Funded by the European Commission
Seventh Framework Programme

Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

Trust chains and Identity

Author(s): Giorgio Fumera (UNICA), Davide Ariu (UNICA), Luca Didaci (UNICA), Enrico Frumento (CEFRIEL)

CC RG-6 and CT RG-3 - Automated ways to identify existing trust chains, improvement of threat management models
CC RG-18 and CT RG-15 - New methodologies and architectures for establishing trust between components of a network
CC RG-42 and CT RG-42 - Byzantine fault tolerant cyber-physical systems
CC RG-43 and CT RG-43 - Secure component certifications
CT RG-77 - Code integrity monitoring
CT RT-64 - Analysis of the threats that can be generated in financial markets driven by crypto currencies

ABSTRACT

Trust is a fundamental component in various aspects of individuals' life (e.g., as users of online services, of the healthcare system, and as employees), as well as in organizations (companies, financial institutions, etc.), institutions (e.g., governments), financial markets, and so on. Interactions between the different actors involved in all such contexts are indeed based on underlying trust chains. Trust chains are also implied between components of hardware and/or software systems, and in particular in complex cyber-physical and Internet-of-things systems, whose complexity, autonomy and scope is constantly increasing, even in critical infrastructures (e.g., transportation systems).

Trust chains are undergoing significant changes due to the widespread use of information technology. In particular, less invasive and adaptive devices (the "disappearing computing" phenomenon) are leading to the emergence not only of novel, but also unnoticed trust chains.

Under this viewpoint, the essence of cybercrime is the abuse of unprotected trust chains. For instance, cyber criminals can abuse the trust chains between individuals to steal personal, sensitive data (e.g., by a phishing attack); similarly, cyber terrorists can exploit vulnerabilities in the trust chains between hardware and/or software components to disrupt cyber-physical systems that control critical infrastructures; they can also abuse the novel trust chains underlying financial markets to disrupt them. More specifically, any attack can be seen as abusing a trust boundary that surrounds a given asset. The identification of trust boundaries is indeed one of the main steps in threat modeling; they are also one of the elements of the threat definition language developed by Microsoft, and widely used by many organizations, including the Open Web Application Security Project (OWASP).

Trust chains between individuals

DISTANCE TO THE MARKET: **5 (TRL)**
COST OF THE TOPIC: **3 STREPs**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **36 months**
ACTORS: **universities, research institutions**

Information technologies are profoundly changing the relationships between individuals, and between individuals and organizations, or institutions. One of the effects is the change in the underlying trust chains, and the emergence of novel and even unnoticed ones, due to the disappearing computing and immersed human paradigms. This exposes trust chains to several kinds of abuses.

For instance, the access to personal information in social networking sites is regulated by a network of trust implied by relationships; however, issues like the lack of strong authentication mechanisms or the willingness to increase one's own popularity can lead to exposing personal information to unknown people, which can lead to a poisoning of the network of trust.

As another example, in the working life of individuals new habits like bring-your-own-device (BYOD), working at home, usage of cloud services, etc., cause the disappearance of the traditional enterprise trust zone, exposing corporate information systems to several new threats coming from different sources (e.g., employees are more easily targeted by modern social engineering attacks).

Analogous issues emerge from rapidly changing environments like healthcare systems.

In general, the digital "ecosystems" supporting the digital experience continuity are nowadays specialized for different contexts: for example, the smartcars ecosystem or the home automation ecosystem. The spreading of a blended style of living across a wide range of citizens, and the seamless experience offered by the digital ecosystems, also enable seamless deception techniques. This implies that services today must have a high degree of Contextual Intelligent Quotient (CQ), i.e., the ability to constantly analyse the surrounding reality from different, uncorrelated points of view and to adjust the decision making process in a matter of days/weeks.

To address these issues, it is therefore important to:

- identifying the underlying trust chains in a given context
- make users, or a whole ecosystem, aware when some of the underlying trust chains are being abused
- understand how users can be part of the protection system without altering their usage experience or transferring responsibilities to them.

Trust chains in cyber-physical systems, IoT, and supply chains

DISTANCE TO THE MARKET: **4 (TRL)**
COST OF THE TOPIC: **4 STREPs, 1 IPs**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **48 months**
ACTORS: **universities, research institutions, industry, critical infrastructure organizations, standardization bodies**

Cyber-physical systems and the Internet-of-things (IoT) are becoming an essential component in fields like building automation and in critical infrastructures like transportation systems. They involve complex hardware and software architectures, with the interaction of a number of different devices, sensors and software modules, with different protocols, standards and interfaces. Such systems are exposed to risks like remote manipulation, e.g., to get unauthorized access to a smart building, to disrupt cyber components, and to impact on the operational capabilities and performance of cyber/physical assets.

A specific issue related to the digital infrastructure is the reliance on trusted hardware and software components in the supply chain, to avoid the usage of compromised components (e.g., with a back door). Current efforts in the field of trusted software components are based on the Component-Based Software Engineering methodology, and the Trusted Platform Module implementation of trusted hardware components proposed by the Trusted Computing Group. However, several issues exist. For instance, "market places" that sell and share trusted software components can be infiltrated by cyber criminals, to modify or to replace components with vulnerable ones; the same standardization processes for secure software components might be undermined, as well as certification authorities of trusted hardware and software components that are likely to be established in the near future; cyber terrorists may even create components that individually pass formal verification tests, but behave maliciously in combination and using a specific set of input parameters.

To address the above issues, research is needed in the following areas:

- solutions for establishing trust between the different components of a network, focusing on the interfaces to external modules and systems
- risk analysis and modeling for cyber-physical systems, aimed at enabling Byzantine fault tolerance
- developing standards and protocols for secure component certifications
- improvement of techniques for monitoring code integrity based on checksums

Trust chains in financial markets

DISTANCE TO THE MARKET: **3 (TRL)**
COST OF THE TOPIC: **3 STREPs**
AVAILABILITY OF COMPETENCE IN EUROPE: **3**
TIME SPAN FOR ADDRESSING THE ACTION: **36 months**
ACTORS: **universities, research institutions, governments, financial institutions**

Financial services are a specific sector affected by the changes in traditional trust chains, and by the emergence of novel ones, as a consequence of disintermediation and decentralization. Financial transactions are managed by increasingly long sequences of peer financial intermediaries, which are not guaranteed to adopt the same quality standards. The trust chains between them become therefore less clear. There are some ongoing efforts in this area, like the development of Payment Card Industry (PCI) standards by the PCI Security Standards Council. They are however not yet satisfactory; for instance, they do not involve bank clerks and their software.

The introduction of crypto currencies like Bitcoin is a prominent example of the replacement of traditional networks of trust (in this case, societal structures like governments) with a distributed network that can act as a third-party trust mechanism. More importantly, the block-chain technology, originally developed as the Bitcoin backbone, is likely to have a relevant role in the development of a number of novel applications involving financial transactions, as well as transactions of different kinds, replacing the networks of trust currently involving centralised institutions and bureaucracies. In essence, the block-chain is a shared, trusted, public, distributed database of transactions based on the peer-to-peer technology, that can be inspected by every user, but cannot be controlled by any single user.

The above changes in the trust chains expose financial markets to several risks, up to their disruption. A thorough analysis of the possible threats is necessary, in order to develop suitable, technical and policy solutions (e.g., encryption among the former, and regulatory frameworks for operators and exchangers among the latter), as well as to increase awareness among financial markets operators.