SECITC - www.secitc.eu brings together computer security researchers, cryptographers, industry representatives and graduate students interested in any aspect of information security and privacy.

One of **SECITC**'s primary goals is to have on the same round table, together security and privacy researchers and professionals from different communities and to provide a forum allowing the informal exchanges necessary for the emergence of new scientific and industrial collaborations.

The post-proceedings for **SECITC 2018**, as SECITC 2017, 2016 and 2015, will be published by Springer in the Lecture Notes in Computer Science (LNCS) series.
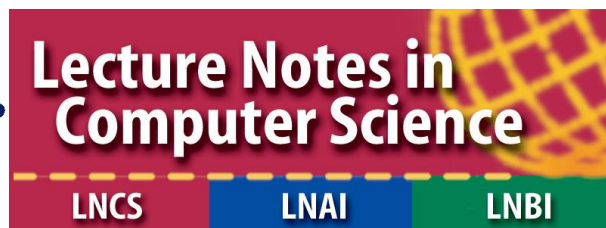
One originality of **SECITC** is its Exploits Session. In this session, new exploit authors will be invited to explain how exploits were discovered and submit a formal research paper describing their discoveries. While the discovery of new exploits is a high-risk high-gain investment that requires creativity and tenacious work, exploits are usually difficult to publish in mainstream research conferences. Exploit paper acceptance criteria will be the exploit's nature, novelty and impact.

The conference topics, but not limited to, are:

Access control	Intrusion detection
Algorithmic tools for security and cryptography	Language-based security Malware
All aspects of cryptography	Mobile security and privacy
Application security Attacks and Defenses	Network security
Authentication biometry	Policy enforcements
Censorship and censorship-resistance	Privacy and anonymity
Cloud Security	Protocol security
Distributed systems security	Reverse-engineering and code obfuscation
Embedded systems security	Security architectures
Digital forensics	Security aspects of alternative currencies
Hardware security	
Information flow analysis	Side channel attacks
Internet of Things (IoT) Security	Surveillance and anti-surveillance
	System security