Luca Viganò, Kings College London: “Explaining Cybersecurity with Movies and the Arts”.

Abstract. There are a large number of movies, TV series, novels and even plays about cybersecurity and, in particular, about hackers. Some are good, some are so-so, most are frankly quite bad. Some are realistic, most make cybersecurity experts cringe. In this talk, I will show how some basic cybersecurity notions (and even some advanced ones) can be explained with the help of some famous and some perhaps less obvious movies and other artworks. This is part of “Explainable Security (XSec)” a new paradigm in security research that Daniele Magazzeni and I proposed recently. I will also discuss the “Six Ws” of XSec (Who? What? Where? When? Why? and How?) and argue that XSec has unique and complex characteristics: XSec involves several different stakeholders (i.e., the system’s developers, analysts, users and attackers) and is multi-faceted by nature (as it requires reasoning about system model, threat model and properties of security, privacy and trust as well as about concrete attacks, vulnerabilities and countermeasures).

Ilaria Matteucci, CNR Pisa: “Automotive Security: Solutions and Open Challenges”.

Abstract. Modern vehicles are full of optionals as a result of the increasing introduction of ICT technologies making them Cyber-physical systems. All vehicles functionalities are regulated by an hundred on Electronic Control Units (ECU) that are present in vehicles. Such ECUs are originally designed and developed to collaborate one another but work in isolation with respect to the external world. For this reason, the communication among ECUs happens trough the Controlled Area Network (CAN) bus protocol that allows to send broadcasting messages in clear among ECUs. In modern vehicles, the CAN network does not work in isolation anymore, hence it is exposed to several vulnerabilities that can be exploited to perpetrated both physical and remote security attacks. The aim of this talk is to provide an overview on security issues affecting the intra-vehicle CAN network by presenting both existing and possible solutions and revise the open challenges in this domain.

Fabio Giubilo, British Telecom: “Cyber Threat Information Sharing: Unity is Strength”.

Abstract. Increasing numbers of Small and Medium Enterprises (SME) are outsourcing or hosting their services on different Cloud Service Providers (CSP). They are also using different security services from these CSPs such as firewalls, intrusion detection/prevention systems and anti-malware. Although for the SMEs the main purpose of using these security services is to protect their cyber assets, either physical or virtual, from security threats and compromises, a very useful and valuable by-product of these security services is the wealth of Cyber Threat Information (CTI) that is collected over time. However, a common problem faced by SMEs is that they lack the resources and expertise for monitoring, analysing and reacting to any security notifications, alerts or events generated by the security services they have subscribed to. An obvious solution to this problem is that the SMEs outsource this problem to a cloud based service as well, by sharing their CTI with this service and allowing it to analyse the information and generate actionable reports or patches. The more CTI obtained from different SMEs, the better the analysis result. In this paper, we try to address some of the privacy and confidentiality issues that arise as a result of different SMEs sharing their CTI with such a third party analysis service for the aggregate analysis scenario we just described. We present the design and architecture of our solution that aims to allow SMEs to perform policy-based sharing of CTI, while also offering them flexible privacy and confidentiality controls.
Luigi Toscano, Red Hat: “Role Base Access Control for OpenStack APIs: Status Quo and Trends”.

Abstract. Companies are moving their services from on-premise deployment to Internet-accessible systems. This shift from infrastructures with precisely controlled access to the cloud exacerbates the already existing need for properly securing access to the (REST) APIs exposed by those services. Amongst cloud architectures, OpenStack is one of the most relevant free and open source platforms and retains REST APIs are a foundational concept. OpenStack is usually provided as infrastructure-as-a-service, and its various components talk to each other using the same public APIs used by any other consumers. There is no distinction between “OpenStack services” and "other services", which requires an even more careful planning of the APIs and their authorization models. Luckily OpenStack, as a community, worked together to build a common solution for modeling role-based access control for the REST APIs exposed by their services. This ensures consistency and helps sharing the best practices for access control in the community. The talk will show how the chosen solution supports Role-Based Access Control policies when implementing REST APIs, and the way the definition of the default policies was recently simplified and made more effective. It will then focus on the way system operators can customize their policies, overriding the defaults, and conclude with an account on the current OpenStack frameworks for testing the policies.