ETSI White Paper No. 18

Tackling the Challenges of Cyber Security

First edition – December 2016

ISBN No. 979-10-92620-12-2

Author:
Charles Brookson, Zeata Security Ltd. and Chairman ETSI TC CYBER

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

Contents

Tackling the Challenges of Cyber Security

The Internet has become a critical infrastructure for both businesses and individual users and its security has therefore become a priority issue. Security is also an important key to the modern connected world and a crucial factor in inspiring the consumer confidence necessary to achieve commercial success for the new technologies emerging in the Internet of Things (IoT), as well as implementation of Industry 4.0 and eHealth.

Another critical development is the growing reliance on virtualization technologies which, in combination with data networking, has enabled Cloud computing. The network operators' model of using this technology is Network Functions Virtualisation (NFV). Virtualization introduces many benefits as well as the potential for some specific security threats. To counter these threats, it is essential to develop trusted computing platforms. This in turn will ensure that consumers can have confidence in the security of the applications deployed on these platforms.

Our growing dependence on networked digital systems, products and services has brought with it a rise in both the variety and quantity of cyber threats which now infiltrate the daily lives of individuals and threaten the stability of the economy. Criminals are becoming ever more inventive. In recent years there have been numerous breaches of security – some accidental, others deliberate – that have had a significant impact on Information and Communications Technologies (ICT) systems and networks. It is universally acknowledged that users must be protected and thus, while the sophistication of cyber-crime is increasing, so too are our efforts to counter it.

At the same time, however, sensitivity towards the privacy of individuals/organizations and their data is intensifying with media exposure of insecure practice by governments and businesses, and there has been a proliferation of legislation worldwide, driven by these growing security concerns.

Balancing the twin demands of privacy and protection is a major challenge. Solutions will certainly include a reliable and secure network infrastructure. But they will also depend on trust on the part of users – both individuals and businesses – that privacy, confidentiality, secure identification, privacy-friendly security, the visibility of security and other issues are properly addressed.

Security standardization, sometimes in support of legislative actions, has a key role to play in protecting the Internet, the communications and business it carries and both the private and corporate users who rely on it.

The timing of the standardization of new technologies, products and services is particularly important; we need to make our ICT secure from the start, as well as throughout their lifetime.

There are many organizations worldwide working on Cyber Security, and co-ordination and liaison is important to ensure that we all pull together and do not duplicate our efforts.

ETSI is an independent, non-profit organization, with over a quarter of a century's experience in producing globally-applicable standards for ICT. We have a long pedigree in security standardization. As the only standards-making organization officially recognized by the European Union (EU) for ICT, we regard Cyber Security as a strategic priority.

This White Paper provides an overview of all of our work related to Cyber Security and outlines some of our targets and aspirations for coming years.

The Organization of Security Work in ETSI

Our technical work is undertaken by a diverse range of Technical Committees (TCs), Partnership Projects and Industry Specification Groups (ISGs). Each group is responsible for standardization in its own technical area.

The scope of some committees is closely related to specific security topics – for example, Lawful Interception (LI), electronic signatures and infrastructures and security algorithms – and many of these committees undertake detailed technical work on Cyber Security in their specific expert areas.

We also have a dedicated committee on Cyber Security, TC CYBER, which co-ordinates our Cyber Security work, acts as a centre of expertise and develops detailed standards itself when required.

Other groups, including the Partnership Projects, have a much broader scope. They deal with security requirements in the process of producing a complete set of standards in a specific technological area. So, for example, the security aspects of ePassports, Machine-to-Machine (M2M) communications and mobile systems are dealt with in mainstream technical committees, rather than by specific security committees. In such instances, TC CYBER provides co-ordination across these areas, acts as an interface and assists where specific cyber security expertise is needed.

How We Work

Most of our standardization work is carried out in committees whose members are technical experts working within our member companies and organizations. Our committees meet typically between two and six times a year, on ETSI premises or elsewhere. The ETSI Secretariat provides a range of support services.

Our standards-making process has been refined over many years. We have adopted an open approach, both in the way we create our standards and also the way our members contribute. We operate by direct participation and by consensus.

Our members decide what work we do and each committee establishes and maintains a work programme which is made up of individual items of work. Our members also decide the timing and resourcing of the tasks and approve the final drafts, so the standards we produce truly respond to the needs of the ICT industry.

Addressing Key Technical Concerns

Privacy by Design

Privacy by Design is an approach to protecting privacy by building protection in up front – right into the design specifications and architecture of new systems and processes, rather than trying to 'bolt it on' as an afterthought.

Designing projects, processes, products or systems with privacy in mind at the outset can minimize privacy risks and build trust. In addition, potential problems can be identified at an early stage, when addressing them is often simpler and less costly.

In co-operation with the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC), ETSI is responding to the European Commission (EC) Mandate on Privacy by Design (M/530). Following the EC's acceptance of our proposals for the production of a set of standards to manage privacy and personal data protection issues from the earliest stages in the design and development of security technologies and services, in addition to during production and provision, we expect to complete up to 11 standards in response to M/530. In particular, TC CYBER has begun work on a practical introductory guide to privacy and a Technical Report (TR) outlining a high-level structured ecosystem of security design requirements for communication and IT networks and attached devices.

In addition, TC CYBER is working on the protection and retention of Personally Identifiable Information (PII) and is defining the technical means to enable the assurance of privacy and the verification of that assurance. We are also addressing identity management and naming schema protection mechanisms, with the aim of establishing a means to prevent identity theft and resultant crime.

The Sharing of Cyber Threat Intelligence

The sharing of information is a crucial weapon in our armoury against cyber-attack.

TC CYBER is preparing a TR on the means for describing and exchanging cyber threat information in a standardized and structured manner. We also provide and regularly maintain a global overview of Cyber Security activities in technical fora.

Statistics and Metrics

Statistics represent a fundamental tool for cyber threat analysis. The absence of a consistent method of analysing the data makes the quality and comparability of results questionable and represents an obstacle in the creation of usable, contextual cyber threat intelligence.

After publishing six specifications which together represent a reference model for the measurement of information security risks, our ISG on Information Security Indicators (ISG ISI) is embarking on a second phase of work. This will include a description of a security information and event management approach involving the whole information security ecosystem (national computer emergency response teams (CERTs) and security operations centres (SOCs)). We will develop an ISI-compliant measurement architecture for Cyber Security, to enable communication between diversified detection tools, and we will produce guidelines for building and operating a secure SOC.

At the same time, we are updating our Key Performance Security Indicators which were developed as a tool to evaluate the maturity of security event detection, with the addition of application examples.

Securing Technologies and Systems

One of ETSI's key strengths is in the securing of overall systems and technologies such as mobile communications, NFV, Future Networks, Intelligent Transport Systems, Digital Enhanced Cordless Telecommunications (DECT™), M2M communications and emergency telecommunications (including Terrestrial Trunked Radio (TETRA)). The security standards required by these technologies are dealt with primarily within dedicated technology-focused technical committees.

For instance, our DECT committee (TC DECT) continues to maintain the DECT base standard with the addition of new features. In particular we are implementing security architecture enhancements in the core technology to better protect end-user privacy and the confidentiality of communications.

To take a second example, our technical committee on Reconfigurable Radio Systems (TC RRS) is protecting the integrity of reconfigurable radio communications. The RRS framework allows for installed radio applications to be updated, or for new applications to be installed on the device, thus enabling RRS-compatible devices to support future radio access technologies. This enhanced flexibility makes RRS a critical enabler for next generation Software-Defined Radio and Cognitive Radio networks, since it will be possible to upgrade devices with new features on a regular basis. But these new capabilities bring new security challenges. Inappropriate use of the radio spectrum can have harmful consequences (in particular to health) so it is important to guarantee the integrity of radio applications and prevent their use as attack vectors against either individual devices or the network itself. We are therefore identifying security issues, preparing a problem statement and proposing solutions. We are identifying security use cases and threats for Reconfigurable Radio Systems, developing a specification with recommendations for countermeasures to security threats and considering the security challenges of specific wireless systems.

We are embarking on new work to support the Network and Information Security Directive, which is intended to increase consumer confidence and maintain the smooth functioning of the European internal market. TC CYBER will identify where new standards are needed, particularly in the area of critical infrastructure protection.

We have begun new work on network gateway cyber defence, aimed at improving Cyber Security by identifying and then advancing changes to technology standards. Potential improvements would be aimed at technology protocols such as the Internet Protocol stack, but could be anywhere or of any form. We are also addressing critical security controls for cyber defence.

Underpinning all our activities is important work on security design and analysis methods, so that tools and techniques are available to test and provide assurance of proper security operation.

Standardization in Key Technical Areas

The Internet of Things

As our world becomes ever more connected, the difficulties in maintaining security multiply. The abuse of IoT infrastructures is becoming mainstream business for cyber criminals. There have been recorded abuses of smart TVs, instances of refrigerator botnets and massive abuse of home appliances with Denial of Service attacks.

But abusing available functions of IoT components is not the worst misuse scenario in IoT environments: information leakage and the invasion of privacy in these ecosystems could lead to threats against human life. Together with data mined from social networking information, IoT data may also be misused to craft the perfect spear phishing attacks.

The IoT is at the edge of cyber-space. As such, Cyber Security must be embedded and ready-to-use by the consumer without any previous specialist technical knowledge. In order to achieve this, we need greater co-operation between producers and operators of technical systems, as well as society and service providers.

As a founding partner of oneM2M, the global standards initiative for M2M and the IoT, we are working with the world's leading ICT Standards Development Organizations and representatives of different industry sectors to create a global standardized platform through which devices and services can be connected. Security is a priority issue for oneM2M, and work is focused on three aspects of security: protecting the oneM2M service layer; providing security as a service to IoT applications, and leveraging communication network security services, where available.

eHealth

Our eHealth Project (EP eHEALTH) is looking at eHealth in general and in particular its relation to the IoT and M2M, including concerns surrounding security and privacy. The scope of EP eHEALTH covers the entire domain of health from measurement through diagnosis to treatment or intervention, as well as follow up. eHealth applications have to operate over the lifetime of a patient (and beyond) and across the borders of politics, nation and technology, and they have to be traceable and accountable at all points.

From a Cyber Security viewpoint, requirements for the protection of privacy make eHealth a particularly difficult M2M/IoT use case. A patient's healthcare and the society he lives, travels and works in are not a simple set of isolated transactions. Over time, many thousands of actors will be involved. Each action may result in a statement being made in a health record that has to be confidential and verifiably correct at all times. Standardization is at the heart of the global development of the eHealth industry and we are pushing for new solutions to be developed that allow appropriate actors to access health records or diagnostic data from sensors, or provide treatment through on-body devices, whilst retaining the necessary system integrity and confidentiality and ensuring that patients are treated ethically and with due dignity. This may require a combination of role-based access rights for medical professionals and care providers, automated and 'robot' assisted management of data ownership and access management for the user/patient, and limited visibility for the existence of sensitive private data.

Trust Service Providers

We support EU Regulation N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (the 'eIDAS Regulation'), and are developing standards to meet the needs of the international community for trust and confidence in electronic transactions. Our Electronic Signatures and Infrastructures committee (TC ESI) is building on its standards for trust services providers (TSPs), electronic signatures, electronic seals and electronic time-stamps, including the definition of security and policy requirements for TSPs providing public key certificates and electronic time-stamps. We are now defining the security and policy requirements for TSPs providing registered eDelivery services, remote signature creation and remote signature validation.

Secure Cards and Elements

Our Smart Card Platform committee (TC SCP) is responsible for developing and maintaining the specification of the UICC, a specific type of secure element mainly (but not only) targeted at telecoms and used in various environments to secure service-related credentials such as ticketing and payment services; its most notable use is as a platform for the Third Generation Partnership Project (3GPP™) (U)SIM application, as well as for 3GPP2.

We are addressing the embedded UICC (eUICC) and the definition of test cases related to the support of multiple secure elements for mobile contactless communication over the Near Field Communication interface.

As the convergence of different market segments such as banking, identity services and fixed line communication with the mobile market is leading to new requirements, we are also considering the future of the secure element. We are looking at improving the existing physical/electrical interface and/or logical interface or defining new ones for removable and non-removable secure elements. We will investigate new flexible form-factors for a secure element and new data structures capable of handling large amounts of data securely, including security functions and storage of data for various different applications in an open environment, while still providing the segment-specific security assurance as required by the relevant market segment and applications.

We are enhancing the requirement specification for the embedded UICC with the addition of a set of requirements related to device-assisted download and installation as well as specific requirements for the testing of the embedded UICC as its integration changes the testing environment.

Future work will cater for the ecosystem of applications. This will cover interfaces between servers involved in secure element management and address the requirements of, for instance, IoT applications.

Cryptography

Strong (and efficient) cryptography is a central building block for security in a huge range of products and systems.

Security Algorithms

Our Security Algorithms Group of Experts (SAGE) provides both ETSI and 3GPP with cryptographic algorithms and protocols specific to fraud prevention, unauthorized access to public and private telecommunications networks and user data privacy. The majority of this work is for mobile telephony; indeed all the standardized algorithms in 3G and 4G, and more recent 2G algorithms, were specified by SAGE.

A well-established principle now in 3GPP security is that systems should support two different algorithms from day one, providing 'belt and braces' security against the possibility that either algorithm may be broken in the future. SAGE endorses this approach, and designs these pairs of algorithms on fundamentally different principles, to make it as unlikely as possible that a single advance in cryptanalytic techniques will affect both algorithms. In 2016 we plan to complete specifications for new algorithms for the General Packet Radio Service (GPRS): a new 128-bit encryption algorithm (GEA5) and new 128-bit integrity algorithms (GIA4 and GIA5). These are being developed primarily for EC-GSM-IoT, a radio interface solution for use in the IoT.

The Impact of the Quantum Computer

The advent of the quantum computer introduces new approaches to solving the classically 'hard' mathematical problems that secure some of the most widely-deployed public key cryptosystems. Encrypted information that has previously been regarded as secure (including bank account numbers, identity information and items relating to military security) could become subject to discovery and misuse.

TC CYBER has published an ETSI Guide (EG 203 310) on the impact of quantum computing on ICT security that reinforces the notion of having cryptographic agility as a root capability of products and services, and also advises that business management, including business continuity, takes due account of the role of cryptography in the business process.

Quantum-Safe Cryptographic Algorithms

We have begun identifying cryptographic primitives that are resistant to both conventional and quantum-computing attacks and have published the results of initial filtering along with recommendations for the use of cryptographic primitives in telecommunications applications. Work is continuing to refine our knowledge and to produce further recommendations for the increasingly specialized deployments of cryptography that are envisaged such as the IoT, Cloud services, collaborative networking and multi-party data sharing.

By the end of 2016 or early 2017, we expect to complete six specifications including a quantum-safe algorithmic framework and a threat and risk assessment for real-world use cases. Two other specifications concern the characterization of cryptographic primitives, benchmarking their performance and their suitability to a variety of applications. We have introduced new work aimed at explaining the upper limits of quantum computing power in the context of cryptography, and we will assess the current state of quantum-safe standardization, identifying where new standards and security architectures are needed.

Quantum Cryptography

Quantum cryptography provides primitives that are intrinsically quantum-safe, as they are based on the laws of nature rather than computation complexity. It allows keys and digital signatures to be shared over optical fibre or free space links and can be used in a general Cyber Security framework, and to complement algorithmic methods for specific applications. Apart from resilience from every possible attack on a quantum computer, quantum cryptography also provides forward secrecy in that recorded communications cannot be decrypted in future when more powerful supercomputers will be available.

Our ISG on Quantum Key Distribution (QKD) is developing specifications that will allow this radically new technology to be adopted in communication networks. We are addressing best-practice security

guidance for implementation security. We are also specifying measurement protocols for characterising optical components and complete QKD transmitter modules, based on measurements developed and validated by several national metrology institutes. Our work is aimed at enabling supply chains for quantum technologies and successful system deployments.

Network Functions Virtualisation

ETSI is pioneering NFV in the work of ISG NFV and security has been a major thrust of that group since its establishment in 2012

Detailed specifications are being developed in support of trusted platforms, remote attestation, public key infrastructure in the NFV environment and others. We are also analysing existing technologies and Open Source platforms. Other work includes the development of security requirements for the Management and Operations (MANO) interfaces and their reliability.

Lawful Interception and Data Retention

Our LI committee (TC LI) is pioneering the development and maintenance of Lawful Interception and Retained Data (RD) capability, and our LI standards are being adopted around the world. LI implementation is required by the EU which allows for LI to prevent crime, including fraud and terrorism.

We are currently developing a new specification on the dynamic triggering of interception, which is required as a result of the diversification of service and network architectures, and a new specification for an internal network interface for LI, covering connections between LI systems and several network elements from different vendors. We are also addressing security for LI and RD systems, a fundamental requirement which is becoming ever more challenging as networks become increasingly IP service-centric, globally distributed and, frequently, software-based. Our work on NFV, which is a key element in this area, is intensifying. We are developing guidance on LI and RD standards and concepts, and on LI for LTE™. Other possible future topics include the media stream handover for encrypted data, for handling intercepted data from communications which have been encrypted by operators.

TC CYBER is also addressing security aspects for LI and RD interfaces to cover assurance of the integrity and originator of approvals/authorisations, the security aspects of internal interfaces for LI, and security issues around the role for global, trusted-third-party or virtualized components of law enforcement equipment.

The **ETSI Security Week**

Our highly acclaimed annual Security Week offers focused thematic streams, time for networking and opportunities for ETSI security-related committees to hold meetings which all delegates (including non-members of ETSI) may attend. The week introduces the latest developments in our security-related work and fosters debate and discussions which help shape the future direction of our security-related standardization.

www.etsi.org/SECURITYWEEK

All published ETSI standards are available free online at www.etsi.org/standards-search.

Details of all upcoming standards can be found online at: http://webapp.etsi.org/workprogram.

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org