviour detection analysing user behaviour, relations and posted content
 - **face similarity** recognition on multimedia content
 - **health ranking** of online social ecosystems
- **technology transfer** to LEAs, also through a joint laboratory with Italian Police (CRAIM) and a collaboration with Italian Presidency of the Council of Ministers





Secure Software Assurance

contact: Eda Marchetti - ISTI

Secure Software aims at assuring integrated approaches to face continuous evolution and criticalities rising during all the development cycle of software-intensive systems

Activities:

- Secure requirements and quality attributes collection;
- Software or system construction and evaluation;
- On-line monitoring, control and assessment of specific security properties and metrics;
- integration of security management and control facilities into all the software process;
- Verification and Validation of access and usage control systems;
- Development of model-driven approaches for specification and evaluation.

Access Control and Trust Management

contact: Fabio Martinelli - IIT

- **Access and usage control:** This theme is devoted to the study and development of access and usage control languages and mechanisms for data, services, network and IoT. It also considers privacy preserving models and protocols.
 - *Authentication protocols.* This sub theme involves the design and analysis of authentication protocols. It also includes the automated synthesis of security protocols.
 - *Languages and mechanism for authorization.* This sub theme develops the languages suitable for expressing authorization and the corresponding evaluation mechanisms.
- **Trust management:** The theme is devoted to model and analyse trust relationships in open systems (and social networks).
 - *Models and languages for trust management.* This sub theme entails the study, definition and analysis of trust models and languages. It includes both qualitative and quantitative aspects of trust.
 - *Trust management services.* This sub theme is devoted to trust management service development and implementation useful also in the realm of access control.

IIT CNR Cyber Security Lab

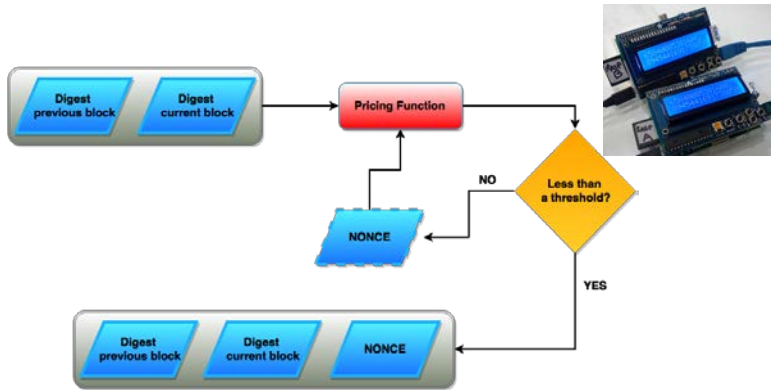
- Lab funded with 1.5ME in 4 years
- All the IIT CNR research groups involved
- ***Cyber Risk, Cyber Protection, Cyber Crime, Cyber Intelligence and Cyber Attacks***
- ***We set up the first master in Tuscany in Cybersecurity and one of the first in Italy***
 - ***25 participants (40 requests)***
 - ***Working on the Tuscan CyberSecurity Competence centre, National one and EU one....***

Comitato Nazionale per La Ricerca in Cyber Security

- Signed between CNR and CINI at CNR premises (currently it has also CNIT).
 - Under the auspices of the Department of Information Security
 - Members of the committee:
 - CNR: Marco Conti, Fabio Martinelli
 - CINI: Roberto Baldoni, Paolo Prinetto

Cryptography

Contact: Giovanni Schmid - ICAR



IoT: Cryptographic primitives (A-codes) for securing LPAN's PHY layer [1, 2]; Mining-free proofs for sustainable, non speculative blockchain systems [3]

[1] Schmid G., Rossi F. A-Code: A New Crypto Primitive for Securing Wireless Sensor Networks, First International Workshop on Trust Management in P2P Systems (2010)

[2] Schmid G., Rossi F. Secure Ad-hoc Routing through A-codes, First International Conference on Pervasive and Embedded Computing and Communication Systems (2011)

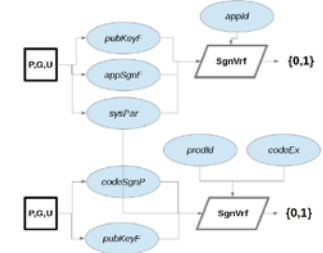
[3] Romano D., Schmid G. - Beyond Bitcoin: A Critical Look at Blockchain-Based Systems, Cryptography 2017, 1, 15; doi:10.3390/cryptography1020015

Anti-counterfeiting: unforgeable analog-digital tags (PACs) which use ID-based crypto in order to face the “Sounding Italy” threat and other frauds against trademarks and good's authenticity [4]

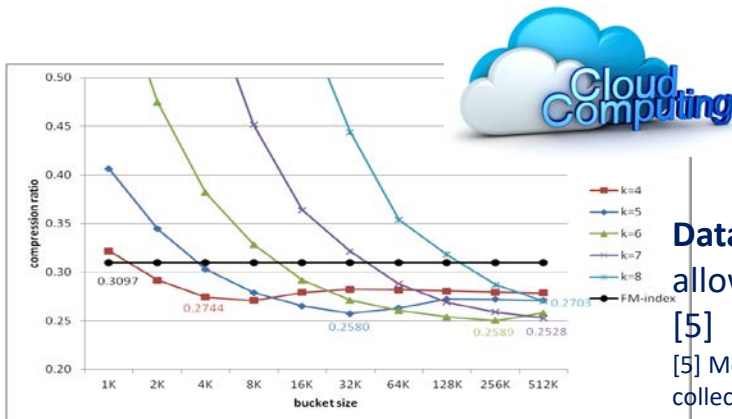
[4] Schmid G., Procedimento anticontraffazione su base collaborativa, Italian Patent n. 0001424336 (2014)



VERIFICA APP:



P=Produttore, G=Gestore, U=Utilizzatore, 0=firma valida, 1=firma invalida Dati pubblici



Database-as-a-Service: encrypted full text in minute space index (E2FM) allowing fast searches on compressed and encrypted data sets and databases [5]

[5] Montecullo F., Schmid G., Tagliaferri R. - E2FM: an encrypted and compressed full-text index for collections of genomic sequences, Bioinformatics, 33(18), 2017, 2808–2817 doi: 10.1093/bioinformatics/btx313

Cryptography

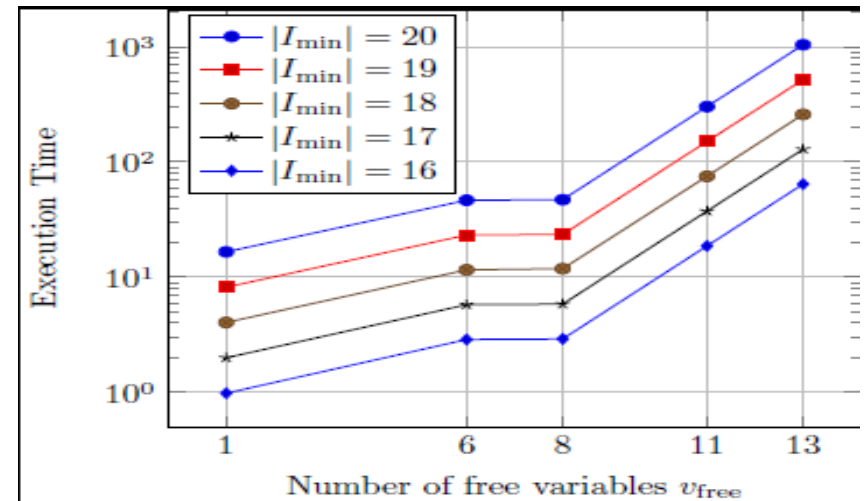
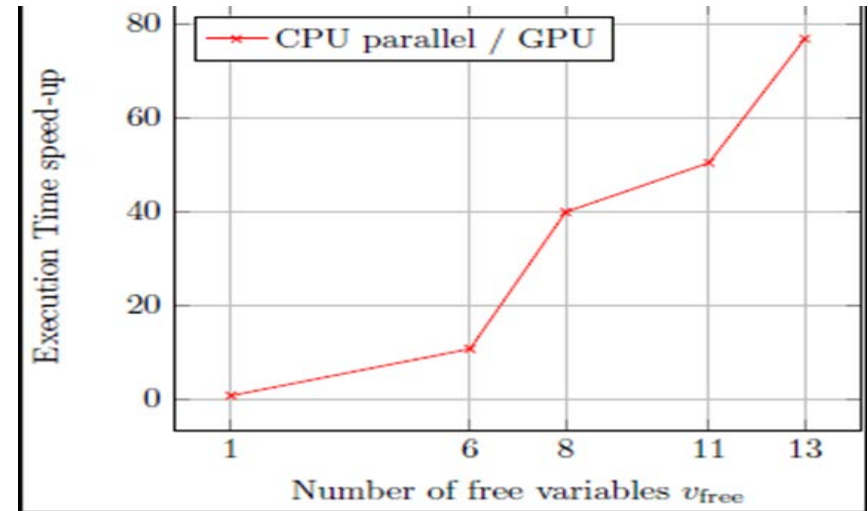
contact: Massimo Bernaschi - IAC

Albeit interesting, the CUBE attack introduced in 2009 by Dinur and Shamir has no implementation capable of breaking any real-world strong cipher. Indeed some success had been obtained on a reduced version of the Trivium cipher (Trivium 735)

IAC, in collaboration with Maths and Physics department of Roma Tre University, managed to create a smart effective general framework implementing a parallel GPU-based version of the attack. Obtained results allowed to improve the state of the art managing to attack Trivium 768. Other brute force and dictionary based attacks have been successfully devised and implemented on GPUs.

Obtained results shed a new light on the CUBE attack effectiveness. Further, other successful brute force dictionary based attacks we implemented on GPUs are relevant in the area.

CUBE-like approaches will need better fine-tuning, considering optimizations based on new hardware capabilities and novel approaches to select better space exploration bit candidates. Based on the relevant obtained achievements, further improvements in quality and quantity of the results are possible.



Cloud Security

contact: Paolo Mori - IIT



Study, design, and implementation of novel and enhanced techniques for protecting services, resources and data that shared on the Cloud, as well as the execution of business or research processes.

Identity and Authentication Management

- Design, and implementation of systems for managing identity and authentication in the Cloud environment, with particular reference to the federation of Cloud scenario

Access and Usage Control

- Design, and implementation of enhanced system for controlling the access to and the usage of services and resources provided on the Cloud, as well as the data that are share through the Cloud

Cloud Platforms for the Public Administrations

- Analysis of the requirements and design of solution for adopting the Cloud in the Public Administration processes, with particular reference to the Electronic Health Record

Future Developments

- The research activity also takes into account the security issues coming from the integration of Cloud with the Internet of Things and the evolution to Edge computing

Cyber Insurance

contact: Alba Orlando - IAC

Cyber insurance is a rapidly developing area which draws more and more attention of practitioners and researchers.

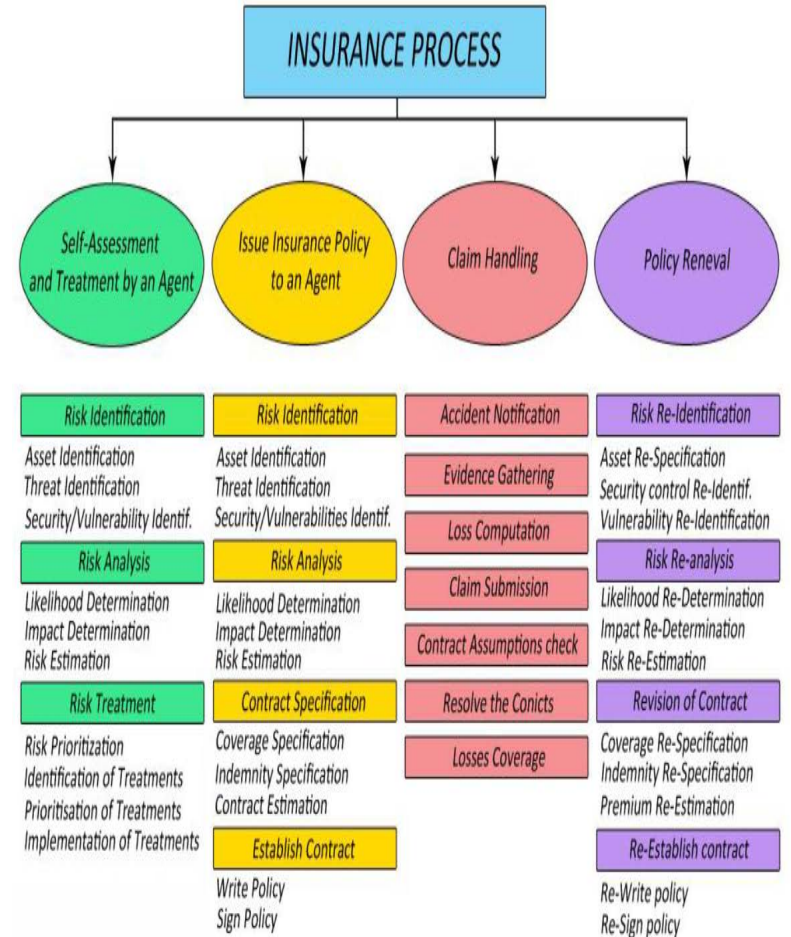
Insurance, an alternative way to deal with residual risks, was only recently applied to the cyber world.

The research activity on this new topic began by a deep analysis of the basic knowledge about cyber insurance from both market and scientific perspectives, summarized in a survey.

We are now focusing on the analysis of cyber insurance as an incentive to invest in security and on new models for pricing and risk measures assessment.

The future research activity will concern the other areas related to cyber insurance which need more attention by the scientific community and practitioners:

- Dynamic cyber-insurance;
- Deal with information asymmetry;
- Methods to define security level and effect of security controls;
- New approaches to damage estimation;
- New theoretical approaches and practical studies of interdependency of security;
- Evaluation of real impact because of correlated risks;
- New liability models for improving overall security.



Conclusions

The current research activities and proposed approaches are showing good results from the theoretical and practical point of view, with successful publications and collaborations with national and international industrial partners, and public bodies. On the one side this shows that the right way has been taken, but also that more resources and effort are needed to provide adequate solutions in a world where cybersecurity is perceived as a major challenge by both citizens and institutions, and rightly so.