

Security assurance and the role of ETSI

Scott Cadzow
STF292 (the follow on from STF268)
C3L

ETSI Security Workshop
16th January 2006
Sophia Antipolis

Contents

- Problems with security practice
- ETSI approach to security
- Tools and techniques
- Results

Common security standards problems

- ❑ **Poor statement of objectives**
 - I want <<my product/service>> to be secure
 - I want to authenticate my users

- ❑ **Prior assumption or declaration of solution**
 - I need to use IPsec
 - Must use PKI

- ❑ **Not clear !!!**

Common security solutions

- ❑ **Secrecy**
 - Don't let anyone know what you're doing
- ❑ **Containment**
 - Once the attacker is in the system and committed a crime keep them locked in the system
- ❑ **Intrusion detection**
 - Find out when an attacker is in the system (before damage occurs)
- ❑ **Access control (restriction)**
 - Only allow known parties into the system
- ❑ **And on and on ...**

Scalability of security solutions

- ❑ Easy to keep a secret with two parties?
 - Basis of symmetric key cryptology
- ❑ Impossible to keep a secret with more than 3 parties?
 - Basis of asymmetric key cryptology (Ellis of UK CESG proposed Non-Secret Encryption in 1970 (6 years before Diffie and Hellman))
- ❑ Scenarios:
 - Correspondents know and trust one another and the network
 - Correspondents know and trust one another but don't trust the network
 - Correspondents know but don't trust one another but trust the network
 - Correspondents don't know one another
 - Communications network is public
 - Communications network is private
 - Etc.

How secure are we?

- ❑ A safe is rated by the number of hours it takes to break the lock
 - Without the key
 - With knowledge of the locking mechanism
 - A safe is safe if
 - You can control access to less than its rating
 - The key is kept secure and separate

- ❑ Security needs to be determined in terms of risk
 - What is the risk if
 - ... our identity leaks?
 - ... our conversation is overheard?
 - ... our credit card details are corrupted?

- ❑ How can we check that risk is mitigated?



What does ETSI mean by security?

- **Security in the standards world refers to a collection of attributes**
 - **Confidentiality**
 - **Integrity**
 - **Authenticity**
 - **Availability**
 - **Assurance**
 - **Maintenance**

- **We try not to use the term security as it is unclear**
 - **Except as an umbrella term to capture the collection**
 - **ETSI also uses security in the context of providing awareness**

ETSI approach to security

- ❑ Risk based analysis and countermeasure development
 - TVRA as primary tool
 - Technology and interface specific security
 - Simplicity
- ❑ Countermeasures based on application of known techniques to critical risk areas
 - ISO based methods
 - SAGE sourced algorithms
- ❑ Collaboration with industry deployments
 - TETRA through MoU SFPG
 - GSM/3GPP through GSM-OA
- ❑ Testing and Maintenance

ITU-T X.805

❑ ETSI approach

- Addresses risk first
- Find solutions to mitigate risk

❑ ITU-T X.805 approach

- Does not address risk
- Offers presentation of security results within 1 of 8 security dimensions
 - (1) Access Control,
 - (2) Authentication,
 - (3) Non-repudiation,
 - (4) Data Confidentiality,
 - (5) Communication Security,
 - (6) Data Integrity,
 - (7) Availability, and
 - (8) Privacy.
- Simplified threat model
 - Interruption, Interception, Modification, and Fabrication.



Understanding of vulnerability and risk

- ❑ Required for every system or product
 - Justifies the security investment and targets that investment
- ❑ Captured in a TVRA document
 - Not an easy document to prepare
- ❑ Requires thinking about attack
 - Good people can't think as criminals
 - Criminals unlikely to admit to it and unlikely to help
- ❑ Security components required depend on risk
 - Risk may depend on motivation of attacker
 - Motivation is difficult to assess and damage may bear no relation to the logical motivation (*suicide attack, pleasure attack*)
- ❑ Vulnerabilities are dynamic
 - Tools available to the attacker change over time
 - First attack may be expensive
 - Later attacks may incur no cost (*script kiddies*)

Proof of security

- **Need to answer the inevitable questions:**
 - What is being secured?
 - For how long will it be secure?
 - What attacks are we safe from?
 - What is the risk we are mitigating?
 - What is the residual risk we are accepting?
- **Furthermore we need to examine:**
 - Can security be measured (security metrics)?
 - Can security be presented (security indicators)?
 - How can security be managed?

Assurance programme assists proof

- Assurance programme offers
 - Process of security development
 - Quality
 - Understanding and visualisation
 - Credible measurement of result

- Assurance offers similarities to standards process
 - Quality
 - Understanding
 - Shared development

Simple solutions

- ❑ **Clarity**
 - A learned technique (not necessarily intuitive)
- ❑ **Exactness**
 - A learned technique (not necessarily intuitive)
- ❑ **Testability**
 - Can a test be written to determine if an objective is fulfilled?
- ❑ **Illustrative**
 - Can the solution be pictured by the end user?
- ❑ **Assurance**
 - Independent testing of security solution

Standards authoring as a tool for clarity

- ❑ **Semi-formal language**
 - **Shall, should, may, can as active verbs**
- ❑ **Design using formal languages**
 - **SDL, UML**
- ❑ **Validation using formal languages**
 - **SDL, UML, TTCNv3**
- ❑ **Testing using formal languages**
 - **SDL, UML, TTCNv3**

Measuring our security

- ❑ To what degree are we assured our security is taken care of?
 - Is there an equivalent to the NCAP rating for cars?
- ❑ To answer this we need to be exact in our design
 - What are we securing? **ASSETS**
 - Against what? **THREATS**
 - For what? **RISK**
 - Protecting it with what? **COUNTERMEASURES**
- ❑ We also need to be exact in our claims for the design
 - It protects against this threat for this length of time
- ❑ We should be ready to test our claims
 - Evaluation of assurance

Illustrating security

- ❑ **Clarity is essential**
 - Security by obscurity cannot be tested
 - Security by secrecy is counter intuitive
- ❑ **But ... clarity is often difficult to achieve**
- ❑ **Tools, methods and language may help**
- ❑ **ETSI has proven expertise in methods to aid standardisation**
 - Guides to the use of UML, SDL, text
 - Normative language: 4 actions - shall, should, may, can



ETSI and STF292 in eEurope

- ❑ Introducing assurance rigour to standardisation
- ❑ Based on Common Criteria for IT security evaluation
 - ISO/IEC 15408
 - <http://www.commoncriteriaportal.org>
 - Offering interpretations from developer view as opposed to evaluator view
- ❑ Extending “Making Better Standards” to security
 - <http://portal.etsi.org/mbs/>
- ❑ Development of a pro-active approach to security

The role of STF268

- ❑ To introduce Common Criteria to ETSI
- ❑ To produce 4 deliverables (published and available):
 - **EG 202 387**
 - Guide to the Common Criteria for an ETSI audience
 - **ES 202 382**
 - Method and proforma for the development of Protection Profiles
 - **ES 202 383**
 - Method and proforma for the development of Security Targets
 - **TR 102 420**
 - Report on issues surrounding CC in Standards

Common Criteria

- ❑ Products offering security features always carefully evaluated (particularly by government bodies)
- ❑ Mid-90s, evaluation bodies got together to define a single set of evaluation requirements, the “Common Criteria (CC)” in ISO/IEC 15408
 - Part 1: Introduction and general model
 - Part 2: Security functional requirements
 - Part 3: Security assurance requirements
- ❑ Rapidly growing interest in security and evaluation within commercial world
- ❑ Key aspects of CC:
 - Formal evaluation process
 - Using trained evaluators
 - International recognition of results

Evaluation Assurance Levels (EAL)

- EAL 1: Functionally tested
- EAL 2: Structurally tested
- EAL 3: Methodically tested and checked
- EAL 4: Methodically designed, tested and reviewed
- EAL 5: Semiformally designed and tested
- EAL 6: Semiformally verified design and tested
- EAL 7: Formally verified design and tested

- Standards should naturally fall into the documentation levels of anything up to EAL6.



Standards and CC [1]

- ❑ CC generally used to evaluate product
- ❑ Communications products often incorporate implementations of standards
- ❑ Standards are rarely evaluated under CC
- ❑ The question for ETSI:
 - Can standards be written in a way that simplifies the evaluation of products implementing them?

Standards and CC [2]

- **Protocol standards are spiritually close to PPs**
 - **Specify implementation independent requirements**
 - **Use formalized text to specify requirements (shall, may, should...)**
 - **Use specification languages for design, validation and testing (SDL, UML, MSC, ASN.1, TTCN)**
 - **Have traceability:**
 - **Title**
 - **Version numbering**
 - **Change control**

Standards content and the PP

- ❑ Implementation independent
 - Spiritually close to PP
- ❑ Outline requirements
 - Sufficient to allow interworking
 - Open to allow innovation in implementation
- ❑ Behaviour and coding rules
 - Protocols and data
- ❑ A PP is written in a different way to a standard. It is, therefore:
 - unlikely (and undesirable) that ETSI will change the style of its standards;
 - unreasonable to expect ISO and the security community to change the way a PP is written;
 - unrealistic to expect an evaluator to find all PP information in an ETSI standard (or multiple standards);
 - inefficient to write out information twice (once in a standard and again in the PP).

“PICS” approach adopted where information is summarized in a table which includes references to text rather than the text itself.

What work needs done?

- ❑ **Method for effective vulnerability analysis**
 - Using UML for illustration and simulation
 - Template and proforma to allow simpler preparation
- ❑ **Security for the NGN**
 - Objectives
 - Requirements
 - New methods
 - Assurance
- ❑ **New techniques**
 - Digital Rights Management over networks
 - Multi-value content over networks
 - Multi-level countermeasures in networks
 - Interoperability



Need more promotion!

- ❑ **ETSI is good at standards**
 - Probably the world leader
- ❑ **ETSI is good at security**
 - Protocols (TETRA, DECT, GSM, 3GPP, TISPAN ...)
 - Algorithms (SAGE)
 - Methods (TISPAN)
- ❑ **Common Criteria and assurance are good practices**
 - Effective when applied
 - Need to be applied across ETSI

Summary

- ❑ Risk based security at core of ETSI approach
 - TVRA method and guide being developed
- ❑ Assurance ready standards development being introduced
 - PP proforma using PICS method
- ❑ Security maintenance developed with industry
 - TETRA SFPG and GSM/3G OA being good examples