REPORT

7th ETSI Security Workshop

18 – 19 January 2012

Sophia Antipolis

http://www.etsi.org/SECURITYWORKSHOP

OVERVIEW

The 7th ETSI Security Workshop, organised and hosted by ETSI in Sophia Antipolis, France, took place on 18-19 January 2012. It counted around 150 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 and KEYNOTE

Session Chair: Charles Brookson, ETSI OCG SEC Chairman

The ETSI OCG SEC Chairman Charles Brookson opened the 7th 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 7th ETSI Security Workshop. He pointed out that speakers and audience are the real actors of this workshop and that security of the citizen is also responsibility of people like us, especially in an increasingly virtualised environment. Any organisation can participate in such efforts within ETSI, and can directly produce standardization work.
Security is crucial and indispensable in any ICT sector in order to make sure that trust is built for the end customer. Without strong security measures, and therefore security standards, the future of ICT can be harmed by lack of trust by the end user, and as a result security standards are essential to ensure interoperability and to help building trust.
Organisations interested in security standardization do not need to become ETSI Members immediately, but instead representative of organisations can be invited by ETSI Chairs to Technical Body meetings in order to find out if our work is useful for their business, and if so, any organisation worldwide is welcome to join us as Member.

Overview of INFSO F5 R&D activities

Vilija Juceviciene, Project Officer, DG INFSO, Unit F5 - Trust and Security, European Commission

The EC strategic view to ICT standardisation consists in indentifying ICT standard needs/relevance, enabling production of ICT standards. For this purpose the following topics need to be addressed: Public Policies, R&D and Innovation, Regulation, International co-operation.
The EC created standardisation roadmaps for 8 “public policies” identified as priority: cloud computing, eHealth, eID, Smart Grids, open data, ITS, IoT and IT Security. It is indispensable to redress the current problem of insufficient level of network and information security across the EU Member States.
The EC has a Framework Programme 7 (FP7) structure for 2007-2013 of available funding for R&D in Trust, Security and Privacy, division between Security programme and ICT research, criteria of differences are in the area of fundamental and deployment oriented research or CIIP and Cybersecurity vs. privacy, trust and security. The current portfolio for Trust and Security has 58 projects for which there are 200m€ of funding.
The Horizon for 2020 is to provide funds for 80 billion € on the following three key priorities:
1) Societal Challenges (35888 mln €): Health, demographic change and wellbeing, Food security, sustainable agriculture, marine and maritime research and the bio-economy, Secure, clean and efficient energy, Smart, green and integrated transport, Climate action, resource efficiency and raw materials, Inclusive, innovative and secure societies;
2) Industrial Leadership (20280 mln €): Leadership in enabling technologies (ICT, nano technologies, etc) & FET, Access to risk finance, Innovation in SMEs;
3) Excellent Science (27818 mln €): Frontier research (ERC & FET), Skills and career development (Marie Sklodowska-Curie actions), Research infrastructures incl. eInfrastructures.

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 and Data Retention, Electronic Signatures, Smart Cards, Machine-to-Machine (M2M), Methods for Testing and Specification (MTS), Emergency Communications / Public Safety, RFID, Intelligent Transport Systems, Quantum Key Distribution (QKD), Identity and access management for Networks and Services (INS), 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.
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 4th Edition of the ETSI Security White Paper was published before this workshop (hence January 2012), which discussed the ETIS 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 Achievements in ICT Security Standardization
Martin Euchner, ITU

The ITU-T SG17 (Security) primary focus is to build confidence and security in the use of ICT.
Various ITU-T Study Groups (SG 5, 9, SG 11, SG 13, SG 15, SG 16, and SG 17 at least) address security and security-related topics at different depth as part of their standardization activities.
The presentation presented the achievements of the Study Groups since January 2011, and gave an outlook and perspective of future and forthcoming security standardization activities within the SGs.
A major emphasis will be 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, cyber security, 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 addressed coordination and collaboration aspects of security such as the Joint Coordination Activities on Identity Management and on Conformance and Interoperability testing.

ISO-ITU cooperation on Security Standardization
Walter Fumy, Bundesdrukerei, ISO SC27 Chairman

ISO/IEC JTC 1/SC 27 (IT security techniques) scope is 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 such as Information Security Management Systems (ISMS), security controls and services; Cryptographic mechanisms; Security aspects of identity management, biometrics and privacy; Conformance assessment, accreditation and auditing requirements in the area of information security; Security evaluation criteria and methodology.
In such areas, between October 2010 and September 2011 13 International Standards and Technical Reports have been published, 14 new projects have been approved (total number of projects: ~ 170), 4 additional P-members (total 46) (total number of O-members: 17), 24 internal liaisons and 29 external liaisons have been made.
ITU-T SG17 and SC 27 collaborate on many projects in order to progress common or twin text documents and to publish common standards. The aim is to produce common or twin (technically aligned) texts: while JTC 1 and ITU-T keep their own processes, approvals are synchronized.
The presentation provides a list of useful references and information on other security related sub-committees.

Overview of ENISA activities including ontology and taxonomies for resilience
Slawomir Gorniak, ENISA

ENISA (European Network and Information Security Agency) was created in 2004 and is based in Heraklion (Greece) with around 30 experts. It supports EU institutions and Member States; facilitates EU institutions, private and public sectors, has an advisory role for NIS topics focusing in prevention and preparedness.
The Agency's principal activities are as follows: Advising and assisting the Commission and the Member States on information security; Collecting and analysing data on security practices in Europe and emerging risks; Promoting risk assessment and risk management methods; Awareness-raising and co-operation between different actors in the information security fields.
The presentation introduced the concept and importance of Network Resilience in the current complex and dynamic network environment, identified the resilience concepts and described an ontology, which describes their content and the interactions among them.
The rationale for introducing resilience as a design goal derives from the need to ensure that society is able to continue to work when the network and its supporting infrastructure is stressed to breaking point. As we introduce smart metering, ITS, the Internet of Things, we will add traffic to our networks but we will also

use the network to influence much more of our daily life. A network failure in future networks will affect almost anything and potentially everything that our society depends on. ENISA works on the development of ontology and supporting taxonomy to define Resilience and how this can be used in the development of Future Networks that demonstrate built in resilience.

SESSION 2: CEN/CENELEC standardization

Session Chair: Ashok Ganesh, Director Innovation, CEN

Responding to the EC/EFTA mandate M/487 for European Standards on security
Ying Ying Lau, Secretary of CEN/TC 391 Societal and citizen security

Mandate 487 is the first, horizontal mandate in the large area of security. A response is expected from the ESOs as follows: study to analyse the current standardisation 'landscape' in the field of security standard, identification of the priority areas for standards development and development of a proposed work programme. EC/EFTA expects future mandates based on the outcome of M/487.
The security concept here includes, among others, protection against threats by terrorism, severe and organised crime, natural disasters, pandemics and major technical accidents. The security research areas in M/487 are: security of the citizen, security of infrastructures and utilities, border security and restoring security and safety in case of crisis.
The overall work will be carried out in two phases. Phase 1 consists in a preparatory study and list of sectors for priority treatment. After the end of the recently started phase 1, phase 2 will provide proposed standardisation work programmes and roadmaps.
Co-ordination Group M/487 has been created to co-ordinate the work for this mandate. The Group includes representatives from the EC and the three ESOs.

Cyber security standards – coordination for European needs
Martin Uhlherr, Secretary of the DIN JTC1/SC 27 mirror committee

Critical infrastructures are increasingly ICT dependent (Smart Grid, e-mobility, etc.), while new and technologically more sophisticated threats have emerged. In a world characterized by free circulation of capital and merchandise national security can only be guaranteed by international cooperation. Cooperation of relevant actors needs to be organized at global level to be effectively able to fight and mitigate security threats.
Secure ICT is in the focus of the EU-Commission. In politics we will see a large portfolio of regulations on IT-security. The occasion to influence these regulations by standardization should not be missed. In such context, Strategic Adivsory Group on Cyber Security (STACS) has been created among the three ESOs, also with involvement of EU Commission DGs, ENISA and the Joint Research Centre (JRC), with the following tasks: make an analysis of existing standards (european and non-european), create a joint view of cyber security among NBs/NCs, be the contact point for EU institutions and foster transatlantic cooperation. With such aims in mind a kick-off meeting was held in December 2011, and work is expected to progress in the near future.

Smart container management, contribution to global security standards (SMART-CM)
Joseph H. McKinney, SCV Solutions

SMART-CM is an EU funded research project under the EU Transport Research Program with the participation of Transport Industry companies, Customs Agencies, Technology providers & Research Organization in order to acquire knowledge of potential new solutions that technology can provide for solving real world problems in door-to-door global supply chain operations.
The SMART-CM Visions is to support implementation of “Green Lane concept” in order to setup and operate Global Secured Trade Lanes. The Project Content consists in Trial use of advanced Container Security Device (CSD) Technology, in proposing standardized procedures and pursues agreements among Customs authorities and in developing and testing electronic platform services.
The delivered SMART-CM solution is a Real-time global container security status monitoring based solution that supports secured information exchange among all involved parties (commercial & regulatory) for implementing the Secured Trade Lanes concept and enhancing the commercial efficiency of the “supply chain”.
Any international trade security solution MUST BE GLOBAL, as global is the nature of commerce in the 21st century. Project SMART-CM has demonstrated a foundation for such a global solution, through broad inclusion of project participants—Customs Agencies and commercial operators around the world.

Transport of dangerous goods (SCUTUM)
Antonella Di Fazio, Telespazio

Today, thanks to the European project SCUTUM, EGNOS is used in the operational transport of dangerous goods in Europe.
SCUTUM has also carried out a CEN2 Workshop. The CEN Workshop Agreement SCUTUM, output of the CEN Workshop SCUTUM, is a technical specification for the development of products and applications based on the EGNOS Commercial Service. The CEN Workshop Agreement SCUTUM is compliant to the guidelines set by the UNECE/OTIF WG on telematics for dangerous goods, and it is also flexible to be applied in ITS systems and various mobility applications, such as personal mobility and traffic information.
The CEN Workshop Agreement SCUTUM has been endorsed by several European stakeholders from industries, institutions and research sector. Additionally, the Ministries of Transport in Italy and France, partners in the SCUTUM project, have validated it, as part of a shared vision for EGNOS adoption and exploitation.
The presentation is focused on the SCUTUM project main results and their possible exploitation in other transport applications, for which accuracy and confidence on the position is an enabler to guarantee higher safety and security.

SESSION 3: INTERNATIONAL STANDARDIZATION

Session Chair: Mike Walker, former ETSI Board Chairman

ETSI TISPAN NGN Security standardization
Paolo De Lutiis, Telecom Italia, ETSI TISPAN WG7 Chairman

ETSI TISPAN WG7 is responsible for the management and co-ordination of the development of security specifications for ETSI TC TISPAN, which produces standards for the Next Generation Network (NGN). As a result of its NGN standardization activities, TISPAN WG7 has defined security requirements; defined a security architecture for NGN; conducted threat and risk analyses for specific NGN use cases; proposed specific countermeasures.
The presentation contains a description of the TISPAN WG7 current activities and achieved results related to the latest NGN release (R3). In particular the following information is provided: TISPAN NGN security overview, main specifications defined and related contents (e.g. TS 187 001 requirements and TS 187 003 architecture), main NGN security topics and their evolution (through the different releases).
Finally hot topics for current and future work are listed, as emerged during WG7 2011 activities and discussion about ETSI Future Networks.

Regional Security Standards: Development Patterns and Impact on International Standardization
Claire Vishik, Intel Corporation

In the course of the last two decades, the importance of global interoperability steadily increased, affecting many aspects of standardization activities. In international standards' bodies as well as in regional standards bodies and industry consortia, global interoperability of standards has become a key requirement. The trend towards global interoperability is strong in security and privacy standardization as well other areas of standards' work. Bus since security and privacy enjoy special positioning among standards, the relationship of regional and international standardization efforts displays interesting patterns in these fields. This presentation describes and analyzes the interplay between regional and international standardization, predominantly in security, and, to a lesser degree, in privacy.
Some of the regional standardization work is examined related in security carried out in the last 20 years in countries such as Japan, India, China, Russia, US, and European countries and the approaches the standards' creators or owners have taken to integrate and incorporate regional standards into the global standardization framework. Security standards in the areas of cryptography, cryptographic protocols, authentication, Trusted Computing, and adjacent areas are studied, in order to determine their influences on the global standardization trends, with regard to the incorporation of new features and development of global interest in initially regionally focused areas of study in security.
To conclude, recommendations are provided to better harness regional developments into global frameworks in security, for the benefit of all standards' creators and users.

Using the CSA Control Matrix and ISO 27017 controls to facilitate regulatory compliance in the cloud
Marlin Pohlman, EMC/CSA

The Cloud Security Alliance, ISO and the ITU-T are aggressively developing best practices and standards to support jurisdictional plurality in the cloud. The presentation explores the standards, best practices and technology security practices that may help to achieve regulatory compliance in the cloud.
The Cloud Controls Matrix (CCM) is the first ever baseline control framework specifically designed for managing risk in the Cloud Supply Chain and serves as the basis for new industry standards and certifications. It comprises 11 domains: Compliance, Data Governance, Facility Security, Human Resources, Information Security, Legal, Operation Management, Risk Management, Release Management, Resiliency, and Security Architecture.
The Consensus Assessments Initiative Questionnaire (CAIQ) is a Cloud Supply Chain risk management and due diligence questionnaire (148 questions).
The CloudAudit Protocol provides an open, extensible and secure interface for automation of Audit, Assertion, Assessment and Assurance (A6) of cloud computing environments. It is a structure for organizing assertions and supporting documentation for specific controls across different compliance frameworks in a way that simplifies discovery by humans and tools.

ETSI Electronic Signatures and Infrastructures
Riccardo Genghini, ETSI TC ESI Chairman

ETSI TC ESI is moving from eSignature Standards to eIdentification, Authentication & Signatures. As a result, TC ESI is assessing conformity of Trust Service Providers (TSP) including eIdentification Authentication & Signatures, common Best practices for TSPs policies and common means of assessing TSP operation.
ETSI TC ESI is also testing Compliance & Interoperability, which includes developing Technical Specifications for testing compliance and interoperability on selected European Norms, creating conformity testing tools and preparing interoperability and conformity test events.

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 results of the work done in 2011: Card Application Toolkit can now be executed on composite devices (e.g., M2M module with an external display); Two customer organizations of TC SCP (3GPP and OMA) use the Secure Channel for the specification of their feature; TC SCP started the following new Work Items: Requirements for an embedded UICC, Memory integrity monitoring in M2M applications, Test Specification of the architecture, functional capabilities and characteristics of the Secure Channel, Test Specification for UICC Application Programming Interface for Java Card™ for Contactless Applications, Requirements and technical solution for a 4th Form Factor (even smaller SIM cards), P2P mode for contactless communications.
In 2011, work on Machine-to-Machine (M2M) applications has given rise to the possibility of having a UICC that is embedded in a communication device in such a way that the UICC is not easily accessible or replaceable. The ability to change network subscriptions on such devices becomes problematic, thus necessitating new methods for securely and remotely provisioning access credentials on these Embedded UICCs (eUICC) and managing subscription changes from one operator to another.

Quantum key distribution services; recent developments and state-of-the-art
Thomas Länger, ETSI ISG QKD, Austrian Institute of Technology

The first part of the presentation displays recent international developments and milestones of technological improvement as well as of practical and commercial application of quantum communications, and specifically quantum key distribution. An overview is given of specific qualities and security properties of quantum key distribution as a cryptographic primitive and show how it can reasonably be combined with other cryptographic primitives in new telecommunications services.

There are many possible ways to define dedicated commercial services exploiting the different characteristics of and options for quantum key distribution and quantum key distribution networks. Most services employ plain secret key distribution for subsequent use in any type of security application, while some provide direct secret communication through the optical channel, which is also used for the quantum communication. The presented services, as well as the connected use cases, are results from recent research carried out in the framework of the ETSI Industry Specification Group on Quantum Key Distribution ISG-QKD, and in linked research projects. The services/use-cases include several fibre-based ones, as well as some employing quantum communications through free space from aircraft and satellites.
The last part of the presentation takes a look into the future and analyzes several potential drivers and inhibitors with influence on further technological advancement and successful market introduction.

Dynamic distributed key infrastructure frameworks (DDKI) and dynamic identity verification and authentication (DIVA) – interoperable, scalable software framework.
André Brisson, Whitenoise Labs

Dynamic Distributed Key Infrastructures (a framework) and Dynamic Identity Verification and Authentication (a protocol) address the following concepts:
Create a security framework that can work with any existing or legacy frameworks or security technologies;
Create a secure IT/Communications framework that can be provisioned with electronic/virtual manufacturing and electronic/secure/remote distribution;
Create a secure IT/Communications framework that can be used ubiquitously and in any context by persons (e-commerce, e-health, and e-government) and non-person (smart grids, critical infrastructures) entities;
Create a protocol that provides Identity Management of all person and non-person entities that access IT networks and provide identity to all the components that comprise the backbone (the actual physical/virtual infrastructure.);
Create an identity management protocol that is 100% accurate (a key based protocol);
Create a single framework and single protocol that will address ALL network security requirements;
Create a framework that is rapidly scalable, completely interoperable, simple to understand, and which is inexpensive to deploy and control key creation, key management and key distribution.

SESSION 4: SECURITY IN THE CLOUD

Session Chair: Carmine Rizzo, ETSI Security Standardization

The Emerging Cloud Ecosystem: cyber security plus LI/RD
Tony Rutkowski, Yaana Technologies

Global network architectures are profoundly, rapidly changing. PSTNs/mobile networks are disappearing. The Internet is disappearing. Powerful end user devices for virtual services are becoming ubiquitous. End user behaviour is nomadic. Huge data centres optimized for virtual services combined with local access bandwidth are emerging worldwide as the new infrastructure.
These changes are real, compelling, and emerging rapidly. Bringing about a holistic "cloud" ecosystem is occupying industry in almost every venue around the world. The changes have significant effects on cyber security, ICT trustworthiness and integrity, and national security requirements.
This presentation 1) describes the current Cloud developments both as to implementations and current industry collaboration, and 2) potential mechanisms for meeting cyber security, ICT trustworthiness/integrity, and national security requirements. The paper also describes why reaching a consensus on appropriate mechanisms and getting them implemented is essential going forward.

Developments in Universal Core-to-Cloud Layered Security Interface Model
Navin Govind, Aventyn UK Ltd

In this presentation are introduced the software framework, programming model and interfaces discussed for executing unique, comprehensive security functions that are software, user and device platform specific for core to cloud security. This framework is currently in discussion for standards proposal at TIA, IEEE Medical Information and Communication Technology and Device security interfaces for improving user identification and authentication, device system software and data protection. This framework co-exists with existing standards for financial and healthcare information management and transaction protocols without changes to current processing infrastructure in place. The framework's objective when implemented is to provide universal seamless and transparent interfaces for key management, encryption and decryption of data using a standard suite of encryption algorithms specific to the user, device and virtualized cloud layers.

Enhancing SIEM Technology for Protecting Critical Infrastructures
Luigi Coppolino, Epsilon

In the last two years an increasing number of coordinated and targeted cyber attacks, characterized by an unprecedented level of sophistication, have been conducted against critical infrastructures. While this is dangerous for any critical infrastructure, it becomes especially worrying when targets of attacks are safety critical infrastructures, i.e. those infrastructures whose failure may result in death of hundreds or thousands of people, as well as serious damages to the environment. The current SCADA technology is not able to cope with malicious attacks, since it was not designed with security in mind. Protection from malicious attacks must be provided by additional technology, which must be integrated with the existing SCADA system in a seamless way. It is presented the approach taken in the MASSIF (MAnagement of Security information and events in Service Infrastructures) project to enhance current SIEM (Security Information and Event Management) technology in order to make it suitable for the protection of Critical Infrastructures. In particular, the focus is on issues related to data collection and parsing. The techniques and the current implementation of the data collection infrastructure of the enhanced SIEM platform are proposed. This is done in the context of a challenging case study, namely monitoring and control of a dam.

SESSION 5: MOBILE / WIRELESS SECURITY

Session Chair: Bengt Sahlin, Ericsson Research NomadicLab, 3GPP SA3 Chairman

3GPP Security
Bengt Sahlin, Ericsson Research NomadicLab, 3GPP SA3 Chairman

The presentation provides an introduction and a short background to 3GPP security. It will goes into some more details about security features introduced recently, and provides status and overview of ongoing security work in 3GPP.
3GPP TSG SA WG3 (Security) has the overall responsibility for security and privacy in 3GPP system: it performs analysis of potential threats to these systems, it determines the security and privacy requirements for 3GPP systems, it specifies the security architectures and protocols and it ensures the availability of cryptographic algorithms which need to be part of the specifications.
“Relay Nodes” consist in a new base station type in E-UTRAN (LTE). The motivations for such new system are to improve coverage of high data rates and to improve cell edge throughput. The challenges are that a Relay Node is “invisible” to the User Equipment (UE) and it looks like a UE to the network in some aspects.
EEA3 and EIA3 are new integrity and confidentiality algorithms for LTE based on the ZUC algorithm, recently approved in 3GPP Release-11, optional to implement in UEs and eNB.
Work is ongoing in 3GPP on system improvements for machine-type communication with analysis of security aspects and considerations on secure connection, triggering security and privacy issues.
New work includes the following: Public Warning System (PWS) Security, Security enhancements for usage of GBA from the browser, GBA extensions for re-use of SIP Digest credentials submitted and Study on IMS Firewall Traversal.

Developing Trusted Services for Mobile using GlobalPlatform Standards
Christophe Colas, GlobalPlatform

Downloading applications directly onto a wireless device - such as a mobile phone - is increasing in popularity yet is undertaken with minimal testing and security evaluation. As a result, the phone is left vulnerable to viruses and malware.
The trusted execution environment (TEE) is a secure area that resides in the main processor of the phone and ensures that sensitive data is stored, processed and protected in a trusted environment. Its ability to offer the safe execution of authorized security software, known as trusted applications, enables the TEE to enforce protection, confidentiality, and integrity and access rights of the data belonging to those trusted applications. This provides end-to-end security.
GlobalPlatform is a cross-industry, not-for-profit association which identifies, develops and publishes specifications which facilitate the secure and interoperable deployment and management of multiple embedded applications on secure chip technology. The GlobalPlatform Device Committee defines the TEE as an open security framework for wireless and multi-application devices, enabling the rapid development and deployment of security applications from multiple service providers. GlobalPlatform’s Device Committee is not completing this activity in isolation; it is currently liaising with the Trusted Computing Group and the Payment Card Industry (PCI) Security Standard council.
This presentation offers an insight into the GlobalPlatform Device Committee’s drive to promote the use of the TEE to facilitate the management of multiple applications on a device. It provides an introduction and

overview of the two specifications that are currently undergoing public review and address the organization's planned future activity to support this technology in achieving its full potential, including the GlobalPlatform Compliance Program, security certification and back office standardization.

Security challenges for Femtocell communication architecture
Ravishankar Borgaonkar, Deutsche Telekom Laboratories

Femtocells are now being rolled out across the world to enhance third generation (3G) coverage and to provide assurance of always best connectivity in the 3G telecommunication networks. It acts as an access point that securely connects standard mobile stations to the cellular operator's core network using existing wired broadband connection. Increased network capacity, lower capital costs, expanded revenue opportunities are some key benefits to the mobile service operator whereas for a user increased indoor coverage, higher speed performance data, higher quality voice, and higher multimedia experience.
Security of femtocells is vital for operators during the deployment process. However, it has already been demonstrated that such devices can be compromised. Extending our previous work on Femtocell device security, we have showed that rogue femtocells pose a serious threat to mobile communication architecture. In addition, we have characterized and tested network based attacks from such devices in order to highlight the design concerns of the femtocell security architecture.
The presentation covers these serious architectural issues and provides meaningful insights to improve the overall Femtocell security architecture. Presentation outline:
Femtocell security architecture;
Femtocell infrastructure weakness analysis;
Critical issues in integrating 3G and femtocell architecture;
Challenges in improving Femtocell security standard.

SESSION 6: SECURITY IN INTELLIGENT TRANSPORT SYSTEMS

Session Chair: Scott Cadzow, Cadzow Communications, ETSI ITS WG5 Chair

ITS Security, a challenge for society and technology
Scott Cadzow, Cadzow Communications, ETSI ITS WG5 Chair

Intelligent transport has the potential to offer significant advantage to users of the transport infrastructure and thus the end users should be at the heart of ITS. ITS is in itself a container of at least five other categories of systems: Advanced Traveller Information Systems (ATIS), Advanced Traffic Management Systems (ATMS), ITS-Enabled Transportation Pricing Systems, Advanced Public Transportation Systems (APTS), Vehicle-to-Infrastructure Integration (VII) and Vehicle-to-Vehicle Integration (V2V).
ITS in all its flavours is intended to positively impact on citizen's lives across the globe in terms of:
Safety: approximately 40,000 people die on European roads each year with a cost for the European economy of approx. 200B€/year;
Efficiency: congestion in the EU costs an estimated 1% of GDP or 100B€/year;
Environmental sustainability: transport accounts for 30% of the total energy consumption in the EU with the vast majority being consumed by road transport.
If we also take note that there are approximately 255million vehicles in Europe (for a population of about 500million (EU-27)) and that none of them are ITS-comms equipped, the challenge is to deploy equipment that addresses the safety, efficiency and environmental sustainability concerns whilst at the same time addressing concerns regarding privacy and security of the users.
In the privacy area across the entire suite of ITS (ATIS, V2I, V2V, ATMS, APTS) there are many areas where data is exchanged and available for processing often revealing detailed personal information related to the behaviour of the user. The presentation introduces the privacy dimension of ITS and examines what, from the set of security solutions that are available, can be deployed to give privacy assurance across ITS in all its variants.
In the area of collaborative machine-to-machine ITS a key security problem is that for the vast majority of information transfers there is no pre-existing security association between the transmitter and the receiver. The creation of trusted security associations that allow transfer of data is difficult and there are a very large number of technologies that are offering solutions.
More details on these key topics in ITS security and ITS privacy are provided in the next two presentations of this session (below).

PKI and Roaming ITS
Haitham Cruickshank, ETSI STF 423

This presentation presents the on-going work in ETSI TC-ITS/WG5 on trust and privacy management in Intelligent Transport Systems (ITS) area. This involves two certification authorities: Enrolment Authority (EA) that provides an ITS station with a pseudonymously identified enrolment ticket (long term) and the Authorization Authority (AA) with multiple authorization tickets (short term), also pseudonymously identified. The efficient use of PKIs in an ITS network is examined for ITS Stations (ITS-Ss) operating within the countries of the European Union (EU) plus issues related to roaming to other areas.
The efficient management of certificates and Certificate Revocation Lists (CRL) is also examined. The ITS PKI system consists of a number of root CAs, which may cross-certify each other. Each root CA is responsible for a certain authoritative domain with multiple EAs and AAs. In this presentation, the decoupling of EA and AA PKI structure is recommended. The EA ticket should be accepted by any AA regardless of the identity of the issuing EA. This can be achieved by using a common root or cross certification of the AA and EA roots. In ITS networks, privacy protection tends to be better with higher frequencies of AA ticket change. However this means more overhead in generating, distributing and revoking these tickets. In the early deployment phase of the ITS network with only few CAs, certificates of all EAs and AAs could be preloaded in every ITS-S. Once full deployment has been achieved, some new EA and AA certificates may also be acquired dynamically when needed, at the cost of increased delays due to communication and processing overheads. The PKI structure should be as flat as possible, depending on the application. For safety applications, very short chains (length 1) could be used, while for commercial applications a longer chain may be required. There will always be problems also with PKI in the areas immediately surrounding a domain border where ITS-Ss from a mix of domains are likely to be present. It should be possible for an ITS-S entering a foreign domain to use its "home" tickets but it will be necessary for it to be prompted by the foreign domain to acquire new "local" AA tickets in order to better protect its privacy.
The deactivation or revocation of an ITS-S ticket is another area addressed in this paper. This can be achieved by two mechanisms: Distribution of a certificate revocation list (CRL); and Non-renewal of expired tickets. Revocation of tickets in ITS communication is challenging for several reasons among which that the European ITS network will include very large numbers of ITS stations (potentially hundreds of millions) and connectivity of ITS-S to the EA or AA is considered as very infrequent. Therefore downloading and distributing CRLs would be difficult. Thus a timely revocation of AA tickets is considered unfeasible. One solution to this problem is not to distribute the CRL to ITS stations but only to the EAs and AAs. The proposed solution in this presentation is using AA tickets with a short expiry period together with rejecting the request for new AA tickets for revoked ITS stations. In the presentation the PKI structure and roaming solutions in ETSI, the European Car-to-Car Communication Consortium (C2C-CC) and the American VSC3 consortium are compared, and the differences are analysed.

Privacy in ITS
Andre Weimerskirch, ETSI STF 423

Wireless dedicated short-range communication (DSRC) is anticipated to play a major role in mid-term reduction of traffic fatalities and increase of passengers' comfort. ITS stations (e.g. on-board units in vehicles, road-side units, personal devices) will regularly broadcast or relay information for a variety of applications, including vehicle-to-vehicle safety applications (e.g. emergency brake warning), driver notifications (e.g. blocked road warning), and commercial applications (e.g. high-speed tolling).
Privacy is a major concern for the deployment of this technology. ITS stations mounted in vehicles will frequently (up to 10 times per second) broadcast location, time, speed, vehicle length and weight, and additional information that might be used to identify and track passengers. There is also a concern that speeding tickets could be issued based on the broadcast messages. Privacy concerns are introduced by the message content (such as vehicle length and weight that might allow tracking an ITS station due to a rare set of attributes) and by security credentials (in particular the public key attached to, or referred to, in each message is unique).
In this presentation we analyze each privacy concern, we conclude that privacy needs to be included in the design and we show that technical solutions are available. Unfortunately, some privacy concern cannot easily be resolved. The message content of cooperative awareness messages (CAM) cannot be encrypted since they are used for V2V broadcast safety applications. CAMs include privacy concerning data such as vehicle length and weight that might provide a footprint of the sender and that might allow tracking of a vehicle. While the footprint might be reduced by lowering the precision of the information (e.g. use vehicle length categories instead of a precise length) it cannot be removed. In the presentation we provide recommendations, especially in the context of the European Data Protection Directive. Finally, we compare the privacy design of the European Car-to-Car Communication Consortium (C2C-CC) to the privacy design of the American VSC3 consortium and analyze the differences.

SESSION 7: SECURITY IN MACHINE TO MACHINE AND SMART GRIDS

Session Chair: Carmine Rizzo, ETSI Security Standardization

The ETSI TC M2M security architecture
Alper Yegin, Samsung for ETSI TC M2M

This presentation introduces the security architecture developed by ETSI TC M2M to address the security challenges encountered in various M2M environments. The interest of specific features is detailed as examples of how this architecture can satisfy the requirements of specific M2M applications and provide the flexibility expected from the horizontal M2M service platform that the committee aims to standardize.
ETSI TC M2M just completed Release 1: Specification of an M2M Service Capability Layer (SCL) servicing M2M applications (independently of verticals) through RESTful APIs.
M2m Service Layer Security is specified in part of TS 102 690 (Stage 2) and TS 102 921 (Stage 3) which include support for mutual authentication, integrity protection, and confidentiality on M2M Device/Gateway-to-Network Interface.
Integrity Validation (IVal) is an optional security feature which enables fine grained access control for both M2M Device/Gateways and M2M Service Providers. Rel-1 supports IVal prior to Bootstrap and during Service Registration procedures.
Potential future work: Release 2 work just started, scope is currently under discussion, candidate work items for the new release would cover roaming, group communication, mla interface security, dla interface security, end-to-end application security and enhanced privacy (hiding real IDs).

Trustworthy Wireless Industrial Sensor Networks
Alexis Olivereau, CEA, LIST

Wireless Sensor Networks provide applications in monitoring and controlling of industrial processes, workers, environmental phenomena, and many more. Because sensors typically communicate over the air, there is always a danger that information can be accessed and modified by unauthorized parties. Within the FP7 project TWISNet (Trustworthy Wireless Industrial Sensor Networks) security issues when applying wireless sensor networks to industrial environments are addressed. A modular and adaptive security architecture able to address the security concerns raised by the deployment of wireless sensor networks into industrial environment is to be developed by the project partners. Therefore, four scenarios are considered in TWISNet, along with possible threats and the resulting security.
The first scenario covers sensors attached to a person moving from PAN to PAN where sensors are attached to workers in order to protect them from environmental threats. A second scenario where sensor networks are used for supply and demand optimization considers smart meters deployed in households. Sensor networks for the monitoring and control of an industrial process are used for the monitoring of industrial processes in order to speed up the process of detecting and handling of incidents in a third scenario. The fourth scenario deals with multi-owner sensor networks where wireless sensors from multiple services/owners/providers form a single network, where a network for each service is sub-efficient or even not viable due to the geographical coverage of the wireless nodes.
The key security requirements for these scenarios are remote key provisioning, authentication, data integrity, data confidentiality, service availability and traceability. TWISNet aims to support and secure the integration of sensor networks into large scale industrial environments. There is a strong need to take standards into consideration in order to obtain product interoperability and quality. Through this proposal, the need for a standardized cross-layer security architecture is asserted. Higher layers functionality as well as the interaction between them should be described and especially resource constrained devices should be strongly considered to cover a wide range of applications and guarantee high interoperability in machine-to-machine communications. The ETSI TS 102 690 standard is under consideration, which specifies application level security and the IETF 6LoWPAN, which standardizes IPv6 for low-power devices. However, in the current state neither of them describes a complete security architecture that can be used for securing industrial sensor networks according to the mentioned needs. Hence there is an opportunity for future standardization efforts in this area.

The Smart Grid security challenges: National regulatory approaches and European standardization efforts
Francois Ennesser, Gemalto

This presentation reviews the main smart grids security challenges (prevention of frauds, privacy preservation, and critical infrastructure protection) with their relation to the different smart grid domains (e.g. Automated Metering Infrastructure, Advanced Distribution Automation, Distributed Energy Resources management in the DSO domain). It will then provide an overview of the smart grids standardization

landscape (applicable standards at the technical, organizational and governance levels) and review ongoing efforts in this area with a focus on Europe (EC M/441 and M/490 Standardization Mandates, M/490 Smart Grid Information Security Group, DG ENER SGTF Expert group 2 Recommendations on Data Security and Privacy, DG INFSO Expert Group on Security and Resilience of Communication Networks and Information Systems for Smart Grids). This is then considered in the perspective of widely deployed national regulations that put additional requirements for implementation, such as organization accreditation and product certification approaches. Under the light of security experiences in other industries (payment systems, wireless communications…), recommendations are given on how to improve this environment to enable the emergence of a successful smart grids ecosystem.

CLOSURE: WRAP UP AND CONCLUSIONS

Moderated by Charles Brookson

The attendants expressed that they found this event useful, and they would welcome ETSI to organise it again next year.

The ETSI Security Workshop is not just about ETSI. We invite and welcome any other organisations: SDOs, EU institutions and public/private organisations. This is of crucial importance to exchange information among interested parties in the most open and objective possible way.

The ETSI Security Workshop is free for everyone, we want to keep it like this to make sure any organisation can easily participate.

Charles Brookson thanked the Programme Committee, all speakers, the attendants, the ETSI staff who organised and ensured a smooth event.

In particular Charles Brookson and Carmine Rizzo warmly thanked **Nathalie Guinet, ETSI**, for having provided her excellent professional experience and support throughout the entire process!

Carmine Rizzo thanked **Dionisio Zumerle, ETSI**, for his work on the first ETSI Security Workshops and the first Edition of the ETSI Security White paper.

Carmine Rizzo thanked **Charles Brookson, ETSI OCG SEC Chairman**, without whom this event could not take place.

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

Final Announcement:

The **8th ETSI Security Workshop** will take place on **16-17 January 2013** In Sophia Antipolis, France.

The **call for papers** will be sent in **July 2012**.