



Security requirements capture from the EU regulatory framework

Scott Cadzow

C3L,
ETSI STF Expert eSecurity (TISPAN WG7)



Abstract

C3L



- Regulation
- Requirements
- ETSI's response
 - TISPAN's NGN security work
- Security modelling
 - Objectives
 - Platforms





European Regulation

C3L



- Framework directive
 - Directive 2002/21/EC of the European Parliament and of the Council on a common regulatory framework for electronic communications networks and services
- Authorisation directive
 - Directive 2002/20/EC of the European Parliament and of the Council on the authorization of electronic communications networks and services
- Access directive
 - Directive 2002/19/EC of the European Parliament and of the Council on access to, and interconnection of, electronic communications networks and associated facilities
- Privacy directive
 - Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
- Universal service directive
 - Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on Universal service and users' rights relating to electronic communications networks and services



Others of note

C3L



- Council Decision 91/396/EEC of 29 July 1991 on the introduction of a single European emergency call number
- Council Decision 92/264/EEC of 11 May 1992 on the introduction of a standard international telephone access code in the Community
- Commission Recommendation 2000/417/EC of 25 May 2000 on unbundled access to the local loop: enabling the competitive provision of a full range of electronic communications services including broadband multimedia and high-speed Internet





C3L



Not forgetting ...

- Lawful interception:
 - COM 96/C329/01: "European Union Council Resolution COM 96/C329/01 of 17 January 1995 on the Lawful Interception of Telecommunications".
- Data retention:
 - Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC



C3L

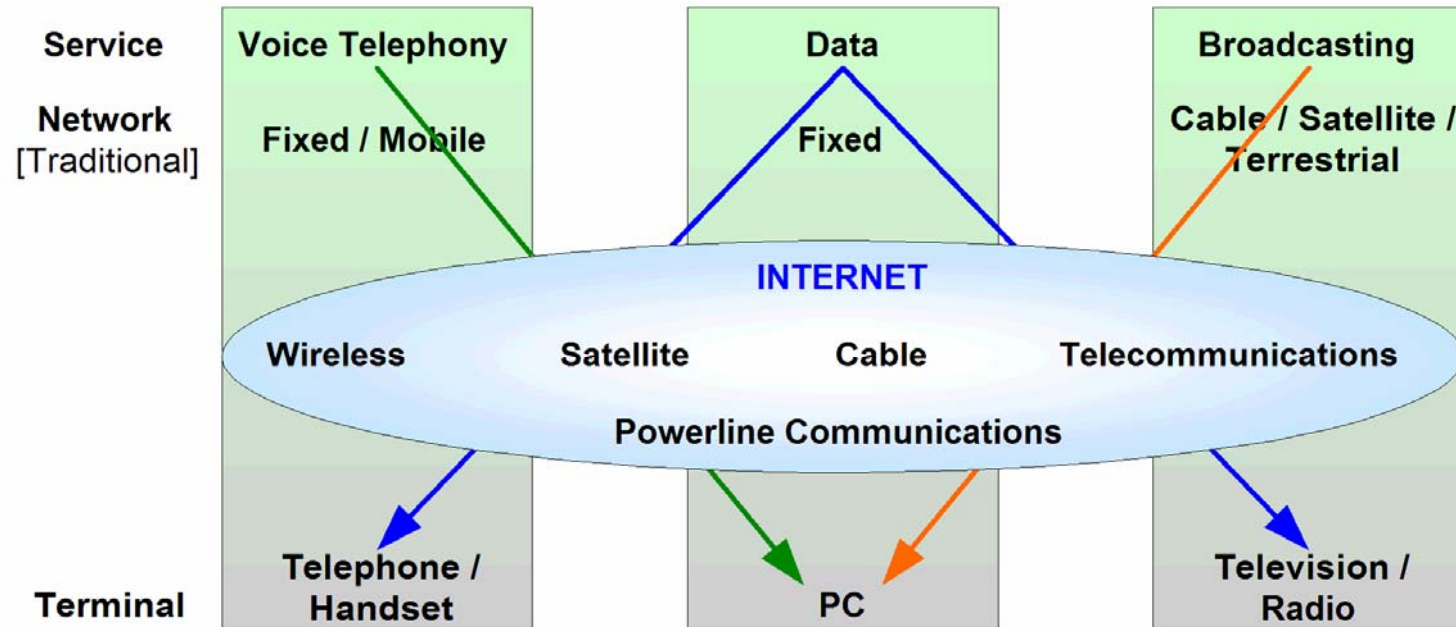


Non-telecomms regulation

- Financial regulation
 - Sarbanes-Oxley act
 - Information technology audit
 - Information technology controls
- Data privacy
- The law (national, regional ...)
- Health and Safety
- ...



Regulator View of networks?



Source: Based upon presentations provided by the European Commission

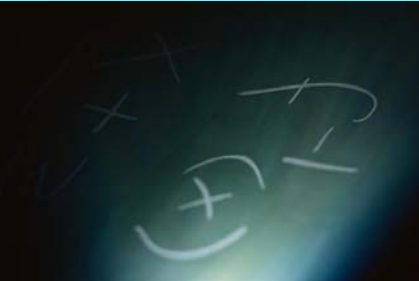


Standardization and regulation

C3L



- Regulator's standardisation benchmarks:
 - Technological neutrality
 - Removal of technical entry barriers
 - Opening up new markets and economic models.
 - Indirectly creates economies of scale
 - Encouragement of multiple representation to be able to respond to the goals of competition
- New challenges for regulation
 - Mobile networks
 - IPv6
 - NGN





C3L



Standardization - a regulatory "tool"

- Standardization is a key element in economic and commercial exchange (opening new markets, establishing economies of scale, etc.)
- Key areas regulators are worrying about:
 - management and regulation of the frequency spectrum
 - the UMTS deployment timetable
 - the ENUM protocol pinpoints what is at stake when numbering, addressing and naming systems converge.
- Market guided standardization with regulatory oversight to ensure:
 - transparency,
 - openness,
 - impartiality,
 - continuity,
 - access to publications,
 - rules for patents,
 - efficiency,
 - responsibility and consistency



C3L



MAKING BETTER STANDARDS PRACTICAL WAYS TO SUCCESS

Getting Started

What Makes
A Standard "Better"?

Market
Expectations

Protocol
Standards

Planning for
Standardization

Test
Specifications

Physical
Characteristics

Specification
Languages

Regulatory
Environment

Validating Standards





Starting point in standards

- Objectives
 - Passive statements of intent (WHAT)
 - Compliance to regulation?
 - Meet the needs of the market?
 - Meet the needs of shareholders?
- Requirements
 - Active statements of intent (HOW)
 - Realize the objectives
 - Testable once implemented, linked to objectives

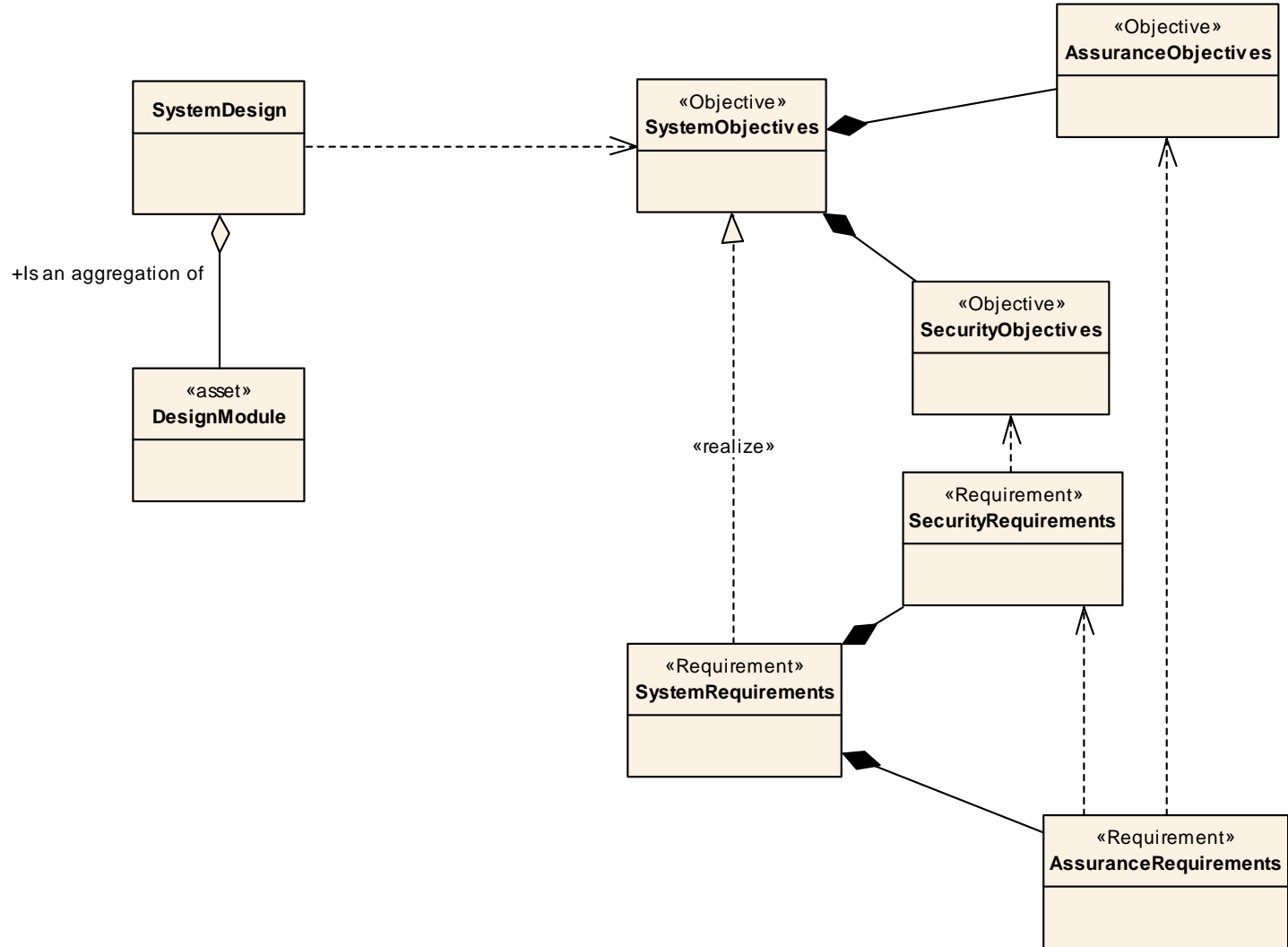


Root relationships

C3L



cd General model





Requirements vs. Objectives

■ Objective

- the expression of what a (security) system should be able to do in very broad terms
- EXAMPLE: The asset must identify and authenticate all users before granting access to the system.

■ Requirement

- a detailed specification of how an objective is achieved.
- EXAMPLE: A user shall be successfully identified and authenticated to the asset by means of a user name and password before all other interactions between the asset and that user.



C3L



Understanding of security

- A **Threat**, enacted by a **Threat Agent**, may lead to an **Unwanted Incident** breaking certain pre-defined **security objectives**
- Aim is to avoid **Unwanted Incidents**
- Countermeasures restrict the ability of **threat agents** to operate



C3L



Unwanted incidents

- What security countermeasures have to avoid
- Answers the question of why the countermeasure exists
- Strongly tied to objectives
- Objectives should link to regulatory compliance

Specific review of directives #1

■ Privacy directive: Article 4: Security

- "1. The provider of a publicly available electronic communications service must take appropriate technical and organizational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.
- 2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved."

■ Interpretation

- In order to determine that the security of a system has been breached the ECS or ECN provider has calculated the risk to the system through a systemic threat and risk analysis and is actively monitoring the system to determine when it is under attack and when the level of acceptable risk has been breached.



C3L



Specific review of directives #2

- Privacy directive: Article 5: Confidentiality of the communications
 - “[...] Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC [27], inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user. ”
- **Interpretation**
 - So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the **knowledge and consent of the users** concerned. The release of data made available by such devices should only be made only with the consent of the user concerned. The user should also have the right to withdraw consent.



C3L



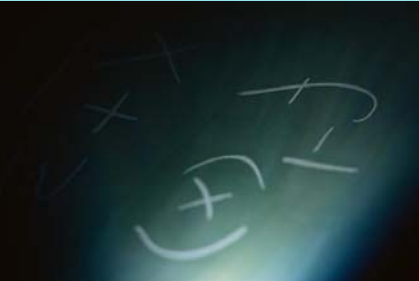


Models from regulation

C3L



- In the “biblical” form:
 - A begat B begat C begat ...
- Cause to effect
 - Regulation A gives rise to system objective B where compliance is achieved through requirements C,D,E ...

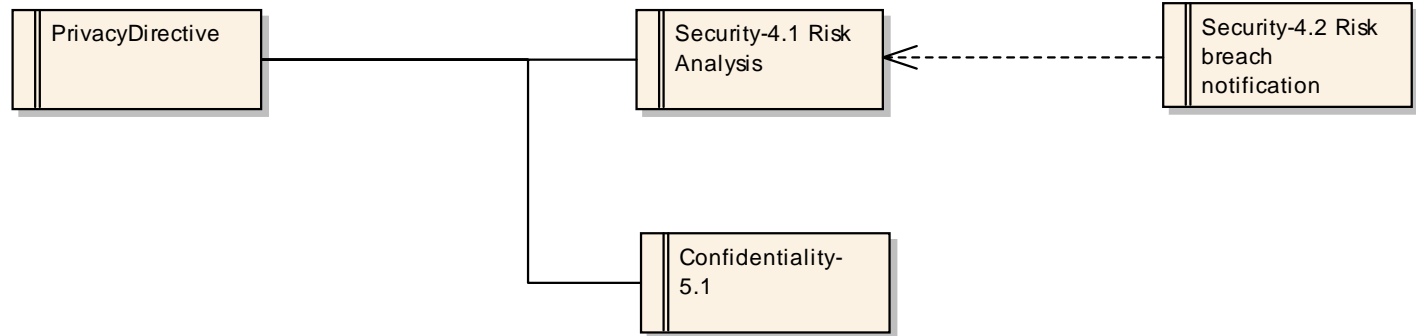




Requirements modelling



req UCI Requirements Model





Risk analysis in standards

C3L

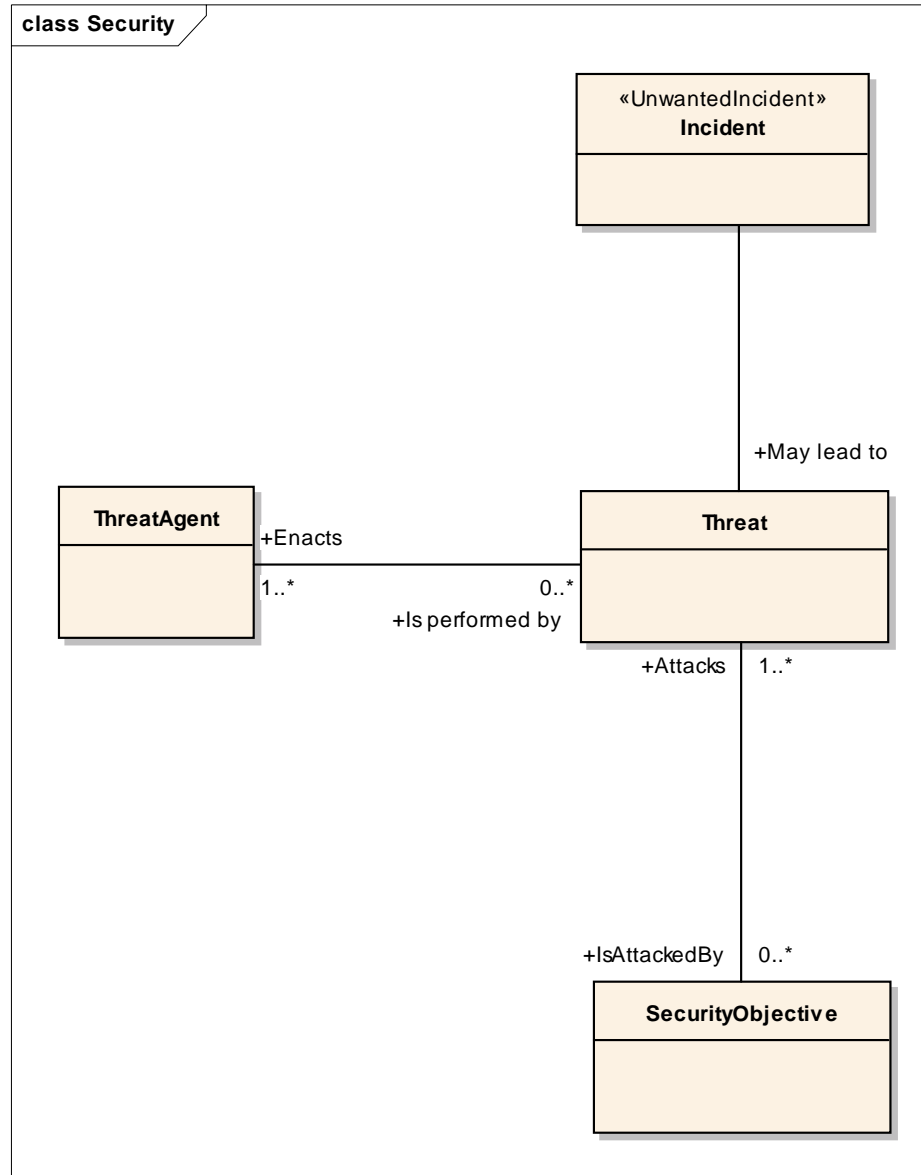
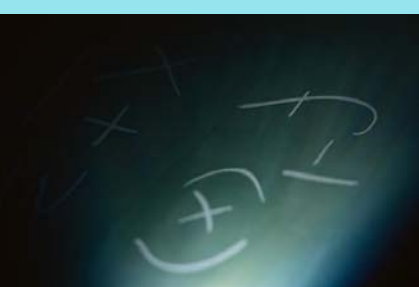


- Risk analysis in standards is different from risk analysis in real life
 - Aim is to ensure core capabilities to protect users are developed
 - Compliance with legal framework that affects all users
- Need to bring technical and real-life worlds together
 - Users don't buy into technical worlds
- Guidelines and methods developed at ETSI
 - eTVRA method
 - Database of threats, assets, systems
 - Register of risk
 - Making better standards
 - Design methods and tools to make it clear what the standardised thing does





The root model for eTVRA





ETSI in the regulation space

- Specific groups
 - OCG ECN&S
 - Article 17 of framework directive
 - ERM
 - Management of R&TTE
 - TC LI
 - Lawful interception and data retention
 - Secretariat
 - Advice
- Technology groups
 - ???



NGN and regulation

C3L



- Seen as a regulation “new challenge”
- TISPAN and 3GPP expanding technical specifications
 - Vice-chair with regulatory responsibility
 - LI covered
 - NNA covered (E.164 and UCI)





Areas being developed #1

C3L



- Risk analysis
 - Underway for NGN subsystems
 - Using eTVRA methodology
 - Providing rationale for detail security developments
 - Regulation analysis key in determining objectives





Areas being developed #2

C3L



- Risk monitoring
 - Relationship with BUGYO project
 - Probe based real-time risk measurement
 - eTVRA used in static analysis phase
 - Path for future standardisation



Summary

- Regulation is extensive
- Compliance to regulation requires detail analysis
- Regulation impacts network design
- Compliance requires careful provision of security countermeasures



C3L



Questions

... maybe some answers