# SECCRIT Newsletter 2 – September 2013

This is the second SECCRIT newsletter from a series that will keep you updated about our research activities and events. It is being sent out to members of the "user and advisory board" (UAB) directly and will also be available at www.seccrit.eu. This issue contains: a short overview of some cloud security standardisation activities relevant to SECCRIT, the current project status incl. first research outputs, and an announcement regarding the next issue and upcoming events.

# 1 Current Related Standardisation Efforts

This section provides a short overview of some selected standardisation efforts that are ongoing in several different standardization bodies, and in which SECCRIT consortium partners are partially involved. The content should not be considered as being a complete overview of either related standardization bodies or related work within these bodies.

## 1.1 IETF

The Internet Engineering Task Force (IETF) is an open standardisation body for Internet protocols, whose mission is to produce high quality, relevant technical and engineering documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. The IETF work is organized in roughly 120 different working groups (WGs), of which some are doing standardisation work that is related to the secure cloud computing context of SECCRIT. Since the IETF mainly standardises protocols, but not architectures, the work may contain pieces that can be used as basis for SECCRIT solutions.

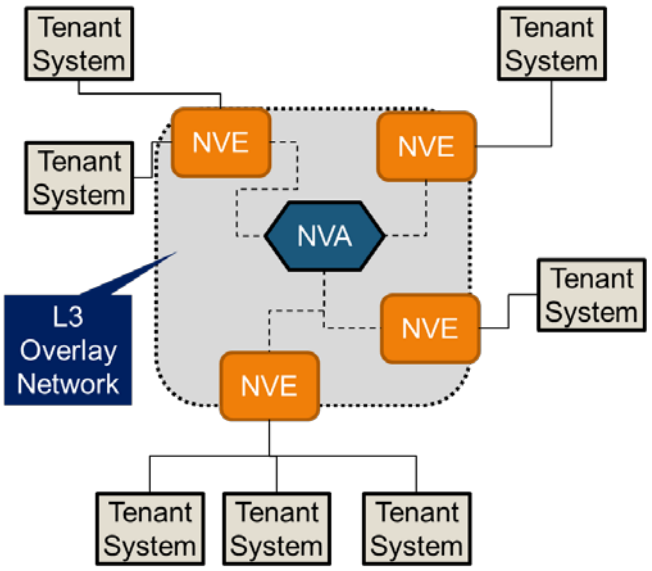


FIGURE 1– NVO3 REFERENCE MODEL FOR DC NETWORK VIRTUALIZATION OVER AN IP INFRASTRUCTURE

The NVO3 (Network Virtualization Overlays) WG is currently working on practical networking problems within data centres that form the basis for physical cloud infrastructures. Nowadays, we see many different tenants within a single data centre, where each tenant may use one or more virtual networks inside a data centre. Challenges are the mixture of virtual and physical data centre resources, isolation of networks (e.g., independent addressing inside the virtual networks – independent of other virtual networks and the data centre infrastructure), and moving virtual machines. Since current layer 2 or layer 3 solutions have limitations, the NVO3 WG is working towards an overlay-based solution for interconnecting various tenant systems into virtual networks within a data centre. Currently, the WG has developed a framework that permits studying forthcoming solutions (cf. Figure 1). An important component is the Network Virtualization Edge (NVE), a network entity that sits at the edge of an underlay network and implements layer 2/layer 3 network virtualization functions. The NVO3 solution will probably be built on layer 3 tunnels between network virtualization edges. For SECCRIT, it would be

interesting to study how NVE or NVA could provide additional functions for monitoring, auditing or anomaly detection.

Further working groups of interest in the SECCRIT context are MILE (Managed Incident Lightweight Exchange) that specified a standardised incident report format (useful to notify security incidents), as well as NEA (Network Endpoint Assessment), and SACM (Security Automation and Continuous Monitoring). NEA defines protocols that support the assessment of the security "posture" of endpoint devices, whereby posture refers to the hardware or software configuration of an endpoint as it pertains to an organization's security policy. This work could be useful for auditing and is taken as basis for SACM, which is a recently formed WG to work on assessment of endpoint posture for a whole environment (e.g., an enterprise). One of its goals is to define a protocol format for retrieving configuration and policy information for driving data collection and analysis and collecting actual endpoint posture. Though NEA and SACM are considering different environments, their work may be extensible for performing audits within the SECCRIT context.

Moreover, typical network monitoring and management WGs like IPFIX (IP flow information export – network monitoring) or NETCONF (Network Configuration – XML and RPC based configuration of network elements) standardised open protocols that could be used within the cloud infrastructure as well as within the (virtual) tenant infrastructure. The earlier work of the SYSLOG (Security Issues in Network Event Logging) WG is also applicable within SECCRIT's work on auditing and root cause analysis, e.g., SYSLOG defined mechanisms for signed log messages.

## 1.2 ETSI NVF/ONF

The *European Telecommunications Standards Institute* (ETSI) has established an *Industry Specification Group* (ISG) for *Network Function Virtualisation* (NFV) in late 2012. NFV aims to leverage standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacentres, Network Nodes and in the end user premises – in other words network functions are moved from purpose-built hardware to the cloud. This activity encompasses any data plane packet processing and control plane function in fixed and mobile network infrastructures. Within the ISG a working group on 'Reliability and Availability' was created to analyse gaps in technology, which hinder the transition from purpose-built hardware to the cloud and to define requirements for dependability and fault management. Dr Marcus Schöller (NEC) was elected as vice-chair to this group who will establish a strong link between this international activity and the SECCRIT project. In addition, an expert group on 'Security' was created. This group focuses on differences with respect to security of said transition, i.e., protection of previously private interfaces that become exposed by running on the cloud. A first set of documents from the ISG will be released to the public in October 2013.

The Open Networking Foundation (ONF) is a standardization body dedicated to the promotion and adoption of Software-Defined Networking (SDN). SDN is a new approach to networking in which network control is decoupled from the data forwarding functionality using a protocol such as OpenFlow. The expected result is an extremely dynamic, manageable, cost-effective, and adaptable architecture that gives administrators unprecedented programmability, automation, and control. A dominant use-case of OpenFlow is data-centre operation and management, as well as cloud infrastructure management. The OpenStack Quantum plugin implements the OpenFlow specification to provide network connectivity to VMs.

In the context of the SECCRIT project, the ONF Security discussion group is of particular interest. It is primarily intended to exchange ideas for securing the protocols and interfaces, and establish best practices for securing SDN implementations. The second intention is to encourage the development of applications of SDN, in order to deliver additional security functionality to systems, applications, and data.

# 2 Project Status

SECCRIT had a successful project-start. The first deliverables were completed and are available on the project webpage. The “Legal Fundamentals” deliverable was influenced by discussions with user and advisory board members at the workshop in May 2013 in Vienna (please see newsletter – issue May 2013 for details). The deliverable explains fundamental legal definitions, concepts and principles from the fields of evidence law and data protection law, which are applicable to most EU member states. It contains examples and links to technical aspects of cloud computing for critical infrastructures (CI). It is intended to be used beyond the SECCRIT project and is thus provided on our project webpage https://www.seccrit.eu.

In the first week of September, a Plenary Meeting was held in Helsinki at the premises of Mirasys Ltd. – one of the project’s demonstrator partners (Figure 2). The meeting focused on the forthcoming deliverables that are due at the end of the year, as well as on the definition of a “SECCRIT reference architecture”. This CI services-aware architecture is briefly introduced in a short paper that was accepted for the IEEE CloudCom conference, which is one of the project’s publications. Our publications are listed at https://www.seccrit.eu/publications.

FIGURE 2 THE SECCRIT CONSORTIUM AT THE 3RD PLENARY MEETING IN HELSINKI

# 3 Next Issue

The next issue of this newsletter is planned for February 2014, and will focus on the SECCRIT architecture and an outlook regarding our next UAB workshop. In the meantime, we will keep you updated via the SECCRIT webpage and twitter (@SECCRIT).