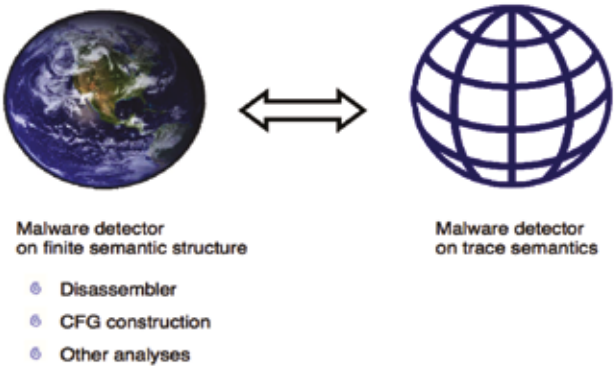

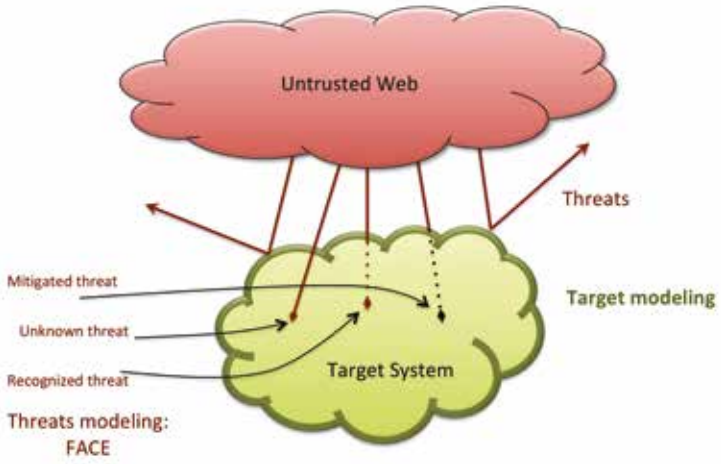

SOFTWARE ENGINEERING AND SECURITY

DESCRIPTION

The Department's research in this area covers a rich variety of topics, including: automated static analysis, cryptography, formal language definitions, formal methods, formal security models, formal software verification, logic and verification, malware and its mitigation, massively parallel systems, network security, parallel programming languages, security protocols, security services, semantics, social aspects of security and privacy, software and application security, software architectures, software functional properties, software reverse engineering, software system models, software verification and validation, system description languages, trust frameworks, Unified Modeling Language (UML), web protocol security.

LABORATORIES

QUILAB: Quantum Informatics Laboratory
REGIS: Research Group in Information Security
SPY: Static Analysis by Abstract Interpretation

PROJECTS (2012-2016)

- **FACE**: Formal Avenue for Chasing malwarE. A FIRB 2013 project aiming at the analysis and detection of modern malware with particular interest in Andorid malware applications. Modern malware attempt to evade both dynamic and static detection by means of anti-debugging, obfuscation and metamorphism techniques. FACE proposes to combine static and dynamic analysis into an hybrid approach in order to better understand and therefore detect modern malware.
- **TRENDS**: Technologies and Resources for Exploiting interNet Documents and Social media, joint project with Techne Media Agency. Nowadays, people make more and more often digital actions related to various aspects of their life. The huge amount of data generated by users is the basis of a behavioral mutation that is not yet well defined, but is a sign of an almost anthropological change in people. The project investigates these aspects, using specialized tools, designed specifically to intercept the communications into the network, and with new ways of understanding the digital lexicon.
- **ABSCRIPT:** Abstract interpretation based analysis of Scripting Languages, joint project with Maxfone. The project is intended to the design and implementation of an static analyzer for PHP based on abstract interpretation and insensible on dynamic code mutations as caused by reflection. Modeling reflection in dynamic languages is a particularly hard problem because this feature breaks on of the fundamental bases of static analysis, which is the static structure of the program to be analyzed.

SELECTED PUBLICATIONS (2012-2016)

- P. Adão, P. Mateus, L. Viganò. Protocol insecurity with a finite number of sessions and a cost-sensitive guessing intruder is NP-complete. Theoretical Computer Science. Vol. 538, pp 2-15, 2014.
- M. Dalla Preda. The Grand Challenge in Metamorphic Analysis. 6th International Conference on Information Systems, Technology and Management, ICISTM. Vol. 285, pp. 439-444, 2012.
- M. Dalla Preda, I. Mastroeni, R. Giacobazzi. Formal Framework for property-driven obfuscation. 19th International Symposium of Fundamentals of Computer Theory FCT, pp. 133-144, 2013.
- D. Macedonio, M. Merro. A Semantic Analysis of Key Management Protocols for Wireless Sensor Networks. Science of Computer Programming, Vol. 81, pp. 53-78, 2014.
- M. Dalla Preda e F. Maggi. Testing Android Malware Detectors Against Code Obfuscation: A Systematization of Knowledge and Unified Methodology. Journal of Computer Virology and Hacking Techniques 2016, pp 1 - 24.
- R. Sartea, M. Dalla Preda, A. Farinelli, R. Giacobazzi e I. Mastroeni. Active Android Malware Analysis: An approach based on Stochastic Games. 6th ACM Workshop on Software Security, Protection and Reverse Engineering SSPREW@ACSAC 2016, pp 5:1 - 5:10.
- R. Giacobazzi, I. Mastroeni e M. Dalla Preda. Maximal Incompleteness as Obfuscation Potency. Formal Aspects of Computing Journal FACJ 2017, Vol. 29, Num. 1, pp 3 - 31.
- M. Dalla Preda, R. Giacobazzi, S. Debray. Unveiling Metamorphism by Abstract Interpretation of Code Properties. Theoretical Computer Science (TCS), Vol 577, pp 71 - 97, 2015.
- Mastroeni and D. Zanardini. Abstract Program Slicing: an Abstract Interpretation-based approach to Program Slicing. In ACM Transactions on Computational Logic (TOCL). 18(1) pages 7:1-7:58. ACM 2017.
- Michael D. Ernst, Alberto Lovato, Damiano Macedonio, Fausto Spoto, Javier Thaine: Locking discipline inference and checking. ICSE 2016: 1133-1144.
- M.D. Ernst, D. Macedonio, M. Merro and F. Spoto. Semantics for locking specifications. In Proc. 8th NASA Formal Methods Symposium. LNCS, vol 9690, pp. 335-372, Springer 2016.

PEOPLE (2017)

Matteo Cristani
Assistant Professor
matteo.cristani@univr.it
+39 045 802 7983

Mila Dalla Preda
Assistant Professor
mila.dallapreda@univr.ti
+390 45 802 7045

Alessandra Di Pierro
Associate Professor
alessandra.dipierro@univr.it
+39 045 802 7971

Roberto Giacobazzi
Full Professor
roberto.giacobazzi@univr.it
+39 045 802 7995

Isabella Mastroeni
Associate Professor
isabella.mastroeni@univr.it
+39 045 802 7089

Massimo Merro
Associate Professor
massimo.merro@univr.it
+39 045 802 7992

Roberto Segala
Full Professor
roberto.segala@univr.it
+39 045 802 7997

Nicola Fausto Spoto
Associate Professor
fausto.spoto@univr.it
+39 045 802 7940

Luca Viganò
Associate Professor
luca.vigano@univr.it
+39 045 802 7070