REPORT

8th ETSI Security Workshop

16 – 17 January 2013

Sophia Antipolis

http://www.etsi.org/SECURITYWORKSHOP

OVERVIEW

The 8th ETSI Security Workshop, organised and hosted by ETSI in Sophia Antipolis, France, took place on 16-17 January 2013. It counted around 160 registered participants, covering a diverse range of professional interests within the security arena, with special focus in Security Standards.

The agenda included seven sessions, each ending with an open panel discussion with the audience. Presentations were given by experts representing organizations such as ETSI, CEN, CENELEC, European Commission, ITU-T, ISO, ENISA, as well as the private sector, government and universities. The workshop was closed with a wrap up session.

This event provided interesting information on all topics covered, with special focus on standardization efforts related to such topics. Besides, it provided co-operation opportunities, professional networking and directions for future work in security standardization.

This report provides brief summaries of each presentation. For more details, **all presentations are available on the ETSI website**:

www.etsi.org/securityworkshop .

SESSION 1: Introduction

Session Chair: Charles Brookson, ETSI OCG SEC Chairman

The ETSI OCG SEC Chairman Charles Brookson opened the 8th ETSI Security Workshop and gave the floor to the ETSI DG Luis Jorge Romero Saro for his welcome speech.

Welcome

Luis Jorge Romero Saro, ETSI Director General

The ETSI DG welcomed all participants to the 8th ETSI Security Workshop. This year's workshop coincides with the 25th anniversary for ETSI. ETSI has strongly focused on security standardization for 25 years, and the focus becomes stronger as technology advances and complexity require security measures increasingly. As well continuiting efforts in any security areas, in recent years ETSI has started new work in areas of increasing importance for the future, such as Machine-to-Machine, Smart Grids, Intelligent Transport Systems, Cloud, with strong attention on privacy aspects, which is a need for the citizen clearly expressed by the European Union.
ETSI has also launched the Cloud Standard Coordination, in which a group of expert will focus on security aspect for the Cloud.
The ETSI DG stressed that, in such complex scenario, good collaboration amongst Standard Developing Organisations is essential, and thanked the SDOs present at this workshop to share information and increase cooperation. In such context, he informed that ETSI will have the pleasure to host the next ISO/IEC JTC1/SC27 meeting in April 2013.

ETSI Security Standardization

Carmine Rizzo, ETSI Security Standardization

ETSI security standardization activities within ETSI Technical bodies (TBS) cover a broad range of ICT areas: Next Generation Networks (NGN) Mobile/Wireless Communications (GSM/UMTS, TETRA, DECT…), Lawful Interception (LI) and Data Retention (DR), Electronic Signatures Infrastructure (ESI), Smart Cards, Machine-to-Machine (M2M), Methods for Testing and Specification (MTS), Emergency Communications / Public Safety, RFID, Intelligent Transport Systems (ITS), Quantum Key Distribution (QKD), Identity and access management for Networks and Services (INS), Information Security Indicators (ISI), Algorithms and various work in 3GPP. This workshop offers detailed presentations from most of these areas from ETSI Chair and top experts in security standardization.
As well as maintaining all published deliverables through revisions as requested by the ETSI Membership, over the last year ETSI has produced new publications in areas including 3GPP, ITS, M2M, LI/DR, ESI, Smart Cards, Broadcast, INS and Future Networks. ETSI is also working on new deliverables expected to be published in 2013.
Internal collaboration within ETSI occurs through regular liaisons among TBs in order to ensure consistency, to avoid duplicate efforts, and to make sure that new work is undertaken by the appropriate body. The ETSI Operational Co-ordination Group on Security (OCG SEC) contributes to such efforts.
External collaboration includes participation in the Global Standards Collaboration (GSC), regular co-operation with main international standardization and EU institutions (ITU, ISO, ENISA, CEN/CENELEC, ...) and active partnership with many other standard developing organisations.
ETSI organises a yearly Security Workshop which takes place each January and brings together the main European and Global players in security standardization.
The 5th Edition of the ETSI Security White Paper was published before this workshop (hence January 2012), which discussed the ETSI achievements and current work in all security areas and lists all security related publications. All publications are freely downloadable. The White Paper provides the links to the folders containing all versions of the publications, including the new versions which will be published in the future.
The PDF of the ETSI Security White Paper can be freely downloaded from:

www.etsi.org/securitywhitepaper .

ITU-T Achievements in ICT Security Standardization

Martin Euchner, ITU

Various ITU-T Study Groups (SG5, 9, 11, 13, 15, 16, and SG17 at least) address security and security-related topics at different depth as part of their standardization activities.

The presentation presents the new structure given by WTSA-12, and the achievements of the Study Groups since January 2012, and gives an outlook and perspective of future and forthcoming security standardization activities within the study groups.
A major emphasis is given to the security activities of ITU-T Study Group 17, Security, with its lead study Questions, being active on security standardization in various areas in the field of ICT and telecommunication security, such as security architecture, information security management, cybersecurity, spam countermeasures, security aspects of ubiquitous telecommunication services, secure application services, service oriented security including cloud computing security, telebiometrics, identity management, and PKI/directory services.
The presentation also addresses coordination and collaboration aspects of security such as the Joint Coordination Activities on Identity Management, on Conformance and Interoperability testing, and on Child Online Protection.

ISO Security Standardization
Marijke de Soete, ISO/IEC JTC1/SC27 vice-Chairman

SC 27 is an internationally recognized centre of information and IT security standards expertise serving the needs of business sectors as well as governments. Its work covers the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects.
ISO SC27 has 49 voting members and 17 observing members, and many liaison partners. Its five WGs are: WG1 Information Security Management Systems, WG2 Cryptography and Security Mechanisms, WG3 Security Evaluation, Testing and Specification, WG4 Security controls and services, WG5 Identity Management & Privacy Technologies.
The presentation discusses major achievements, main challenges, and provide an informative list of standards produced by the five working groups.

Privacy in the EU context
Slawomir Gorniak, ENISA

In the new virtual world there are no national border, no uniform legal system, but instead different aapproaches which can put security and privacy in contradiction, and different perceptions across countries/regions.
From the EU perspective, the challenges in network and information security are technological, economic, in terms of legal framework and governance, standardization, and user perspective.
According to the Article 8 of The European Convention on Human Rights, privacy is a human right: "Everyone has the right to respect for his private and family life, his
home and his correspondence." and according to Article 16, The Treaty of Lisbon, The Treaty on the Functioning of the European Union states "Everyone has the right to the protection of personal data concerning them".
It is indispensable to move towards acceptable governance and security, privacy is a crucial aspect but at present the role of standardization is not clear. ENISA is working to address this gap.

SESSION 2: International standardization

Session Chair: Carmine Rizzo,ETSI

ETSI Smart Card Platform
Klaus Vedder, Giesecke & Devrient GmbH, ETSI TC SCP Chairman

ETSI TC SCP was founded in March 2000 as the successor of SMG9, the people who specified the most successful smart card application ever with well over 5 billion subscribers using one or more of the over 25 billion SIMs, USIMs, R-UIMs, CSIMs, … delivered to the market. ETSI TC SCP has published over fifty specifications on smart cards encompassing for every topic the whole range from requirements via the technical solution to the test specification; topics range from administrative commands to APIs, browsers, Internet connectivity, Machine-to-Machine, new interfaces for high speed and NFC as well as remote management. SCP standardized the UICC which is *the* smart card platform providing a clear separation of lower layers and applications residing on it.
The major results of the work done in 2012: include the Specification for UICC forth form factor and new specifications for Secure Channel between UICC and Terminal endpoint.

New Digital Agreement: to be or to be not (digitally)
Riccardo Genghini, ETSI TC ESI Chairman

The aim of EU Regulation draft for eIDs and Ess is the full harmonisation and full interoperability of eIDs, Electronic Signatures, Electronic Delivery, Long Term Preservation of (signed) Electronic Documents, Website strong Authentication and Other EU Qualified Trust Services (and thereof Supervision schemes). Part 2 of M490 requires a rationalized framework for Electronic Signatures and ancillary services, implementing not only DIR 1999/93/EC, but also preparing for EU draft Regulation on eIDs and Trust Services, and a transformation of stabilized CEN and ETSI Technical Specifications (CWA TS TR) into Ens. The presentations shows several use cases and discussed digitalization and productivity gains.

ETSI ISG ISI (Information Security Indicators) Standardization
Paolo De Lutiis, Telecom Italia

Standards for IT security indicators and for tied up event classification model are missing (or are still very poor), and are hindering IT security measures benchmarking. The ETSI ISG ISI initiative (launched during fall 2011), which is based on 4-year experience and frameworks of the European network of Club R2GS "clone" grassroots associations in Cyber Defence and SIEM (France, UK and Germany today), fills this gap while being strictly compliant to ISO 2700x IT security standards. It addresses the full scope of security event detection issues through 5 Working Items:

- ISI Indicators (ISI-001-1 and its associated Guide ISI-001-2), which is a powerful way to assess security measures level of effectiveness (through a full set of some 90 indicators),
- ISI Event Model (ISI-002), which is a comprehensive security event classification model (with detailed taxonomy and representation),
- ISI Maturity (ISI-003), which is necessary to assess the maturity level regarding overall event detection (technology/people/process) and to weigh event detection results,
- ISI Event Detection (ISI-004), which is meant to demonstrate through examples how to produce indicators and how to detect the related events with various means and methods (with categories of use cases/symptoms),
- ISI Event Testing (ISI-005), which proposes a way to produce security events and to test the effectiveness of existing detection means.

The goal is to show how new standards (in a deemed difficult field) can be developed based on a strong user community experience.

Supply Chain Integrity: Building a Coordinated Framework
Claire Vishik, Intel Corporation

In today's global economy, almost all technology products depend on global supply chains. As the dependence on ICT technologies increases in all areas of life and work, concerns have been expressed about the integrity of diverse international supply chains. Standards bodies, from NIST to JTC1, responded to these concerns by developing standards addressing various aspects of supply chain integrity, and organizations in industry segments developed best practices to deal with international suppliers and global supply chains.
Now that fundamental rules and standards have been defined for many areas of ICT, the need emerged to move to defining a coordinated framework that could uplevel the current standards and best practices and begin the exploration of more general and broadly applicable best practices. This exploration was part of a recent ENISA paper on the supply chain integrity.
This talk will provide an overview of currently available standards in supply chain integrity, examine gaps in the current coverage, and present early ideas of a coordinated integrity framework that could emerge as the next step of supply chain standardization.

SESSION 3: CEN/CENELEC standardization

Session Chair: Luc Van den Berghe, CEN CENELEC

Cyber Security Coordination Group towards a coordinated approach on cyber Security Standardization
Martin Uhlherr, DIN Deutsches Institut für Normung e.V.

The reasons for the creation of a Cyber Security Coordination Group (CSCG) are: Cybersecurity is in focus of EU-politics, the need to raise the stakeholders needs, the need for EU - International coordination, there are no european committee for ICT Security Standardization. Hence the idea is to use the infrastructure of standardization.
The CSCG Membership consists of the delegations of National Bodies, and delegations from European institutions. The Terms of Reference include the following: provide strategic advice on cyber security to the technical steering committees of CEN/CENELEC and ETSI, analyse existing European and International Standards on cyber security, define joint European requirements for European and International Standards on cyber security, suggest a European roadmap on standardization of cyber security taking into account EU Commission mandates as appropriate, act as contact point for all questions of EU institutions relating to standardization of cyber security, cooperate with US SDOs and SDOs in other countries working in the same field of standardization, suggest a joint US and European strategy for the establishment of a framework of International Standards on cyber security, coordinate European activities in International standards committees with the aim of implementing such a joint transatlantic strategy.

CEN/TC224 eSign activities
Béatrice Peirani, Gemalto

The Digital Agenda for Europe as expressed by the European Mandate M/460 on Information and Communication Technologies applied to Electronic Signatures (launched end 2010) encompasses the decision to revise the Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures.
This Mandate is for CEN TC224 and ETSI TC ESI, for the years 2011-2014 with the objective to simplify the use of European eSignature Standards. Actions include: create a rationalized framework, provide guidance helping to implement eSignature in an interoperable way, fill in details where existing standards have been too open to interpretation.

CEN-CLC-ETSI smart grid security standards activities
Jean-Pierre Mennella, Alstom

The European Commission – DG ENERGY – M/490 Mandate has the following scope and objectives: to develop or update a set of consistent standards within a common European framework that will achieve interoperability and will enable or facilitate the implementation in Europe of Smart Grid services and functionalities. It will answer the technical and organizational needs for sustainable "state of the art" Smart Grid Information Security (SGIS), Data protection and privacy (DPP). This will enable smart grid services through a Smart Grid information and communication system that is inherently secure by design within the critical infrastructure of transmission and distribution networks, as well as within the connected properties (buildings, charging station – to the final nodes).
Current SGIS Standards Landscape has been analysed accordingly, in terms of relevance for Smart Grid Operators & Product Manufacturers / Services Provider and relevance for Technical and Organisational Guidance.
The conclusion is that Standards needed to establish the basis of the Smart Grid Information Security are available today. Nevertheless there is a need for enhancement and for additional standards to integrate Smart Grid specific needs. The real challenge will be to maintain this effort and to have standards evolving as fast as the Smart Grid Information Security needs

RFID data protection and privacy activities in CEN/TC225
Gerard Dessenne, Chair of CEN/TC225/WG5

M/436 is a standardization Mandate of 8 December 2008 to the European Standards Organisations CEN CENELEC ETSI in the field of ICT technologies applied to RFID systems. M 436 Mandate is divided in two phases: Phase 1: Jan 2010 to September 2011 to analyse the gaps in terms of standardization. The deliverable is the document ETSI 187020 of April 2010 and Phase 2: Jan 2011 to March-May 2014. There are 11 deliverables under the form of EN, TS, TR.

The M/436 Project Pahse 2 consists of 11 deliverables in three groups derived from EC Recommendation of 15th February 2009: Information Privacy Impact Assessment, Technical. The presentation provides ample details on the current work.

SESSION 4: Machine-to-Machine and Smart Grid Security

Session Chair: Charles Brookson, ETSI OCG Security Chairman

Security in M2M communication: The role of the Network Operator
Francois Ennesser, ETSI TC M2M Security WG Chairman

Based on practical experience with M2M application security, this presentation analyzes the different attacks that have been encountered, from their causes to the prevention methods that can be implemented. The clear trend is that existing threats from the internet are more and more migrating to the Internet of Things, where appropriate mitigation tools and processes are not as mature. Recommendations are made on how to cope with these threats, focusing on the central role played by the network operators and the tools and assets they can leverage on to improve the M2M ecosystem.

Trustworthy Security Framework for Wireless Industrial Sensor Networks
Laura Gheorghe, University Politehnica of Bucharest d

The Trustworthy Security Framework developed in "TWISNet: Trustworthy Wireless Industrial Sensor Networks" project includes a number of modules for ensuring security, trustworthiness and reliability in large-scale industrial sensor networks. We present the Data Trust Evaluation module, the SoftwareMechanisms for Device Reconfiguration module, the Sensor Co-Management module and the Failure and Abnormal Behavior Detection module.
The Data Trust Evaluation (DTE) module is responsible with in-network data validation. The module runs on sensor nodes and analyzes data packets, evaluates the trustworthiness of sensed data and blocks untrustworthy data packets. DTE also reduces energy consumption by preventing the delivery of invalid data packets.
The Failure and Abnormal Behavior Detection (FABD) module is responsible with detecting when a node is likely to fail based on the data it sends. Moreover, it can predict future failures for nodes that have been sending large amounts of data or that are likely to run out of battery. The main feature of the FABD system is analyzing data from the nodes (according to the security level chosen); if a failure is detected appropriate actions are taken.
The Software Mechanisms for Device Reconfiguration (SMDR) module provides sensor parameter monitoring and reconfiguration. Parameter data collected on the running sensor node can be queried and modified manually, by users, and automatically, by other modules, via the provided Application Server interface. The module also integrates redundancy and backup functionalities for stored data.
Sensor Co-Management module grants access to network parameters and data to third parties that have authorization. It interfaces with the SMDR module to modify parameters and gathers other data from all other modules running on the network nodes. The module runs exclusively on the Application Server, authenticates and provides an interface for parameters and data.
These modules are mandatory for ensuring secure, trustworthy and reliable operation of a large scale Wireless Industrial Sensor Network.

German Smart Metering and European Privacy Needs
Markus Bartsch, TÜViT GmbH

To secure the communication between the smart meter in each household and the smart grid as well as to cover German privacy laws a smart meter protection profile (PP for the Gateway of a Smart Metering System) according to the international Common Criteria (CC) was specified by the Federal Office of Information Security (Bundesamt für Sicherheit in der Informationstechnik - BSI) in Germany.
This Smart Meter Gateway contains a security module (specified in PP for the Security Module of a Smart Metering System), is able to collect data of meter devices, aggregates these data based on process profiles and sends these data to 3rd parties in the backend systems. The overall architecture of this German approach is now being specified in the Technical Guideline 3109 (Smart Energy) of the BSI.

This contribution describes how this German approach secures smart meter systems on a very high level and how this approach fulfills European privacy recommendations that are listed in "European Commission Recommendation on preparations for the roll-out of smart metering systems" published on 9th of March 2012.

Lessons learned from the new Smart Meter Risk Analysis Methodology in the Netherlands
Johan Rambi, Alliander

The Dutch Risk Analysis Methodology for Smart Meters/Grid is a version of the HMG methodology from the UK with adaptions due to the Dutch Privacy & Security situation of the Smart Meters. This methodology is different from the European M/490 Security toolbox and I will show these differences to point out why we think that our version is more complete and more effective to meet the goals and requirements. This presentation first shows the reason to use this new methodology, then describes the steps of the methodology. Then it points out the European version and the differences between the versions. Finally it gives an insight the vision and Security Maturity Model for the Smart Meters/Grid.

SESSION 5: Mobile and network security

Session Chair: Bengt Sahlin, 3GPP SA3 Chairman

3GPP Security update
Bengt Sahlin, 3GPP SA3 Chairman

3GPP Rel-11 Stage 2 was frozen in March 2012. The presentation covers the security features that are part of 3GPP Rel-11, and it also provides status and overview of ongoing security work in 3GPP. 3GPP TSG SA WG3 is the WG has the overall responsibility for security and privacy in 3GPP systems. It performs analysis of potential threats to these systems, determines the security and privacy requirements for 3GPP systems, specifies the security architectures and protocols, ensures the availability of cryptographic algorithms which need to be part of the specifications.
In 2012 3GPP SA3 finalized the encryption algorithm 128-EEA3, and the integrity algorithm 128-EIA3, based on ZUC. All security specifications from Release 10 were updated to the new Release 11. In addition, IMS media plane security has been specified for real-time media. The media plane can be protected end-to-access-edge using SDES. End-to-end media plane protection is also specified, either using SDES or using a Key Management Server (KMS). Rel-12 will extend the media plane security to cover IMS Messaging, IMS Conferencing and Communications Diversion.

Enhancing Trust in Mobile Services Using the Latest GlobalPlatform Standards
Christophe Colas, GlobalPlatform

GlobalPlatform, the association which standardizes the management of applications on secure chip technology, is working with its members to develop industry specifications that are standardizing the Trusted Execution Environment (TEE). The TEE is an isolated execution environment integrated in portable devices such as mobile phones and tablets. The TEE offers greater security of mobile applications with specific protections for data storage, user authentication, displayed content and near field communication (NFC)-based transactions.
In response to the trend of migrating sensitive services such as payment, banking, corporate and content protection on mobile devices, GlobalPlatform is specifying standard interfaces for the TEE, as well as developing the resources required for application and service providers to leverage the TEE in an interoperable manner.
Basing their developments on GlobalPlatform's TEE Specifications will enable service providers to design and deploy products independently of the TEE implementations bolstering market reliability and confidence.
Long-term, the GlobalPlatform TEE Compliance Program and security evaluation instruments will enable standards bodies operating in specific markets to rely upon its state of the art testing – much in the same way that EMVCo endorsed the GlobalPlatform Secure Element Compliance Program earlier this year.
Delegates attending this presentation will receive:

- An introduction to GlobalPlatform's work to date to standardize the TEE.

- An overview of the TEE Compliance Program, the TEE Security Evaluations Group and the impact its efforts are having on the market.
- Details of the long-term plans of GlobalPlatform's TEE standardizations.

The need for security assurance standards and compliance methodology for telecom
Gavin McWilliams, CSIT, Centre for Secure Information Technologies

ZeuS, the infamous banking trojan has fuelled an underground economy where stolen credentials and banking information can be traded between criminals and organised crime gangs. The detection rate of Zeus Trojan binaries by anti-virus products is quite low and hence alternative methods of detecting infections on end systems are needed. This presentation gives a detailed analysis of the network communications that occur between a Zeus bot and its master as part of the periodic command and control traffic interchanges. Six key network traffic attributes which provide a reliable way of detecting hosts infected by the malware are presented.
Rather than developing a bespoke proof-of-concept demonstrator for this work, a commercial SIEM (Security Information and Event Management) product from Q1 Labs (an IBM company) was used to implement and demonstrate the ZeuS detection ruleset. The QRadar rules used to detect bots in a corporate network environment is presented also.

Malware detection methods for fixed and mobile networks
Mats Nilsson, Ericsson

Today a main trend is clearly the growth of the cyber world through everything becoming connected. Meaning lots of the new functionalities becoming available as part of this connected society as well as societal and business processes becoming integrated in, and therefore also dependent of, the connected society. The increased economic and social value of this cyber world means increased vulnerabilities, unless the industry can keep pace with such threats and vulnerabilities and ensure mechanisms that mitigate any such threat.
The presentation provides the rationale behind the contributions leading to the 3GPP SA3 study item on Security Assurance Methodology, aiming at finding the best suited standards and assurance methodology to facilitate compliance to very strict security requirements, ensuring that within the open global standards framework the dynamic innovation of the connected world and its security can go hand in hand. This presentation explains along the lines above the rationale behind the contributions leading to the 3GPP SA3 study item on security assurance, and how to take this and the broader questions forward regarding how to link security assurance with the open standards based on innovation and the market driven nature of the cyber world.

SESSION 6: Intelligent Transport Systems

Session Chair: Carmine Rizzo, ETSI ITS

A novel Pseudonym Framework for ITS
Haitham Cruickshank, University of Surrey

The presentation proposes a complete Pseudonym Framework (PF) for ITS. The word "pseudonym"that stems from the Greek means (pseudos, false) which refers to the adoption of a false name, Pseudonymity is the use of pseudonyms as Identity. The framework is divided into three phases, and each phase is divided further into detailed steps. Phase-1 is setup phase, composed of pseudonym credential, pseudonym identity and certificate issuance and multiple pseudonym sub protocols. Phase-2 is the communication phase, this phase consist of pseudonym changeover and unlikable communication protocol. Phase-3 is accountability phase, which includes the sub protocols such as pseudonym to real identity resolution and pseudonym revocation.
Phase-1 (Setup phase), grant every ITS station a pseudonym credential which is used for issuing a pseudonym identity and certificate (X.509). This phase involved one designated certificate authority, and one random certificate authority, the former know about the real identity of the ITS station but not the

pseudonymised identity and certificate, while the later do not know about the real identity of ITS station but also the newly generated pseudonymised identity is impossible for it to resolve alone if presented later. Phase-2 (Communication phase), this phase define a mechanism which allows ITS station to communicate with another ITS station without revealing its real identity. The destination ITS station may or many not acquired the pseudonym identity and certificate in phase-1. The communication phase compares MIX network, Onion Routing and group communication for providing anonymity and unlinkability. The pseudonym changeover protocol allows ITS station to change from one pseudonym to another in a non observable way, also make it impossible for the adversary to correlate two or more communication session to one pseudonym holder or link two or more pseudonym identity to one ITS station.
Phase-3 (Accountability phase), this phase proposes two procedures i.e. Resolution and Revocation, the former define a policy for revoking of those ITS stations involved in malicious activities, also a mechanism for distributing revoked identities and certificates to every user accurately and on time, because the European ITS network will include very large numbers of ITS stations and connectivity of ITS-S to the revocation server cannot be assumed always. Therefore this work proposes a new revocation mechanism in which every local/regional RSU/CA keeps revoked certificates and ITS station before accept a message from other ITS station confirm from local RSU/CA, to which the connectivity is easy and cheap (communication cost). The Resolution protocol involves one designated and must certificate authority and two random certificate authorities, which make impossible for adversary to compromise these CA's. This mechanism does not allow any authority to resolve the pseudonym to real identity alone, also after resolution only the designated regional certificate authority know about the real identity of the ITS station.

PRESERVE – Making Secure V2X Communication a Reality S
Norbert Bißmeyer, Fraunhofer SIT(on behalf of the EU FP7 Project PRESERVE)

The EU FP7 project PRESERVE aims at providing a security subsystem for Vehicle-2-X communication that provides a full-blown security solution for on-going V2X FOTs and future pilot trials. Besides a software component that is easy to integrate in V2X communication stacks, this also includes a Public Key Infrastructure (PKI) and an ASIC-based Hardware Security Module that provides the crucial cryptographic performance, secure key storage, and a number of other important functions that are needed to achieve the necessary assurance levels that critical safety functions will require.
The presentation explains the current status of implementation, the results of first tests conducted internally and together with the Score@F Field-Operational-Trial, which also highlights the easy integration of our system. It also discusses the contributions of PRESERVE and the open challenges ahead. This research continues with an outlook to the ASIC-based HSM that is currently under development. Finally, the presentation shows the implementation and testing plans for 2013/14, which include a cooperation with DRIVE C2X in order to test the final V2X security subsystem on an even larger scale.

SESSION 7: Privacy and Cloud security

Session Chair: Tony Rutkowski, Yaana Technologies LLC

Outsourcing personal data processing to the cloud
Christopher Mitchell, Royal Holloway London University

Under data protection legislation, when you process personal data in the cloud you may outsource the processing but you keep the legal obligations. So how do you find and engage a cloud service provider you can rely on to meet your legal obligations?
It would be valuable to have an auditable standard for cloud service providers who process personal data. Under such a standard an auditor could perform an independent check and issues a compliance certificate acceptable to you and to your local data processing authority. Audited compliance to this standard could be written into your outsourced data processing contract.
ISO/IEC 27018 is being developed as such a standard to solve a key problem for the cloud industry.
This presentation covers:

- the need for transparency about how a cloud service provider meets the data protection obligations of his customers;
- the benefits to both cloud service providers and customers that an auditable standard will bring;
- when the standard will be produced and what it will contain;

- the challenges that need to be overcome to realise the standard; and
- the inputs from stakeholders that those developing the standard would like to receive.

Enforcing Privacy for Critical Infrastructures
Nils Ulltveit-Moe, University of Agder, Norway

One area of cyber security, that until now has largely been neglected, is ensuring a structured approach for limiting leakage of private or confidential information in person sensitive or graded systems. Better protection and control of sensitive information in critical infrastructures is important, especially in the light of recent attacks like the Duku worm, which is a tool especially designed for espionage on critical infrastructures.
The presentation shows a framework and methodology that provides a structured approach for increasing the cyber security of critical infrastructures and mobile systems, with a particular focus on detecting leakage of private or confidential information. The method supports XACML-based authorisation and reversible anonymisation of sensitive information for event-based systems like Security Information and Event Mangement systems (SIEM) and also for SOA-based web services in general. The method supports the well-known Plan Do Check Act improvement cycle: planning of an information protection scheme, enforcement of a privacy policy, checking that the policy works as intended on anonymised data and triggering actions if measured privacy leakages exceed given thresholds. The approach may be useful in scenarios where telecommunication or critical infrastructure providers, operations or management services may not be fully trusted, for example if security monitoring is outsourced or for protecting sensitive information if the service provider of telecommunication systems is not fully trusted.
The proposed privacy leakage detection method is based on, and extends, recent research and innovation related to quantitative information flow analysis and differential privacy. The approach fits both fixed and mobile computing scenarios.
The proposed approach will be embedded in a comprehensive critical infrastructure protection solution with supporting tools as part of the PRECYSE FP7 EU-project. This project does research on protection and prevention of cyber-attacks on critical infrastructures, with case studies in the energy and transport sector.

STIX and CLIX: powerful new virtualization security platforms and synergies
Tony Rutkowski, Yaana Technologies LLC

The cyber threat intelligence community is facing a challenge in the acquisition, integration, and exchange of real-time attack information. Threat actors exploit the very complex, dynamic, distributed virtual network and service architectures which exist today. Those architectures include vast arrays of mobile devices, apps, and cloud computing and virtualization implementations found in large data centres
The cyber threat intelligence community is relying on coherent integration of standardized, structured representations of the relevant information including attack pattern analysis. A powerful new platform for dealing with these challenges is emerging - known as STIX (Structured Threat Information eXpression).
Cyber threat intelligence community needs and approaches are very similar to those of law enforcement. Indeed, it is critical in both the cybersecurity and LEA assistance domains to create a common service and infrastructure agnostic framework for packaging and sharing observables and related context information.
An envisioned solution is new work designated CLIX (Cloud/virtualization Lawful Interception eXpression).
This presentation briefly describes both STIX and CLIX, including their value propositions and the substantial synergies that exist between the two platforms.

Scalable privacy, trust & confidence through evolving open standards
Gershon Janssen, OASIS

Today's demanding hyper-connected application environments are rapidly becoming more complex when embracing trends and technologies such as Cloud Computing and BYOD.
Providing online trust in such identity-dependent, networked and cloud-based environments becomes very

challenging, as gaps and deficiencies in global privacy policies and regulatory structures become more exposed due to the fundamental nature of these technologies.
The importance of these issues is also illustrated by the attention and focus of policymakers on government initiatives, such as the proposed EU Data Protection Regulation and the U.S. Federal Trade Commission's Recommendations for Consumer Privacy.
This presentation offers a look at the challenging set of issues and examines new standards underway that can make federated, interoperable, privacy-enabled cloud-based services.

SESSION 8: Security Testing

Session Chair: Scott Cadzow, Cadzow Communications

Methods to develop security standards – a review of work old and new in ETSI and why it's important to use
Scott Cadzow, Cadzow Communications

Over the lifetime of ETSI there has been a lot of work to assist developers in writing standards covering guidelines for the use of language, the use of modelling tools such as SDL, UML and in testing the means to use languages such as TTCN and TPlan. As services become more complex there is an ever increasing challenge to show that the designs of services work to properly and assuredly provide security and privacy protection of other users. Underpinning privacy and security assurance are the much quoted paradigms of "Design for Assurance" and "Privacy by Design" and the aim of this paper is to outline the work undertaken in ETSI TC MTS (Methods for Testing & Specification) in the past year to expand the toolset of design guides in the security and privacy domains.
The figure that follows illustrates some of the areas in which ETSI has prepared standards for security technologies. In some cases ETSI's deliverables have made combinations of some of these technologies. The aim of the work in MTS that carries on some of the previous work done in TISPAN and TIPHON is to further develop tools for standards makers in the "Design for Assurance" and "Privacy by Design" domains. In particular it is timely to reintroduce the role of the ETSI TVRA approach and how it has been extended to include some of the considerations required to determine the impact and role of private data (for conventional PII as well as location and behavioural privacy data) on systems and the standards that support them. The presentation focuses on work being done to map between security requirements and resulting security controls, and the extension of this work to the privacy domain.

Security Testing: Terminology, Concepts, Lifecycle
Ari Takanen, Codenomicon

The purpose of security testing is to find out whether the system meets its specified security objectives, or security requirements. This presentation gives an overview of the security testing landscape, with introduction to the techniques and terminology, and mapping them to the product lifecycle. Security testing is performed at various phases in the product lifecycle, starting from requirements definition and analysis, through design, implementation and verification, all the way to maintenance.
Security engineering starts with Risk and Threat Analysis, which are covered by the ETSI TVRA. Risk and threat analysis are focused on identification of risks and threats to a system at early phase during requirements analysis, or late in the process, reactively during security assessments and acceptance analysis at the validation phase. Tests during the implementation of the software are mostly based on static code analysis. During verification and validation, security tests can be divided in three main domains:

- Testing for correctness of security features
- Testing for performance and unexpected load scenarios
- Testing for robustness and reliability with unexpected inputs

Functional security testing tests against a specific conformance criteria, a set of security requirements implemented as security features. Functional security testing is defined in ETSI TVRA.
Performance testing prepares for attacks using unexpected load, such as Distributed Denial of Service attacks. Performance testing is a new work area for ETSI MTS.

Robustness testing using unexpected inputs is at simplest form based on mutations in data or behavior, but can also be fully model-based automatically generated testing. Robustness testing is a new work area for ETSI MTS.

Case Study Experiences with Risk-based Security Testing and Model-based Fuzzing
Ina Schieferdecker, Fraunhofer Fokus

Today's networked systems are challenged by various security threats, which are traditionally treated in terms of constructively securing a system against attacks. Many of these systems have critical requirements: their failure may endanger human life and the environment, imply serious damage to industrial and social infrastructures, jeopardize confidentiality and privacy, and undermine the viability of whole business sectors. The European ITEA2 project DIAMONDS investigates security issues of industrial-scale networked systems from various domains (including smart cards, IT, software radio, and banking) to derive common security testing principles and methods so as to enable efficient security testing methods of industrial relevance. This presentation discusses selected approaches from the DIAMONDS case studies.
Risk-Based Security Testing (RBST) relates security risk analysis with testing. A comprehensive model based risk assessment that indicates potential threats, vulnerabilities, and incidents as well as related probabilities and consequences, is used as a basis for the identification and selection of appropriate security test pattern and testing approaches.
One of these approaches is Model Based Behavioural Fuzzing (MBBF). In contrast to data fuzz testing techniques, MBBF is based on the intelligent modification of the behaviour of the system. A behaviour description (e.g. represented by an UML2 sequence diagram) is subsequently, systematically, and repeatedly modified by a chain of newly developed fuzzing operators, so that a large number of slightly different behaviour descriptions are generated. The modified descriptions are converted to test code which is executed on the test target to challenge the system's robustness and to find indications for vulnerabilities.
The presentation assesses the approaches in the context of case studies from the automotive and banking domain. This includes an outline of the technical environment as well as a report on lessons learned, benefits and challenges. Moreover the next steps towards standardization and industrial deployment are outlined.

WORSHOP CLOSURE

Charles Brookson and Carmine Rizzo

Charles Brookson thanked the Programme Committee, all speakers, the attendants, **Intel** for sponsoring the networking cocktail, the ETSI staff who organised and ensured a smooth event.
In particular Charles Brookson and Carmine Rizzo warmly thanked the ETSI colleagues Marie-Noëlle Girard for her wonderful help during the workshop, and **Nathalie Guinet**, for having provided her excellent professional experience and support **throughout the entire one-year long process**!
Finally I, Carmine Rizzo, want to thank **Charles Brookson, ETSI OCG SEC Chairman**, for his endless dedication to ETSI, through his immense knowledge and experience.

Please keep in touch! carmine.rizzo@etsi.org

Final Announcement:

The **9th ETSI Security Workshop** will take place on **15-16 January 2014** In Sophia Antipolis, France.

The **call for papers** will be sent in **July 2013**.