SAPIENZA
UNIVERSITÀ DI ROMA

Corso di Laurea Magistrale in Cybersecurity
Facoltà di Ingegneria dell'Informazione, Informatica e Statistica

Honours Programme for the Master of Science in Cybersecurity - LM-66

Topics for the Honours Programme to be chosen for the call for applications relating to the Academic Year 2018-2019

Docente: Prof. Daniele Venturi

====== TOPIC 1: Non-malleable codes ======

Description: Non-malleable codes encode a given message in such a way that mauling attempts with a codeword (within a certain class of allowed tampering functions) have the effect that decoding a modified codeword yields either the original message or a completely unrelated value. Such codes are interesting on their own right, but also have several applications to cryptography.

During this Honours Programme the student will try to tackle open research questions in this context, e.g. studying the relationship between different flavors of non-malleable codes, constructing new codes for larger tampering families, and exploring new cryptographic applications.

References:
http://eprint.iacr.org/2014/173
http://eprint.iacr.org/2013/702

====== TOPIC 2: Leakage and Tamper Resilient Cryptography ======

Description: The security of modern cryptographic algorithms is typically analyzed under the assumption that an adversary has neither partial knowledge nor she can modify the underlying secrets. Unfortunately, several realistic attacks (so called leakage and tampering attacks) do not obey this assumption, which creates a gap between theoretical cryptography and the real word.

During this Honours Programme, the student will design new cryptographic primitives with provable guarantees against leakage and tampering attacks.

References:
http://eprint.iacr.org/2015/517
http://eprint.iacr.org/2016/529

Docente: Prof. Leonardo Querzoni

====== TOPIC 1: Binary similarity applied to malware analysis ======

Description: The binary similarity problem consists in determining if two functions are similar by only considering their compiled form. Advanced techniques for binary similarity recently gained momentum as they can be applied in several fields, such as copyright disputes, malware analysis, vulnerability detection, etc., and thus have an immediate practical impact. Current solutions compare functions by first transforming their binary code in multi-dimensional vector representations (embeddings), and then comparing vectors through simple and efficient geometric operations.

Didactic Office
Via Salaria, 113 – 00198 Rome
Room 329 – Tel. 064991 8440-8537
Email: cybersecurity_info@uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

Corso di Laurea Magistrale in Cybersecurity
Facoltà di Ingegneria dell'Informazione, Informatica e Statistica

During this Honours Programme the student will experiment the applicability of state-of-the-art binary similarity solutions to the problem of malware homophily analysis to identify automatically how malware evolves in a familty.

References:
https://arxiv.org/abs/1808.04706
https://arxiv.org/abs/1811.05296

====== TOPIC 2: The (In-)Security of the Internet of Things ======

Description: The impressive growth of the IoT we witnessed in the recent years, came together with a surge in cyber attacks that target such systems. Recent studies reported that cyber attacks targeting IoT systems show peculiar behaviors that hamper the applicability of standard security approaches. Is therefore crucial to understand such new behaviors in order to design more appropriate countermeasures that will pave the way for new responsible IoT systems.

During this Honours Programme the student will apply techniques from different computer science filelds to analyze the behaviour of current live IoT attacks. This knowledge will help the student to identify effective strategies for attack detection.

References:
https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

Docente: Prof. Luigi V. Mancini

====== TOPIC 1: Automatic prediction and remediation of cyberattacks ======

Description: Study of active defense systems (annoyance, attribution and attack) to ensure the security of information systems. Classic security systems, such as firewalls, antivirus and intrusion detection/prevention systems, are ineffective against the most sophisticated attacks. Active defence is based on the assumption that an attacker already has access to parts of the system, and proposes security solutions aimed at slowing down progress and, where possible to sanitize the system from the malware used. A related need for efenders is not only to detect malicious activity as it happens, but also to predict the specific steps that will be taken by an adversary when performing an attack (predicting malicious events and the specific steps that an attacker would undertake).
During this Honours Programme the student will try to tackle open research questions in this context.

References:
https://dl.acm.org/citation.cfm?id=2994481
http://www0.cs.ucl.ac.uk/staff/G.Stringhini/papers/tiresias-ccs2018.pdf

====== TOPIC 2: Blockchain Technologies ======

Description: Study the structure of blockchain and its applications, such as Virtual currencies (Bitcoin and derivatives) and smart contracts (e.g., Ethereum). Analysis of possible future extensions and new applications that can benefit from the use of blockchain.

References:
- Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. *(2008)*
- Redactable Blockchain -- or -- Rewriting History in Bitcoin and Friends. Redactable Blockchain -- or -- Rewriting History in Bitcoin and Friends. *2017 IEEE European Symposium on Security and Privacy (EuroS&P 2017)*

Didactic Office
Via Salaria, 113 – 00198 Rome
Room 329 – Tel. 064991 8440-8537
Email: cybersecurity_info@uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

Corso di Laurea Magistrale in Cybersecurity
Facoltà di Ingegneria dell'Informazione, Informatica e Statistica

====== TOPIC 3: Secure Machine Learning ======

Description: Study of machine learning techniques such as neural networks and deep learning, from the point of view of their security and privacy. Today, modern applications based on the use of machine learning techniques are applied also to sensitive data, such as: medical data, clinical, photos, audio and video recordings. How can you design neural networks privacy-preserving that are accurate and at the same time prevent the leak of sensitive data contained in the training data set? How can you design neural networks that are resistant to external manipulation, and are able to preserve the data privacy?

References:

- *Giuseppe Ateniese, et al. Hacking Smart Machines with Smarter Ones: How to Extract Meaningful Data from Machine Learning Classifiers. International Journal of Security and Networks (2015)*
https://arxiv.org/abs/1702.07464

Docente: Prof. Daniele Cono D'Elia

====== TOPIC 1: Extracting and analyzing code from protected executables ======

Description: Executable protectors are largely employed by malware writers to hinder static analysis of their artifacts, for instance revealing malicious code only when about to execute it. While recent research improved automatic code unpacking schemes, attackers can still draw upon different protection schemes, such as self-modifying code and more general dynamic code modification schemes.

The student will get acquainted with state-of-the-art protection techniques, and try to tackle open research problems such as automatic extraction of code blocks and identification of their relationships, or control flow graph reconstruction starting from recorded instruction traces.

References:
https://drive.google.com/file/d/1P6MW6HU3faBbJaPaT4wE29a_Zr7dgDTg/view?usp=sharing
https://www.blackhat.com/docs/us-16/materials/us-16-Mariani-Pindemonium-A-Dbi-Based-Generic-Unpacker-For-Windows-Executables-wp.pdf
http://tigress.cs.arizona.edu/transformPage/docs/dynamic/index.html

====== TOPIC 2: Evasive malware ======

Description: With thousands of new malware samples surfacing every day, dynamic analysis plays a fundamental role in the automatic characterization and detection of malicious behaviors. A significant fraction of strains adopt however evasion techniques to hide their malicious behavior if they are under the magnifying glass of an analyst, hindering the analysis.

The student will learn sophisticated evasion techniques seen in the wild, and explore open research problems, such as devising realistic wear-and-tear designs for sandboxes, or finding new evasive patterns by leveraging uncoventional attack surfaces (e.g., caches, latencies, hardware counters) for execution virtualization technologies in order to improve the transparency of current automatic solutions.

References:
https://www.computer.org/csdl/proceedings/sp/2017/5533/00/07958622.pdf
https://www.usenix.org/legacy/event/hotos07/tech/full_papers/garfinkel/garfinkel.pdf

Didactic Office
Via Salaria, 113 – 00198 Rome
Room 329 – Tel. 064991 8440-8537
Email: cybersecurity_info@uniroma1.it

SAPIENZA
UNIVERSITÀ DI ROMA

Corso di Laurea Magistrale in Cybersecurity
Facoltà di Ingegneria dell'Informazione, Informatica e Statistica

Didactic Office
Via Salaria, 113 – 00198 Rome
Room 329 – Tel. 064991 8440-8537
Email: cybersecurity_info@uniroma1.it