



7th ICCG

Design and Development of a Knowledge-based Tool for ST Developers Based CC V3.1

Soka University
JAPAN

Guillermo Horacio RAMIREZ CACERES

Yoshimi TESHIGAWARA

Graduate School of Engineering, Soka University, Tokyo, Japan

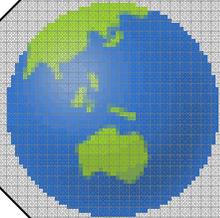
E-mail:{guillerm,teshiga}@soka.ac.jp

21 September 2006



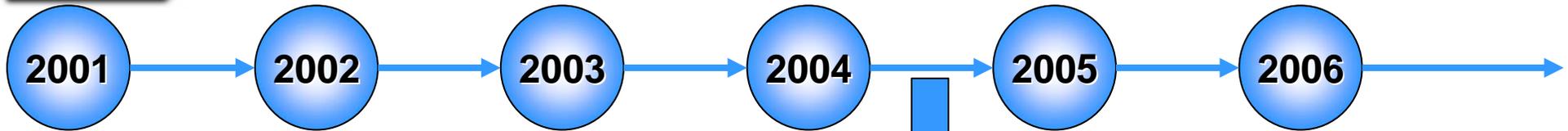
Contents

- Introduction
- Research Issues
- Fundamental Research Target
- Knowledge-base Architecture
- Conclusion
- Future Works



Introduction

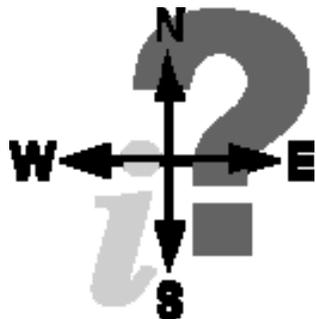
Introduction



International Standard

ISO 15446

ISO 15408

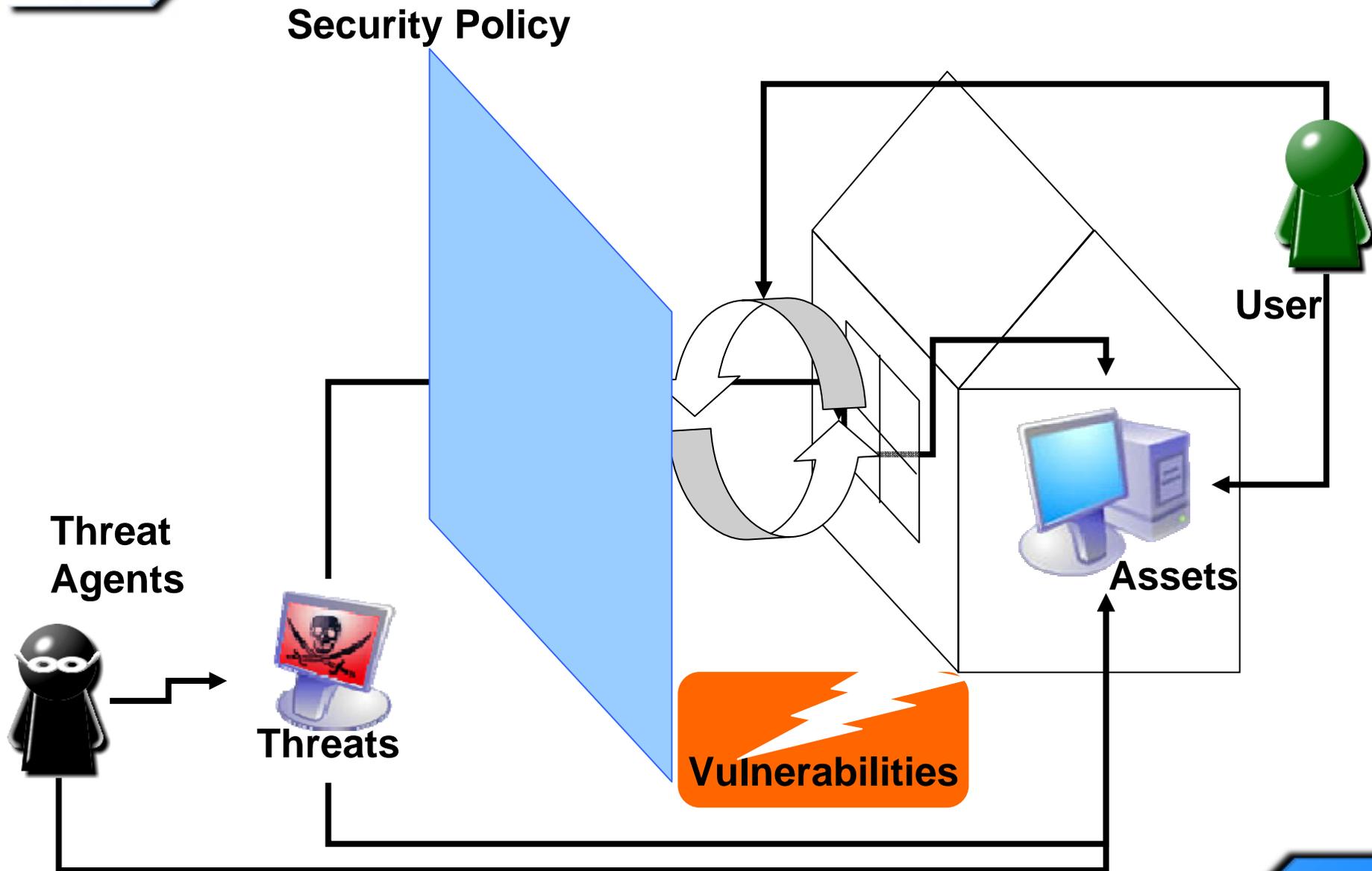


- ST developers can find the necessary information in ISO/IEC 15408
- ST Developer's knowledge shortage can be supplemented by using this tool to access the necessary information in international standards

- The new version of Knowledge base also include a self training tool.

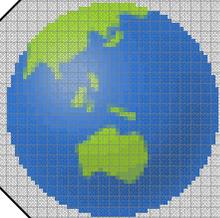
- The technical languages used with the large number of new words

Security Concepts





Research Issues



Research Issues

● Knowledge required

- ISO/IEC 15408 consists of approximately 700 pages.
- ISO/IEC TR 15446 consists of approximately 180 pages.
- The ST developer must read many times when trying to create a ST for evaluation.

● Relevant experience

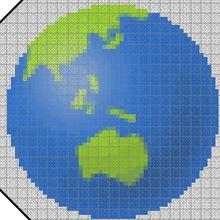
- The ST developer must write a document between 50 and 200 pages long.
- STs or PPs evaluated by CC are published on the Internet, and the ST developer can use this evaluated STs or PPs as references.

2.5 The PP and ST Development Process

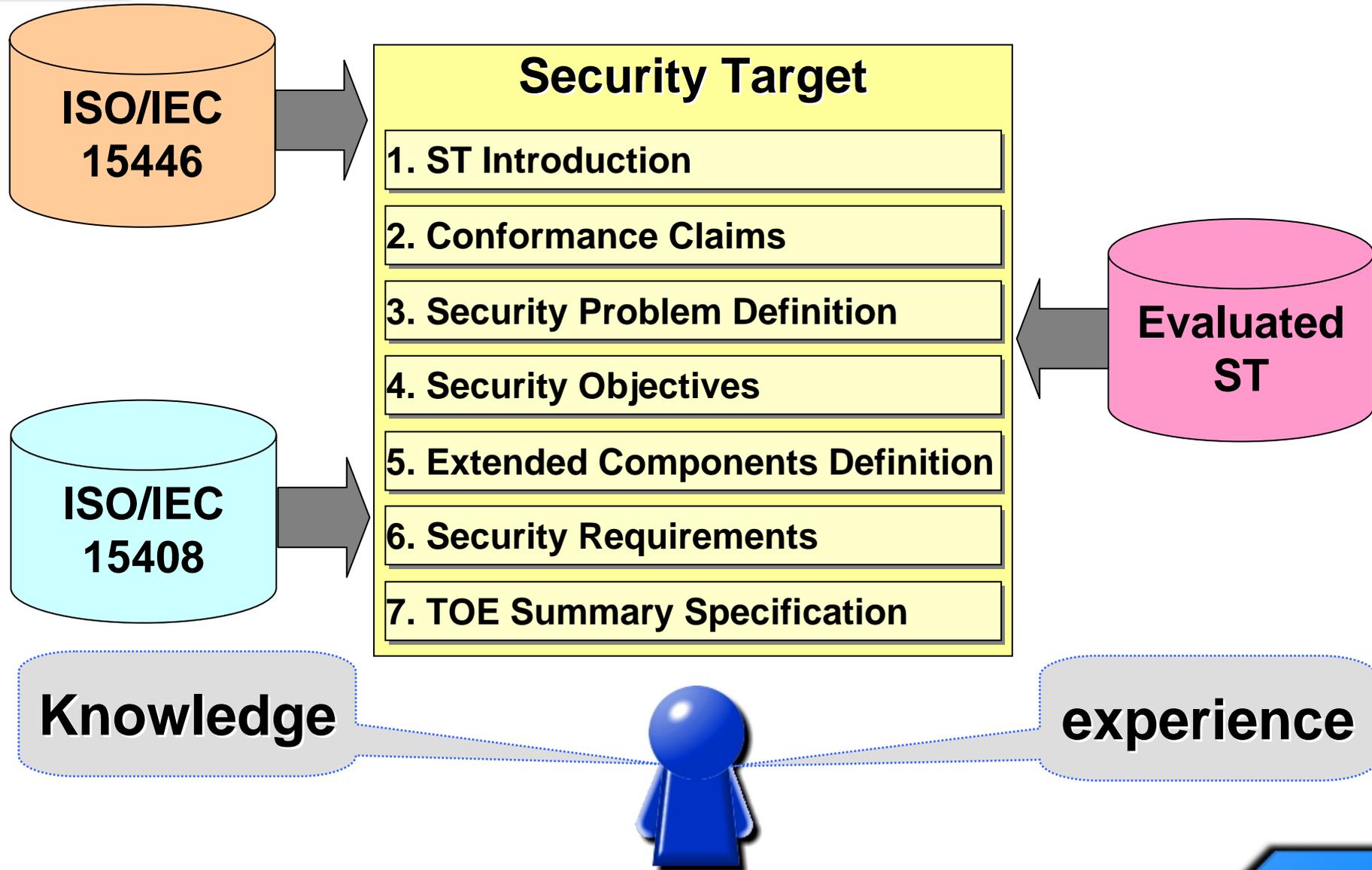
The presentation of the requirements for PPs and STs in [15408-1] annexes B and C, and in [15408-3] clauses 3 to 5, might suggest that it is expected that PPs and STs are always developed in a logical ‘top-down’ manner, e.g. (in the case of a PP) that: (47)

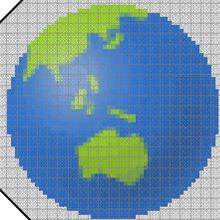
1.4.3 Usage of the PP and ST

A PP may be used to define a ‘standard’ set of security requirements with which one or more products may claim compliance, or which systems used for a particular purpose within an organisation must comply. (See [15408-1] subclause 2.3 for the definition of the terms *product* and *system*, and also [15408-1] subclause 4.1.2 for a general discussion of the distinction between the two). A PP may apply to a particular type of TOE (e.g. operating system, database management system, smartcard, firewall, and so on), or it could apply to a set of products grouped together in a *composite* TOE (system or product). (21)



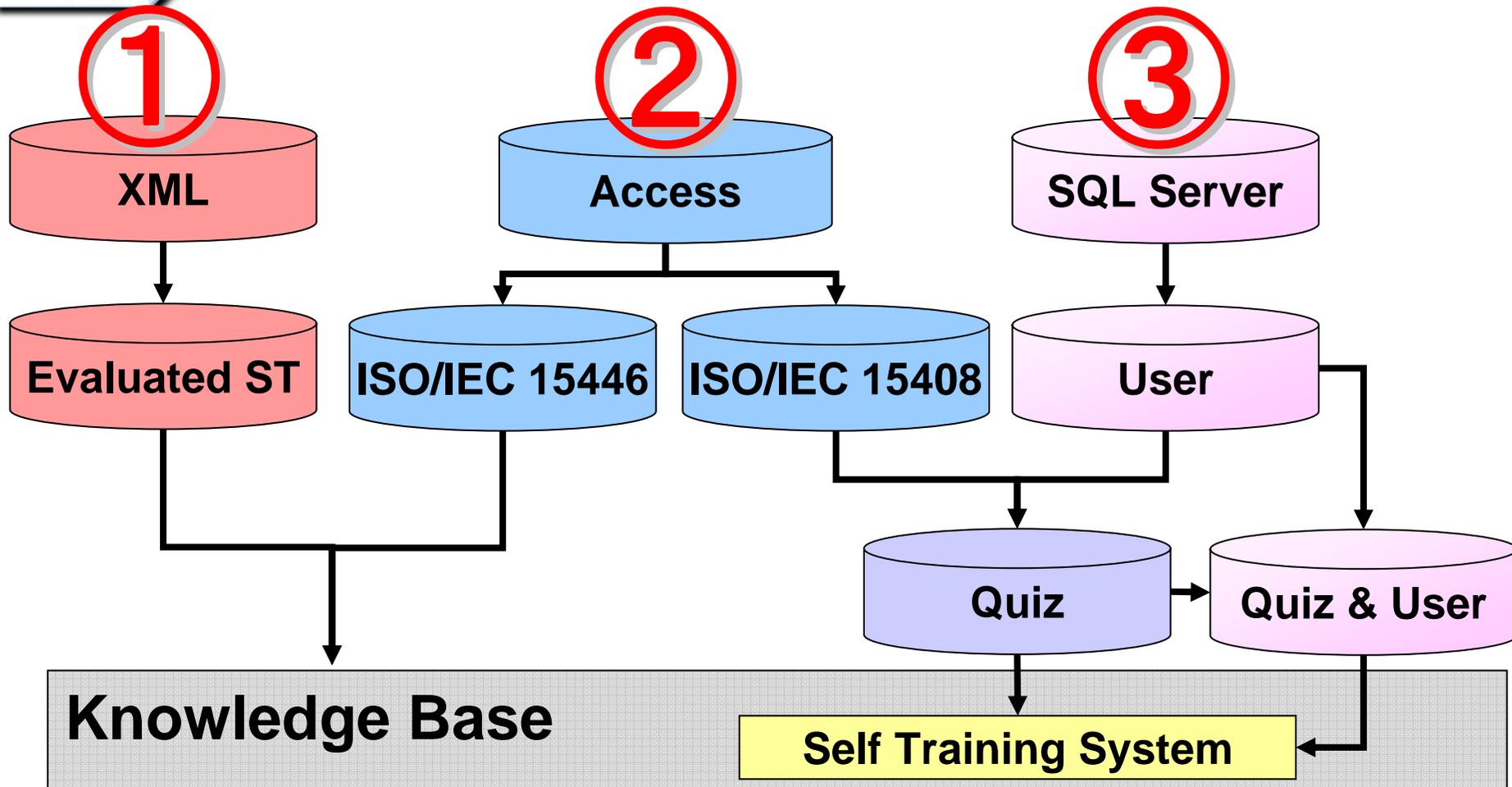
Fundamental Research Target

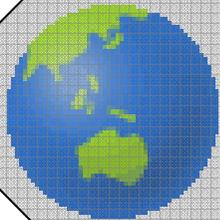




Knowledge-base Architecture

Knowledge base Architecture





Published ST Knowledge-base

1

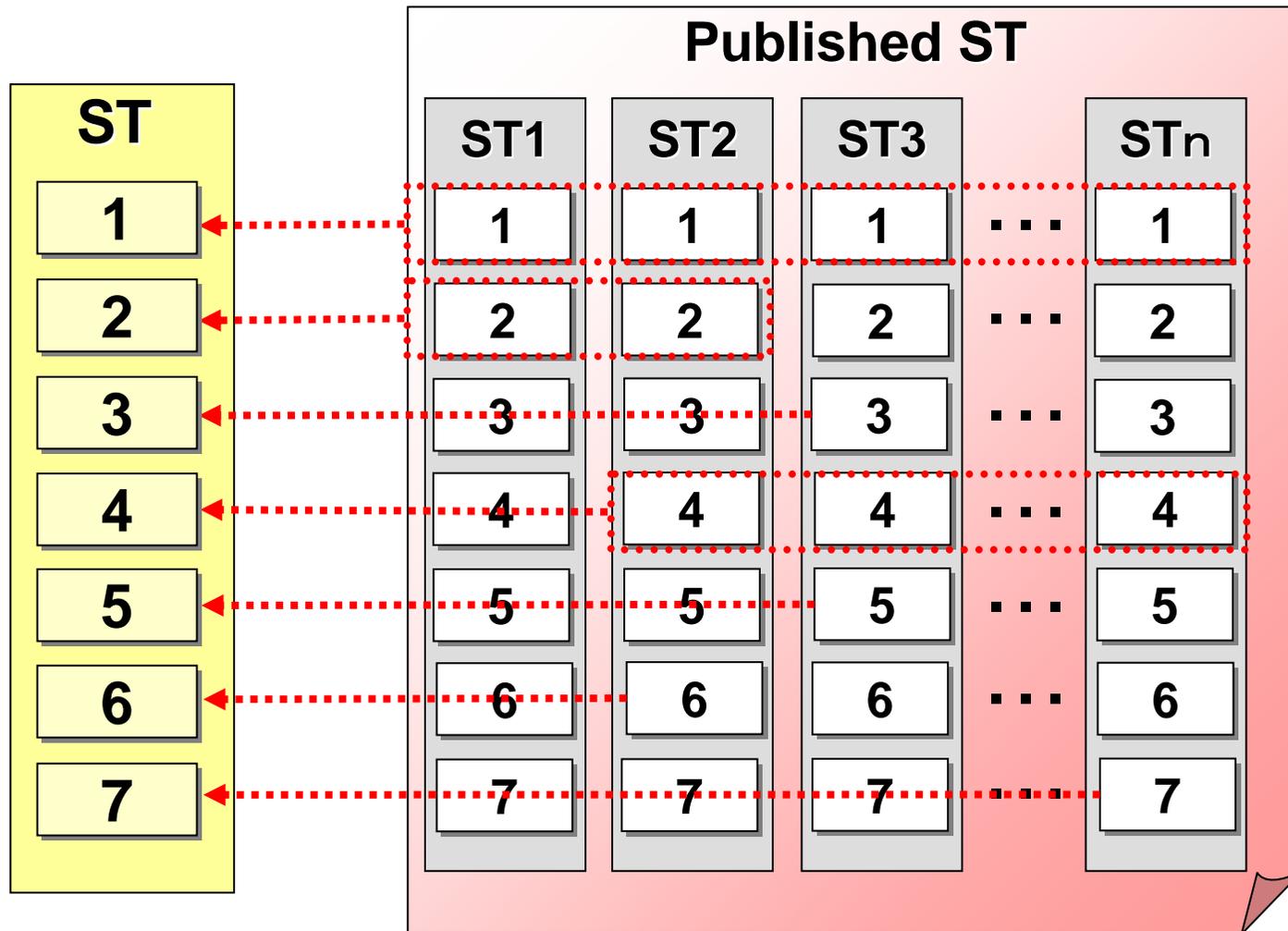
Published ST Knowledge-base



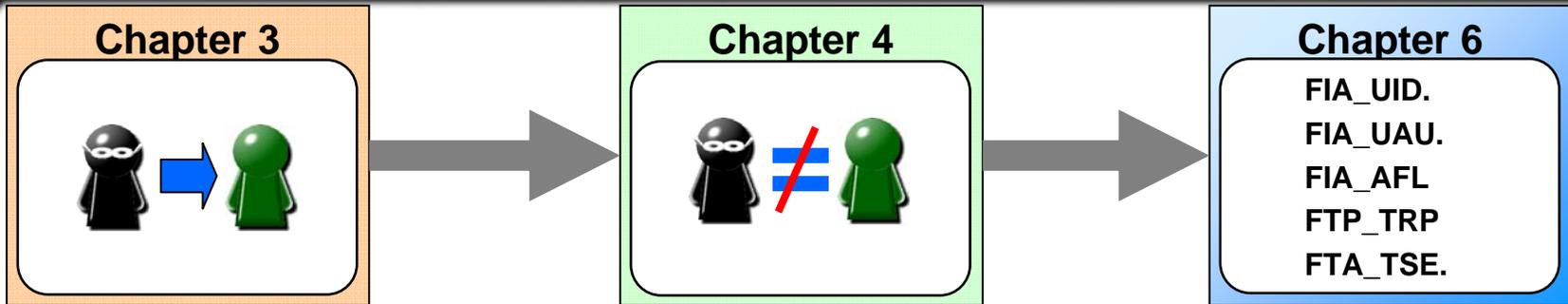
- IT products evaluated and authenticated based on CC are published on the Web Page of each country

ST_Id	ST_Tipo	Product	Manufacturer	EAL	EAL_Observation	Date	Country	ST_PDF
39	Firewalls	Stonesoft StoneGate Firewall V2.0.5	Stonesoft Corporation	EAL 4	, augmented ALC_FLR1	9/03	USA	<input checked="" type="checkbox"/>
40	Firewalls	Symantec Enterprise Firewall, v8.0	Symantec Corporation	EAL 4		7/04	England	<input type="checkbox"/>
41	Firewalls	Symantec Enterprise Firewall, v7.0.4 running	Symantec Corporation	EAL 4		9/03	England	<input type="checkbox"/>
42	Firewalls	Symantec Enterprise Firewall, v7.0	Symantec Corporation	EAL 4		5/02	England	<input type="checkbox"/>
43	Firewalls	Symantec Enterprise Firewall on the Symar	Symantec Corporation	EAL 4		3/04	England	<input type="checkbox"/>
44	Firewalls	Symantec Gateway Security v2.0 5400 Series	Symantec Corporation	EAL 4	augmented ALC_FLR1	4/04	England	<input type="checkbox"/>
45	Firewalls	TeleWall System, V 2.0 for NT 4.0	SecureLogix Corporation	EAL 2	Augmented ACM_CAP.3	0/01	Canada	<input checked="" type="checkbox"/>
46	Firewalls	Watchguard LiveSecurity System w/Firebox	Watchguard Technologies	EAL 2		8/01	USA	<input checked="" type="checkbox"/>
47	Guards	DragonFly Companion, V3.02, Build 129	ITT Industries	EAL 2		0/01	USA	<input checked="" type="checkbox"/>
48	Guards	DragonFly Guard Model G1.2	ITT Industries	EAL 2		0/01	USA	<input checked="" type="checkbox"/>
49	Guards	Owl Computing Technologies Data Diode Vi	Owl Computing Technologies,	EAL 2		1/02	USA	<input checked="" type="checkbox"/>
50	IDS/IPS	Cisco Intrusion Detection System Appliance	Cisco Systems, Inc.	EAL 2		5/04	USA	<input checked="" type="checkbox"/>
51	IDS/IPS	Cisco Intrusion Detection System Module 0	Cisco Systems, Inc.	EAL 2	Augmented ALC_FLR1	5/04	USA	<input checked="" type="checkbox"/>
52	IDS/IPS	Enterasys Dragon-EAL™ Intrusion Defense	Enterasys Networks	EAL 2		9/04	USA	<input checked="" type="checkbox"/>
53	IDS/IPS	IntruShield Intrusion Detection System	McAfee, Inc.	EAL 3		8/04	USA	<input checked="" type="checkbox"/>
54	IDS/IPS	Intrusion, Inc. SecureNet Pro™ Intrusion Det	Intrusion, Inc. SecureNet Pro™	EAL 2		2/02	USA	<input checked="" type="checkbox"/>
55	IDS/IPS	Lancope StealthWatch and StealthWatch +	Lancope, Inc.	EAL 2	Augmented ALC_FLR2	6/04	USA	<input checked="" type="checkbox"/>
56	IDS/IPS	Symantec CyberWolf, Version 2.0	Symantec Corporation	EAL 2		6/04	USA	<input checked="" type="checkbox"/>
57	IDS/IPS	Symantec Manhunt Version 2.11	Symantec Corporation	EAL 3		2/03	USA	<input checked="" type="checkbox"/>
58	IDS/IPS	TippingPoint UnityOne™ Version 1.2	TippingPoint Technologies, Inc	EAL 2		8/03	USA	<input checked="" type="checkbox"/>
59	IDS/IPS	Top Layer Networks IDS Balancer TM Vers	Top Layer Networks	EAL 2		8/04	USA	<input checked="" type="checkbox"/>
60	Miscellaneous	BKK SignCubes, Version 1.5 (BSI-DSZ-CC-	Bundsvverband der Betriebskra	EAL 3	Augmented ADV_IMP.1 A	5/04	Germany	<input type="checkbox"/>
61	Miscellaneous	Canon imageRUNNER 2200/2800/3300 Ser	Canon U.S.A., Inc.	EAL 3		6/04	USA	<input checked="" type="checkbox"/>
62	Miscellaneous	Data-Defender V1.0	IBH-IMPEX Elektronik GmbH	EAL 1		5/02	Germany	<input type="checkbox"/>
63	Miscellaneous	DEP/PCI Version 3.0	Banksys N.V.	EAL 3	Augmented ADV_FSP.2	8/03	Germany	<input type="checkbox"/>
65	Miscellaneous	IBM Directory Server 5.2 (BSI-DSZ-CC-02	IBM Corporation	EAL 3		3/04	Germany	<input type="checkbox"/>
66	Miscellaneous	IBM LPAR for POWER 4 for the IBM pSerie	IBM Corporation	EAL 4	Augmented ALC_FLR1	1/04	Germany	<input type="checkbox"/>
67	Miscellaneous	IBM Tivoli Access Manager for e-business	IBM Corporation	EAL 3	+	0/03	Germany	<input type="checkbox"/>
68	Miscellaneous	Image Overwrite Security for Xerox WorkCe	Xerox Corporation	EAL 2		5/04	USA	<input checked="" type="checkbox"/>
70	Miscellaneous	Sharp Corporation Multifunction Device with	Sharp Electronics Corporation	EAL 2		2/02	USA	<input checked="" type="checkbox"/>
71	Miscellaneous	Sharp Data Security Kit (AD-EP1/AD-EP2)	Sharp Electronics Corporation	EAL 2		4/01	USA	<input checked="" type="checkbox"/>

ST evaluated and certificated by CC

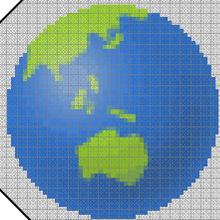


Example



	TOE			IT Environ			Non - IT Environ					
	O.ADMIN	O.DETECT	O.MONITOR	O.QUEUE	O.AUTH_ACCESS	O.ENV_ADMIN	O.SEP	O.TIME	O.INSTALL	O.PERSON	O.PHYSICAL	O.HARDWRE
Assumptions	[Redacted]											
A.LOCATE												
A.PROTECT									x	x	x	
A.MANAGE										x		
A.NOEVIL										x		
A.CONFIG									x	x		
A.IDENT					x							
A.SYSPRCT					x						x	
A.HARDWRE												x
A.SYSTIME								x				
Threats	[Redacted]											
T.ACCESS DATA					x		x				x	
T.OVRLOAD			x									
T.UNAUTH					x		x			x	x	

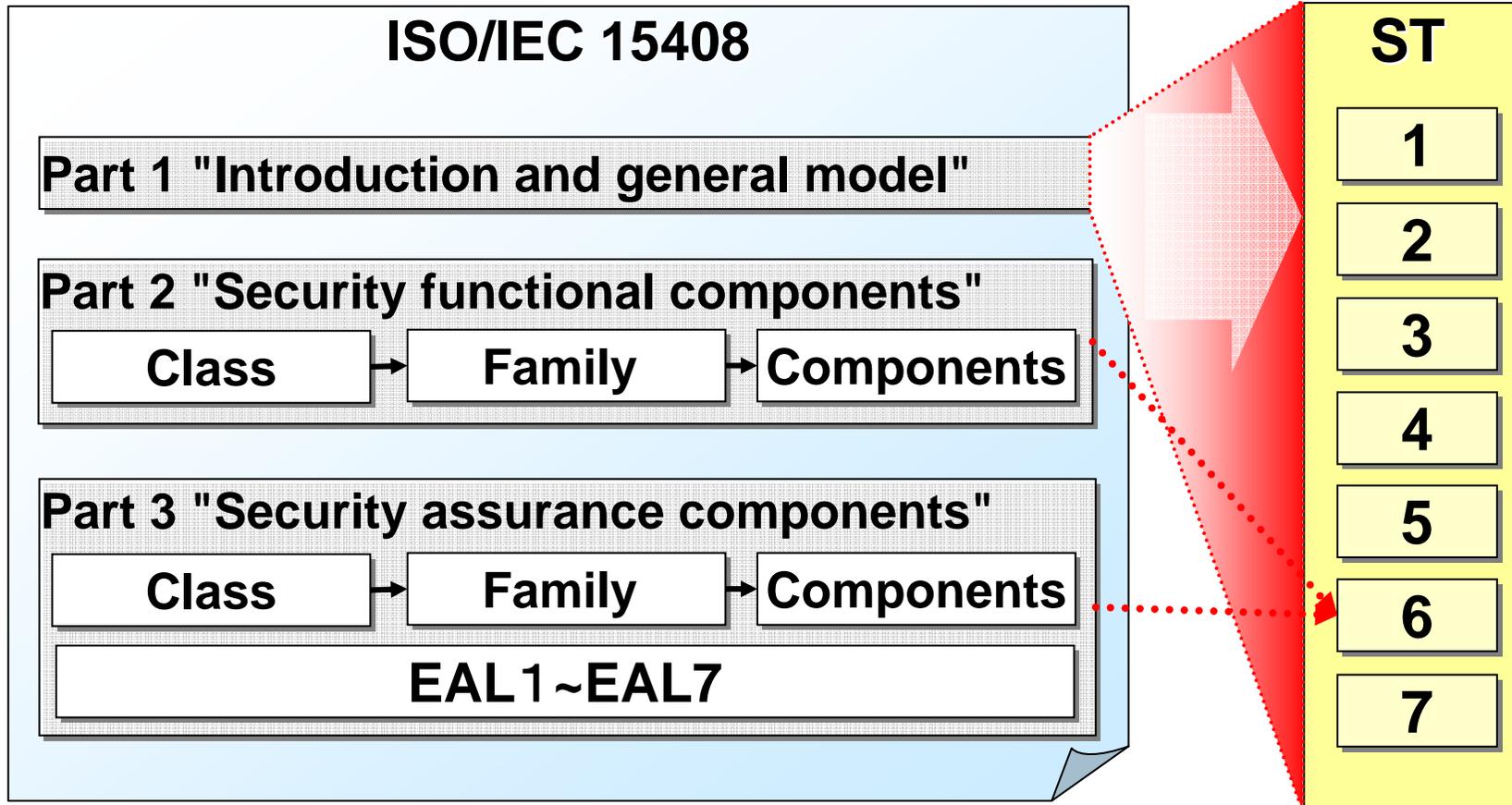
Objectives	FAU_ARP.1	FAU_GEN.1	FAU_GEN.2	FAU_SAA.1	FAU_SAR.1a	FAU_SAR.1b	FAU_SAR.1c	FAU_SAR.3a	FAU_SAR.3b	FAU_SAR.3c	FDP_IFC.2	FDP_IFF.1	FMT_SMF.1	FPT_RVM.1	FMT_SMR.1	FIA_UID.1	FPT_SEP.1	FPT_STM.1	
	TOE																		
O.ADMIN	x	x	x	x	x	x		x	x	x			x		x	x			
O.DETECT											x	x	x		x	x	x		
O.MONITOR		x	x														x	x	
O.QUEUE											x	x		x			x		
IT Environment	[Redacted]																		
O.AUTH_ACCESS															x	x			
O.ENV_ADMIN							x												
O.SEP																	x		
O.TIME																		x	

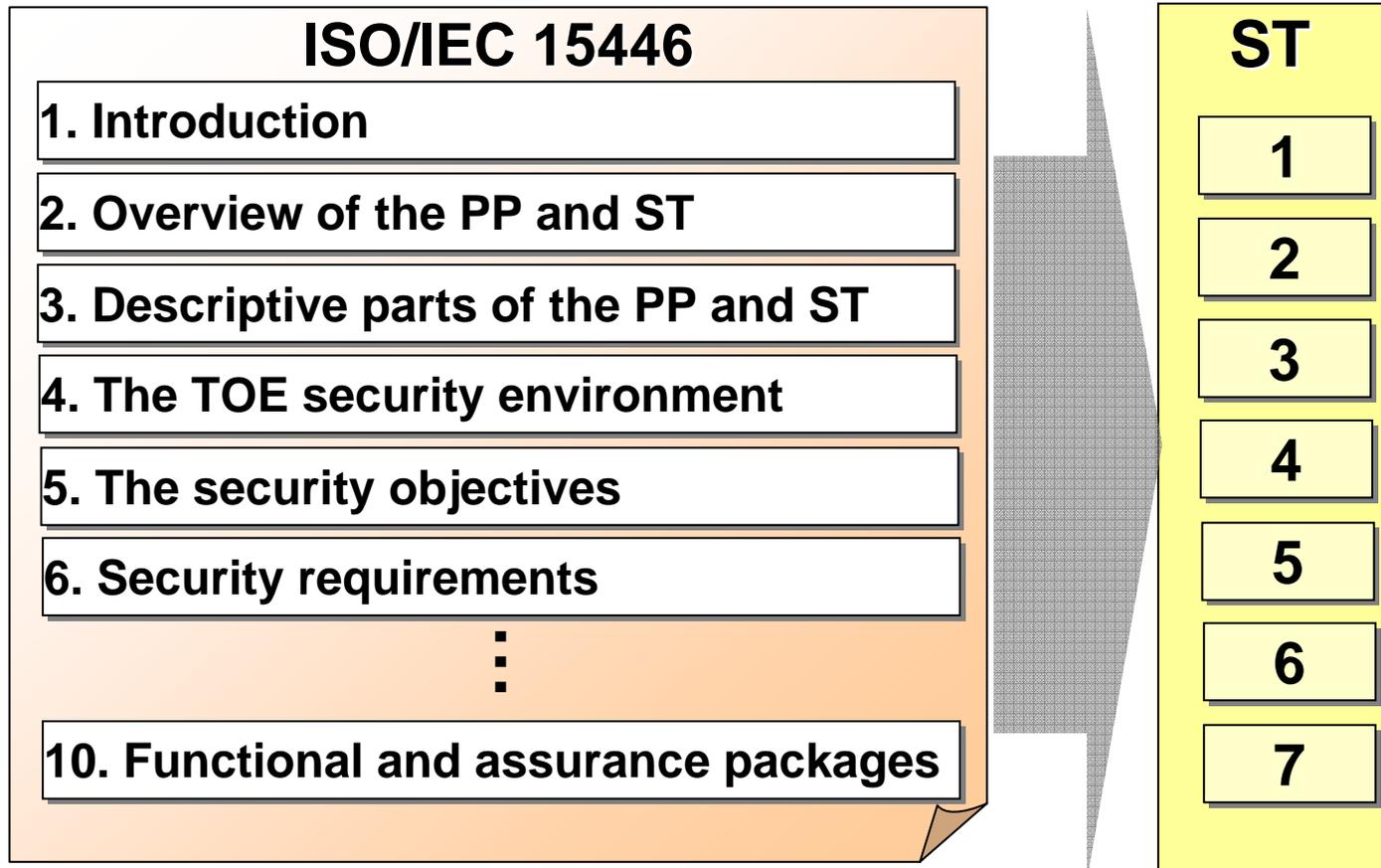


ISO/IEC 15408

ISO/IEC TR 15446

②





Security Target Contents

1. ST Introduction

2. Conformance Claims

3. Security Problem Definition

Threats

Organisational Security
Policies

Assumptions

4. Security Objectives

Security objectives for
the TOE

Security objectives for
the operational
environment

5. Extended Components Definition

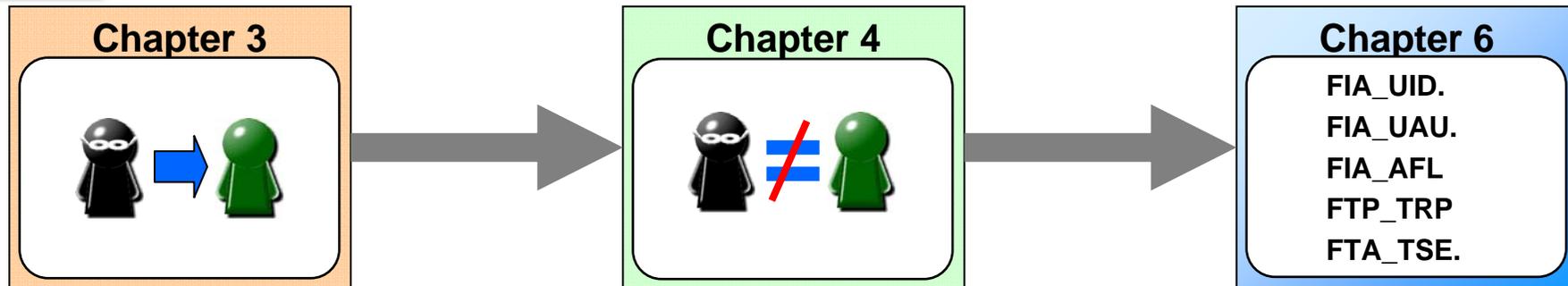
6. Security Requirements

Security Functional
Requirements

Security Assurance
Requirements

7. TOE Summary Specification

Security Target Contents



3. Security Problem Definition

Threats

Organisational Security Policies

Assumptions

4. Security Objectives

Security objectives for the TOE

Security objectives for the operational environment

6. Security Requirements

Security Functional Requirements

Security Assurance Requirements

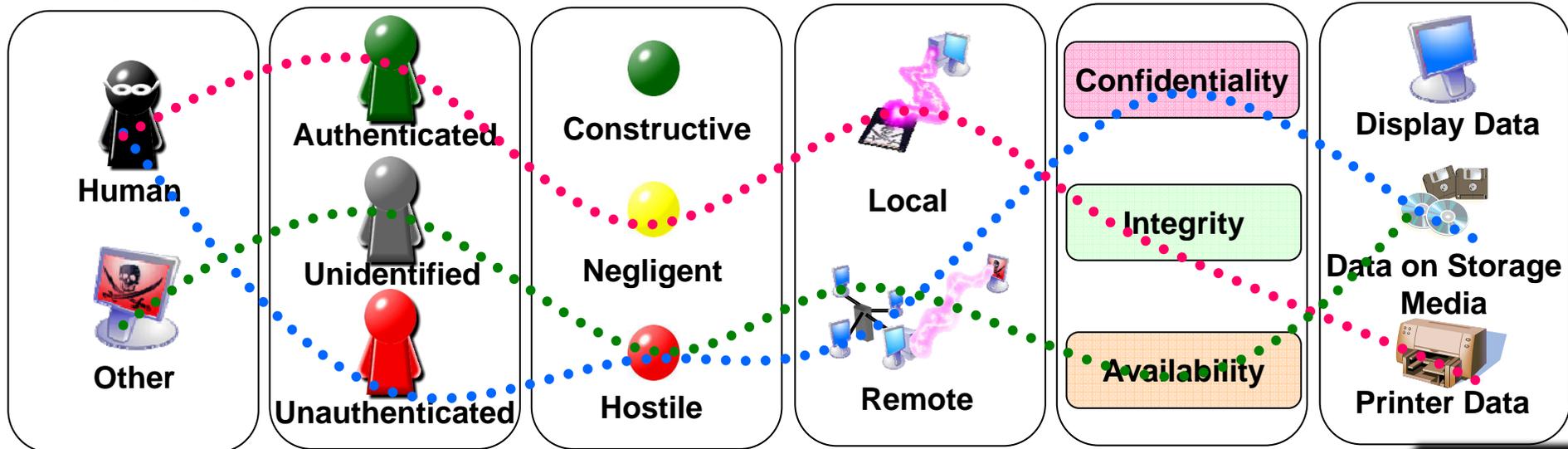
3. Security Problem Definition

Threats

Organisational Security Policies

Assumptions

- The security problems to be addressed by the TOE
- CC does not provide a framework for risk analysis
- ST developers would be able to use a Threats Model tools

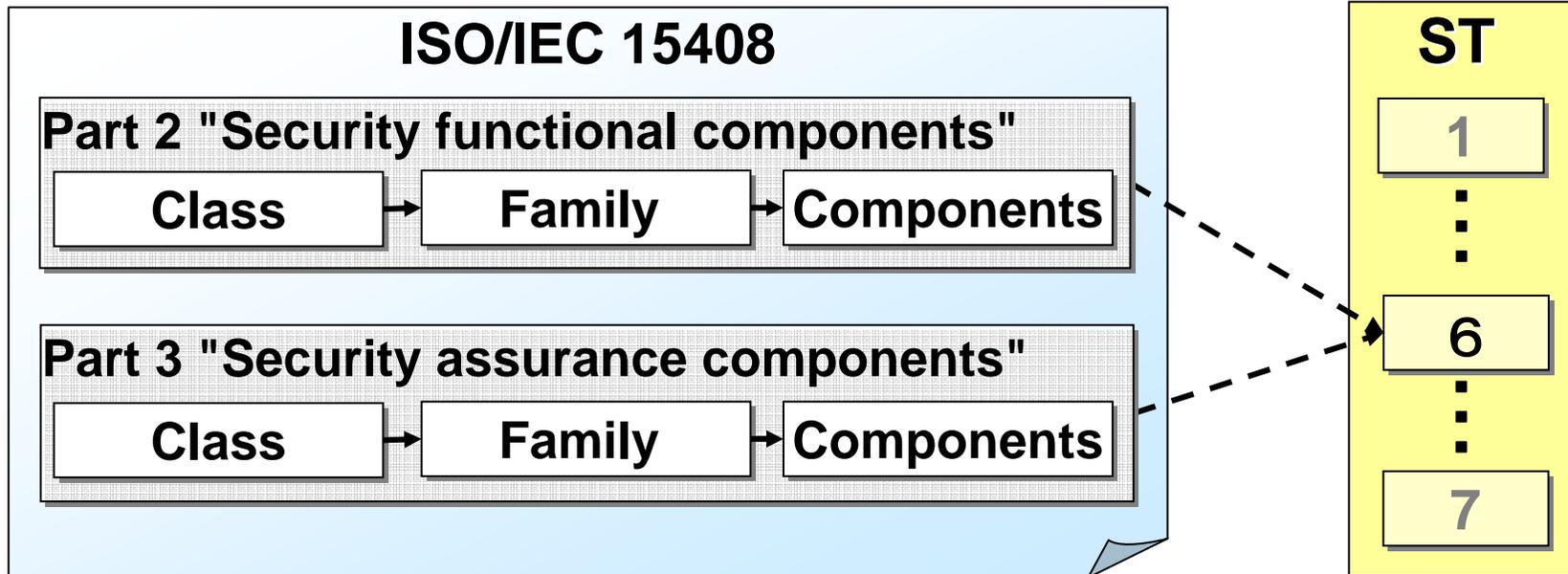


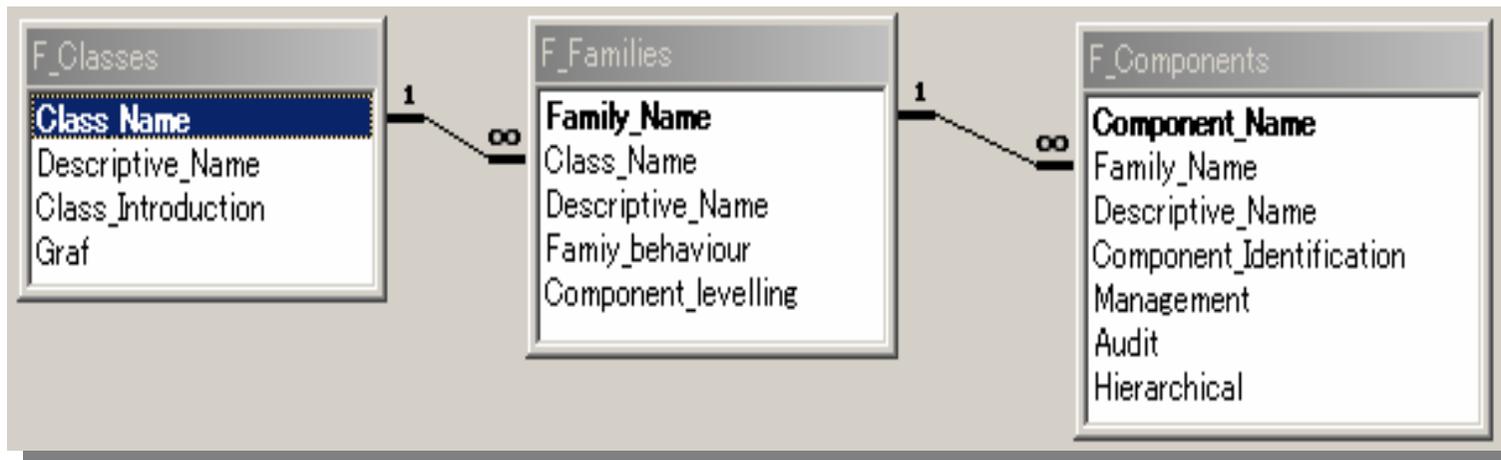
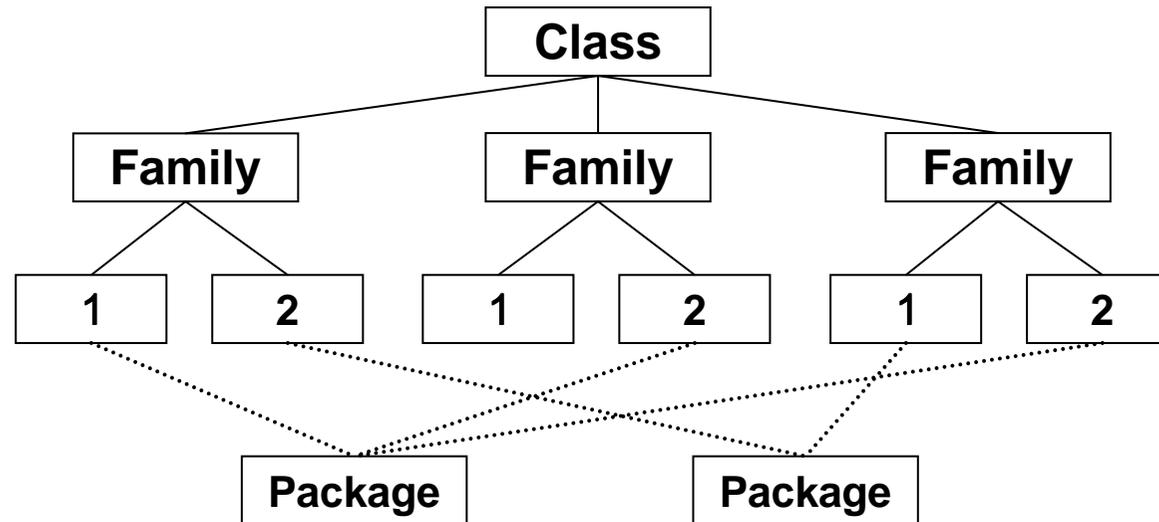
Section 6

6. Security Requirements

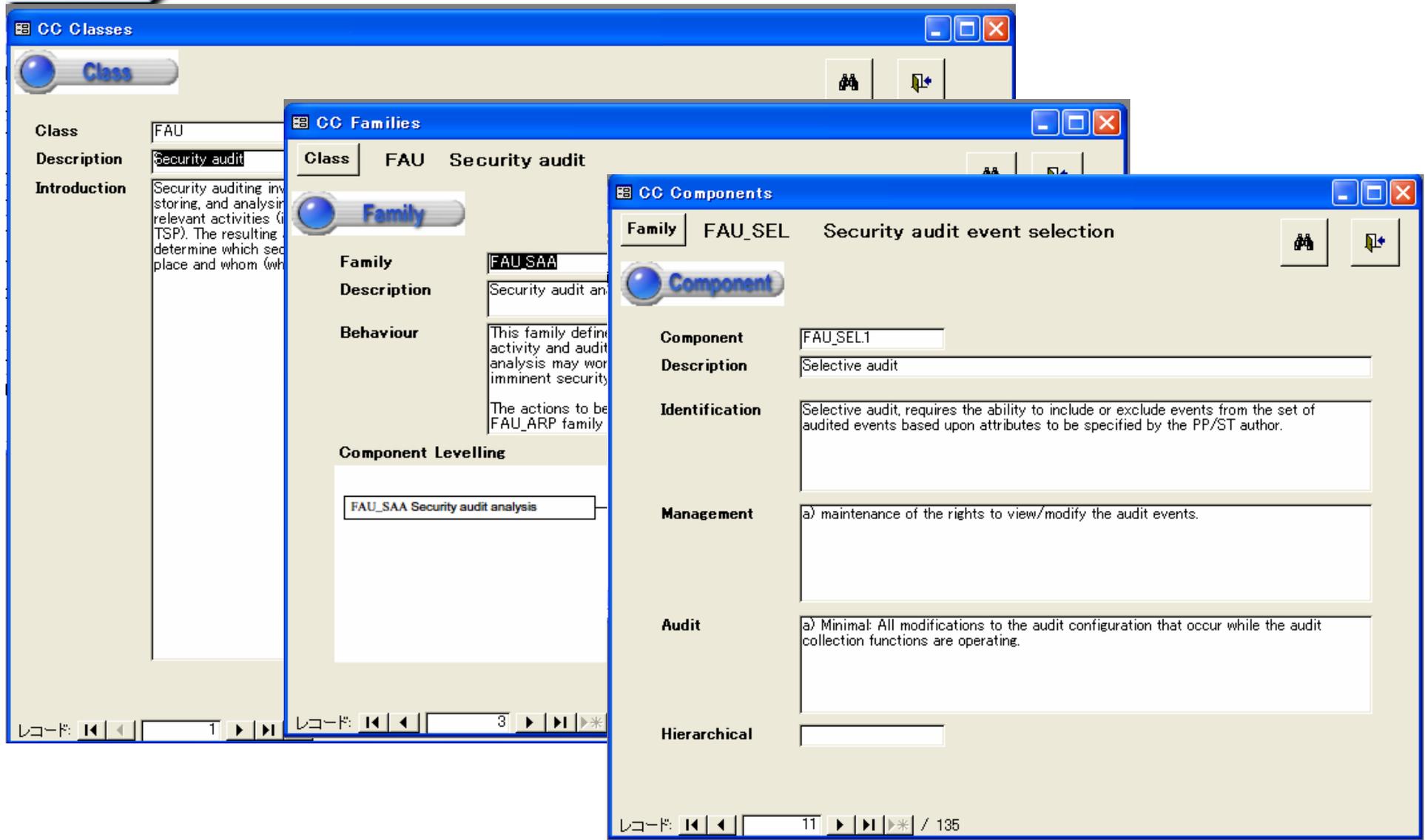
Security Functional Requirements

Security Assurance Requirements





ISO/IEC 15408 Knowledge-base



The screenshot displays three overlapping windows from the ISO/IEC 15408 Knowledge-base software:

- CC Classes Window:** Shows details for the class 'FAU' (Security audit). The description is 'Security auditing involves storing, and analysing relevant activities (TSP). The resulting determine which place and whom (wh'.
- CC Families Window:** Shows details for the family 'FAU_SAA' (Security audit analysis). The description is 'Security audit an'. The behaviour is 'This family define activity and audit analysis may wor imminent security. The actions to be FAU_ARP family'.
- CC Components Window:** Shows details for the component 'FAU_SEL1' (Selective audit). The description is 'Selective audit'. The identification is 'Selective audit, requires the ability to include or exclude events from the set of audited events based upon attributes to be specified by the PP/ST author.' The management is 'a) maintenance of the rights to view/modify the audit events.' The audit is 'a) Minimal: All modifications to the audit configuration that occur while the audit collection functions are operating.' The hierarchical field is empty.

Navigation controls are visible at the bottom of each window, including record numbers (e.g., 1, 3, 11) and a total count of 135 records.



Security Functional Requirement : Class

Class	Name	Introduction
FAU	Security audit	Security auditing involves recognising, recording, storing, and analysing information related to security relevant activities (i.e. activities controlled by the TSP). The resulting audit records can be examined to determine which security relevant activities took place and whom (which user) is responsible for them.
FCO	Communication	This class provides two families specifically concerned with assuring the identity of a party participating in a data exchange. These families are related to assuring the identity of the originator of transmitted information (proof of origin) and assuring the identity of the recipient of transmitted information (proof of receipt). These families ensure that an originator cannot deny having sent the message, nor can the recipient deny having received it.
FCS	Cryptographic support	The TSF may employ cryptographic functionality to help satisfy several high-level security objectives. These include (but are not limited to): identification and authentication, non-repudiation, trusted path, trusted channel and data separation. This class is used when the TOE implements cryptographic functions, the implementation of which could be in hardware, firmware and/or software. The FCS class is composed of two families: FCS_CKM Cryptographic key management and FCS_COP Cryptographic operation. The FCS_CKM family addresses the management aspects of cryptographic keys, while the FCS_COP family is concerned with the operational use of those cryptographic keys.
FDP	User data protection	This class contains families specifying requirements for TOE security functions and TOE security function policies related to protecting user data. FDP is split into four groups of families (listed below) that address user data within a TOE, during import, export, and storage as well as security attributes directly related to user data.



Soka University - Teshigawara Laboratory

IT Security: Knowledge Base



[Home](#) [ISO/IEC](#) [Projects](#) [Membres](#) [Link](#)

Security Functional Requirement : Class - Family

Family	Class	Name	behaviour
FAU_ARP	FAU	Security audit automatic response	This family defines the response to be taken in case of detected events indicative of a potential security violation.
FAU_GEN	FAU	Security audit data generation	This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.
FAU_SAA	FAU	Security audit analysis	This family defines requirements for automated means that analyse system activity and audit data looking for possible or real security violations. This analysis may work in support of intrusion detection, or automatic response to an imminent security violation. The actions to be taken based on the detection can be specified using the FAU_ARP family as desired.
FAU_SAR	FAU	Security audit review	This family defines the requirements for audit tools that should be available to authorised users to assist in the review of audit data.
FAU_SEL	FAU	Security audit event selection	This family defines requirements to select the events to be audited during TOE operation. It defines requirements to include or exclude events from the set of auditable events.

1 2 3 4 5 6 7 8 9 10 ...



Security Functional Requirement : Class - Family - Components

Component	Family	Name	Identification	Management	Audit	Hierarchical
FAU_ARP.1	FAU_ARP	Security alarms	the TSF shall take actions in case a potential security violation is detected.	a) the management (addition, removal, or modification) of actions.	a) Minimal: Actions taken due to imminent security violations.	No other components.
FAU_GEN.1	FAU_GEN	Audit data generation	Audit data generation defines the level of auditable events, and specifies the list of data that shall be recorded in each record.			
FAU_GEN.2	FAU_GEN	User identity association	User identity association, the TSF shall associate auditable events to individual user identities.			
FAU_SAA.1	FAU_SAA	Potential violation analysis	Potential violation analysis, basic threshold detection on the basis of a fixed rule set is required.	a) maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.	a) Minimal: Enabling and disabling of any of the analysis echanisms; b) Minimal: Automated responses performed by the tool.	



IT Security: Knowledge Base

Soka University - Teshigawara Laboratory

[Home](#) [ISO/IEC](#) ▶ [Projects](#) ▶ [Membres](#) [Link](#)



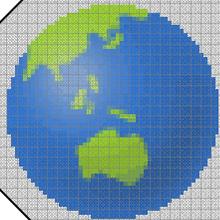
• **Security Guidelines for Home User**

The knowledge base tool based on international standards was developed in this research. ST Developer's knowledge deficiency can be supplemented by using this tool to access the necessary information on international standards. Moreover, ST developer's experience shortage can be supplemented by referring evaluated ST information which are classified by product types and countries.

• **Knowledge Base for Production of ST**

The ISO/IEC 15408 is a standard to be used as the basis for evaluation of security properties of IT products and systems. This Mutual Recognition Arrangement of CC (Common Criteria) is established by eight countries including the United States. The IT products evaluated based on ISO/IEC 15408 are increasing every year. However, one of the problems to make STs (Security Targets) is that sufficient knowledge and experience is critically required for ST developers. The knowledge base tool based on international standards was developed in this research. ST Developer's knowledge deficiency can be supplemented by using this tool to access the necessary information on international standards. Moreover, ST developer's experience shortage can be supplemented by referring evaluated ST information which are classified by product types and countries.

• **Threats Model**



Self-Training System

③

Target audience of the CC



	Consumers	Developers	Evaluators
Advanced			
Intermediate			
Beginners			

Knowledge-based



Soka University - Teshigawara Laboratory

IT Security: Knowledge Base

Home ISO/IEC Projects Membres Link

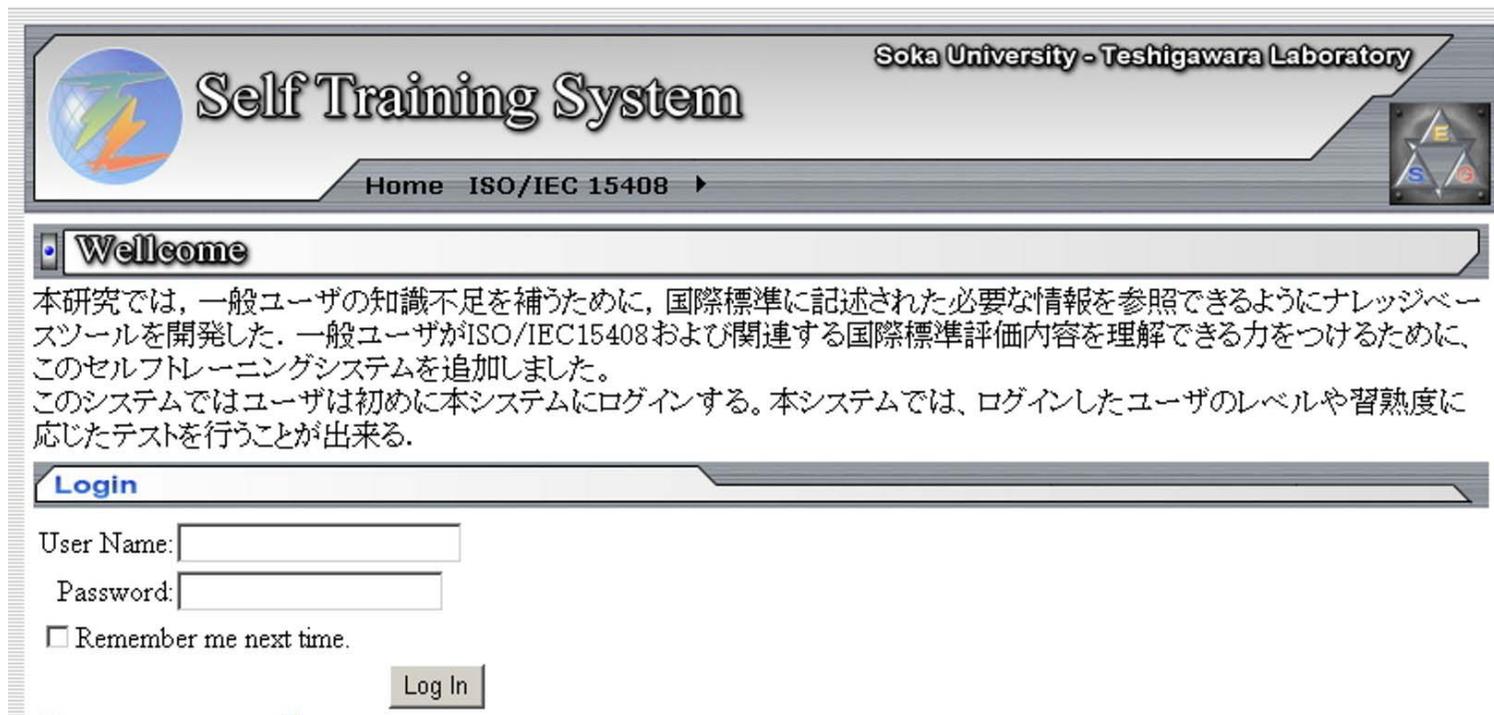
Self-Training
Help File
Threats Model
Security Guidelines
ASF

Teshigawara Laboratory

情報ネットワークの進展は、まさしく日進月歩のようになってきています。インターネット利用者数の急上昇、ギガビットLANや無線LANの普及、すでに4500万人を超える携帯

Projects Membres

Self-Training
Help File
Threats Model
Security Guidelines
ASF



Soka University - Teshigawara Laboratory

Self Training System

Home ISO/IEC 15408

Wellcome

本研究では、一般ユーザの知識不足を補うために、国際標準に記述された必要な情報を参照できるようにナレッジベースツールを開発した。一般ユーザがISO/IEC15408および関連する国際標準評価内容を理解できる力をつけるために、このセルフトレーニングシステムを追加しました。このシステムではユーザは初めに本システムにログインする。本システムでは、ログインしたユーザのレベルや習熟度に応じたテストを行うことが出来る。

Login

User Name:

Password:

Remember me next time.

Log In

Soka University - Teshigawara Laboratory

Self Training System

Home ISO/IEC 15408 ▶

Welcome

本研究では、一般ユーザの知識不足を補うために、国際標準に記述された必要な情報を参照できるようにナレッジベースツールを開発した。一般ユーザがISO/IEC15408および関連する国際標準評価内容を理解できる力をつけるために、このセルフトレーニングシステムを追加しました。
このシステムではユーザは初めに本システムにログインする。本システムでは、ログインしたユーザのレベルや習熟度に応じたテストを行うことができる。

Login

User Name:

Password:

Remember me next time.

[Forgot your password?](#)

New User? Please Register

User Name:

Password:

Confirm Password:

E-mail:

Security Question:

Security Answer:

Copyright 2006. Soka University - Teshigawara Laboratory

Login

Create a new account



Self Training System

Home ISO/IEC 15408 ▶

Soka University - Teshigawara Laboratory



Main Menu

horacio welcome to the Self Training Test Application based on International Standards.
国際標準についてセルフトレーニングシステムへようこそ

Available Test

[ISO/IEC 15408 Part 1 概説と一般モデル](#)
 パート1:概説と一般モデルでは、全体的に、STを作成ツールに使う。特に、附属書C「セキュリティターゲットの仕様」が各章に分けられて記述されている。

[ISO/IEC 15408 Part 2 セキュリティ機能要件](#)
 パート2:セキュリティ機能要件には、機能クラス、機能ファミリー、及び機能コンポーネントのセットをカタログ化している。機能コンポーネントはエレメントに分けている。このエレメントは最小のセキュリティ機能要件である。ファミリーは、2つ以上のコンポーネントが含まれる。そして、機能ファミリー内でのコンポーネント間の関係は、階層関係になっている。

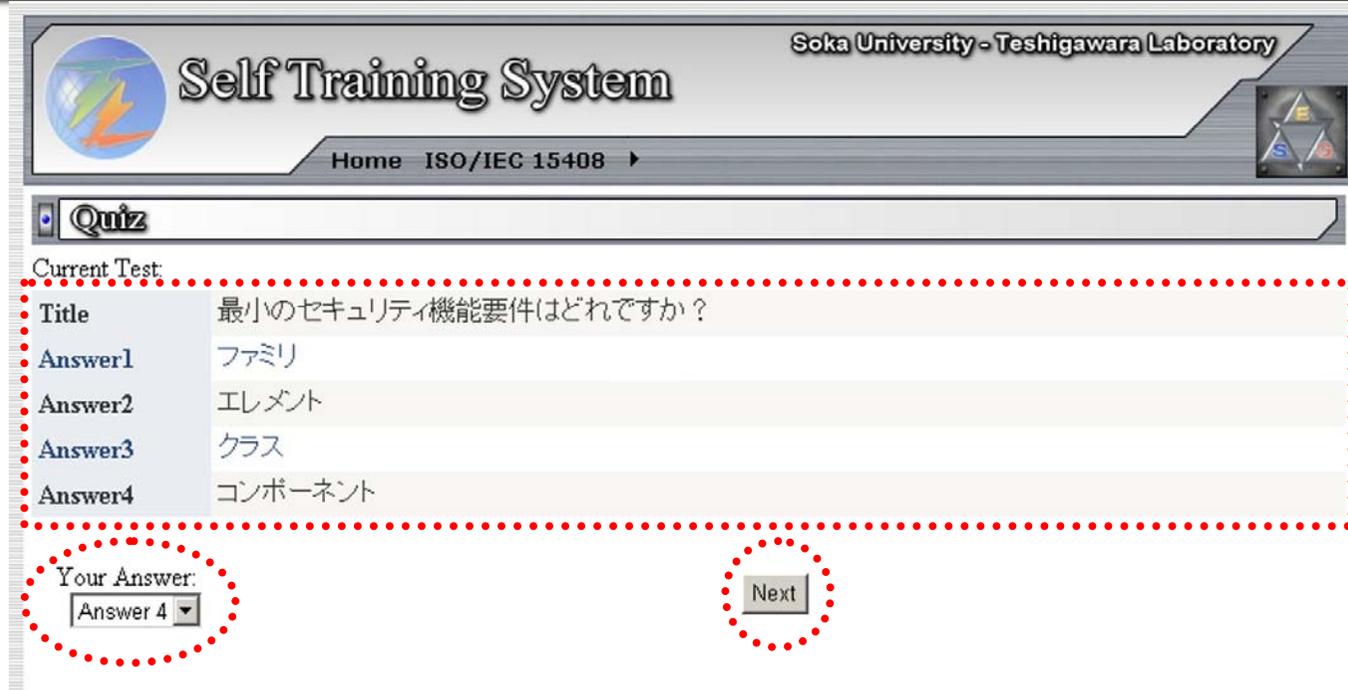
[ISO/IEC 15408 Part 3 セキュリティ保証要件](#)
 パート3:セキュリティ保証要件には、保証クラス、保証ファミリー、及び保証コンポーネントのセットをカタログ化している。また、STの評価基準も定義しており、EALの保証要件パッケージの情報を述べている。

Test Result History

Quiz	Completed	Score%
ISO/IEC 15408 Part 1	2006/05/01 14:40:00	20
ISO/IEC 15408 Part 1	2006/05/01 14:41:00	100

List of available tests

The user should be able to review the results of the tests taken in the past



The screenshot shows a web interface for a 'Self Training System' at Soka University - Teshigawara Laboratory. The page title is 'Quiz'. Under 'Current Test', there is a table of possible answers for a question about security requirements. The 'Your Answer' section shows 'Answer 4' selected in a dropdown menu, and a 'Next' button is visible.

Current Test	
Title	最小のセキュリティ機能要件はどれですか？
Answer1	ファミリー
Answer2	エレメント
Answer3	クラス
Answer4	コンポーネント

Your Answer:

The user will see the questions and the possible answers, [1],[2],[3],[4]... they will pick one and click the next button

Results of the quiz



Self Training System

Home ISO/IEC 15408 ▶

Soka University - Teshigawara Laboratory



Results

	Question	Correct Answer	Your Answer	Result
Select	1	3	3	Correct
Select	2	2	2	Correct
Select	3	4	4	Correct
Select	4	2	4	Incorrect
Select	5	3	4	Incorrect

Review

Question No.: 5

Question: 機能ファミリー名で分類するために、何文字が必要ですか？

Answer 1: 5

Answer 2: 6

Answer 3: 7

Answer 4: 8

Correct Answer: 3

Explanation: ファミリー名の節は、機能ファミリーを識別し分類するのに必要な分類情報と記述情報を提供する。各機能名は一意の名前を持つ。分類情報は7文字の短い名前から構成されており、その最初の3文字はクラスの短い名前と同じもので、その後には下線文字とファミリーの短い名前が続き、XXX_YYYのような形式になる。ファミリー名の一意の短い形式は、コンポーネントの主な参照名を提供する。

[Return to Main Menu](#)

Knowledge Based Tool



Consumers



Developers

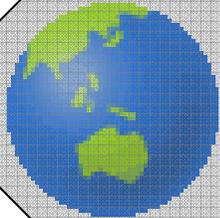


Evaluators

Security Functional Requirement : Class - Family - Components

Component	Family	Name	Identification	Management	Audit	Hierarchical
FDP_ETC.2	FDP_ETC	Export of user data with security attributes	Export of user data with security attributes requires that the TSF enforce the appropriate SFPs using a function that accurately and unambiguously associates security attributes with the user data that is exported.	The following actions could be considered for the management functions in FMT Management: a) The additional exportation control rules could be configurable by a user in a defined role.	The following events shall be auditable if FAU_GEN Security audit data generation is included in the PP/ST: A) Minimal: Successful export of information. B) Basic: All attempts to export information.	

beginners · Intermediate · Advanced



Conclusion & Future Works

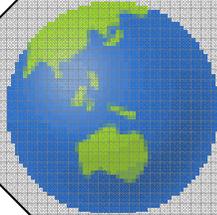
Conclusion

- Design and development of a knowledge-based tool for ST developers based on CCV3.1.
- It was explained the architecture of the knowledge-based tool and showed how it can help ST developers create STs that are to be evaluated by CC.
- ST developer's **knowledge** deficiency can be supplemented by using this tool to access the necessary information on international standards.
- ST developer's relevant **experience** faced by ST developer can also be supplemented by referring to evaluated information of STs which are classified by types and countries.



Future Works

- ISO/IEC 19791 is an international standard that must be used as the basis for evaluation of operating system.
- This new standard will be included in the knowledge-based tool.



Questions & Answers



<http://www.teshilab.net>

Guillermo Horacio RAMIREZ CACERES

Yoshimi TESHIGAWARA

Graduate School of Engineering, Soka University

Tokyo, Japan

E-mail: {guillerm,teshiga}@soka.ac.jp