Information & Communication Security (SS 15)

Evaluation Criteria

Dr. Jetzabel Serna-Olvera
@sernaolverajm
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
www.m-chair.de

Agenda

- Motivation
- Where do the Criteria come from?
- What is being Evaluated?
- Organisation of Protection Profiles

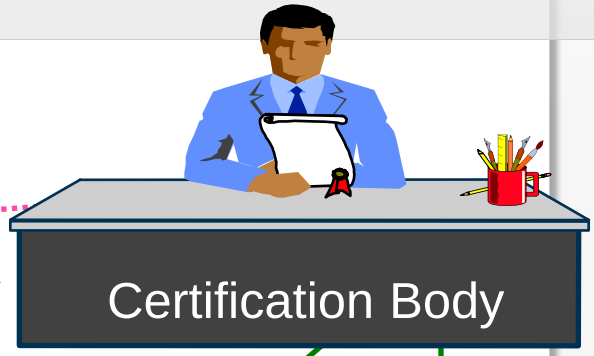
Why IT Security Certification and Evaluation ?

- People use **more and more complex** technology to interact in the information society
- Users need **help what technology** to trust:
  - Does the **offered system, product or service** meet **the requirements?**
  - Does **it** fulfil **legal requirements?**
  - Is the given organization trustworthy?
- Vendors‘ marketing information does not (always) help
- Some kind of independent evaluation and certification is needed
  - Check **products, systems, services or organization**
  - **Report** on their **security/privacy properties**

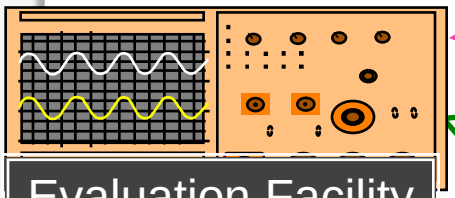
The Certification and Evaluation Process

Monitoring

3



Certification Body



Evaluation Facility (ITSEF)

Evaluation Report

4

5

4

Certificate + Certification Report

Product/System TOE

2

Sponsor

1

Application for Certification

Who is using Certification ?

- Vendors
  - Product Evaluation
  - Product Marketing
  - Image
- Procurers / Users
  - Decision Support
  - System Evaluation
- Evaluation Facilities
  - Market
- Certification Bodies
  - Task
  - Market

Certifications and Users

Certificate +
Certification Report

- How to compare certificates and evaluation results?

Why standardized Criteria for IT Security Evaluation?

- The IT market is complex.
- Standardized criteria
  - ease **comparing** evaluation results
  - avoid re-evaluation in each country
    „One test per planet !“
- Criteria can help to **structure evaluation results** (and **security requirements**).

mobile business

Agenda

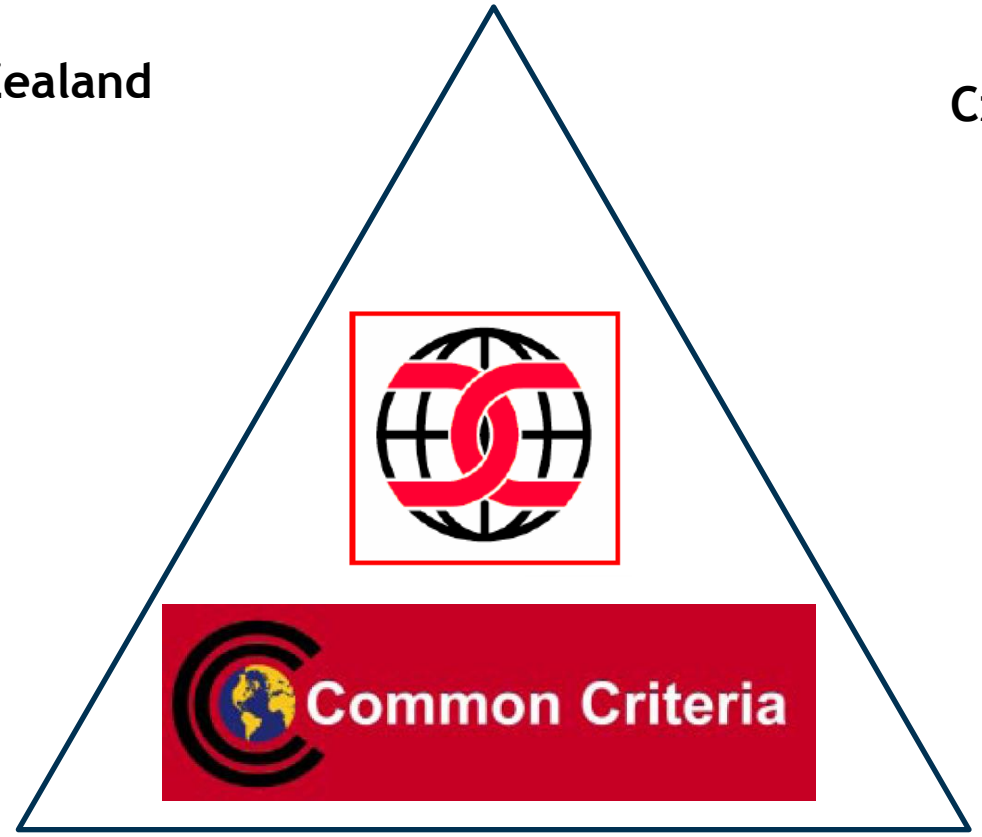
- Motivation
- Where do the Criteria come from?
- What is being Evaluated?
- Organisation of Protection Profiles

Who writes which Criteria?

- 1983/85 **USA** DoD — **TCSEC** (Orange Book)
  Trusted **C**omputer **S**ystem **E**valuation **C**riteria
- 1990/91 **EU** Commission — **ITSEC**
  Information **T**echnology **S**ecurity **E**valuation **C**riteria V. 1.2
- 1990/?? **ISO/IEC** JTC 1/SC 27/WG 3 — **ISO-ECITS**
  Evaluation **C**riteria for **IT S**ecurity ISO/IEC 15408:1999,2005,2009
- 1992/93 **Canada** CSSC/CSE — **CTCPEC**
  Canadian **T**rusted **C**omputer **P**roduct **E**valuation **C**riteria V. 3.0
- 1992/93 **USA** NIST&NSA — **FC-ITS**
  Federal **C**riteria for **I**nformation **T**echnology **S**ecurity Draft V. 1.0
- 1993/?? **CDN/D/F/GB/NL/USA/…** Agencies (CCxB) — **CC**
  Common **C**riteria for IT Security Evaluation V. 3.1

International Acceptance of the CC 2007

Australia and New Zealand
Canada
France
Germany
Japan
Netherlands
Norway
Republic of Korea
Spain
United Kingdom
United States



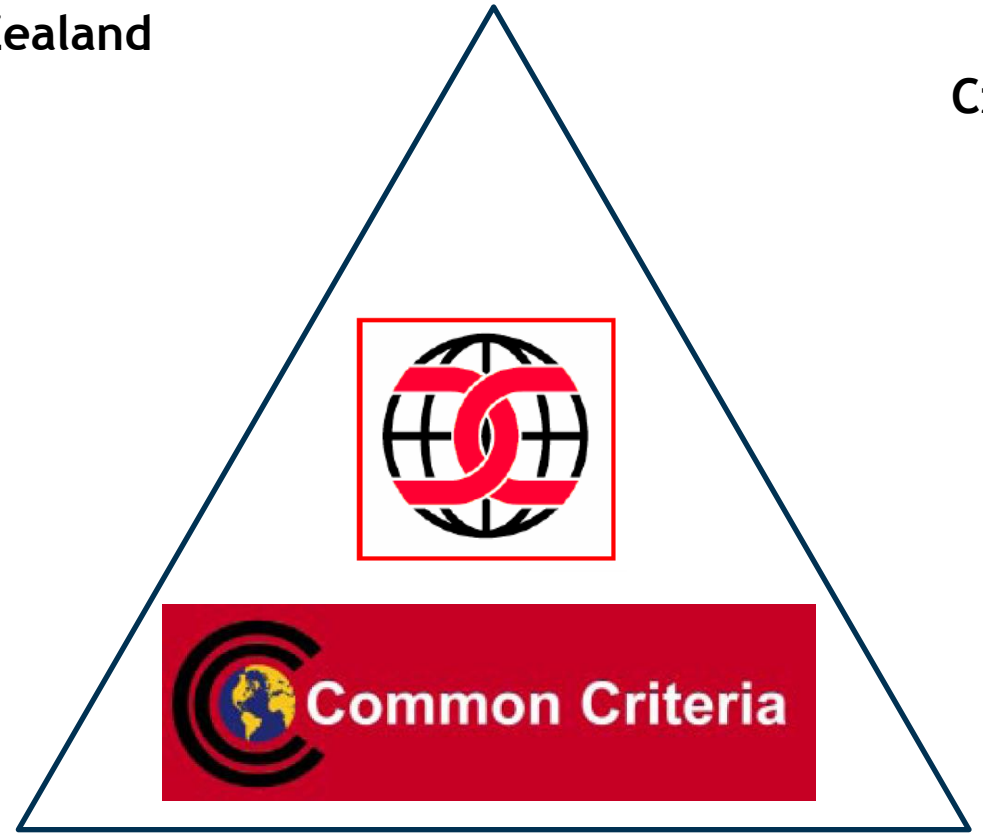
Austria
Czech Republic
Denmark
Finland
Greece
Hungary
India
Israel
Italy
Singapore
Sweden
Turkey

“Certificate Authorizing” “Certificate Consuming”

[CCP, 2007]

International Acceptance of the CC 2015

Australia and New Zealand
Canada
France
Germany
India
Italy
Japan
Malaysia
Netherlands
Norway
Republic of Korea
Spain
Sweden
Turkey
United Kingdom
United States



Austria
Czech Republic
Denmark
Finland
Greece
Hungary
Israel
Pakistan
Singapore

“Certificate Authorizing” “Certificate Consuming”

[CCP, 2015]

mobile business

Agenda

- Motivation
- Where do the Criteria come from?
- What is being Evaluated?
- Organisation of Protection Profiles

What is being Evaluated?

2 Types of **Targets of Evaluations (TOE)**

- **Products**
- Operational Environment not known during Evaluation
- Usually COTS Product, e.g.
  - Standard Software
  - PC Security Tool
  - Operating System
  - Chipcard Reader
  - Communication Server
  - Oneway Function
  - …

- **Systems**
- Operational Environment is known and part of the Risk Analysis, e.g.
  - Internal Military System
  - Banking System used by Customers
  - …
- Combinations of Products

Security á la Criteria

Security: Functionality & Assurance

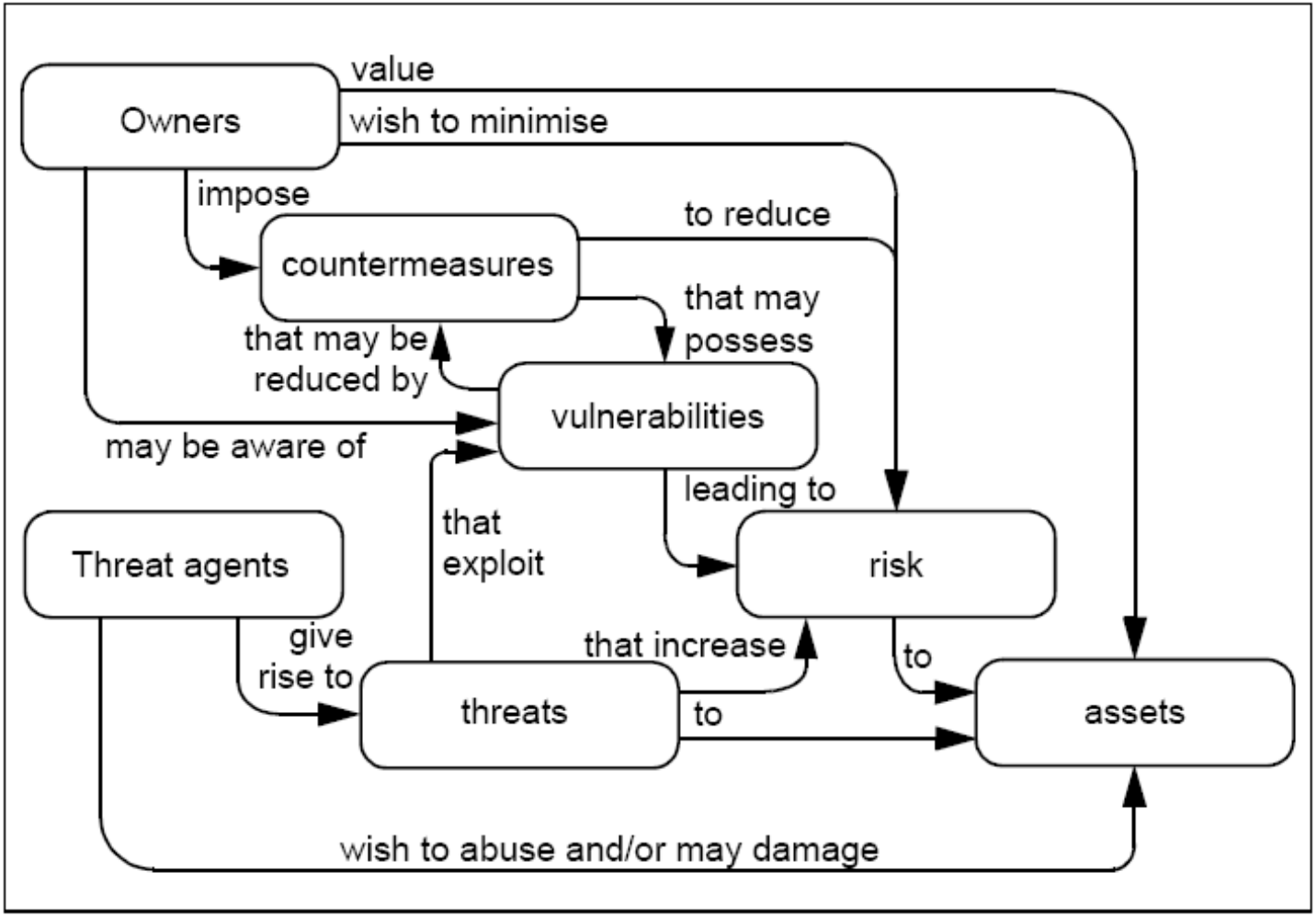
- **Functionality**
- "What can the TOE do to be secure?"
- Aspects of
  - Confidentiality
  - Integrity
  - Availability
  - Accountability
- Protection for users and customers ??

- **Assurance**
- "What was done to assure that the TOE does what it shall do / does not what it shouldn't do?"
- Intensity of evaluation
- Correctness of implementation
- Strength of mechanisms, e.g. crypto (but …)
- Possible strength of attackers

The Common Criteria approach

- Determine Threats
- Define Security Policy
- Select Functional Requirements
- Evaluate against Assurance Requirements
- Privacy treated as a part of Security, i.e. as part of Multilateral Security

Security concepts and relationships



[CC2006]

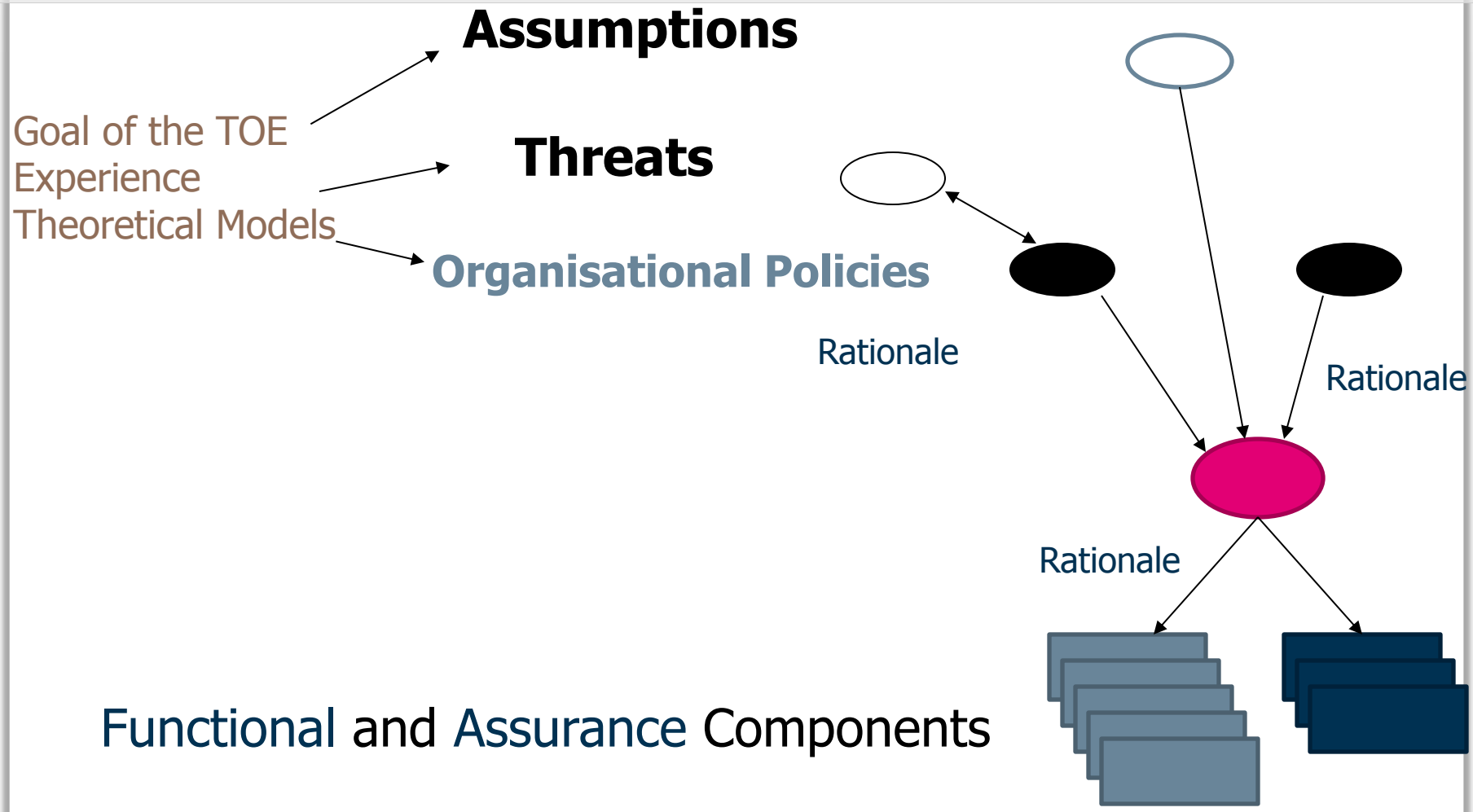
Agenda

- Motivation
- Where do the Criteria come from?
- What is being Evaluated?
- Organisation of Protection Profiles

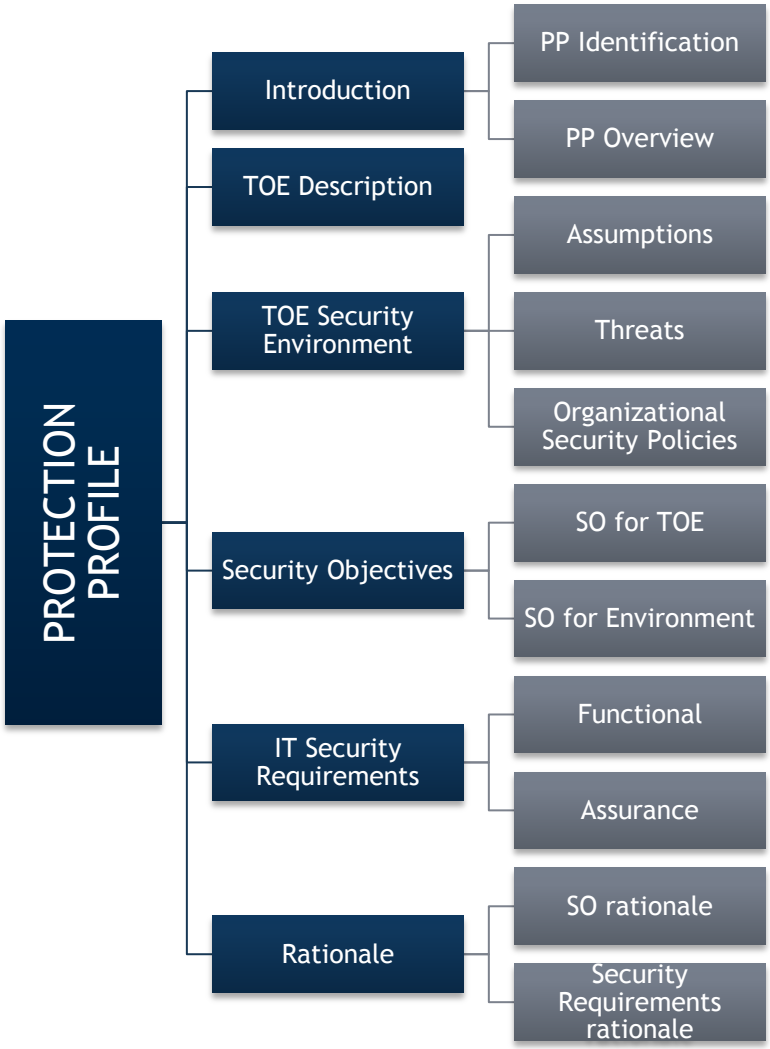
What is a Protection Profile (PP)?

- **"Your"** criteria **subset**
- **Implementation independent** set
  - of security objectives and **requirements**
  - for products/systems that meet **similar user needs** for IT security
- To be **user driven** (formulated by user groups)
- Help to **rationalise security requirements**
- To be a **reference** for **Security Targets** of concrete **TOEs**
- **Examples:**
  - Firewalls
  - C2-TCSEC
  - Role based access control
  - Smart Cards (SCSUG, VISA)
  - Mix networks
  - Electronic Voting Systems (BSI, GI)
  - Smart Meters (BSI)

How a Protection Profile works



Content of a Protection Profile



[CC2006]

PP introduction

- PP identification

  The identification shall provide the labelling and descriptive information about the TOE inclusive some keywords and existing cross-references

  Example:

  Protection Profile for an Unobservable Message Delivery Application

PP Description (1/2)

- The Description shall provide a narrative overview.
- It shall be as detailed that it allows a potential user to decide whether the PP is of potential usage or not.
- It also should be as meaningful enough to stand as an abstract alone.

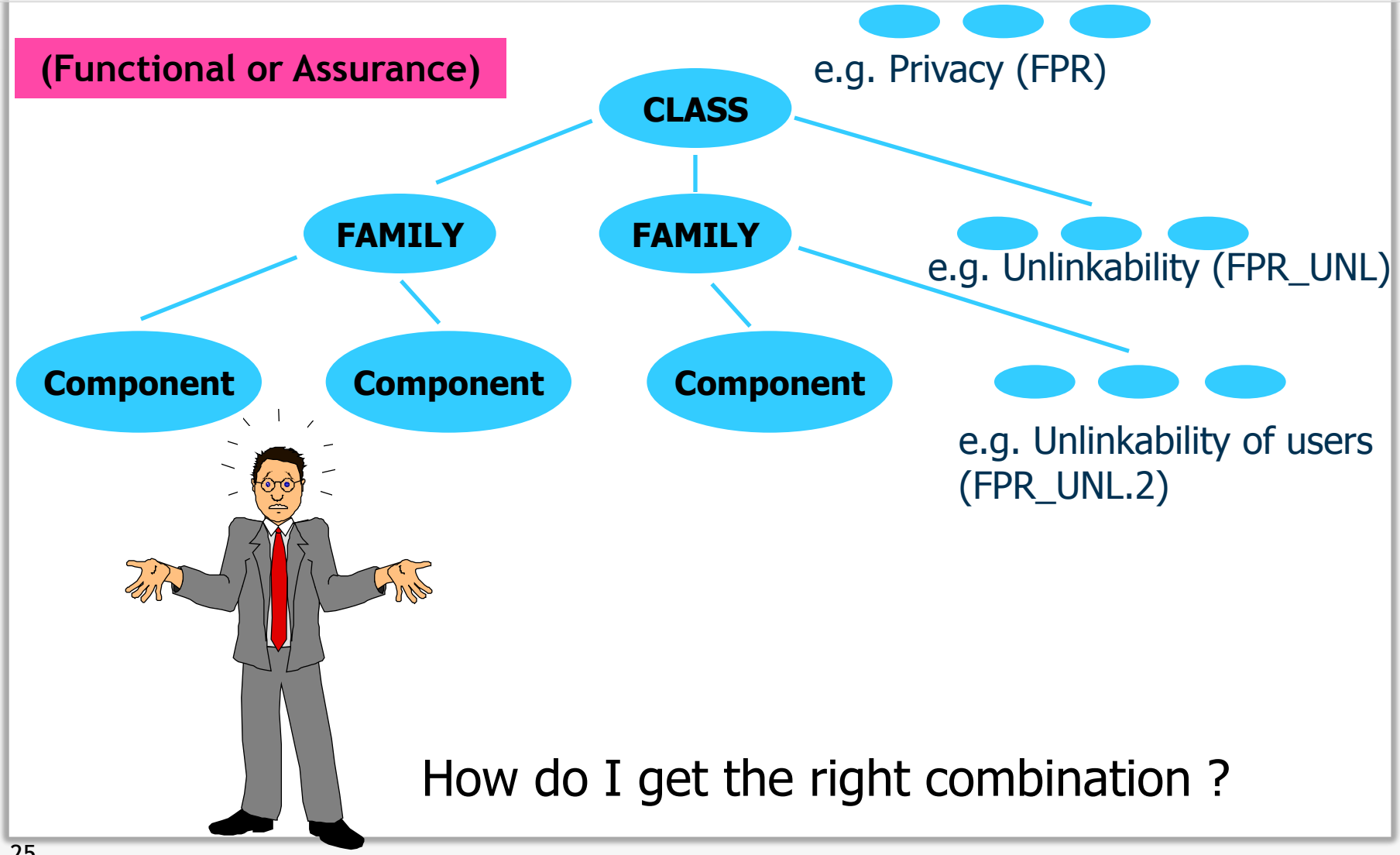
PP Description (2/2)

- Example:

- A Mix is an anonymous remailer application with the goal of hiding the link between the origin and destination of the message transiting through it… .
- Keywords: Mix, anonymous electronic mail

Criteria Elements

(Functional or Assurance)



How do I get the right combination ?

TOE Security environment

- This section contains details about:
  - Assumptions (A)
    - Assumptions about the security aspects of the environment in which the TOE will be used or is intend to be used.
  - Threats (T)
    - Lists possible threats to the assets against which specific protection within the TOE or its environment is required.
  - Organisational security policies (O)
    - Rules and organisational security policy statements with which the TOE must comply

Example Assumptions (1/2)

- A.PhysSec
  - **Users** take care of **securing** their **physical access** to the message traffic handled by the TOE.
- A.MinimalConnectivity
  - **No** attacker is able to **block all access points** of the user to the mix network.
- A.MinimalTrust
  - **Not all** nodes (**mixes**) of the network are **subverted**.

An example Threat Collection

- T.UntrustworthyMix
  - Some mix(es) in the network may be compromised and hold, process and/or disclose information useful to trace, and/or reveal the content of, communications.
- T.MixConspiracy
  - Some mixes in the network may be compromised and share information useful to trace, and/or reveal the content of, communications.
    - *This threat represents an extension to the T.UntrustworthyMix threat, in that it introduces the concept of information sharing between parts of the TOE.*

An example of Organisational Security Policies

- O.Anonymity
  - The TOE shall provide for an anonymous message delivery service; that is, the recipient of a message shall not be able to know the origin of the message, unless the author expressly inserts this information in the message body.
- O.Untraceability
  - The TOE shall provide for an untraceable message delivery service; this means that, taken any message transiting through the system at any time, it shall not be possible to obtain enough information to link its origin and destination users.

Relevant Security Objectives (1/2)

- SO.DivideSecurityInformation
  - The TOE shall be constructed as to provide the user the ability, and enforce the correct use of such ability, of determining the allocation of unlinkability-relevant data among different parts of the TOE.
- SO.DivideSecurityProcessing
  - The TOE shall provide to the user the ability, and enforce the correct use of such ability, of freely choosing a combination of mix nodes among which to allocate the processing activities achieving unlinkability.
- SO.EnforceTrustDistribution
  - The TOE shall be constructed to enforce the user's choice of information and processing distribution.

Security Objectives to Threats and Organisational Policies mapping

	T.DenialOfService	T.MessageInterception	T.Misuse	T.MIXPeek	T.OneStepPath	T.TOESubstitution	T.UnreliableNetwork	TE.MIXConspiracy	O.Anonymity	O.Untraceability
SO.Anonymity									*	
SO.ConcealMessages		*				*				
SO.DistributedTOE	*									*
SO.DivideTrust					*					*
SO.ErrorDetection							*			
SO.KeyManagement						*				
SO.MinKnowledge				*				*		*
SO.NoResidualInformation										*
SO.ProperUse			*							
SOE.IndependentAdministration								*		*

Relevant Functional Requirements

- FCS_CKM.1 Cryptographic key generation
- FDP_ACC.2 Complete access control
- FDP_ACF.1 Security attribute based access control
- FDP_IRC.2 Full information retention control
- FDP_RIP.2 Full residual information protection
- FIA_ATD.1 User attribute definition
- FIA_UID.1 Timing of identification
- FMT_MSA.1 Management of security attributes
- FMT_MSA.2 Secure security attributes
- FMT_MSA.3 Static attribute initialisation
- FMT_SMR.1 Security roles
- FPR_ANO.2 Anonymity without soliciting information
- FPR_TRD.2 Allocation of information assets
- FPR_TRD.3 Allocation of processing activities

Functional Requirements to Security Objectives mapping

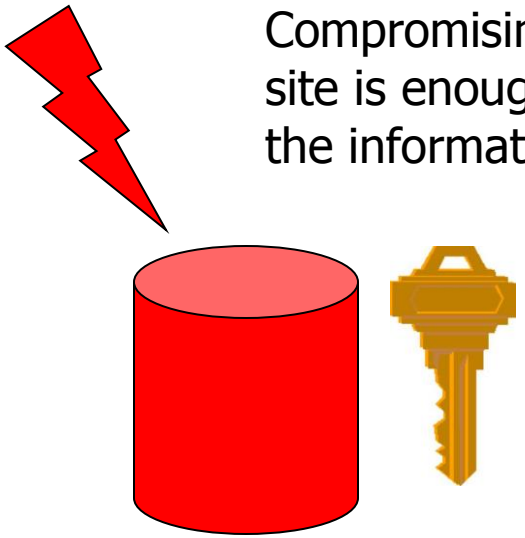
	FCS_COP.1	FCS_CKM.1	FCS_CKM.2	FCS_CKM.4	FDP_IFC.1	FDP_ITT.1	FDP_ITT.3	FDP_RIP.2	FMT_MSA.1	FMT_MSA.2	FMT_MSA.3	FPR_ANO.2	FPR_UNL.1 (1)	FPR_UNL.1 (2)	FPR_UNO.2	FPT_FLS.1	FPT_ITT.1	FPT_ITT.3	FTP_TRP.1
SO.Anonymity												*	*						
SO.ConcealMessages	*				*	*											*		*
SO.DistributedTOE															*	*			
SO.DivideTrust									*	*	*								
SO.ErrorDetection							*											*	
SO.KeyManagement	*	*	*	*					*	*	*								
SO.MinKnowledge	*												*	*	*				
SO.NoResidualInformation								*											
SO.ProperUse										*	*								

Example: Distribution of Trust

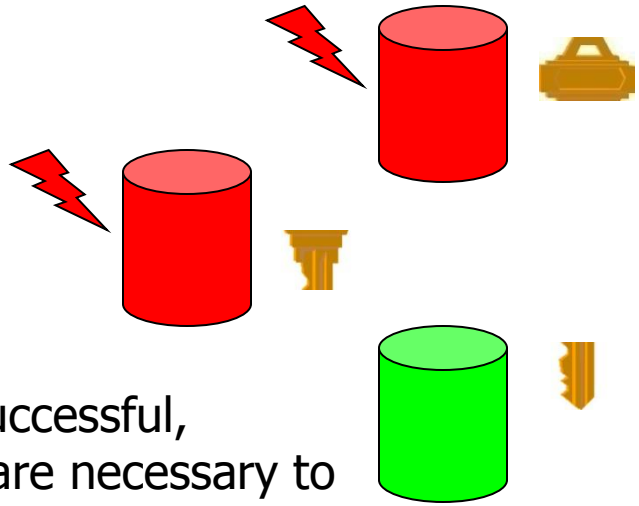
Decentralise Trust: reduce damage in the case of

- successful external attack
- malicious or careless management

Centralized trust vs. Distributed trust



Compromising a single site is enough to access the information



Many, successful, attacks are necessary to access the information

mobile business

Distribution of Trust

- Define “Administrative Domains”
  - Each domain is administered and operated independently from the others
  - The administrators of one domain do not have access to the others
- Set requirements on the allocation of
  - information
  - processing activities (generates information)

References

- [CCP] Commoncriteriaportal.org, www.commoncriteriaportal.org, accessed 2007-01-23, 2011-02-01, 2012-07-02
- [CC2006] Common Criteria for Information Technology Security Evaluation, Version 3.1, September 2006
- [NSA2003] National Security Agency: Fact Sheet, National Information Assurance Acquisition Policy (Includes deferred compliance guidelines and procedures), July 2003, http://niap.nist.gov/cc-scheme/nstissp_11_revised_factsheet.pdf
- Kai Rannenberg: Zertifizierung mehrseitiger IT-Sicherheit – Kriterien und organisatorische Rahmenbedingungen; Reihe DuD-Fachbeiträge im Verlag Vieweg, Braunschweig u.a. 1998; ISBN 3-528-05666-5; 250 Seiten
- Kai Rannenberg: IT Security Certification and Criteria – Progress, Problems and Perspectives; pp. 1-10 in Sihan Qing, Jan H.P. Eloff: Information Security for Global Information Infrastructures; Proceedings of the 16th Annual Working Conference on Information Security (IFIP/SEC 2000); August 22-24, 2000, Beijing, China; Kluwer Academic Publishers, Boston; ISBN 0-7923-7914-4
- Kai Rannenberg; Giovanni Iachello,
  Protection Profiles for Remailer Mixes
  In: Pp. 181-230 in Hannes Federrath: Designing Privacy Enhancing Technologies - Post-Proceedings of the International Workshop on Design Issues in Anonymity and Unobservability; July 25-26, 2000, Berkeley

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Dr. Jetzabel M. Serna-Olvera
Goethe University Frankfurt
E-Mail: Jetzabel.Serna-Olvera@m-chair.de
WWW: www.m-chair.de