Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Behavioural security

Author(s): Luca Didaci (UNICA), Giorgio Fumera (UNICA)

CC RG-64 and CT RG-59 - Novel techniques for access control that cannot be enforced through violence, real-time detection methods of attacks
CC RG-75 and CT RG-70 - Next generation of analysis, fingerprinting tools with context
CC RG-78 - Behavioural security
CT RG-18 - Innovative process-aware behavioural-based intrusion detection system capable of identifying any deviation from normal activities for the processes being monitored
CT RG-77 - Devise innovative technique for the detection of anomalous changes in the process activities and status
CT RG-80 - Technologies to monitor and control the production process and detect deviations from acceptable behaviour

ABSTRACT

The widespread use of digital technologies in the private and working life of individuals led to a proliferation of online services that allow users to remotely store, access and share both personal and corporate sensitive data, from different physical places and from a variety of devices. This trend is re-shaping many aspects of individuals' life, such as people's working habits (e.g., through the bring-your-own-device - BYOD - policy) and healthcare services (e.g., automated collection of personal health data through wearable devices). Current authentication mechanisms for protecting the access to users' data, mainly based on passwords, are no more suitable to such novel usage scenarios, and to the corresponding security threats. This demands to strengthen current authentication systems, through:

- continuous authentication based on users' behaviour modelling and anomaly detection, for recognizing users' identity based on the dynamic and history of their interaction with a given service or device, as well as on the usage context

- no-password authentication techniques, like the ones based on biometrics, that can also be used together with continuous authentication

The behavioural security paradigm is also desirable in complex IoT-empowered systems, like industry and utilities, in which the increasing automatization opens the way to novel attack opportunities that cannot be properly dealt with using current signature-based detection techniques. In this context, behavioural approaches can enable the detection of anomalous changes in the normal activities of processes being monitored.

Additionally, behavioural analytics can also provide additional, useful tools to forensic investigators for cybercrime attribution.

RESEARCH ACTION #1

Behavioural user authentication and no-password systems

DISTANCE TO THE MARKET: **TRL 4**
COST OF THE TOPIC: **5 STREPs**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **48 months**
ACTORS: **universities, research institutions, online service providers, companies specialized in biometric authentication systems**

Password-based user authentication mechanisms currently used in most online services exhibit well-known limitations, e.g., passwords are often easy to guess, they can be sniffed, revealed through social engineering (e.g., by phishing attacks), or automatically stolen by malware. Moreover, password-based solutions are suited to isolated systems, whereas the current landscape of digital technologies and their use cases (e.g., mobile devices, wearables, cloud computing, social media, BYOD policy) is increasingly made up of highly interconnected systems characterized by the possibility of accessing different kinds of online services from different devices and with different delivery models. It is therefore necessary to strengthen current authentication systems and access policies. To this aim, the behavioural paradigm is the most promising one. Behavioural authentication is based on exploiting several, soft identity cues related to users' behaviour in accessing and using online services, possibly taking into account also the usage context. In particular, the following issues need to be addressed:

- developing continuous authentication systems based on the analysis of users' behaviour, exploiting different "input signals" or "pieces of evidence" including, e.g., soft biometrics like keystroke dynamics, and contextual factors like the specific service being used, the device used to access it, and user's location
- developing anomaly detection techniques based on the history of past interactions and on behavioural analytics to detect suspect deviations from normal user activities, as cues of compromised accounts or systems
- developing fuzzy logic and machine learning techniques to effectively combine the different authentication signals
- securing users' behavioural data collected for authentication purposes against the risk of being in turn stolen or misused
- exploiting behavioural analytics in forensic tools as a further source of evidence for cybercrime attribution

No-password authentication systems based on biometrics can also be used in certain application contexts, possibly in combination with behavioural-based, continuous authentication. Current biometric authentication systems are however not yet mature for a widespread adoption; further research is needed to address issues like the following:

- performance improvement in uncontrolled environments
- security improvement against "spoofing" attacks, that consist of using falsified biometric traits

Behavioural analytics for IoT-empowered systems

DISTANCE TO THE MARKET: **TRL 4**
COST OF THE TOPIC: **4 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **3**
TIME SPAN FOR ADDRESSING THE ACTION: **48 months**
ACTORS: **universities, research institutions, industries**

IoT and related technologies are deeply transforming the industry, infrastructure and utility landscape. For instance, industrial production processes are evolving toward the Industry 4.0 paradigm, that exploits the benefits of cyber-physical systems and the Internet of Services, beside IoT. The Just-in-Time-Production paradigm is also going to transform factories into a network of highly-interconnected, decentralized and self-organizing "smart" devices, in which the IoT trend will play a leading role. Similarly, increasing automation and remote, centralized control systems are being adopted in utilities (e.g., for water process management). Beside their benefits, such technologies also offer new opportunities of attack to cybercriminals and cyber terrorists. For instance, the lack of authentication features in most used control systems protocols allow intruders to access and compromise control processes, forcing field equipment to misbehave.
Current security solutions mostly rely on signature-based IDSs, which aim at detecting attacks by recognizing specific patterns in network data streams or process behaviour. They are however doomed to fail in scenarios like the ones above, due to the increasing sophistication and customization of future attacks.

Future solutions to enforce security have to include strong authentication schemes, access control systems and improved attack detection systems. To this aim:

- behavioural analytics solutions based on anomaly detection approaches are required, to exploit their ability to detect deviations from a baseline behaviour, thus naturally including unknown and previously unseen attacks
- such solutions must be capable of continuously monitoring utilities and industrial processes, detecting suspicious activities that can be due to attacks (e.g., changes in the manufacturing process and activities), as well as detecting compromised components
- solutions to limit the number of false alarms, which is a drawback of anomaly-based techniques, have also to be developed
- behavioural analytics can be exploited in forensic tools also in the above contexts, as a further source of evidence for cybercrime and cyber terrorism attribution