Welcome to the World of Standards

ETSI

World Class Standards

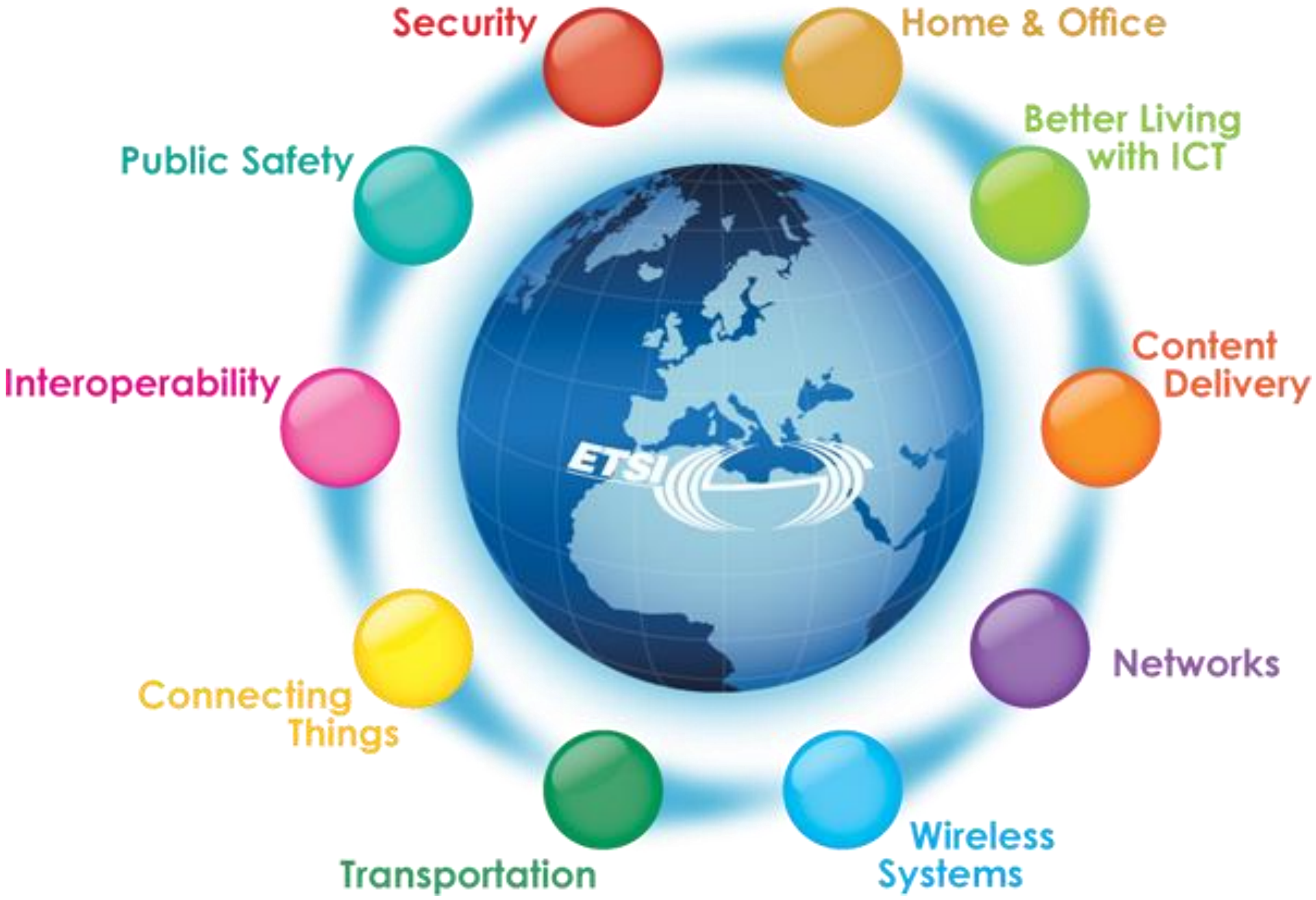
ETSI CLUSTERS

Overview with focus on Security

Presented by S. Compans for ILNAS workshop – 7 July 2017

sonia.compans@etsi.org

Main areas of work



Connecting Things Highlights

- SmartM2M & oneM2M
- eHEALTH and IoT
  - EP eHEALTH is preparing an ETSI White Paper on Use Cases for eHealth. Closer collaboration with SmartM2M and AIOIT is going on about Ontology and SAREF extensions.
- SmartBAN and IoT
  - progressing well and cooperating on SmartBAN Ontologies with AIOTI and IoT Large Scale Pilots.
- ERM TG28 and IoT
  - LPWA/LTN development continues in TC ERM TG28
- New ETSI ISG CIM (Context Information Management)

Interoperability Highlights

- A total of **12 Plugtests** were held in 2016 (NFV, ITS, 112, ESI ASiC, eCall, Digital Cinema, etc)
- Plugtests in preparation
  - First Mission Critical Push-to-Talk (MCPTT)
  - Sustainable Smart City Interoperability Showcase
- Project co-ordination/support for Open Source initiatives
  - Open Source Mano (OSM)
  - TC MTS development of OS toolset for the Test Description Language (TDL)
- Proof of concepts for MEC, NFV, NTECH
- Testing frameworks and specifications for 3GPP LTE UE, ITS, SmartM2M/oneM2M

Public Safety Highlights

- 3GPP SA6 - Mission Critical specifications
- Mandate M/493, location enhanced emergency call service
  - ES 203 283: Stage 3 defining protocols, based on the M493 functional architecture, being completed
- SC EMTEL - Technical Report on Recommendations for public warning making use of pre-defined libraries

Home & Office Highlights

- Wireless Accesses/Home Control
  - Revised Harmonized Standard EN 300 328 V2.1.1 (RED) for 2,4 GHz published and cited in the OJEU
  - Revised Harmonized Standard EN 301 893 (RED) for 5 GHz on national vote
- DECT
  - Working Group Ultra Reliable and Low Latency Communications (URLLC) created
  - URLLC to address IMT-2020 objectives in terms of latency and reliability
- Wireless Industry Applications (WIA)
  - Harmonized Standard for WIA in the 5,8 GHz band close to finalization

Better Living with ICT Highlights

- Energy Efficiency and environmental matters
- Human factors
- Speech and Media Quality

Content Delivery Highlights

- JTC Broadcast
  - Following the general move by broadcasters from the original DAB audio coding to the more efficient DAB+ audio coding, DAB audio coding was removed from the system standard into a separate TS.
  - Revision of the DVB specification for the use of Video and Audio Coding in Broadcasting Applications
    - This specification that encompasses UHDTV features was revised to include advanced audio-visual features e.g. High Dynamic Range (HDR), High Frequency Range (HFR), Next Generation Audio (NGA).
- ISG intelligent Compound Content Management (CCM)
  - GS for Ultra High Definition (UHD) TV High Dynamic Range (HDR) and Wider Color Gamut (WCG) is published.
  - The ISG has asked the ETSI Director General for closure.
- ISG Mobile and Broadcast Convergence (MBC)
  - The group continues to be active with regular F2F meetings and conference calls.
  - An early draft of their Group Report should be made available by May.

Networks Highlights

- Seen in other presentation

Wireless Systems Highlights

- Harmonized standards for the Radio Equipment Directive (RED) (TC ERM, BRAN, SES, DMR)

Transportation Highlights

- Automotive ITS
- Rail communications
- Aeronautics
- Maritime communications

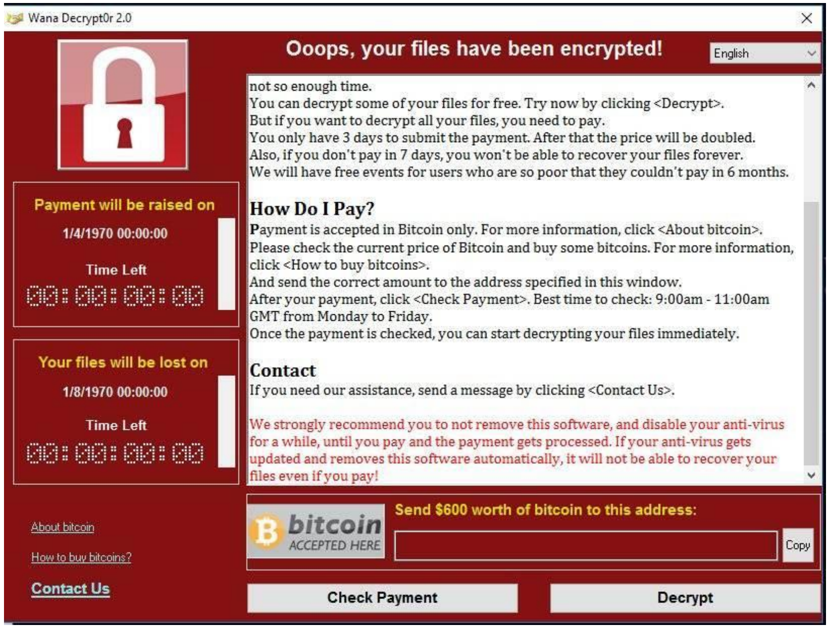
Security

- Horizontal cybersecurity
  - Privacy by design
  - Security controls
  - Information Security Indicators
  - Network and Information Security
- Securing technologies and systems
  - Mobile/Wireless Comms (3G/4G, TETRA, DECT, RRS, RFID…)
  - IoT and Machine-to-Machine (M2M)
  - Network Functions Virtualisation
  - Intelligent Transport Systems
  - Broadcast
- Security tools and techniques
  - Lawful Interception and Retained Data
  - Digital Signatures and trust service providers
  - Secure elements
  - Cryptography

Horizontal cybersecurity

Security controls (TC CYBER)

- 20 critical security controls (TR 103 305)
- Applying the 1st three controls would have avoided Wannacry



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.
Once the payment is checked, you can start decrypting your files immediately.

Contact

If you need our assistance, send a message by clicking <Contact Us>.

We strongly recommend you to not remove this software, and disable your anti-virus for a while, until you pay and the payment gets processed. If your anti-virus gets updated and removes this software automatically, it will not be able to recover your files even if you pay!

Payment will be raised on
1/4/1970 00:00:00
Time Left
00:00:00:00

Your files will be lost on
1/8/1970 00:00:00
Time Left
00:00:00:00

Send $600 worth of bitcoin to this address:

Horizontal cybersecurity

Critical Infrastructure protection (TC CYBER)

- Guidance for the deployment of security technologies and management to deliver and maintain effective Critical Infrastructures that are reliant on ICT technology
- Defining ICT metrics for the identification of critical infrastructures
- Writing practical guideline on standards to adopt for implementing the EU NIS Directive

Horizontal cybersecurity

Information Security Indicators (ISG ISI)

- From a qualitative to a quantitative culture in IT security measurements
- Specifications adopted by more than 100 large European companies and organizations, including Information Security Government Agencies
- Considered as unique in the standardization world filling a gap in the Cybersecurity field
- Phase 2
  - Language to model threat intelligence information and enable detection tools interoperability,
  - Guidelines to build a secure Security Operations Centre,
  - Description of a Security information and event management (SIEM) approach truly integrated within an overall organization-wide and not only IT-oriented cyber defence.

Horizontal cybersecurity

Privacy measures (TC CYBER)

- Practical introductory guide to privacy
- Technical means to enable the assurance of privacy and the verification of that assurance
- Identity management and naming schema protection mechanisms: identifying means to prevent identity theft and resultant crime
- Personally identifiable information (PII)
  - Report on protection of PII in mobile and Cloud services.
  - Attribute-Based Encryption (ABE): data protection for Cloud, Mobile, IoT + ABE protocol toolbox for Attribute Based Access Control
- In support of EC Mandate M/530 on Privacy by Design

Horizontal cybersecurity

Network gateway cyber defence (TC CYBER)

- Analysis of the ecosystem, technical requirements, new challenges and techniques
- Ongoing work on Middlebox Security Protocol to enable trusted, secure communication sessions between network endpoints and one or more middleboxes between them using encryption

Securing technologies and systems

3GPP

- Mission Critical Push to Talk over LTE
- Security studies of mobile systems for IoT
- Security Assurance Specification
- Working on architecture and security for next generation (5G) system

Securing technologies and systems

- M2M and IoT (oneM2M)
  - Security architecture allows exposing security services to IoT applications
  - Enrolment services
    - Credentials Provisioning/Security Configuration of the M2M System
  - Secure communications services
    - Methods for Securing Information (PSK/PKI/Trusted Party)
    - Protocols (TLS/DTLS)
    - Point-to-point and End-to-end solutions
  - Access Control services
    - Authentication and Authorization
    - Static (ACL based) and Dynamic (e.g. token) solutions
    - Privacy Management tools
  - Release 3: Secure Environment abstraction and management

Securing technologies and systems

- Network Functions Virtualization (ISG NFV) key themes
  - Host security
  - Trust domains
  - Lawful Interception
  - Monitoring and management
  - MANO domain security

- Lawful Interception and Retained Data (TC LI)
  - Law Enforcement Monitoring Facility interface to support (as a minimum) European Investigation Orders (EIOs)
  - Baseline security requirements regarding sensitive functions for NFV and related platforms

Security tools and techniques

Digital signatures and related trust services (TC ESI)

- Framework of standards supporting Regulation (EU) No 910/2014 (eIDAS) as well as supporting the general requirements of the international community to provide trust and confidence in electronic transactions
  - Policies for Trust Service Providers & certificate profiles
  - Procedures and formats for signatures creation and validation
  - Cryptographic suites
  - Trusted Lists
- Ongoing: registered eDelivery, remote signature creation and validation

Security tools and techniques

- Attribute Based Encryption for Attribute Based Access Control (TC CYBER)
- Quantum Key Distribution (ISG QKD)
  - characterizing optical components for QKD systems
  - Coming work: Threat actor description for QKD and Basic level side-channel resistance

Security tools and techniques

QSC (Quantum-Safe Cryptography)

- Identification of proposals from industry and academia for quantum safe cryptographic primitives, and the development of a framework for quantum safe algorithms
- Published ISG work (ISG closed)
  - Quantum safe algorithmic framework
  - Cryptographic primitive suitability assessment
  - Quantum safe threat assessment
  - Quantum safe standards assessment
  - Fundamental limits of quantum computing applied to cryptography
- Work transferred or created in new TC CYBER WG QSC
  - Quantum safe key exchanges
  - Quantum Safe Signatures
  - Quantum Safe Virtual Private Networks

Events

- White paper on Tackling the Challenges of Cyber Security published in December 2016
- ETSI Security Week (12-16 June 2017) www.etsi.org/securityweek (all presentations available online)
    - Workshop 1: Making standards in support of cybersecurity legislation
    - Workshop 2: eIDAS one year after entry in application
    - Workshop 3: Registered eDelivery
    - Workshop 4: NFV security (+ NFV tutorial day before)
    - Workshop 5: 5G security
    - Workshop 6: 5G-ENSURE Project
    - Workshop 7: ISE Project (on ITS security)
- Quantum-Safe Cryptography workshop #5
    - 13-15 September 2017, London, hosted by UK Quantum Hub

Summary

- Horizontal cybersecurity
  - Privacy by design
  - Security controls
  - Information Security Indicators
  - Network and Information Security
- Securing technologies and systems
  - Mobile/Wireless Comms (3G/4G, TETRA, DECT, RRS, RFID…)
  - IoT and Machine-to-Machine (M2M)
  - Network Functions Virtualisation
  - Intelligent Transport Systems
  - Broadcast
- Security tools and techniques
  - Lawful Interception and Retained Data
  - Digital Signatures and trust service providers
  - Secure elements
  - Cryptography