Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Authentication and Anonymization

Author(s): Jart Armin (CDF), Bryn Thompson (CDF), Piotr Kijewski (NASK), Przemek Jaroszewski (NASK), Janusz Urbanowicz (NASK)

CC NO ID 01 & CT RG-65 De-anonymization of internet users
CC RG-17 Standardized Security measures with strong authentication.
CC RG-19 Innovative data leakage detection system capable to capture any anomalous path taken by sensitive data
CC RG-3 Improvement of the monitoring tools either for personal usage, as it is already happening of the credit card market
CC RG-4 Advanced research in security and privacy concerning virtual worlds
CC RG-59 Watermarks and Fingerprints that survive enrichments and aggregation
CC RG-60 Watermarks that are resilient against collusions and do only have a negligible impact on the results
CC RG-7 & CT RG-4 Advanced research in authentication and anonymization
CT RG-95 Novel techniques for access control

ABSTRACT

Low prosecution rates for acts of cybercrime and cyberterrorism are due, to some extent, to an inability to identify the actors involved. Without this knowledge the capacity for mitigation, prevention of future attacks and bringing perpetrators to justice is severely limited. The advent of Big Data and the Internet of Things will see anonymization increase with further pressures on authentication systems from both the inside and the outside. To stem this tide, appropriate measures are necessary to ensure that the safety and security of users is protected and enhanced in a world where social networks and wearable devices are commonplace and people are exposed to an increase in the dangers from phishing, identity theft, and information disclosure.

The goal is to design, formulate and create innovative solutions appropriate for a future where authentication is still possible and anonymization does not protect and give further advantage to cybercriminals and cyberterrorists.

RESEARCH ACTION #1

Counter measures to abuses of anonymity tools and protocols

DISTANCE TO THE MARKET: **TRL 3**
COST OF THE TOPIC: **3 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **3**
TIME SPAN FOR ADDRESSING THE ACTION: **30 months**
ACTORS: **Research institutions, Industry**

In anticipation of an increase in the number of personal and wearable devices in an IOT future measures are needed that protect the identity of users and militate against the theft of anonymized data.

Anonymity tools and protocols are easily abused for nefarious purposes and yet such tools provide an essential aid for legitimate reasons. Correlation of online and offline surveillance data can generate new insights, provide sources for measurement and information useful to the development of products and applications.

The right to be forgotten should be explored through novel approaches such as improved anonymization techniques that are safe from abuses. Areas for investigation include advanced psychological profiling and automated risk evaluation.

Improved information sharing between parties with standardization of protocols and legal frameworks at local and international level

DISTANCE TO THE MARKET: **TRL 5**
COST OF THE TOPIC: **3 STREPs + 2 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **3**
TIME SPAN FOR ADDRESSING THE ACTION: **36 months**
ACTORS: **Law enforcement, industry, research, cyber security professionals, legal**

Evidences show that cybercrime is under-reported with prevalent reasons given as confusion over where attacks should be reported and lack of trust in the body to which the report is made or in anything worthwhile resulting from the of reporting incidents.

An important action is to improve information sharing between parties from the ground level to those correlating the data and up the governments and other bodies where future decisions are made.

Areas for improvement include clarity of information sharing, differences and misunderstandings relating to privacy, traffic monitoring, data storage & analysis. What can legally be shared is important for advances in cyber forensics and the question of attribution.

RESEARCH ACTION #3

Improvements to the stability and security of systems using strong, innovative authentication methods, encryption and digital forensics

DISTANCE TO THE MARKET: **TRL 5**
COST OF THE TOPIC: **4 STREPs + 2 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **36 months**
ACTORS: **Industry, research**

Novel techniques and tools are needed to improve the stability and security of systems without compromising authentications. Building systems with standardized security measures with strong authentication and sanity checks adds resilience against attack. Additionally, more research is needed into how system access controls can be customised including modular approaches that are easy to administer.

Advanced encryption techniques are needed across all user bases. Currently attackers have higher levels of encryption than ordinary users who may not understand how, when or why encryption is needed.

Improved techniques that lead to attribution will advance security through enhancement of cybercriminal and cyberterrorist identification. Areas for investigation include malware reverse engineering, stylometry and linguistic obscuration. Defeating attacker obscuration with advanced digital forensics tools aids cyber intelligence on malware and attack tool behaviour and signatures.

Other areas for research include watermarks and fingerprints used in the prevention of anonymized data theft.