¿ Certified Secure?

Assurance and Functional Security Requirements and Standards in Practice and Theory

A socio-technical

“jaded “ academic” perspective

FRISCO Winter School 2013

(Friday 2013-04-26)

Professor Dr Stewart Kowalski
University College Gjøvik
Norway
stewart.kowalski@hig.no

Goal of this Lecture

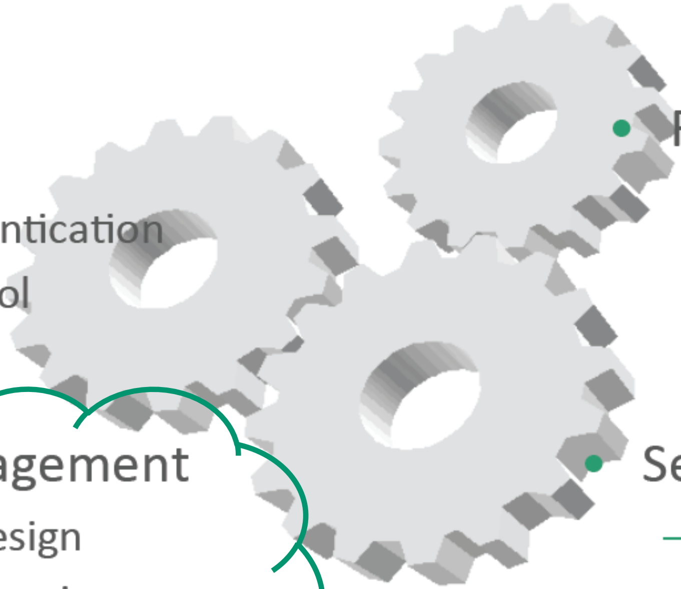
- Give you some background and history of security assurance problems and story from an industrial supplier and socio-technical systems security research perspective.
- Give you some back ground to the Common Criteria as a “security researcher”
- Encourage more “naïve“ inductivist” and empirical research in information security systems security
- Improve the strength of our common socio-technical security value chain.

Outline

- Background War Stories
  - Why I am Jaded!
- A Naïve inductivist
  - Why I use a socio-technical systems approach to deal with information security, past and present
- Practise and Standard choose for certification
  - "All is not quite on the Western/Eastern Front!"
  - Past and Present experience with using common criteria

Mission & Collaboration

NISlab – Working Areas

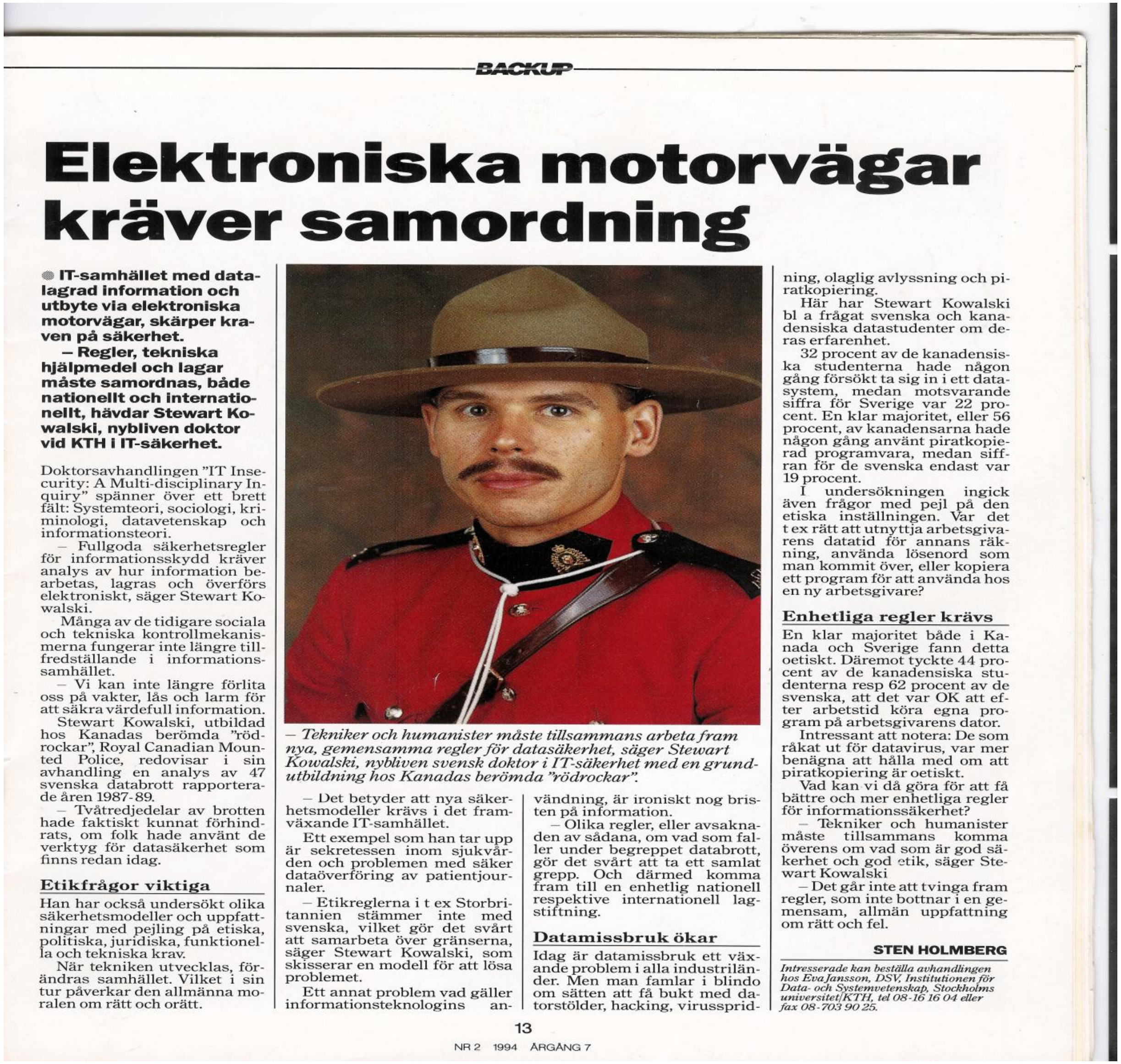


- Biometrics
  - User Authentication
  - BTA Protocol
- Forensics
  - Forensic Readiness
  - Incidence Response
  - Investigation/Analysis
- Security Management
  - Risk-based Design
  - Security Economics
  - System/Adversary Modeling
  - Human Factors, Policies
- Security Technology
  - Software Security
  - System Administration
  - Network and Critical Infrastructure Protection

2013-05-03

We are here “system modeling”.

Background



BACKUP

Elektroniska motorvägar kräver samordning

IT-samhället med datalagrad information och utbyte via elektroniska motorvägar, skärper kraven på säkerhet.

– Regler, tekniska hjälpmedel och lagar måste samordnas, både nationellt och internationellt, hävdar Stewart Kowalski, nybliven doktor vid KTH i IT-säkerhet.

Doktorsavhandlingen ”IT Insecurity: A Multi-disciplinary Inquiry” spänner över ett brett fält: Systemteori, sociologi, kriminologi, datavetenskap och informationsteori.

– Fullgoda säkerhetsregler för informationsskydd kräver analys av hur information bearbetas, lagras och överförs elektroniskt, säger Stewart Kowalski.

Många av de tidigare sociala och tekniska kontrollmekanismerna fungerar inte längre tillfredställande i informationssamhället.

– Vi kan inte längre förlita oss på vakter, lås och larm för att säkra värdefull information.

Stewart Kowalski, utbildad hos Kanadas berömda ”rödrockar”, Royal Canadian Mounted Police, redovisar i sin avhandling en analys av 47 svenska databrott rapporterade åren 1987-89.

– Tvåtredjedelar av brotten hade faktiskt kunnat förhindrats, om folk hade använt de verktyg för datasäkerhet som finns redan idag.

Etikfrågor viktiga

Han har också undersökt olika säkerhetsmodeller och uppfattningar med pejling på etiska, politiska, juridiska, funktionella och tekniska krav.

När tekniken utvecklas, förändras samhället. Vilket i sin tur påverkar den allmänna moralen om rätt och orätt.

– Tekniker och humanister måste tillsammans arbeta fram nya, gemensamma regler för datasäkerhet, säger Stewart Kowalski, nybliven svensk doktor i IT-säkerhet med en grundutbildning hos Kanadas berömda ”rödrockar”.

– Det betyder att nya säkerhetsmodeller krävs i det framväxande IT-samhället.

Ett exempel som han tar upp är sekretessen inom sjukvården och problemen med säker dataöverföring av patientjournaler.

– Etikreglerna i t ex Storbritannien stämmer inte med svenska, vilket gör det svårt att samarbeta över gränserna, säger Stewart Kowalski, som skisserar en modell för att lösa problemet.

Ett annat problem vad gäller informationsteknologins användning, är ironiskt nog bristen på information.

– Olika regler, eller avsaknaden av sådana, om vad som faller under begreppet databrott, gör det svårt att ta ett samlat grepp. Och därmed komma fram till en enhetlig nationell respektive internationell lagstiftning.

Datamissbruk ökar

Idag är datamissbruk ett växande problem i alla industriländer. Men man famlar i blindo om sätten att få bukt med datorstölder, hacking, virusspridning, olaglig avlyssning och piratkopiering.

Här har Stewart Kowalski bl a frågat svenska och kanadensiska datastudenter om deras erfarenhet.

32 procent av de kanadensiska studenterna hade någon gång försökt ta sig in i ett datasystem, medan motsvarande siffra för Sverige var 22 procent. En klar majoritet, eller 56 procent, av kanadensarna hade någon gång använt piratkopierad programvara, medan siffran för de svenska endast var 19 procent.

I undersökningen ingick även frågor med pejl på den etiska inställningen. Var det t ex rätt att utnyttja arbetsgivarens datatid för annans räkning, använda lösenord som man kommit över, eller kopiera ett program för att använda hos en ny arbetsgivare?

Enhetliga regler krävs

En klar majoritet både i Kanada och Sverige fann detta oetiskt. Däremot tyckte 44 procent av de kanadensiska studenterna resp 62 procent av de svenska, att det var OK att efter arbetstid köra egna program på arbetsgivarens dator.

Intressant att notera: De som råkat ut för datavirus, var mer benägna att hålla med om att piratkopiering är oetiskt.

Vad kan vi då göra för att få bättre och mer enhetliga regler för informationssäkerhet?

– Tekniker och humanister måste tillsammans komma överens om vad som är god säkerhet och god etik, säger Stewart Kowalski

– Det går inte att tvinga fram regler, som inte bottnar i en gemensam, allmän uppfattning om rätt och fel.

STEN HOLMBERG

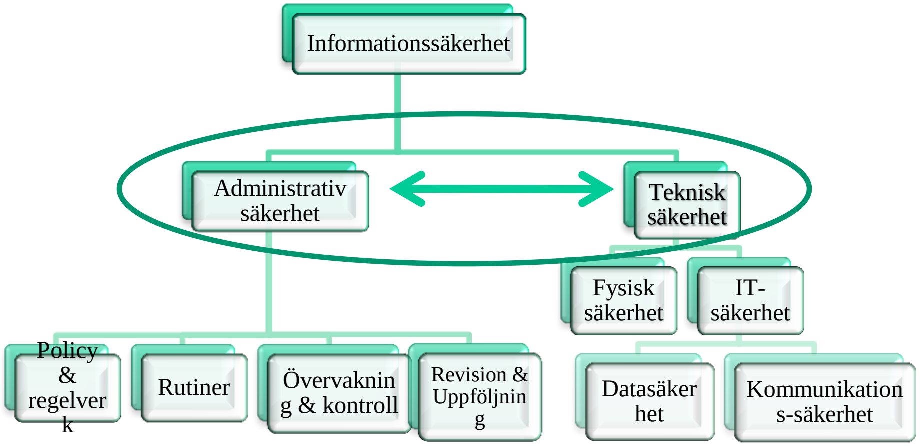
Intresserade kan beställa avhandlingen hos Eva Jansson, DSV, Institutionen för Data- och Systemvetenskap, Stockholms universitet/KTH, tel 08-16 16 04 eller fax 08-703 90 25.

ABC’s of Professor (Killer) Kowalski

A. research focuses on understanding and improving how administrative security and technology security work together.

The real Killer Kowalski

http://www.youtube.com/watch?v=lKr9qDL6_h4&NR=1 &feature=endscreen



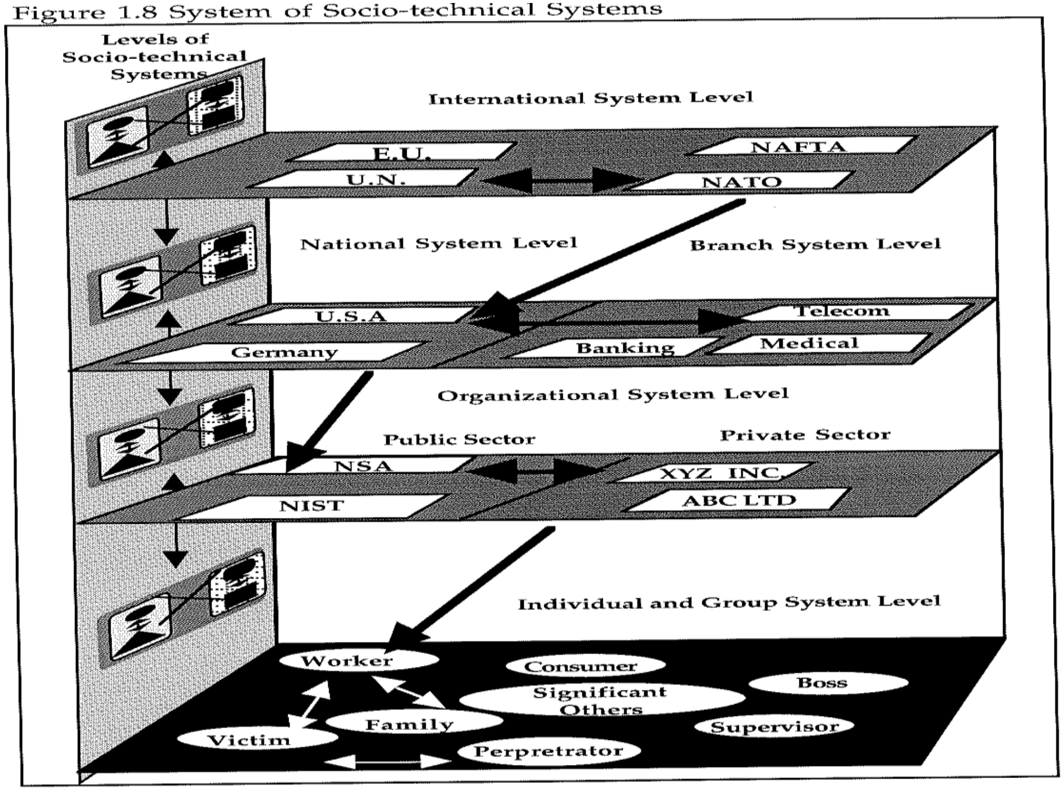
Informationssäkerhet (HB 550)

ABC's of Secure Socio-technical systems scientist Kowalski

B. uses a socio-technical research paradigm and studies information security at many different levels of society included <u>national, organizational and individual levels.</u>

Kowalski, S. (1994) *IT Insecurity: A Multi-disciplinary Inquiry.* Diss. The Royal Institute of Technology, Department of Computer and Systems Science Stockholm Univ. Report series No. 94-040, Stockholm.

Figure 1.8 System of Socio-technical Systems



ABC’s of Security Worker Kowalski

C. **research work and industrial work in security stretch over 30 years and included both theoretical and empirical research and product and services**

HUAWEI
ERICSSON
hp
telia
PHILIPS
BNP PARIBAS
digital
HØGSKOLEN I GJØVIK
STOCKHOLMS UNIVERSITET
KTH
HÖGSKOLAN I GÄVLE
UNIVERSITÉ LAVAL
Concordia
CPC CCP
WHENEVER MY CUP RUNNETH OVER, I JUST HAVE TO CLEANNETH IT UP.

Work with security in Industrial vs University

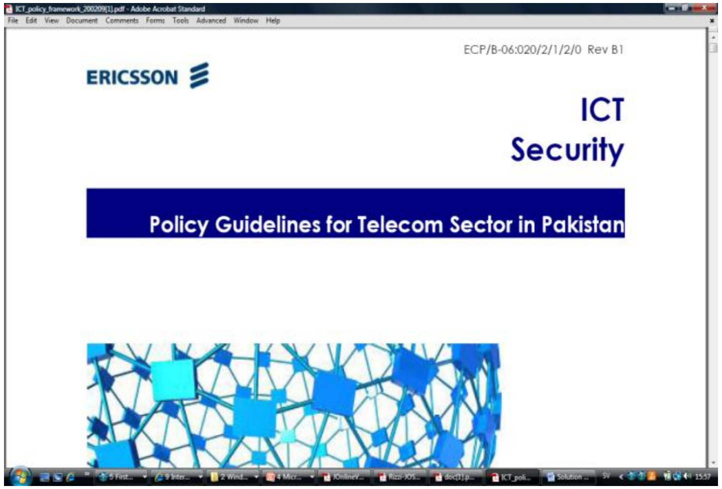
Industry

- Deal with complex problems.
- Must give simple solutions.

Islamabad November 25, 2008 : Chairman Pakistan Telecommunication Authority (PTA), Dr.Mohammed Yaseen chairing a meeting of Expert Group Forum on Information Security Guidelines held at PTA Headquarters.

University

- Deal with simple problems.
- Must give complex solutions to get published, ☺.



ICT_policy_framework_200209[1].pdf - Adobe Acrobat Standard
File Edit View Document Comments Forms Tools Advanced Window Help

ECP/B-06:020/2/1/2/0 Rev B1

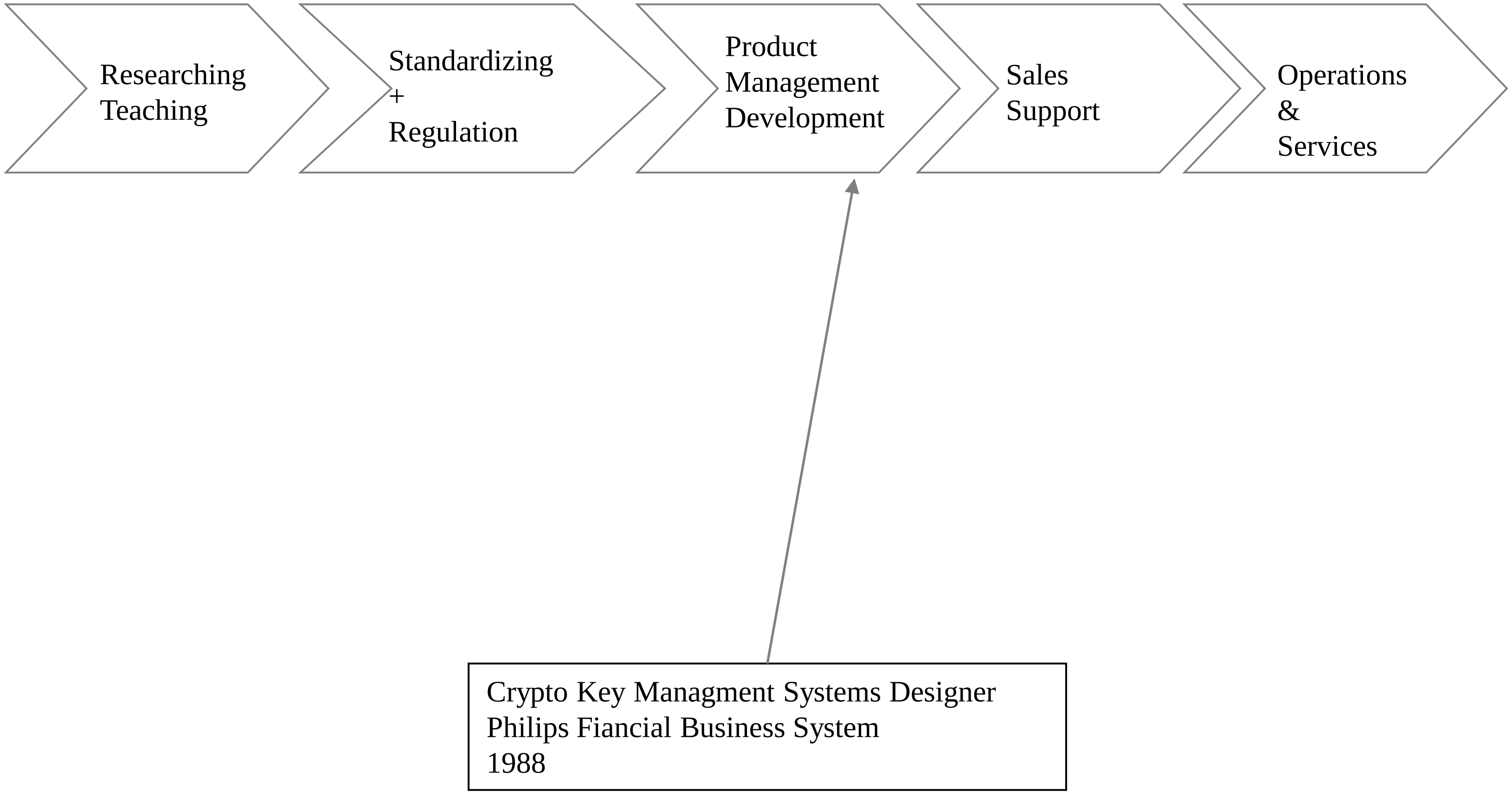
ERICSSON

ICT Security

Policy Guidelines for Telecom Sector in Pakistan

Work Experience Stretched Over
our common IT/IS Security Value Chain

Work Experience Stretched Over our common IT/IS Security Value Chain



Researching
Teaching

Standardizing
+
Regulation

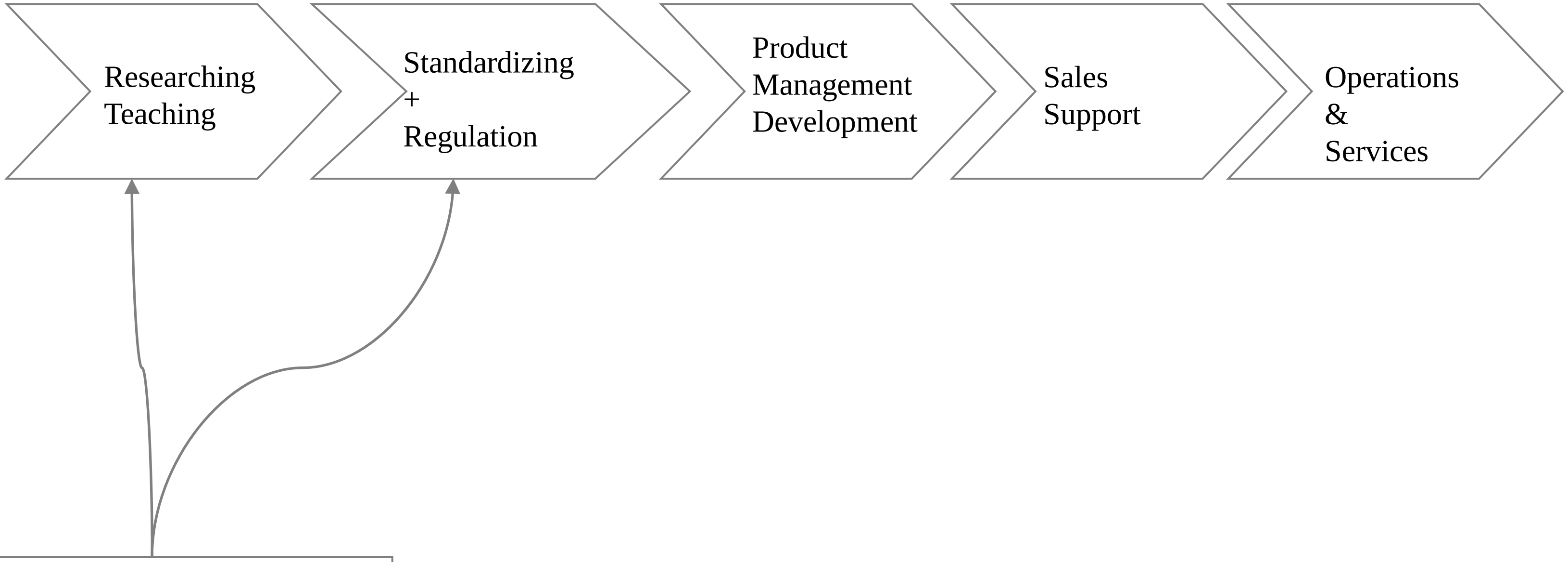
Product
Management
Development

Sales
Support

Operations
&
Services

Crypto Key Managment Systems Designer
Philips Fiancial Business System
1988

Stewart Kowalski Work Experience Along the IT/IS Security Value Chain



Researching
Teaching

Standardizing
+
Regulation

Product
Management
Development

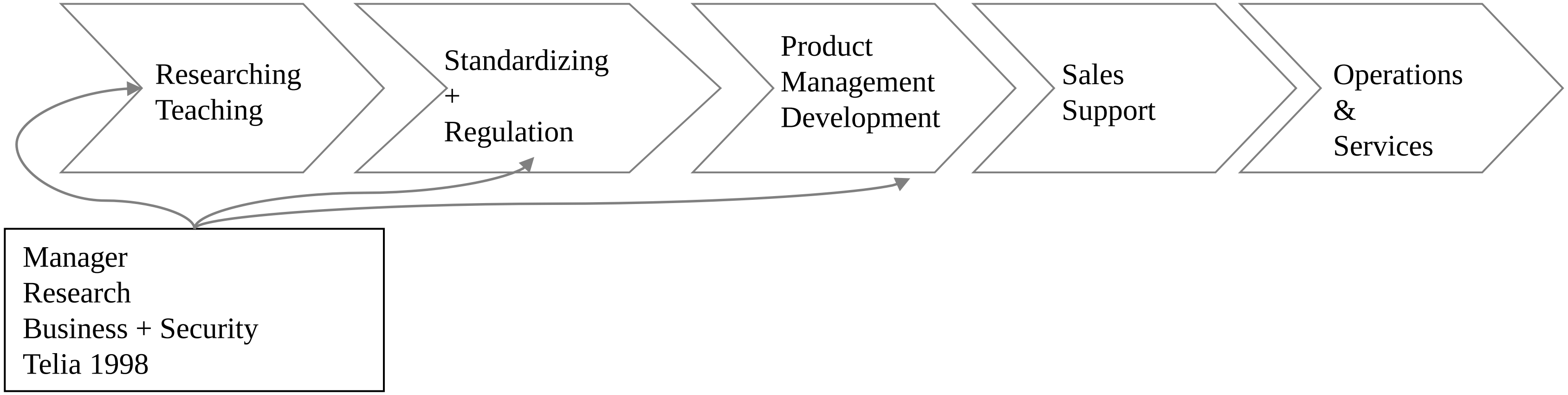
Sales
Support

Operations
&
Services

Assitant Professor
Computer & Telecom
Secruity and Business
1989
Stockholm Universtiy
Royal Institute of Technology
University College Gävle
Stockholm School of Economics

Crypto Key Managment Systems Designer
Philips Fiancial Business System
1988

Stewart Kowalski Work Experience Along the IT/IS Security Value Chain



Researching
Teaching

Standardizing
+
Regulation

Product
Management
Development

Sales
Support

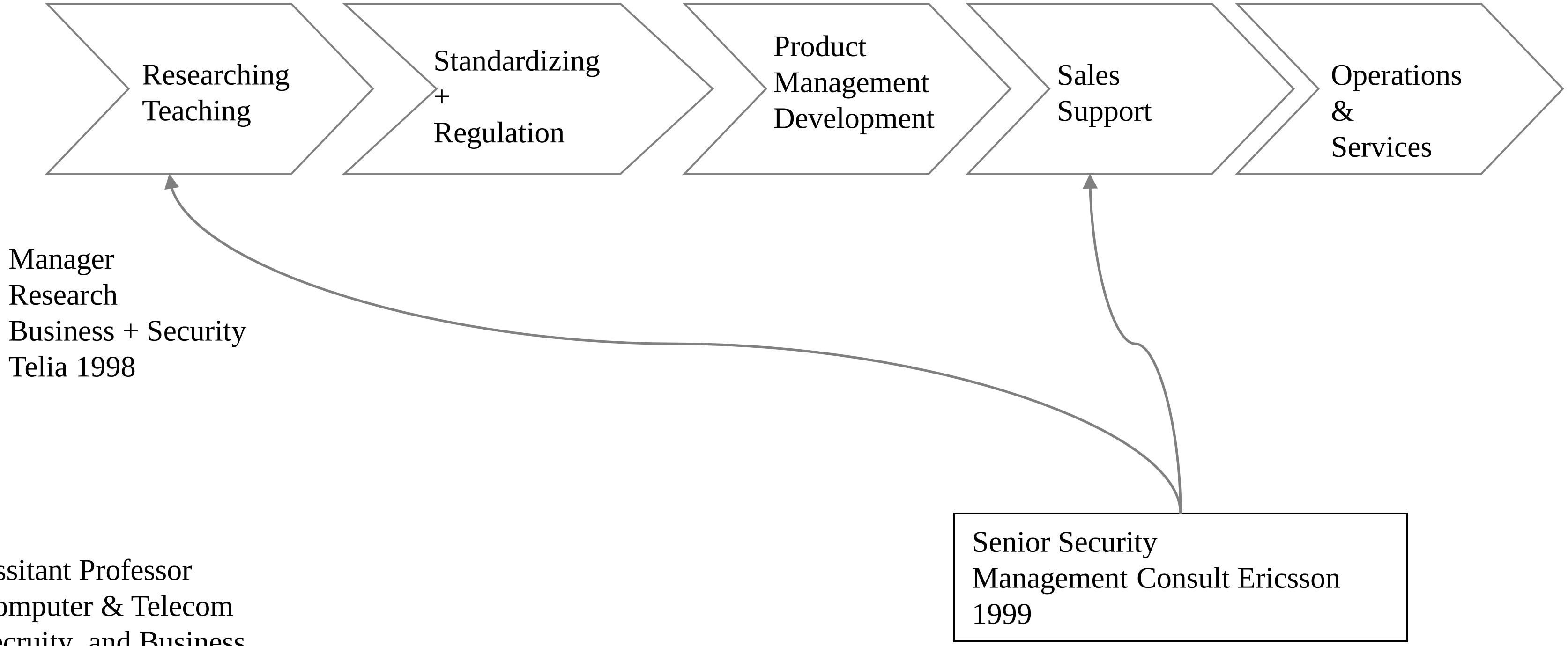
Operations
&
Services

Manager
Research
Business + Security
Telia 1998

Assitant Professor
Computer & Telecom
Secruity and Business
1989
Stockholm Universtiy
Royal Institute of Technology
University College Gävle
Stockholm School of Economics

Crypto Key Managment Systems Designer
Philips Fiancial Business System
1988

Stewart Kowalski Work Experience Stretched along IT/IS Security Value Chain



Researching
Teaching

Standardizing
+
Regulation

Product
Management
Development

Sales
Support

Operations
&
Services

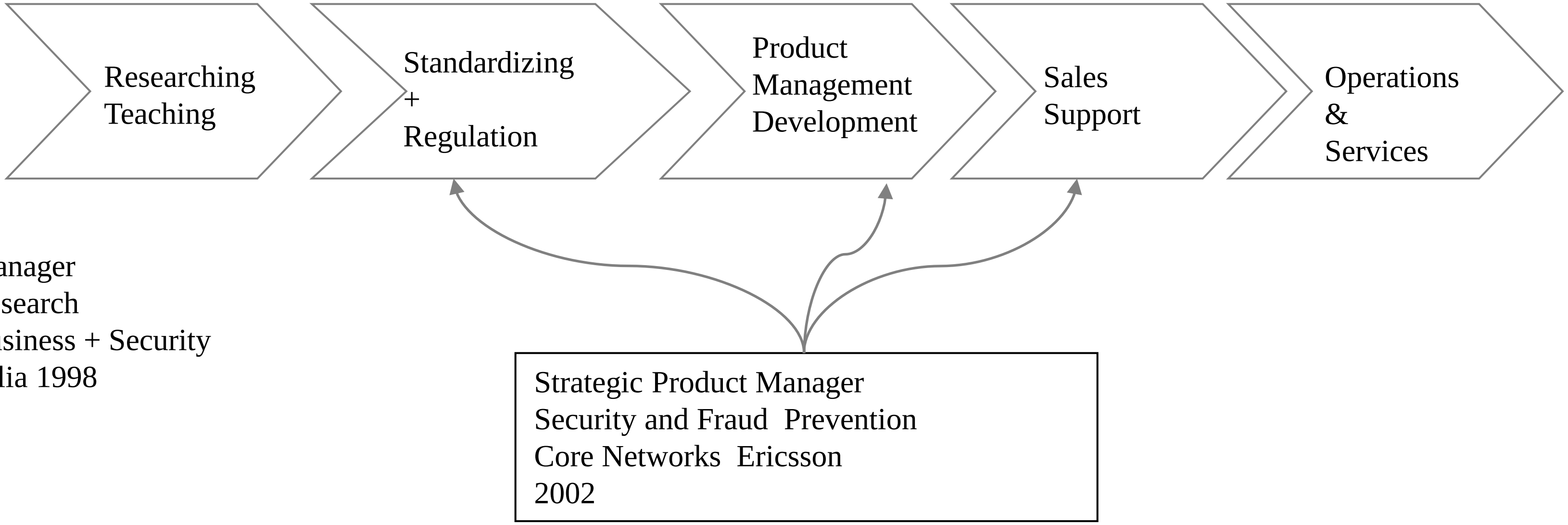
Manager
Research
Business + Security
Telia 1998

Senior Security
Management Consult Ericsson
1999

Assitant Professor
Computer & Telecom
Secruity and Business
1989
Stockholm Universtiy
Royal Institute of Technology
University College Gävle
Stockholm School of Economics

Crypto Key Managment Systems Designer
Philips Fiancial Business System
1988

Stewart Kowalski Work Experience Stretched along IT/IS Security Value Chain



Researching
Teaching

Standardizing
+
Regulation

Product
Management
Development

Sales
Support

Operations
&
Services

Strategic Product Manager
Security and Fraud Prevention
Core Networks Ericsson
2002

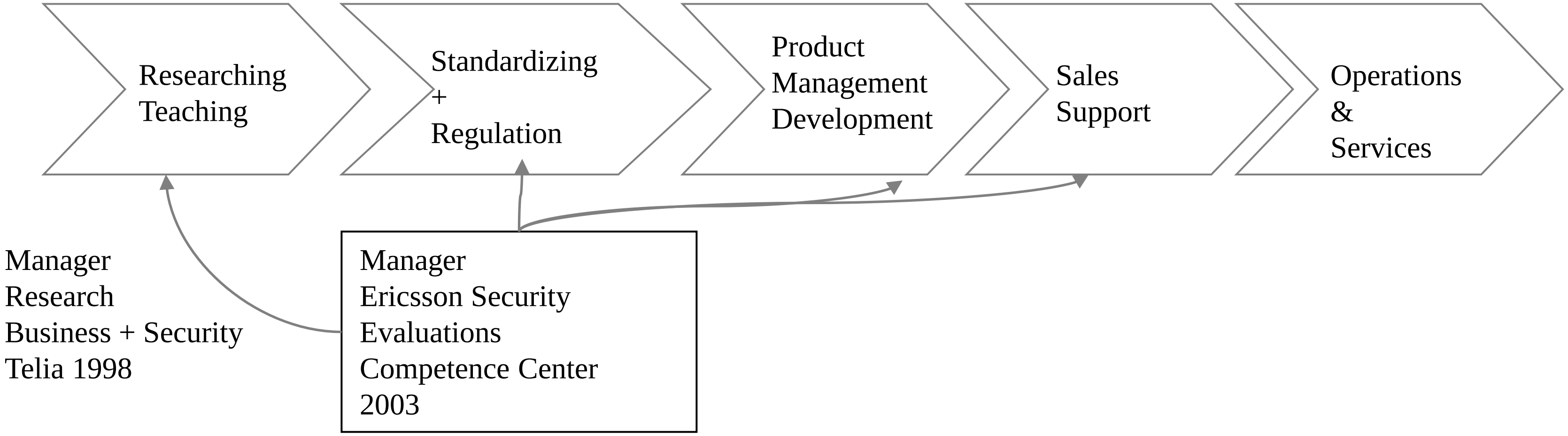
Manager
Research
Business + Security
Telia 1998

Senior Security
Management Consult Ericsson
1999

Assitant Professor
Computer & Telecom
Secruity and Business
1989
Stockholm Universtiy
Royal Institute of Technology
University College Gävle
Stockholm School of Economics

Crypto Key Managment Systems Designer
Philips Fiancial Business System
1988

Stewart Kowalski Work Experience Stretched along IT/IS Security Value Chain



Researching
Teaching

Standardizing
+
Regulation

Product
Management
Development

Sales
Support

Operations
&
Services

Manager
Research
Business + Security
Telia 1998

Manager
Ericsson Security
Evaluations
Competence Center
2003

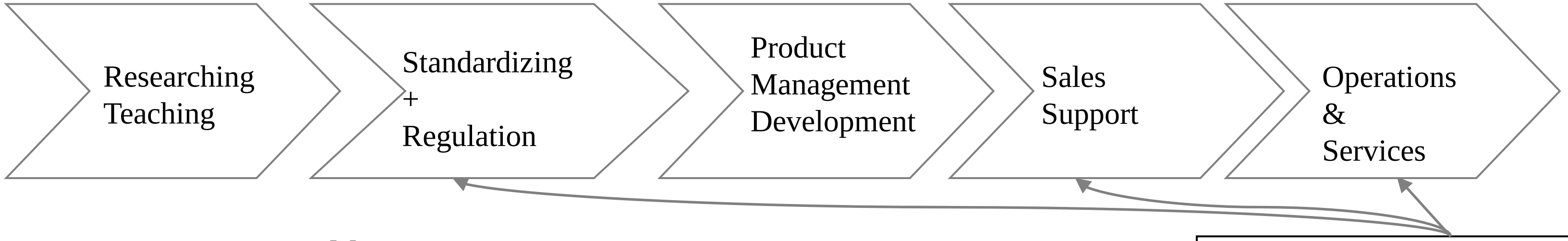
Strategic Product Manager
Security and Fraud Prevention
Core Networks Ericsson
2002

Senior Security
Management Consult Ericsson
1999

Assitant Professor
Computer & Telecom
Secruity and Business
1989
Stockholm Universtiy
Royal Institute of Technology
University College Gävle
Stockholm School of Econmics

Crypto Key Managment Systems Designer
Philips Fiancial Business System
1988

Stewart Kowalski Work Experience Stretched along IT/IS Security Value Chain



Researching
Teaching

Standardizing
+
Regulation

Product
Management
Development

Sales
Support

Operations
&
Services

Manager
Research
Business + Security
Telia 1998

Manager
Ericsson Security Evaluations
Competence Center
2003

Manger
Risk & Security
Business Unit Global Services
Global Network Operations Center
2006-2009

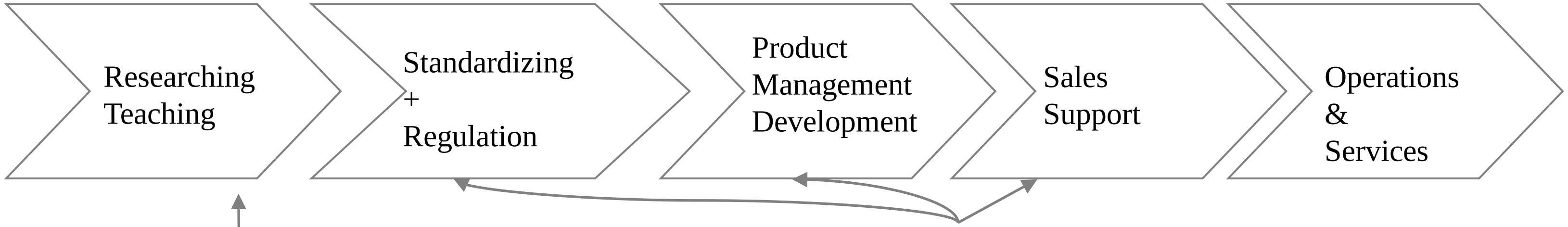
Strategic Product Manager
Security and Fraud Prevention
Core Networks Ericsson
2002

Senior Security
Management Consult Ericsson
1999

Assitant Professor
Computer & Telecom
Secruity and Business
1989
Stockholm Universtiy
Royal Institute of Technology
University College Gävle
Stockholm School of Economics

Crypto Key Managment Systems Designer
Philips Fiancial Business System
1988

Stewart Kowalski Work Experience Stretched along IT/IS Security Value Chain



Researching
Teaching

Standardizing
+
Regulation

Product
Management
Development

Sales
Support

Operations
&
Services

Manager
Research
Business + Security
Telia 1998

Manager
Ericsson Security Evaluations
Competence Center
2003

Senior Security Architecte and
Product Manager
Huawei Technologies
2009- 2011

Manger
Risk & Security
Business Unit Global Services
Global Network Operations Center
2006-2009

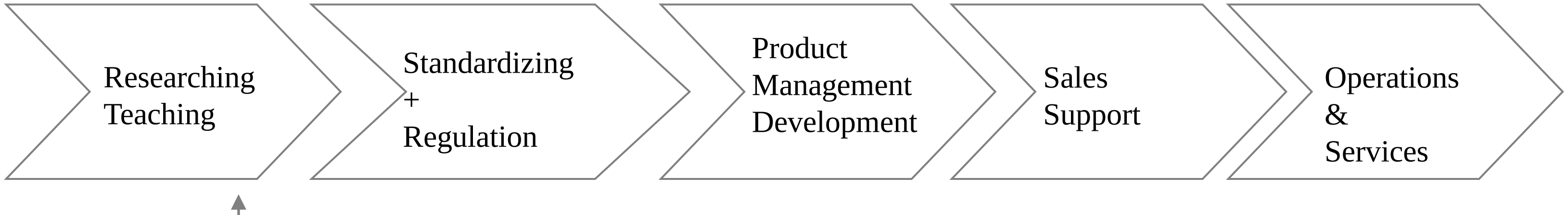
Strategic Product Manager
Security and Fraud Prevention
Core Networks Ericsson
2002

Senior Security
Management Consult Ericsson
1999

Associate Professor 17 May 2010
Assitant Professor
Computer & Telecom
Secruity and Business
1989
Stockholm Universtiy
Royal Institute of Technology
University College Gävle
Stockholm School of Economics

Crypto Key Managment Systems Designer
Philips Fiancial Business System
1988

Stewart Kowalski Work Experience Stretched along IT/IS Security Value Chain



Researching
Teaching

Standardizing
+
Regulation

Product
Management
Development

Sales
Support

Operations
&
Services

Manager
Research
Business + Security
Telia 1998

Manager
Ericsson Security Evaluations
Competence Center
2003

Senior Security Architecte and
Product Manager
Huawei Technologies
2009- 2011

Manger
Risk & Security
Business Unit Global Services
Global Network Operations Center
2006-2009

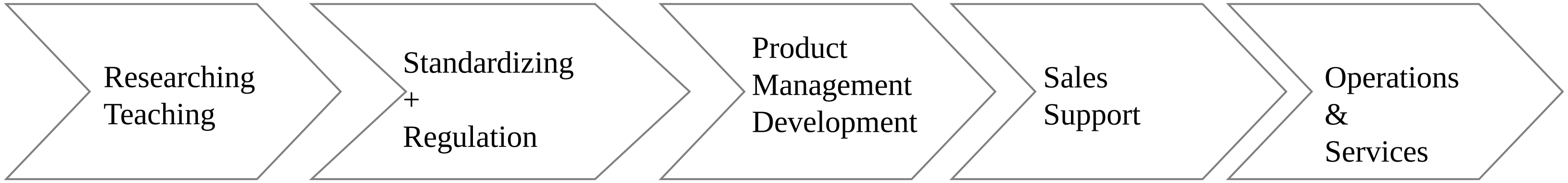
Strategic Product Manager
Security and Fraud Prevention
Core Networks Ericsson
2002

Senior Security
Management Consult Ericsson
1999

Full time academic 1st April 2011
Associate Professor
Computer & Telecom
Secruity and Business
1989
Stockholm Universtiy
Royal Institute of Technology
University College Gävle
Stockholm School of Business

Crypto Key Managment Systems Designer
Philips Fiancial Business System
1988

Stewart Kowalski Work Experience Stretched along IT/IS Security Value Chain



Researching
Teaching

Standardizing
+
Regulation

Product
Management
Development

Sales
Support

Operations
&
Services

Manager
Research
Business + Security
Telia 1998

Manager
Ericsson Security Evaluations
Competence Center
2003

Senior Security Architecte and
Product Manager
Huawei Technologies
2009- 2011

Manger
Risk & Security
Business Unit Global Services
Global Network Operations Center
2006-2009

Strategic Product Manager
Security and Fraud Prevention
Core Networks Ericsson
2002

Senior Security
Management Consult Ericsson
1999

Full Professor Information Security 1st August 2012
Associate Professor
Computer & Telecom
Secruity and Business
1989
Stockholm Universtiy
Royal Institute of Technology
University College Gävle
Stockholm School of Business
University College Gjøvik

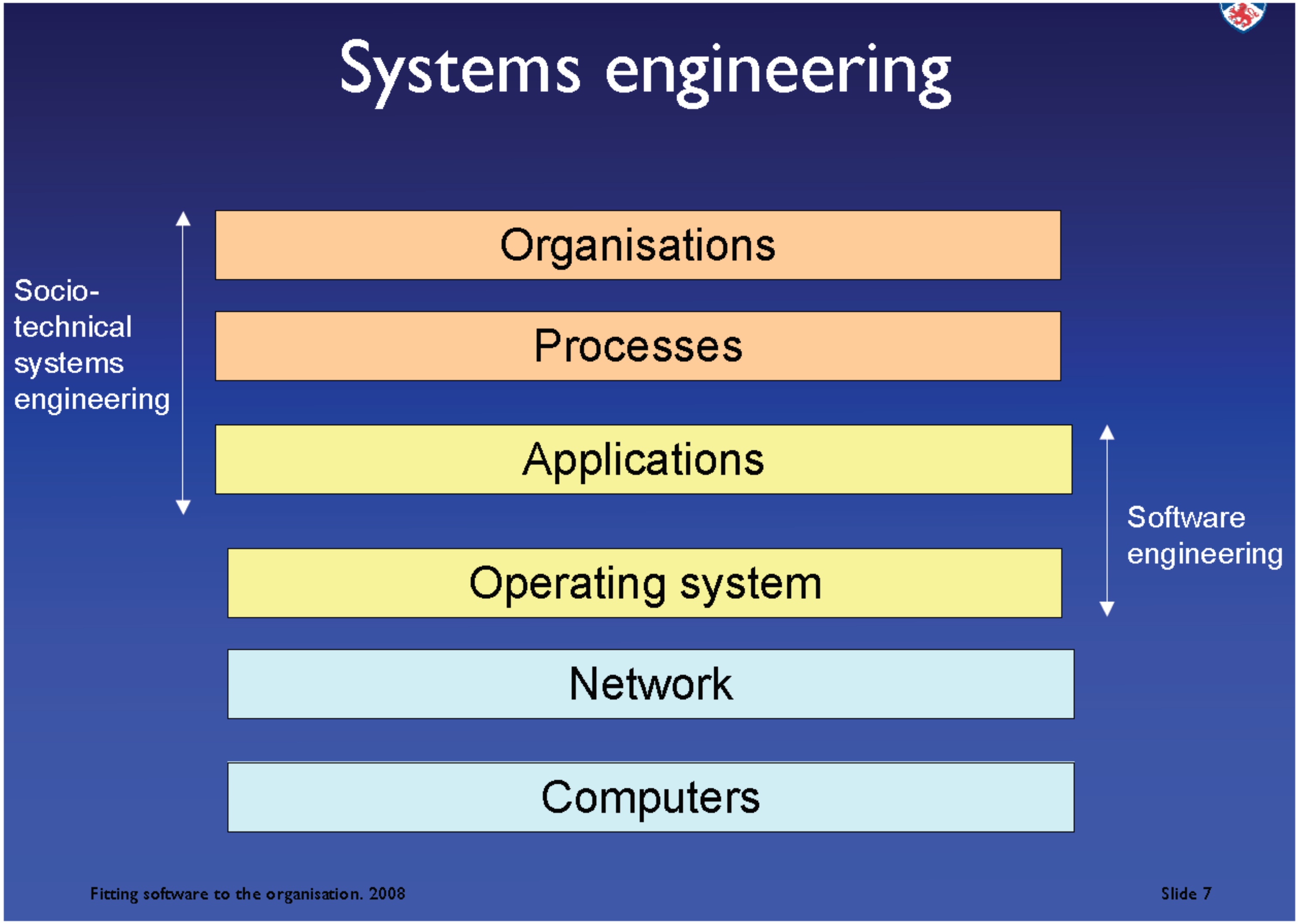
Crypto Key Managment Systems Designer
Philips Fiancial Business System
1988

The Socio Techncial Systems Approach

- Eric Trist and Ken Bamforth
  - 1950
  - Coal mine
  - Three levels
    - primary work system
    - the whole organization
    - macro-social phenomena

- IS area

- http://www.fsc.yorku.ca/york/istheory/wiki/index.php/Socio-technical_theory



Systems engineering

Socio-technical systems engineering

Organisations

Processes

Applications

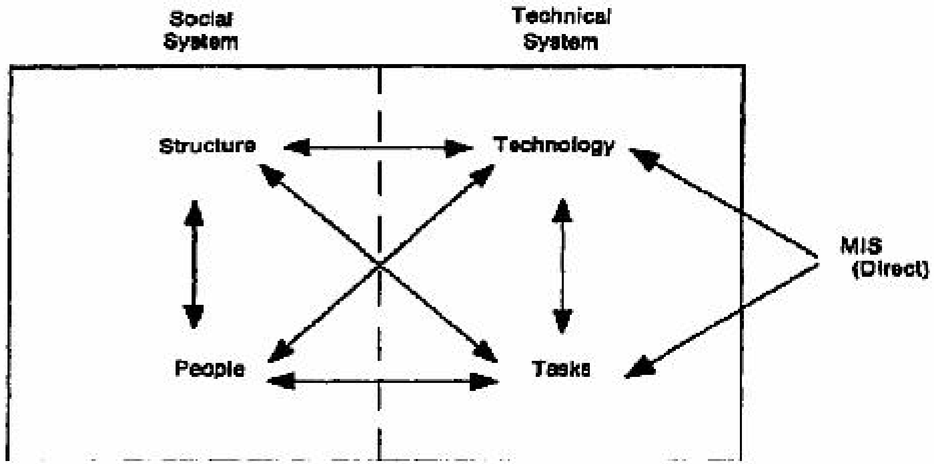
Software engineering

Operating system

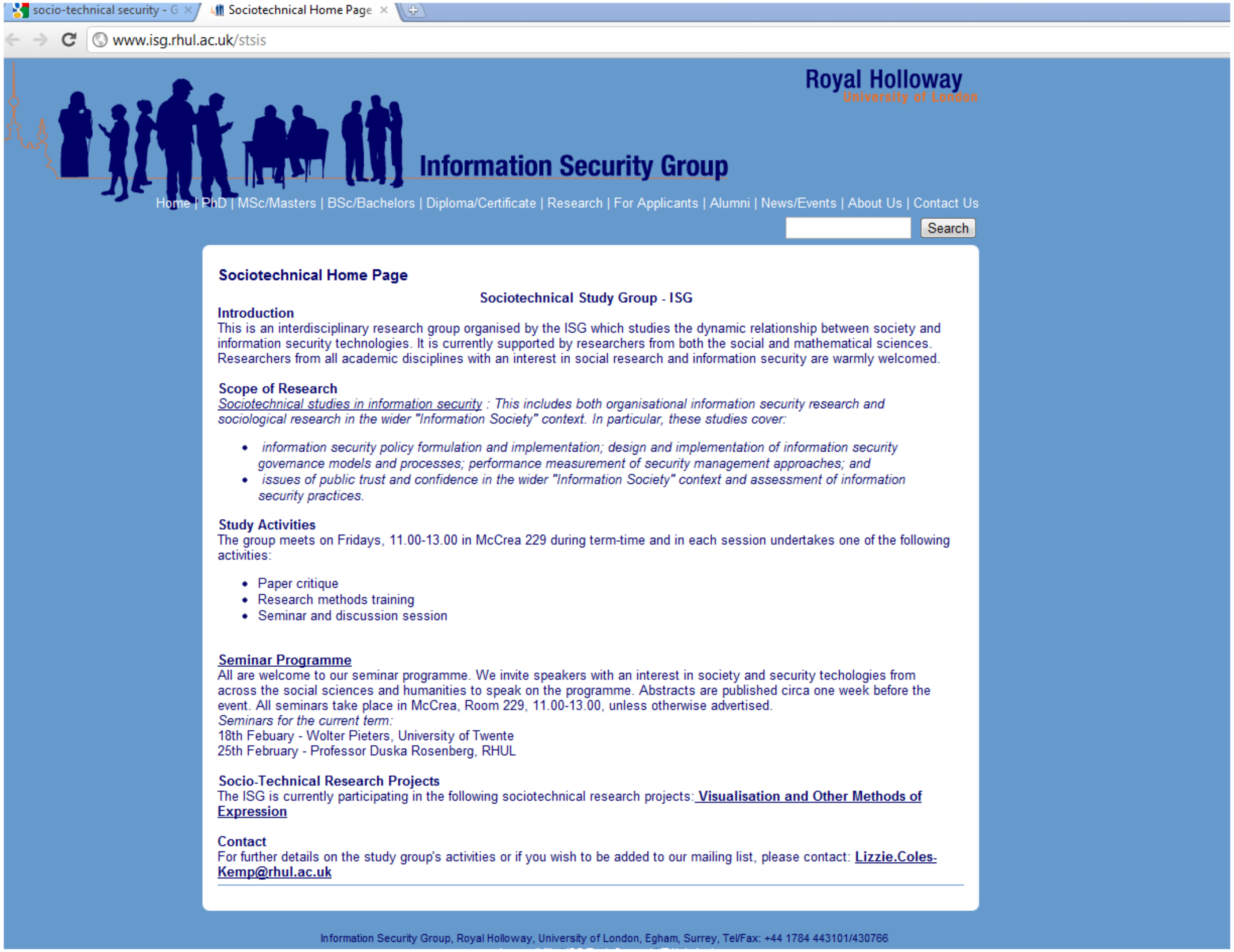
Network

Computers

Diagram/schematic of theory



MIS Problems and Failures: A Socio-Technical Perspective. Bostrom, Robert P.; Heinen, J. Stephen. MIS Quarterly, Sep77, Vol. 1 Issue 3


socio-technical security - G
Sociotechnical Home Page
www.isg.rhul.ac.uk/stsis
Royal Holloway
University of London
Information Security Group
Home | PhD | MSc/Masters | BSc/Bachelors | Diploma/Certificate | Research | For Applicants | Alumni | News/Events | About Us | Contact Us
Search

Sociotechnical Home Page

Sociotechnical Study Group - ISG

Introduction
This is an interdisciplinary research group organised by the ISG which studies the dynamic relationship between society and information security technologies. It is currently supported by researchers from both the social and mathematical sciences. Researchers from all academic disciplines with an interest in social research and information security are warmly welcomed.

Scope of Research
Sociotechnical studies in information security : This includes both organisational information security research and sociological research in the wider "Information Society" context. In particular, these studies cover:

- *information security policy formulation and implementation; design and implementation of information security governance models and processes; performance measurement of security management approaches; and*
- *issues of public trust and confidence in the wider "Information Society" context and assessment of information security practices.*

Study Activities
The group meets on Fridays, 11.00-13.00 in McCrea 229 during term-time and in each session undertakes one of the following activities:

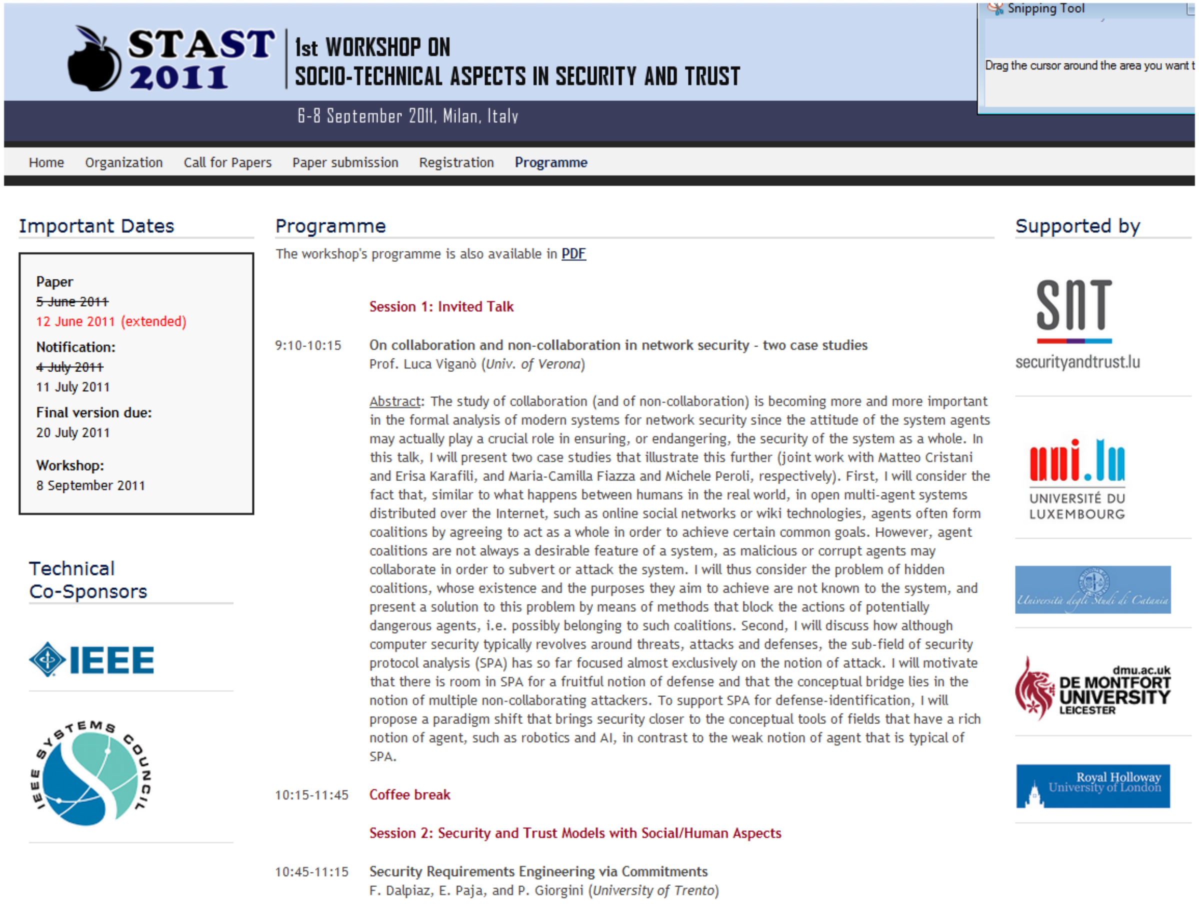
- Paper critique
- Research methods training
- Seminar and discussion session

Seminar Programme
All are welcome to our seminar programme. We invite speakers with an interest in society and security techologies from across the social sciences and humanities to speak on the programme. Abstracts are published circa one week before the event. All seminars take place in McCrea, Room 229, 11.00-13.00, unless otherwise advertised.
Seminars for the current term:
18th Febuary - Wolter Pieters, University of Twente
25th February - Professor Duska Rosenberg, RHUL

Socio-Technical Research Projects
The ISG is currently participating in the following sociotechnical research projects: **Visualisation and Other Methods of Expression**

Contact
For further details on the study group's activities or if you wish to be added to our mailing list, please contact: **Lizzie.Coles-Kemp@rhul.ac.uk**

Information Security Group, Royal Holloway, University of London, Egham, Surrey, Tel/Fax: +44 1784 443101/430766



Drag the cursor around the area you want t

Important Dates

Paper
~~5 June 2011~~
12 June 2011 (extended)

Notification:
~~4 July 2011~~
11 July 2011

Final version due:
20 July 2011

Workshop:
8 September 2011

Technical Co-Sponsors

Programme

The workshop's programme is also available in PDF

Session 1: Invited Talk

9:10-10:15 On collaboration and non-collaboration in network security - two case studies
Prof. Luca Viganò (*Univ. of Verona*)

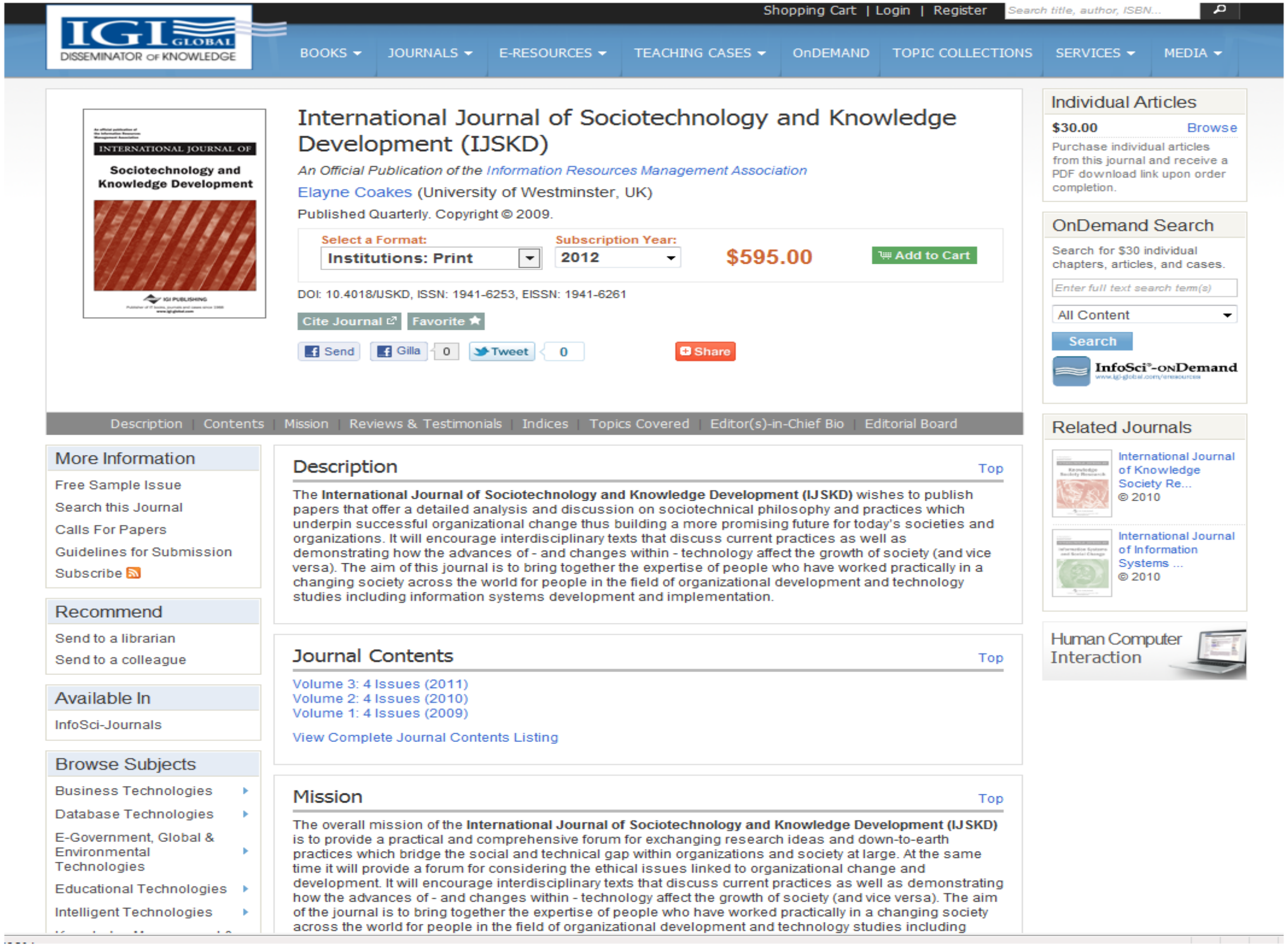
Abstract: The study of collaboration (and of non-collaboration) is becoming more and more important in the formal analysis of modern systems for network security since the attitude of the system agents may actually play a crucial role in ensuring, or endangering, the security of the system as a whole. In this talk, I will present two case studies that illustrate this further (joint work with Matteo Cristani and Erisa Karafili, and Maria-Camilla Fiazza and Michele Peroli, respectively). First, I will consider the fact that, similar to what happens between humans in the real world, in open multi-agent systems distributed over the Internet, such as online social networks or wiki technologies, agents often form coalitions by agreeing to act as a whole in order to achieve certain common goals. However, agent coalitions are not always a desirable feature of a system, as malicious or corrupt agents may collaborate in order to subvert or attack the system. I will thus consider the problem of hidden coalitions, whose existence and the purposes they aim to achieve are not known to the system, and present a solution to this problem by means of methods that block the actions of potentially dangerous agents, i.e. possibly belonging to such coalitions. Second, I will discuss how although computer security typically revolves around threats, attacks and defenses, the sub-field of security protocol analysis (SPA) has so far focused almost exclusively on the notion of attack. I will motivate that there is room in SPA for a fruitful notion of defense and that the conceptual bridge lies in the notion of multiple non-collaborating attackers. To support SPA for defense-identification, I will propose a paradigm shift that brings security closer to the conceptual tools of fields that have a rich notion of agent, such as robotics and AI, in contrast to the weak notion of agent that is typical of SPA.

10:15-11:45 Coffee break

Session 2: Security and Trust Models with Social/Human Aspects

10:45-11:15 Security Requirements Engineering via Commitments
F. Dalpiaz, E. Paja, and P. Giorgini (*University of Trento*)

Supported by


Shopping Cart | Login | Register
Search title, author, ISBN...
IGI GLOBAL
DISSEMINATOR OF KNOWLEDGE
BOOKS
JOURNALS
E-RESOURCES
TEACHING CASES
OnDEMAND
TOPIC COLLECTIONS
SERVICES
MEDIA
INTERNATIONAL JOURNAL OF
Sociotechnology and Knowledge Development
IGI PUBLISHING
Cite Journal
Favorite
Send
Gilla
0
Tweet
0
Share
Description | Contents | Mission | Reviews & Testimonials | Indices | Topics Covered | Editor(s)-in-Chief Bio | Editorial Board
Top
Search
InfoSci®-onDemand
www.igi-global.com/eresources
Human Computer Interaction

International Journal of Sociotechnology and Knowledge Development (IJSKD)

An Official Publication of the Information Resources Management Association

Elayne Coakes (University of Westminster, UK)

Published Quarterly. Copyright © 2009.

Select a Format: Institutions: Print

Subscription Year: 2012

$595.00

Add to Cart

DOI: 10.4018/IJSKD, ISSN: 1941-6253, EISSN: 1941-6261

More Information

- Free Sample Issue
- Search this Journal
- Calls For Papers
- Guidelines for Submission
- Subscribe

Recommend

- Send to a librarian
- Send to a colleague

Available In

- InfoSci-Journals

Browse Subjects

- Business Technologies
- Database Technologies
- E-Government, Global & Environmental Technologies
- Educational Technologies
- Intelligent Technologies

Description

The **International Journal of Sociotechnology and Knowledge Development (IJSKD)** wishes to publish papers that offer a detailed analysis and discussion on sociotechnical philosophy and practices which underpin successful organizational change thus building a more promising future for today's societies and organizations. It will encourage interdisciplinary texts that discuss current practices as well as demonstrating how the advances of - and changes within - technology affect the growth of society (and vice versa). The aim of this journal is to bring together the expertise of people who have worked practically in a changing society across the world for people in the field of organizational development and technology studies including information systems development and implementation.

Journal Contents

- Volume 3: 4 Issues (2011)
- Volume 2: 4 Issues (2010)
- Volume 1: 4 Issues (2009)

View Complete Journal Contents Listing

Mission

The overall mission of the **International Journal of Sociotechnology and Knowledge Development (IJSKD)** is to provide a practical and comprehensive forum for exchanging research ideas and down-to-earth practices which bridge the social and technical gap within organizations and society at large. At the same time it will provide a forum for considering the ethical issues linked to organizational change and development. It will encourage interdisciplinary texts that discuss current practices as well as demonstrating how the advances of - and changes within - technology affect the growth of society (and vice versa). The aim of the journal is to bring together the expertise of people who have worked practically in a changing society across the world for people in the field of organizational development and technology studies including

Individual Articles

$30.00 Browse

Purchase individual articles from this journal and receive a PDF download link upon order completion.

OnDemand Search

Search for $30 individual chapters, articles, and cases.

Enter full text search term(s)

All Content

Related Journals

- International Journal of Knowledge Society Re... © 2010
- International Journal of Information Systems ... © 2010

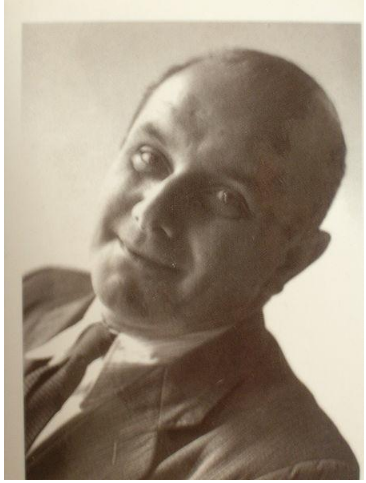
Outline

- Background
- Why do we model?
- How do we model?

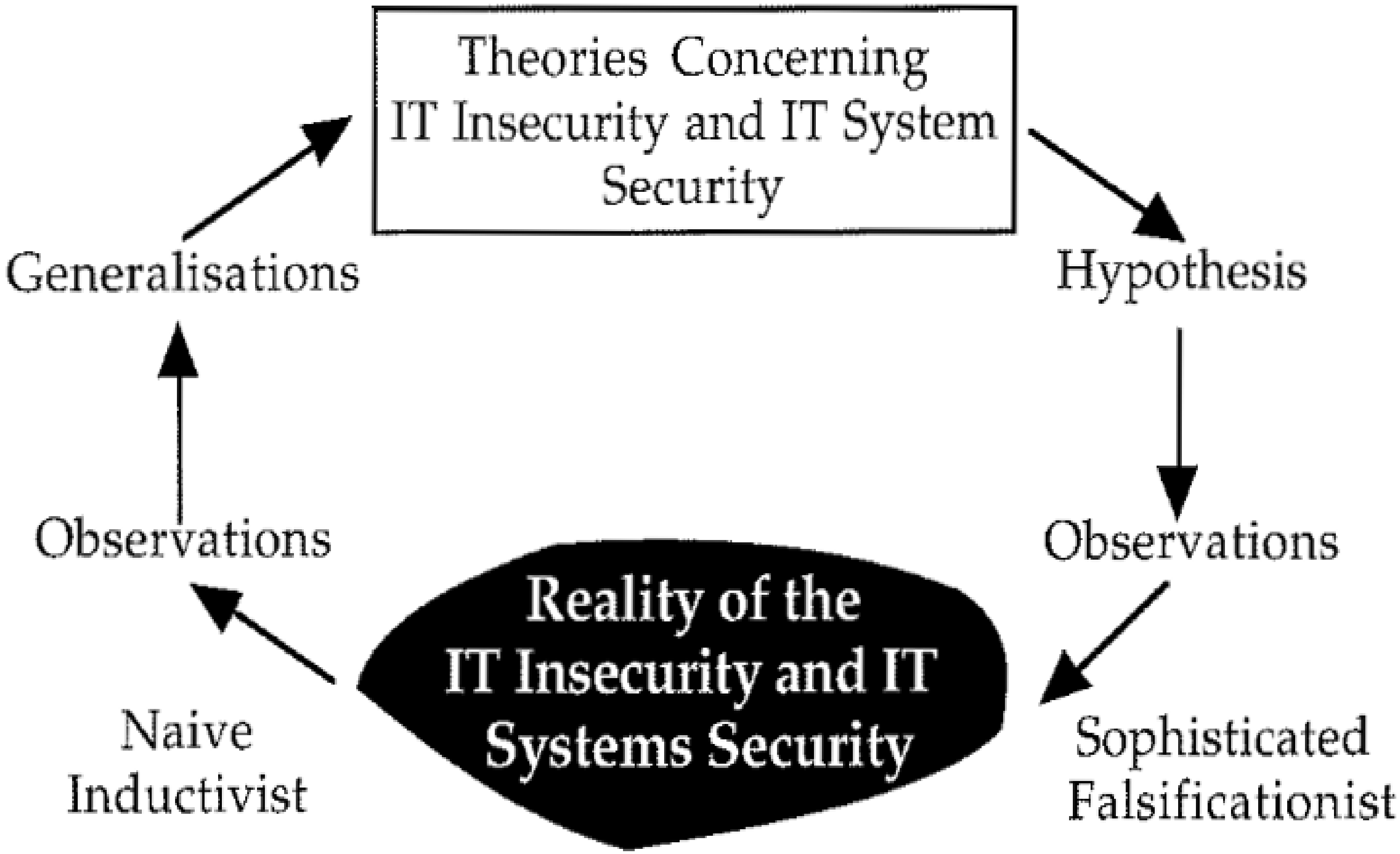
Why Do We Model

Some like to undestand what they believe in.
Others like to believe in what they understand.
(Stainslaw Jerzy Lec)

Which one are you?



Niave Mental Models
”engineering vs science”


Theories Concerning IT Insecurity and IT System Security
Hypothesis
Observations
Sophisticated Falsificationist
Reality of the IT Insecurity and IT Systems Security
Naive Inductivist
Observations
Generalisations

Some like to believe in what they understand

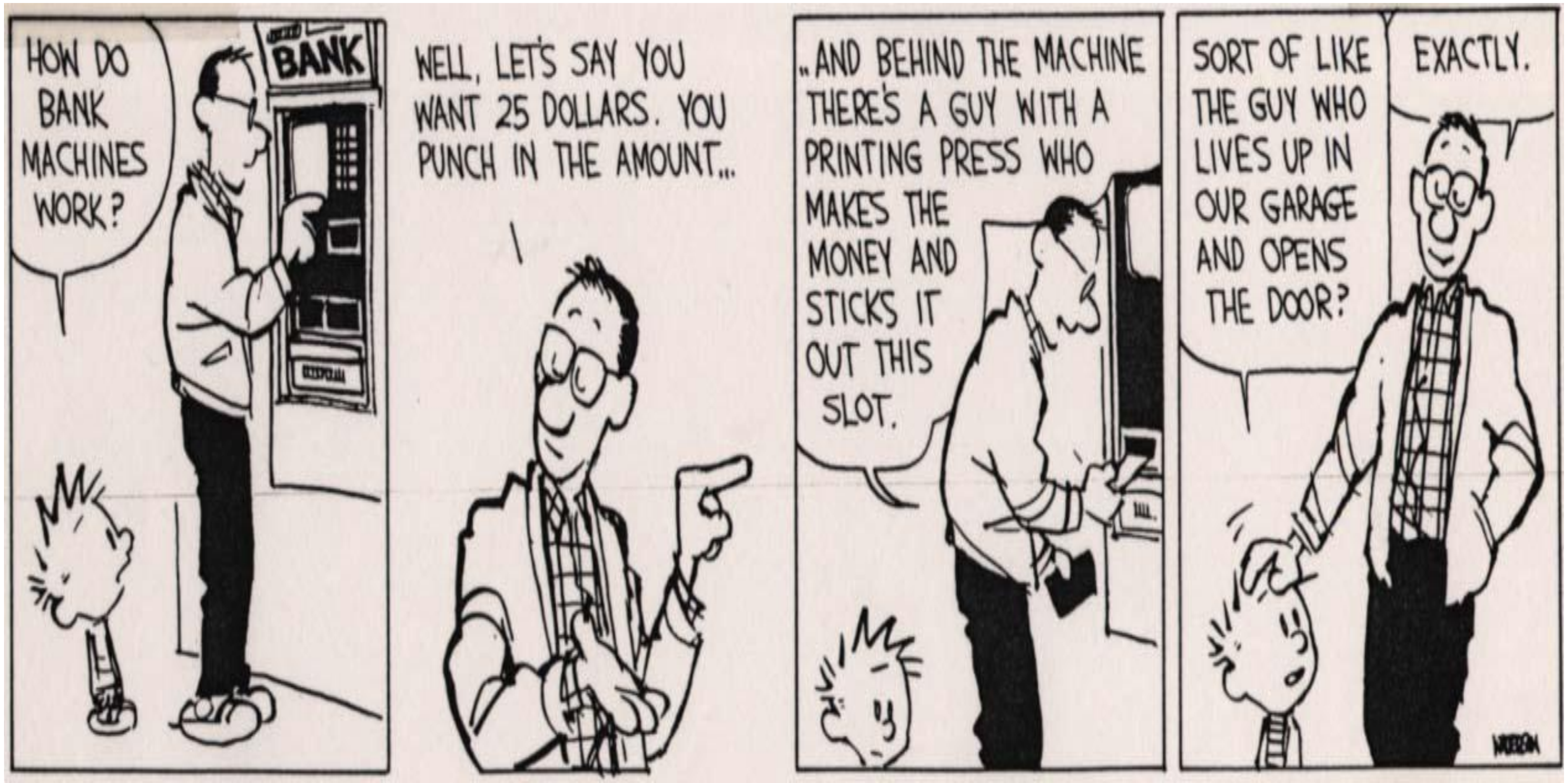
Some like to undestand what they believe in.

Naïve inductivist and sophisticated falsificationist [Kowalski, 1994]

Mental Models

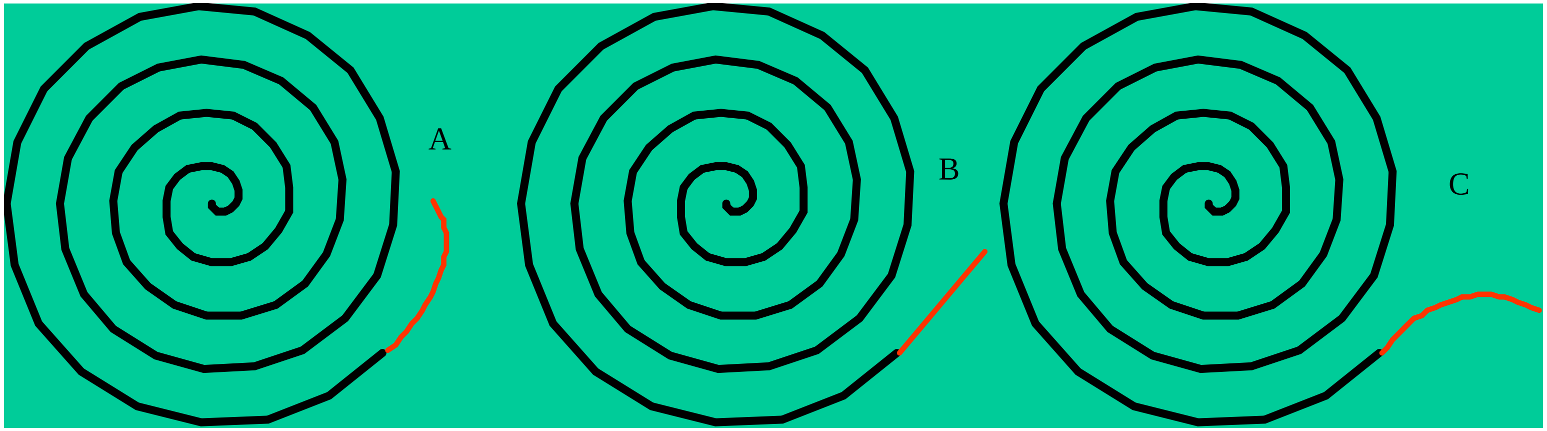
- The concept was first introduced by Kenneth Craik in his book *The Nature of Explanation* (1943).
  - that the mind forms models of reality and uses them to predict similar future events.
- User gain experience by seeing and using thinks and systems
- User gradually form a working model of the systems based on their past experience.
- As they use gain more experience they develop a model to predict how the system works or does not work
- http://managementhelp.org/systems/systems.htm

Mental Model ATM

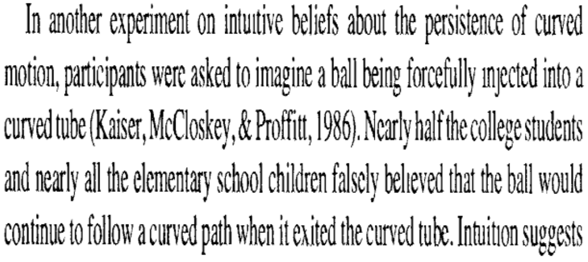

HOW DO BANK MACHINES WORK?
BANK
WELL, LET'S SAY YOU WANT 25 DOLLARS. YOU PUNCH IN THE AMOUNT...
..AND BEHIND THE MACHINE THERE'S A GUY WITH A PRINTING PRESS WHO MAKES THE MONEY AND STICKS IT OUT THIS SLOT.
SORT OF LIKE THE GUY WHO LIVES UP IN OUR GARAGE AND OPENS THE DOOR?
EXACTLY.
WATTERSON

Naïve physics (Visual Logic)

- What would happen to a ball shot through this pipe?

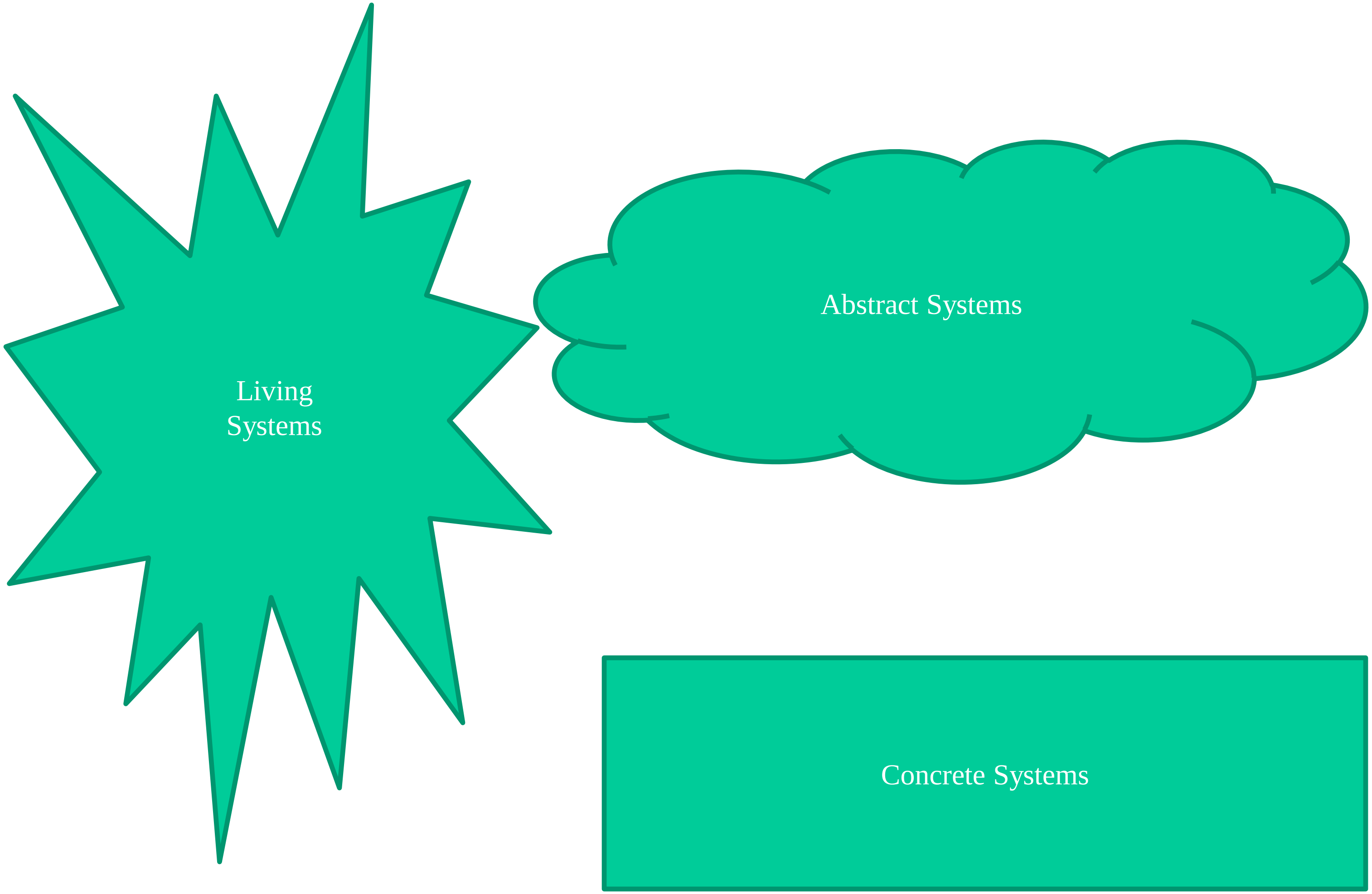


- People often respond by assuming curvilinear momentum
  - McCloskey and Proffitt

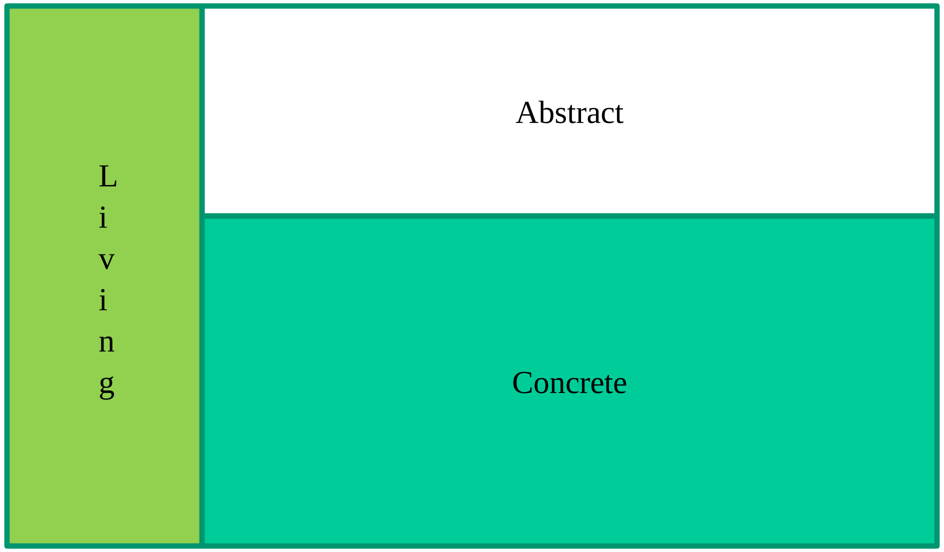


In another experiment on intuitive beliefs about the persistence of curved motion, participants were asked to imagine a ball being forcefully injected into a curved tube (Kaiser, McCloskey, & Proffitt, 1986). Nearly half the college students and nearly all the elementary school children falsely believed that the ball would continue to follow a curved path when it exited the curved tube. Intuition suggests

Basic System Theory Model



System Theory Architecture

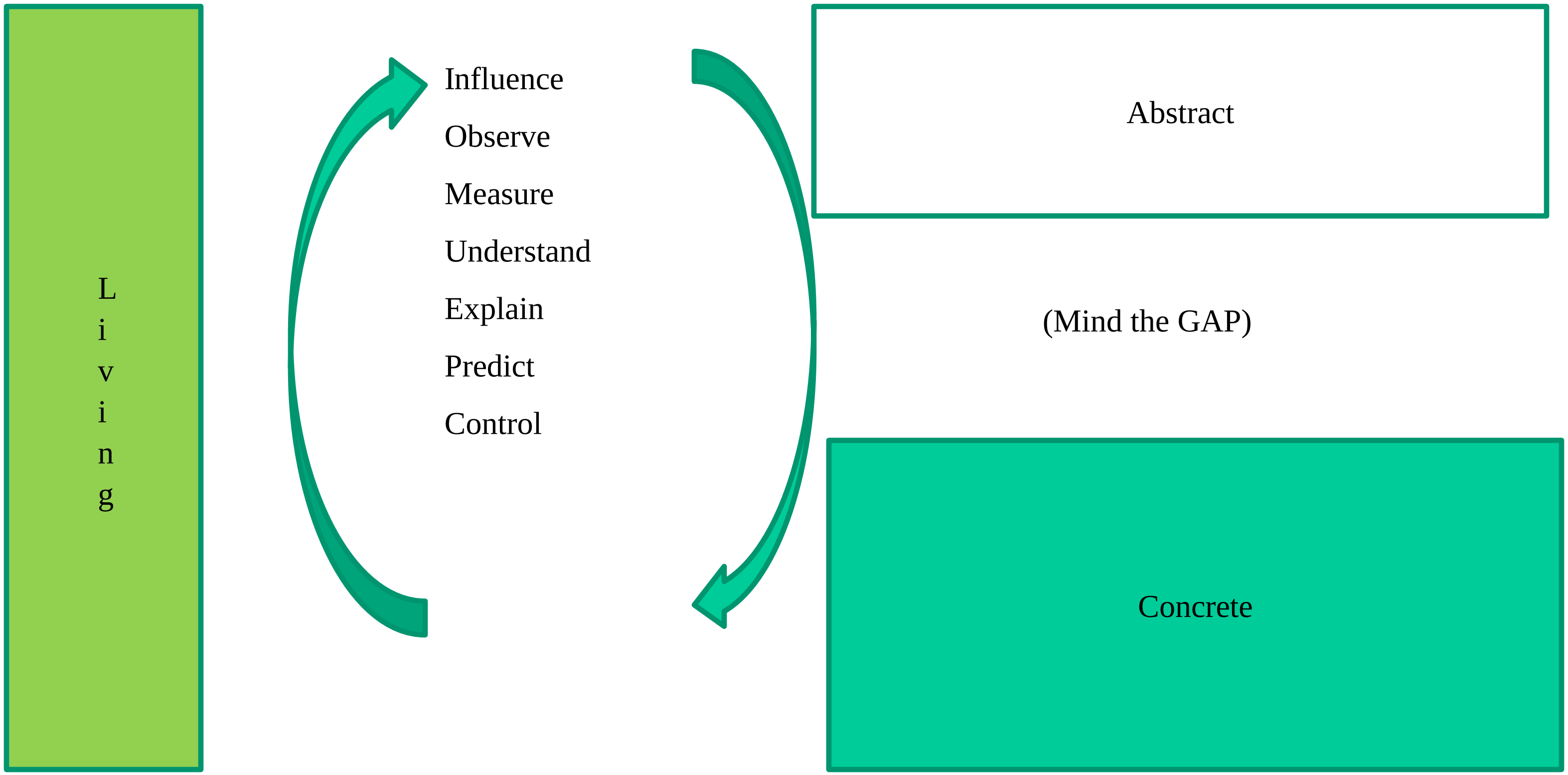


Living

Abstract

Concrete

System Theory
Action Architecture



Living

Influence

Observe

Measure

Understand

Explain

Predict

Control

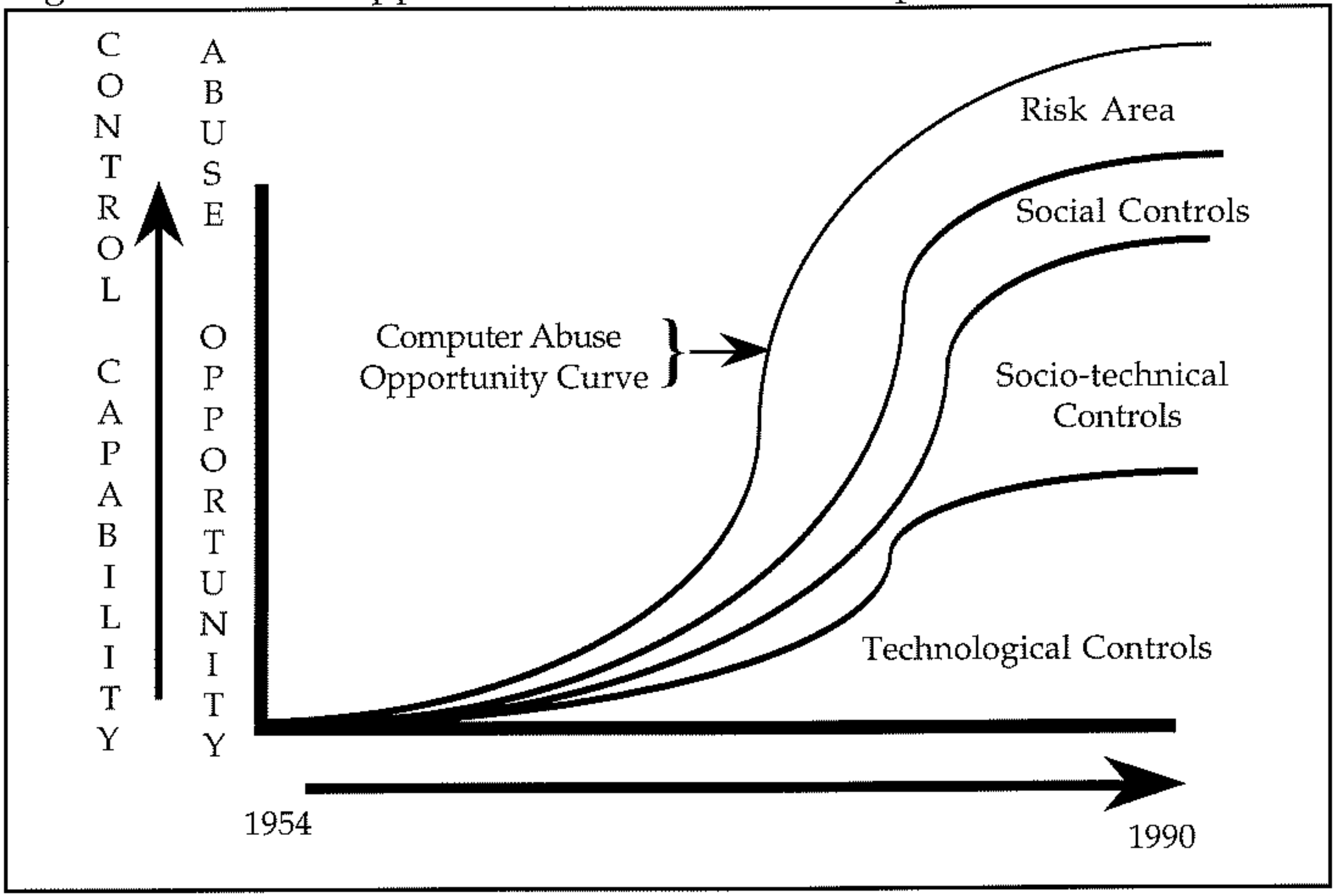
Abstract

(Mind the GAP)

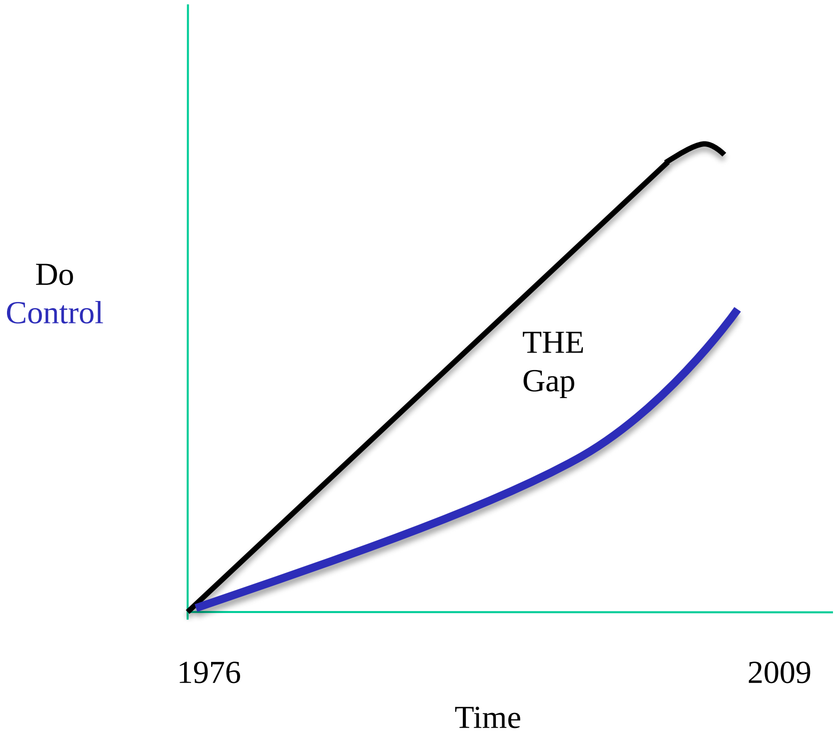
Concrete

Control Gaps

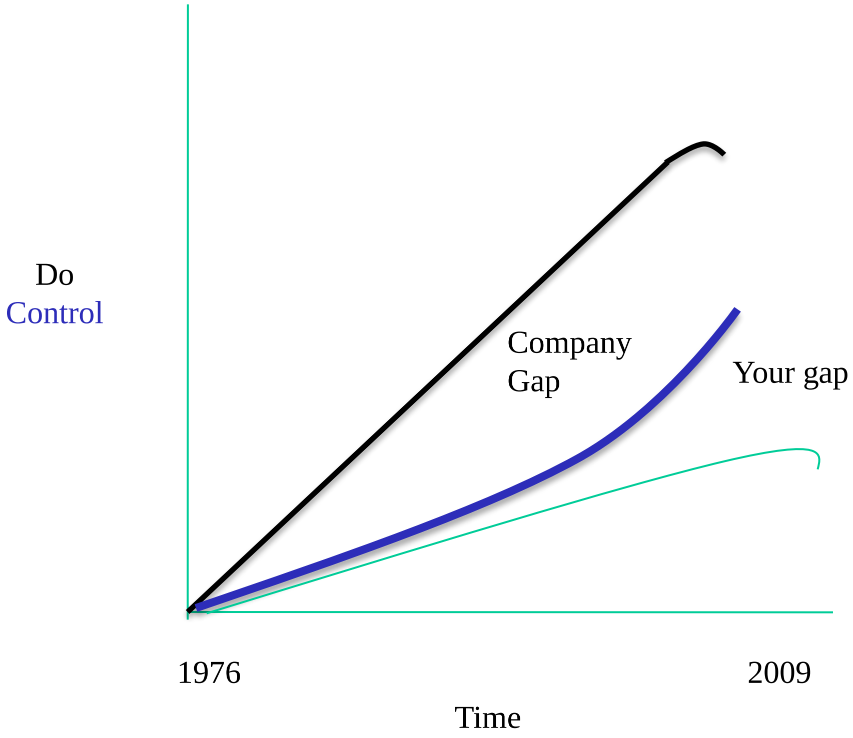
Figure 3.1 Abuse Opportunities and Control Capabilities vs. Time



What we/they can do with IT
&
What we can control with IT
Vs
Time

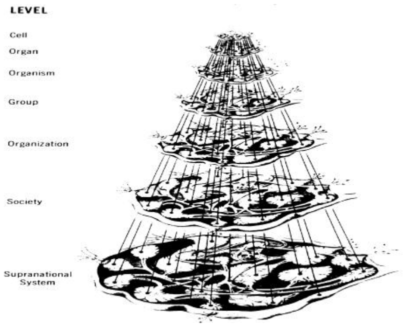


What we/they can do with IT
&
What you can control with IT
Vs
Time



System Theory
Action Architecture

You & Me



Influence

Observe

Measure

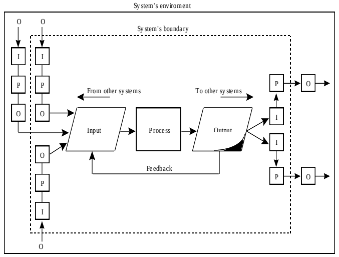
Understand

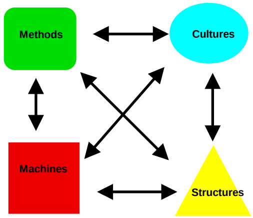
Explain

Predict

Control

Abstract

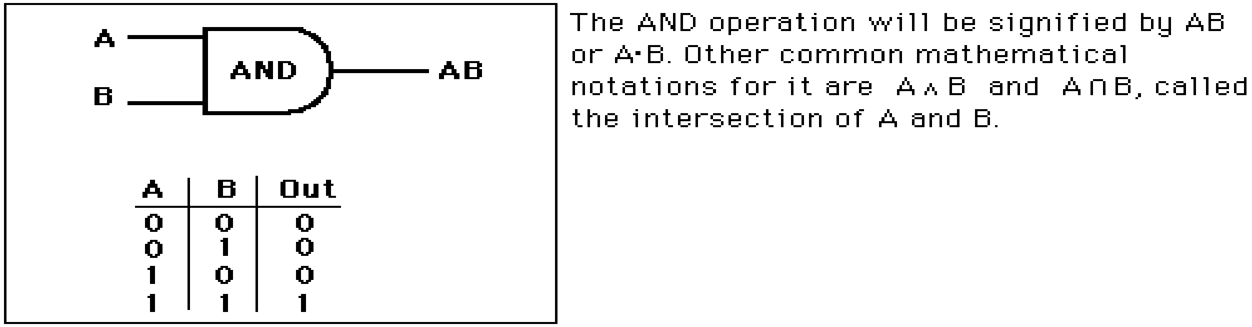




Concrete

Abstract and Concrete Model (AND GATE)

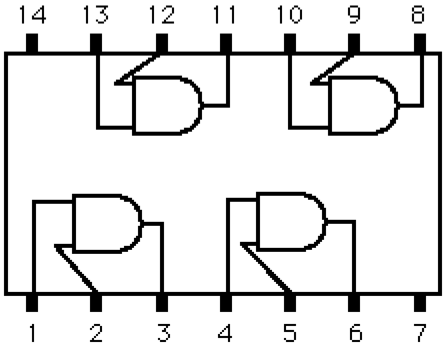
Abstract GATE



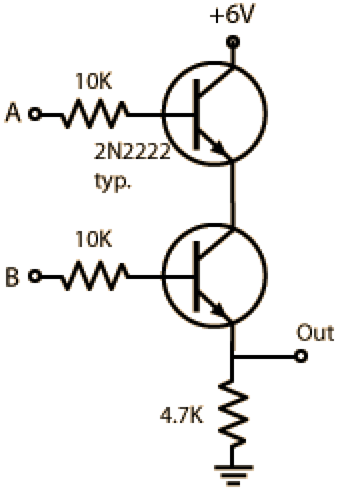
A	B	Out
0	0	0
0	1	0
1	0	0
1	1	1

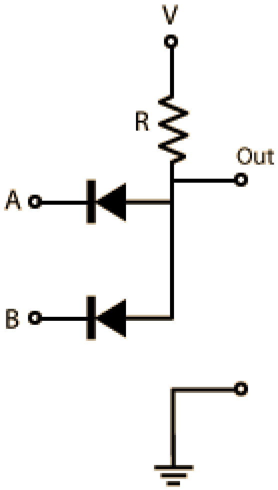
The AND operation will be signified by AB or A·B. Other common mathematical notations for it are $A \wedge B$ and $A \cap B$, called the intersection of A and B.

Contet lAND GATE

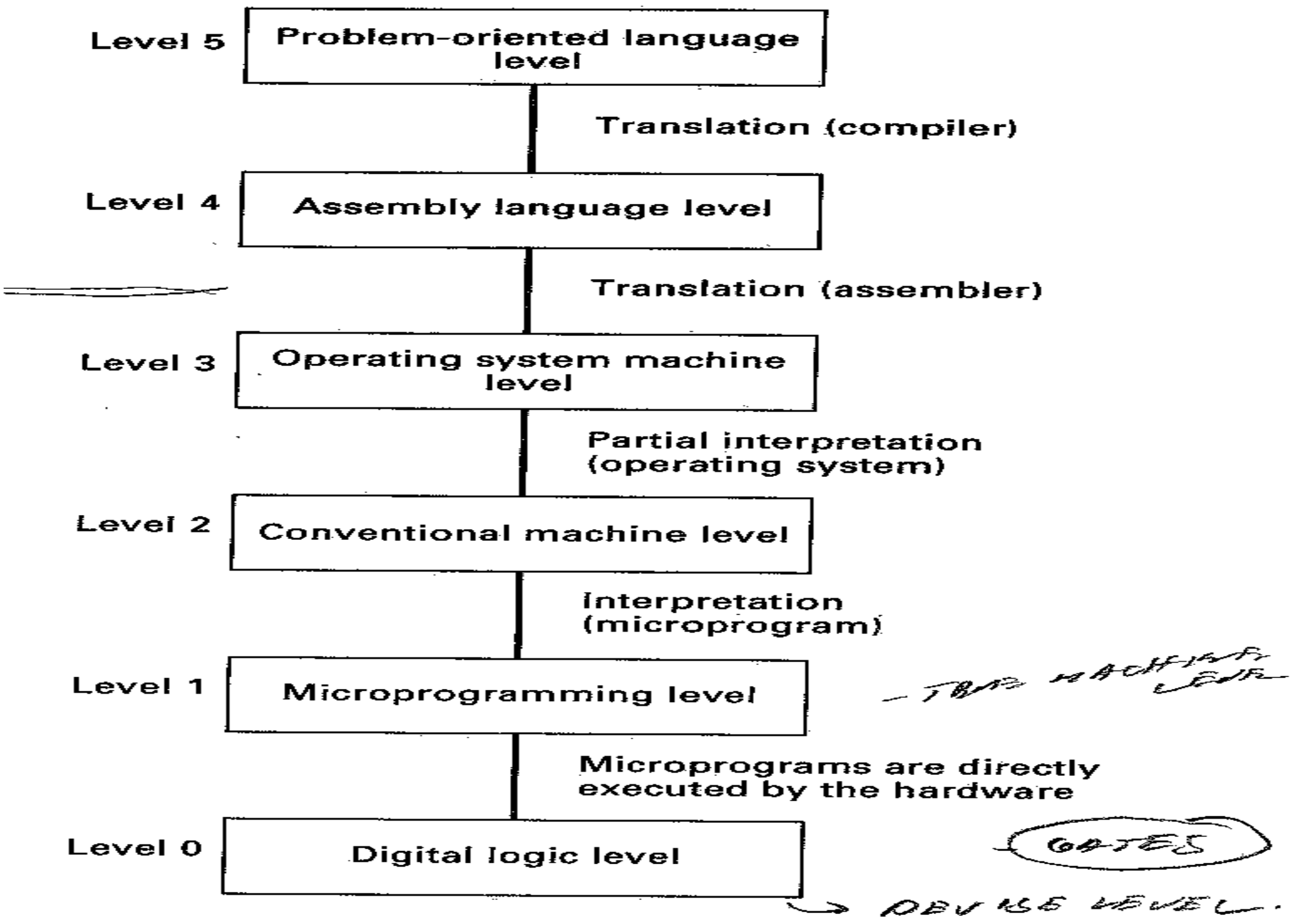


CHIP
IC7408





Abstract Model
Computer System



Level 5 — Problem-oriented language level

Translation (compiler)

Level 4 — Assembly language level

Translation (assembler)

Level 3 — Operating system machine level

Partial interpretation (operating system)

Level 2 — Conventional machine level

Interpretation (microprogram)

Level 1 — Microprogramming level

Microprograms are directly executed by the hardware

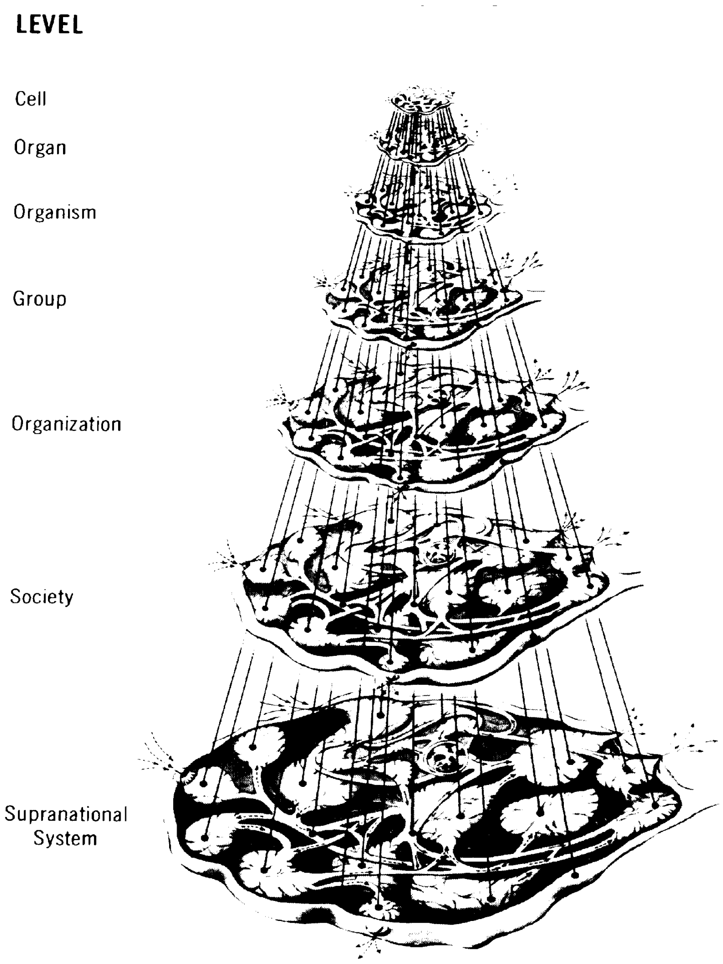
Level 0 — Digital logic level

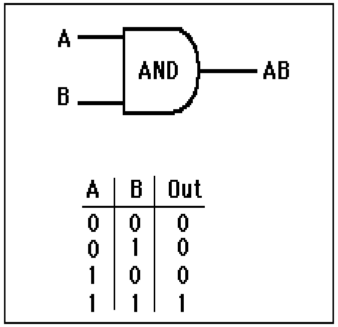
- THE MACHINE LEVEL

GATES

→ DEVICE LEVEL.

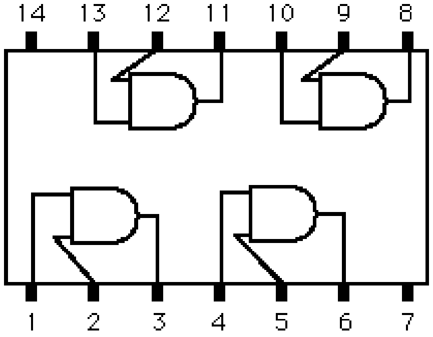
Mental Model
Systems of Systems



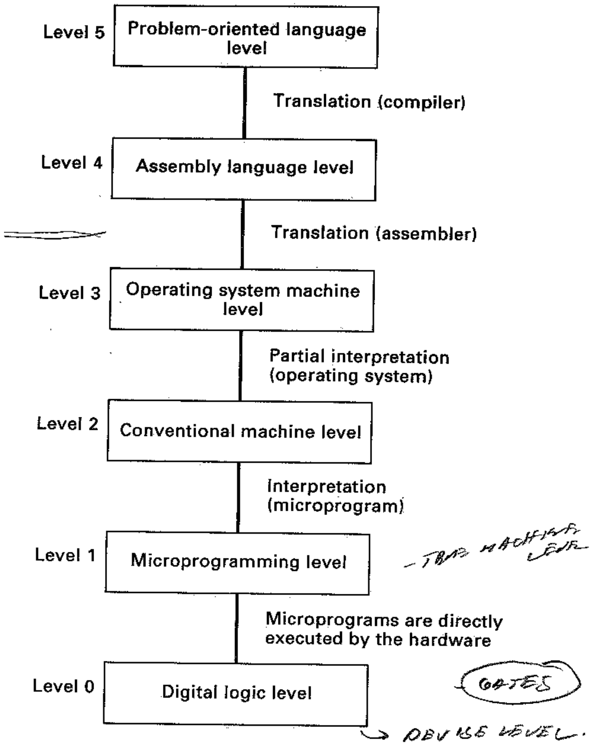


A	B	Out
0	0	0
0	1	0
1	0	0
1	1	1

The AND operation will be signified by AB or A·B. Other common mathematical notations for it are A∧B and A∩B, called the intersection of A and B.



Mental Model ICT



Level 5 Problem-oriented language level

Translation (compiler)

Level 4 Assembly language level

Translation (assembler)

Level 3 Operating system machine level

Partial interpretation (operating system)

Level 2 Conventional machine level

Interpretation (microprogram)

Level 1 Microprogramming level

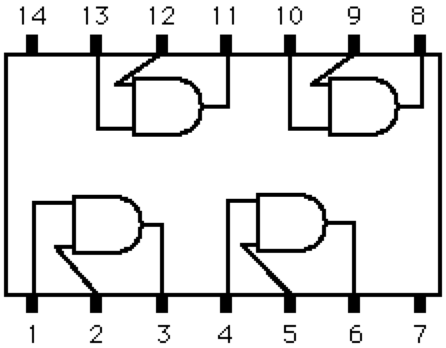
– THE MACHINE LEVEL

Microprograms are directly executed by the hardware

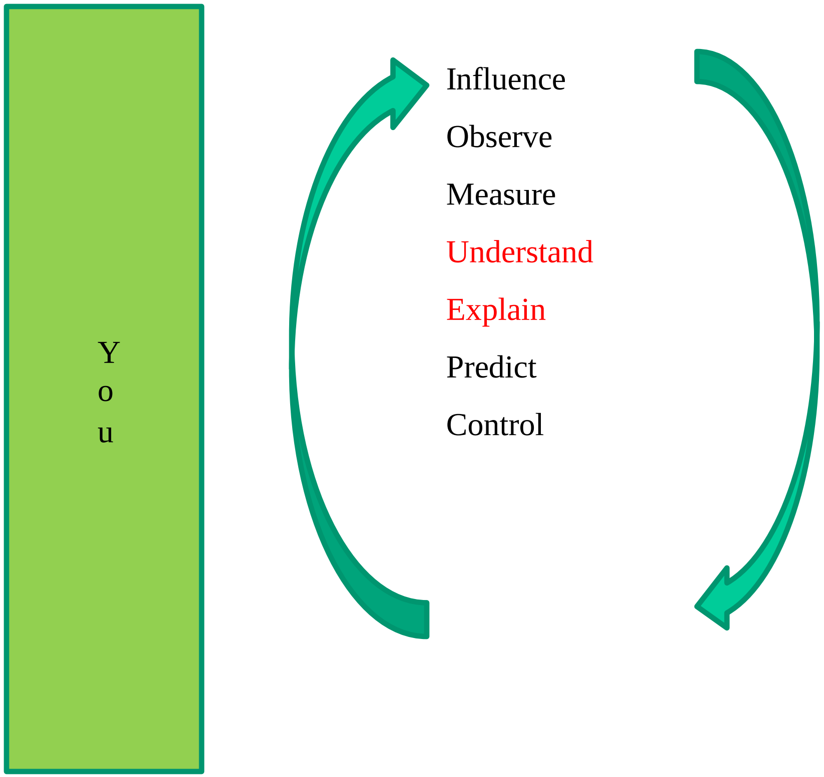
Level 0 Digital logic level

GATES

DEVICE LEVEL.



System Theory
Action Architecture ICT



Influence

Observe

Measure

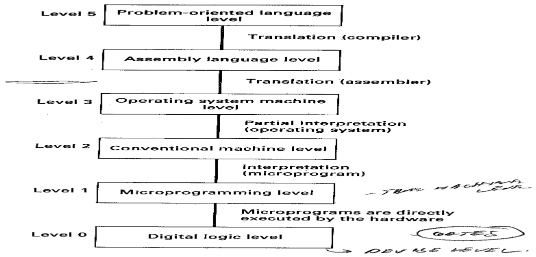
Understand

Explain

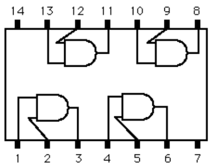
Predict

Control

Abstract


Level 5
Problem-oriented language level
Translation (compiler)
Level 4
Assembly language level
Translation (assembler)
Level 3
Operating system machine level
Partial interpretation (operating system)
Level 2
Conventional machine level
Interpretation (microprogram)
Level 1
Microprogramming level
Microprograms are directly executed by the hardware
Level 0
Digital logic level
GATES
DEVICE LEVEL

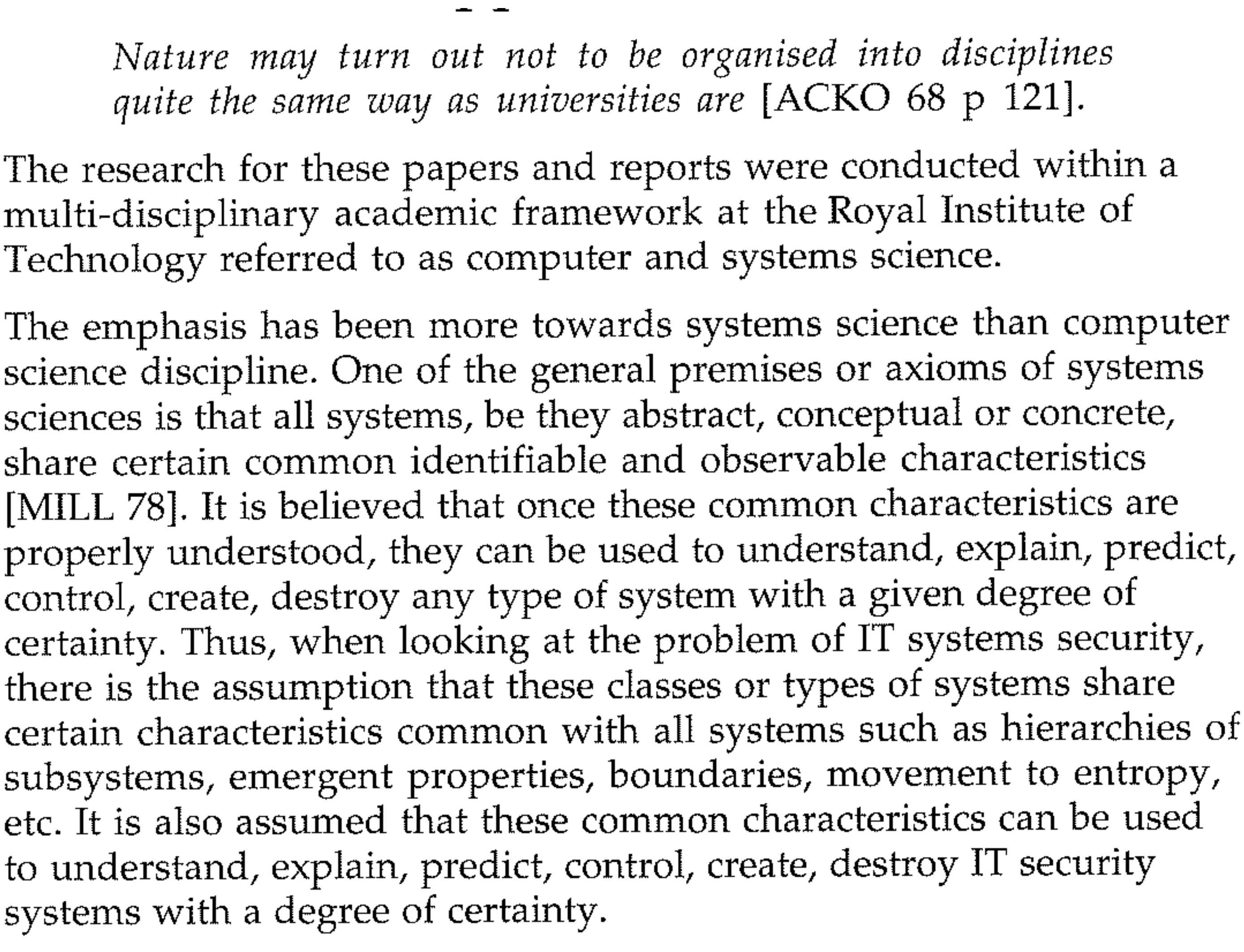
Concrete



Outline

- Background
- Why do we model?
- How do we model?

Research Approach



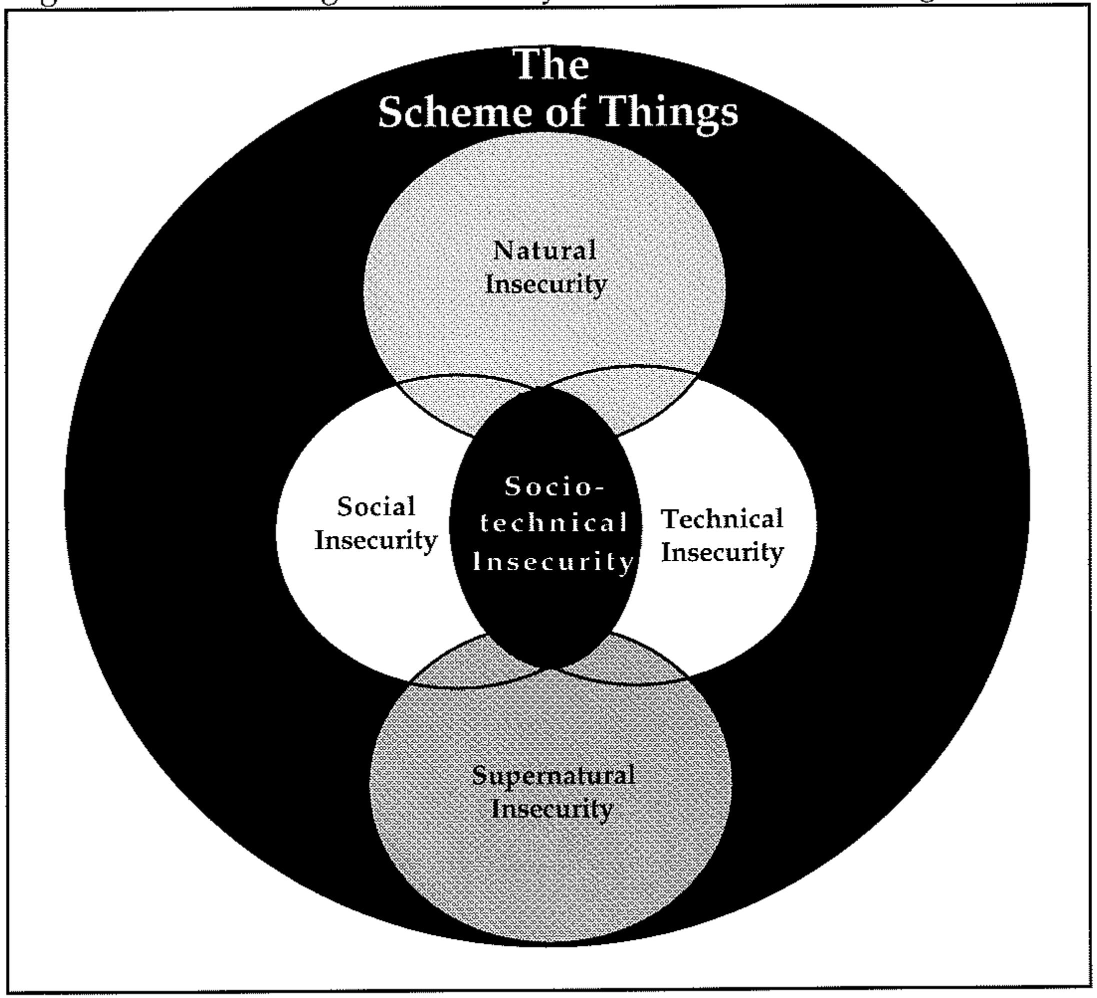
> *Nature may turn out not to be organised into disciplines quite the same way as universities are* [ACKO 68 p 121].

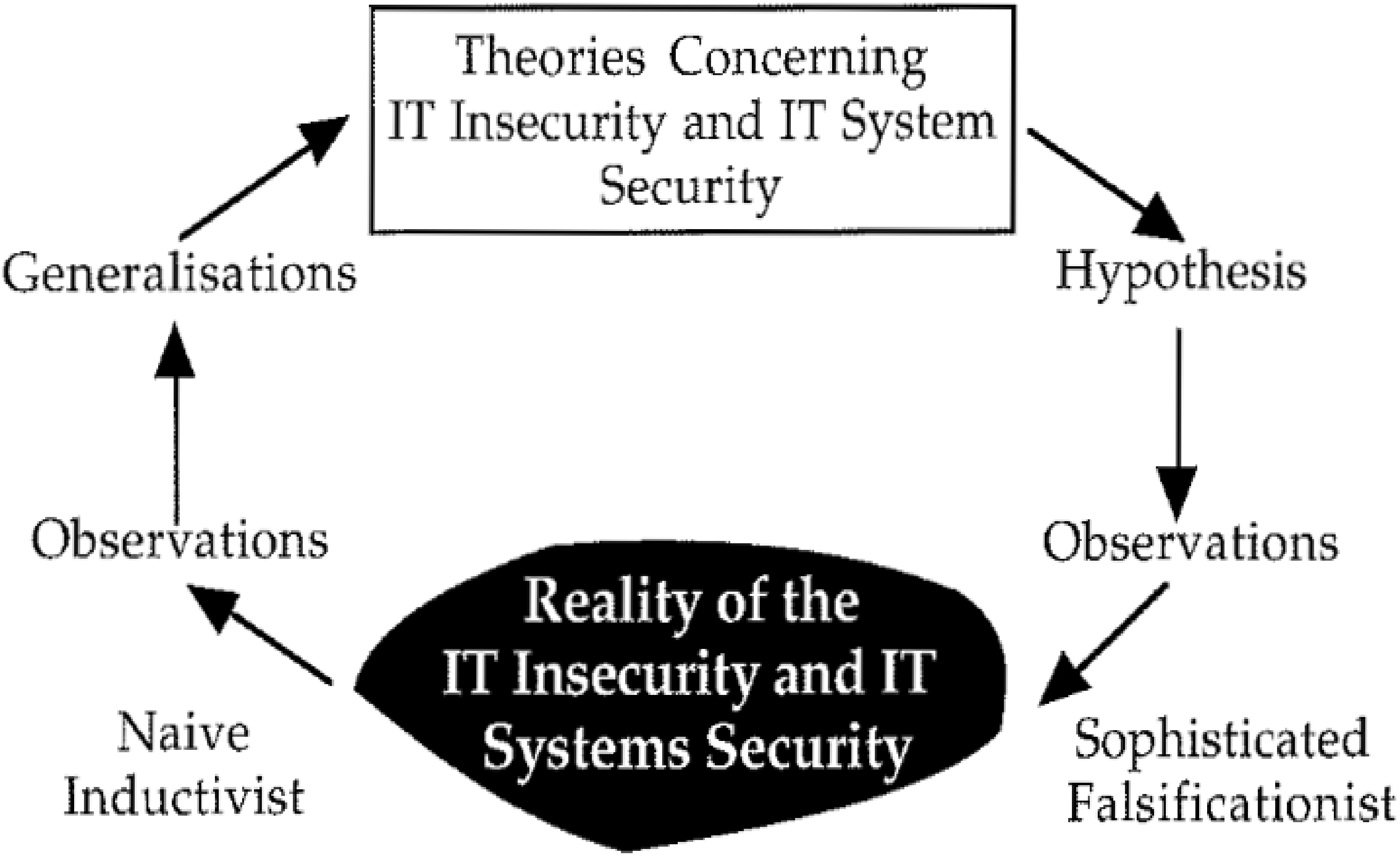
The research for these papers and reports were conducted within a multi-disciplinary academic framework at the Royal Institute of Technology referred to as computer and systems science.

The emphasis has been more towards systems science than computer science discipline. One of the general premises or axioms of systems sciences is that all systems, be they abstract, conceptual or concrete, share certain common identifiable and observable characteristics [MILL 78]. It is believed that once these common characteristics are properly understood, they can be used to understand, explain, predict, control, create, destroy any type of system with a given degree of certainty. Thus, when looking at the problem of IT systems security, there is the assumption that these classes or types of systems share certain characteristics common with all systems such as hierarchies of subsystems, emergent properties, boundaries, movement to entropy, etc. It is also assumed that these common characteristics can be used to understand, explain, predict, control, create, destroy IT security systems with a degree of certainty.

Modeling Social Technical Systems
Abstract Insecurity

Figure 1.3 Venn Diagram Insecurity in The Scheme of Things



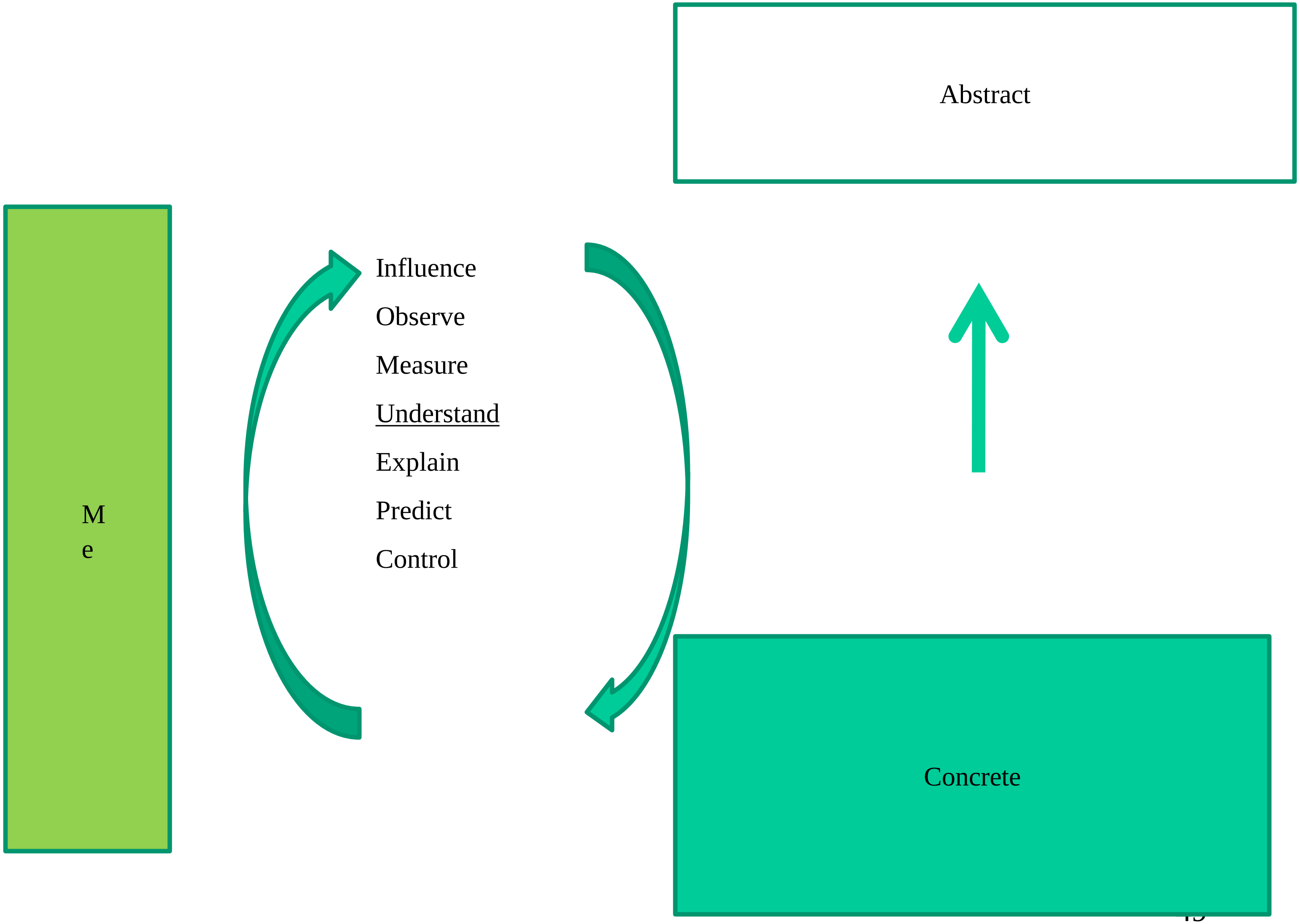

Theories Concerning IT Insecurity and IT System Security
Hypothesis
Observations
Sophisticated Falsificationist
Reality of the IT Insecurity and IT Systems Security
Naive Inductivist
Observations
Generalisations

Some like to believe in what they understand

Some like to undestand what they believe in.

Naïve inductivist and sophisticated falsificationist [Kowalski, 1994]

System Theory
Action Architecture ICT



Abstract

M
e

Influence

Observe

Measure

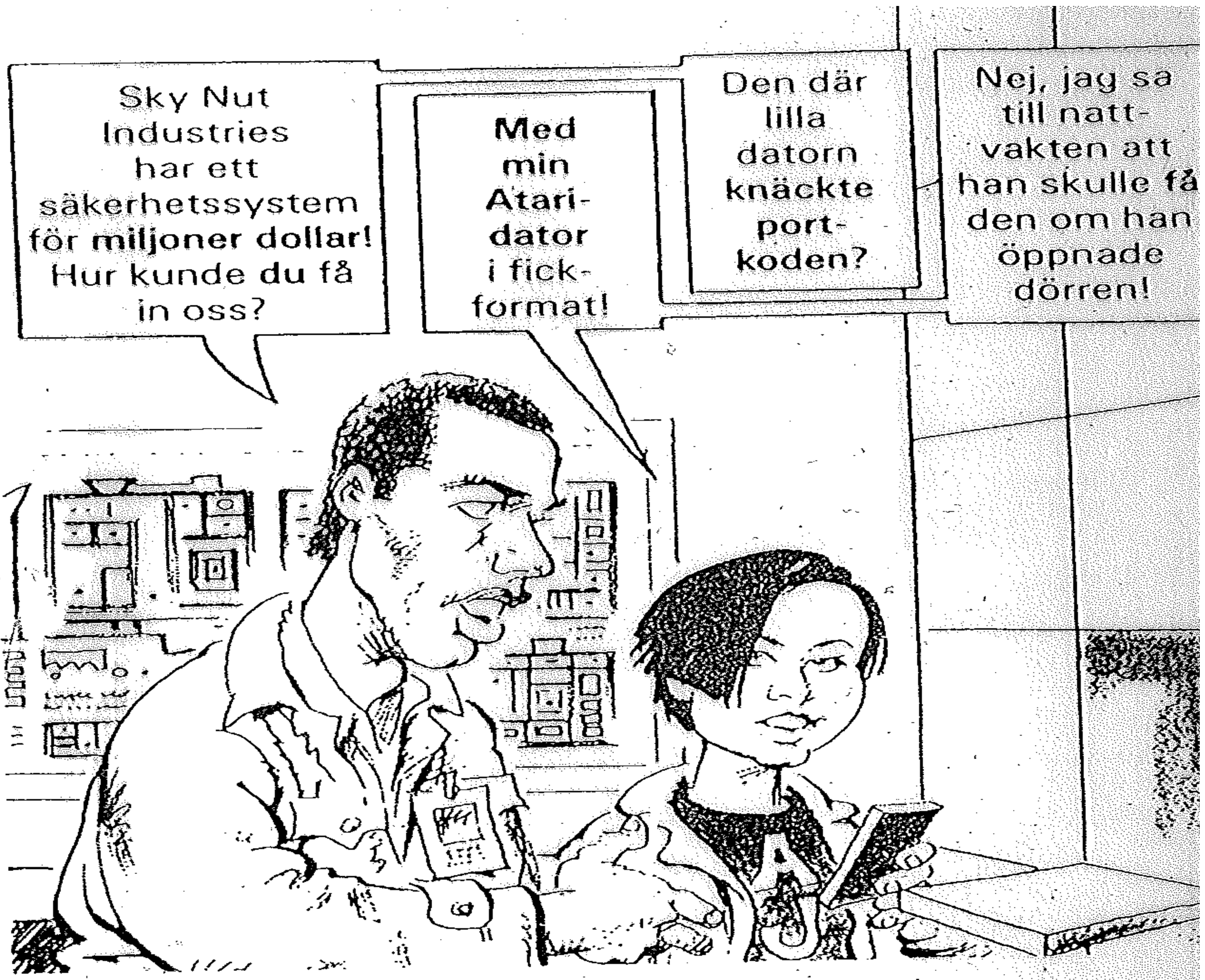
Understand

Explain

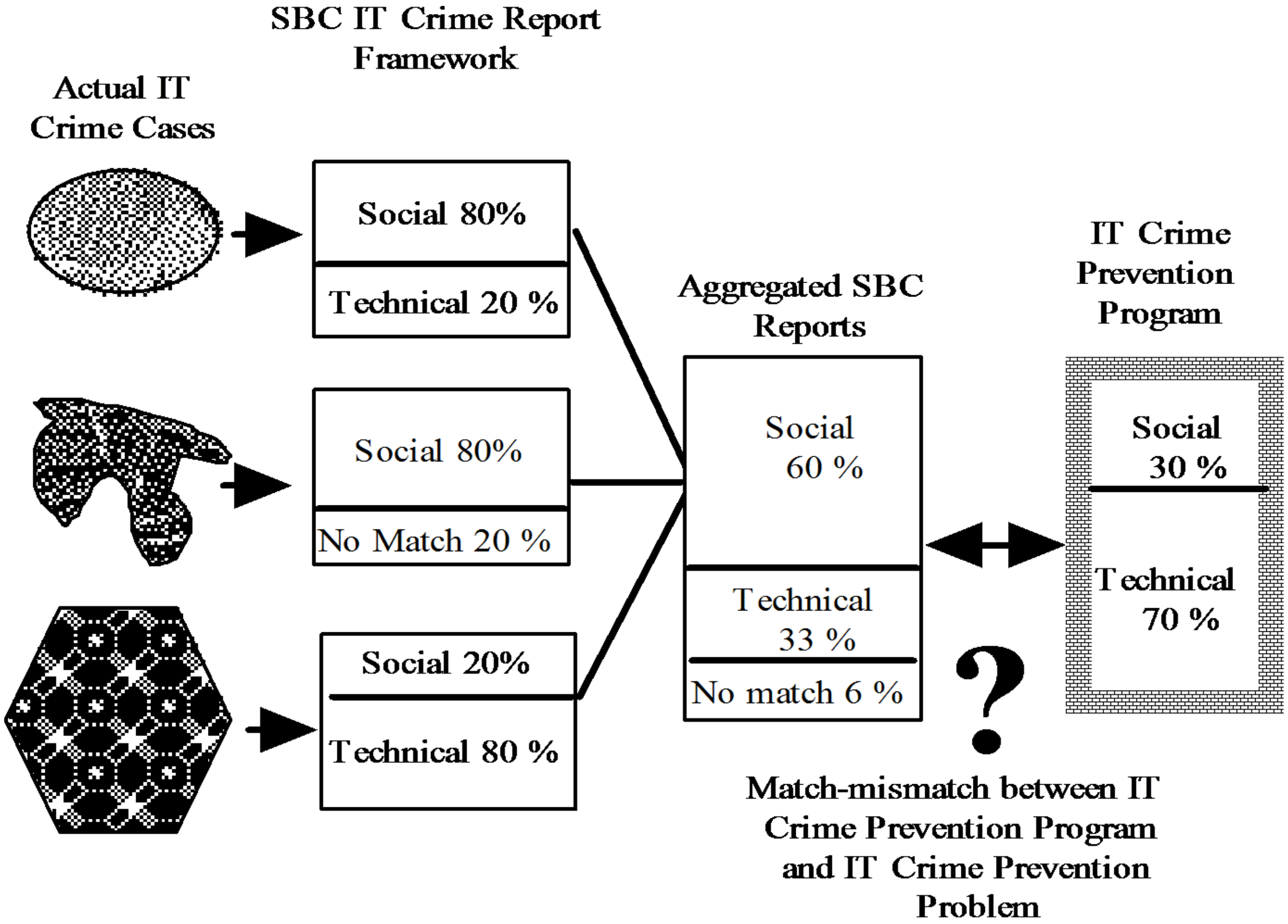
Predict

Control

Concrete

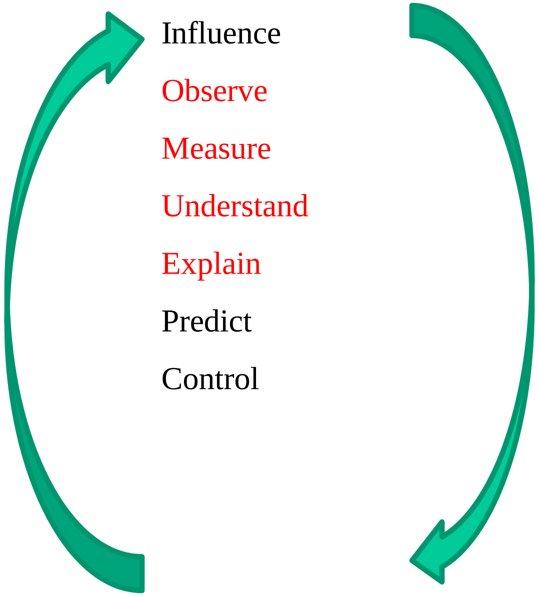

Sky Nut Industries har ett säkerhetssystem för **miljoner dollar!** Hur kunde du få in oss?
Med min Atari-dator i fick-format!
Den där lilla datorn knäckte port-koden?
Nej, jag sa till natt-vakten att han skulle få den om han öppnade dörren!

49 Computer Crime Cases



System Theory
Action Architecture ICT

Abstract



Influence

Observe

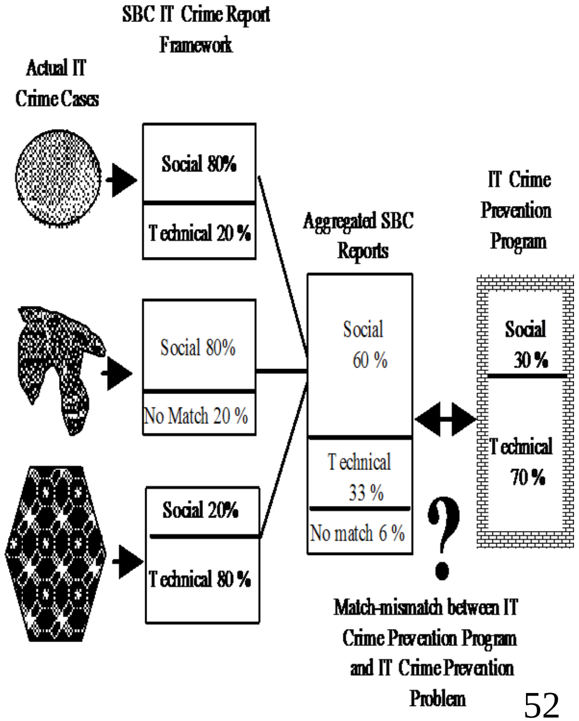
Measure

Understand

Explain

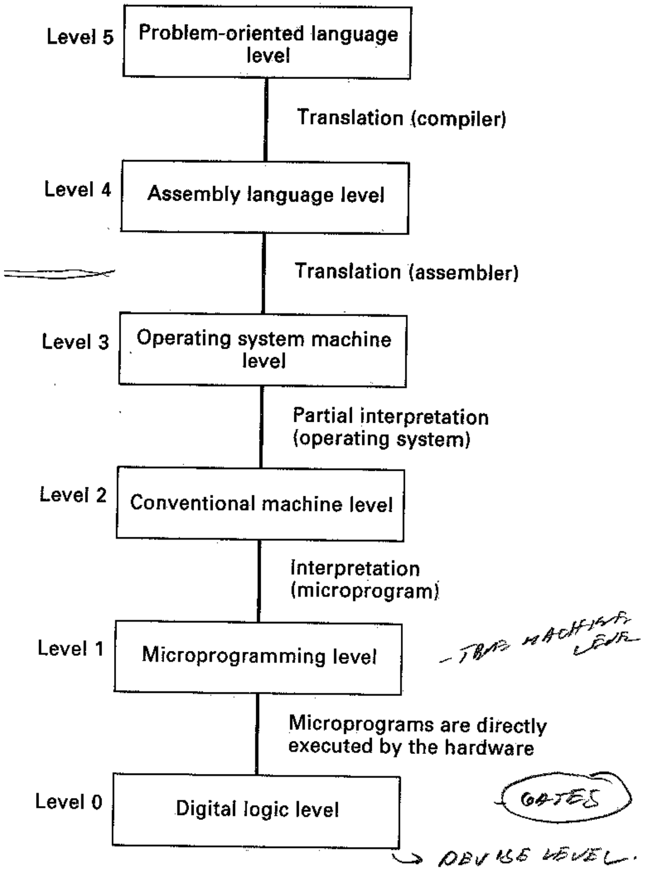
Predict

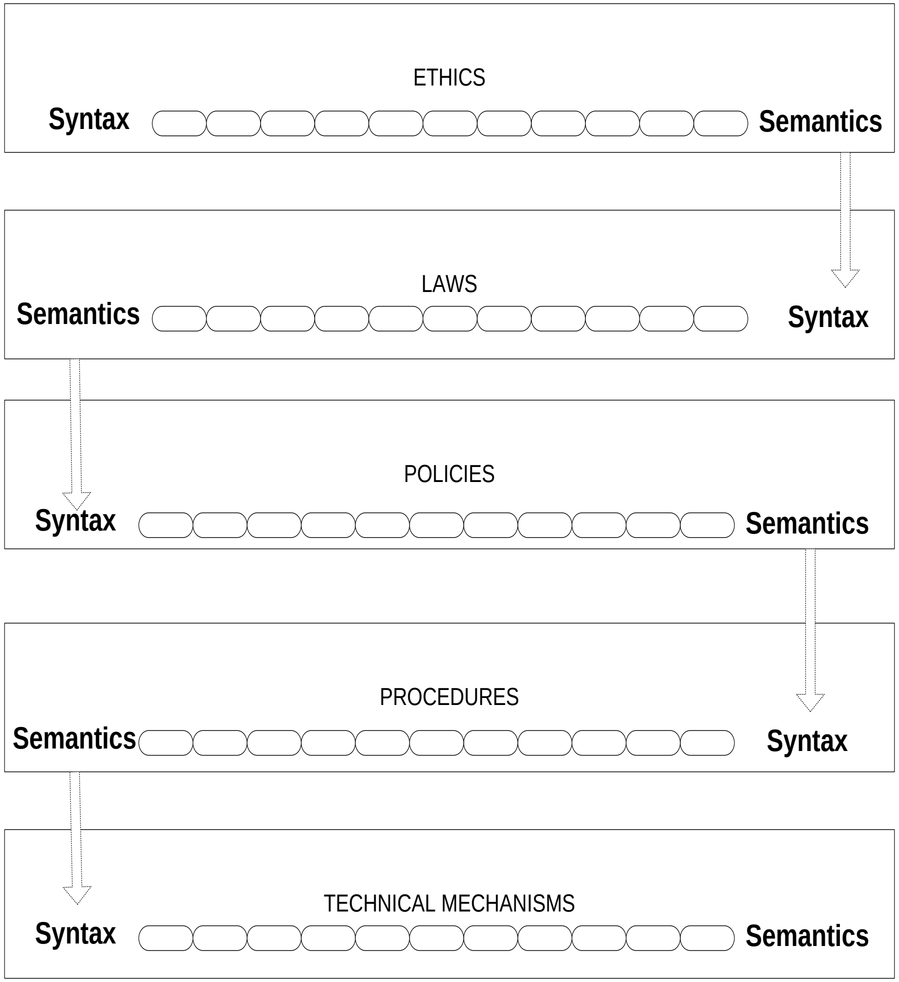
Control



M
e

My Mental Model ICT Insecurity ”Stacks of Controls”


Level 5
Problem-oriented language level
Translation (compiler)
Level 4
Assembly language level
Translation (assembler)
Level 3
Operating system machine level
Partial interpretation (operating system)
Level 2
Conventional machine level
Interpretation (microprogram)
Level 1
Microprogramming level
- TRUE MACHINE LEVEL
Microprograms are directly executed by the hardware
Level 0
Digital logic level
GATES
DEVICE LEVEL.


ETHICS

Syntax Semantics

LAWS

Semantics Syntax

POLICIES

Syntax Semantics

PROCEDURES

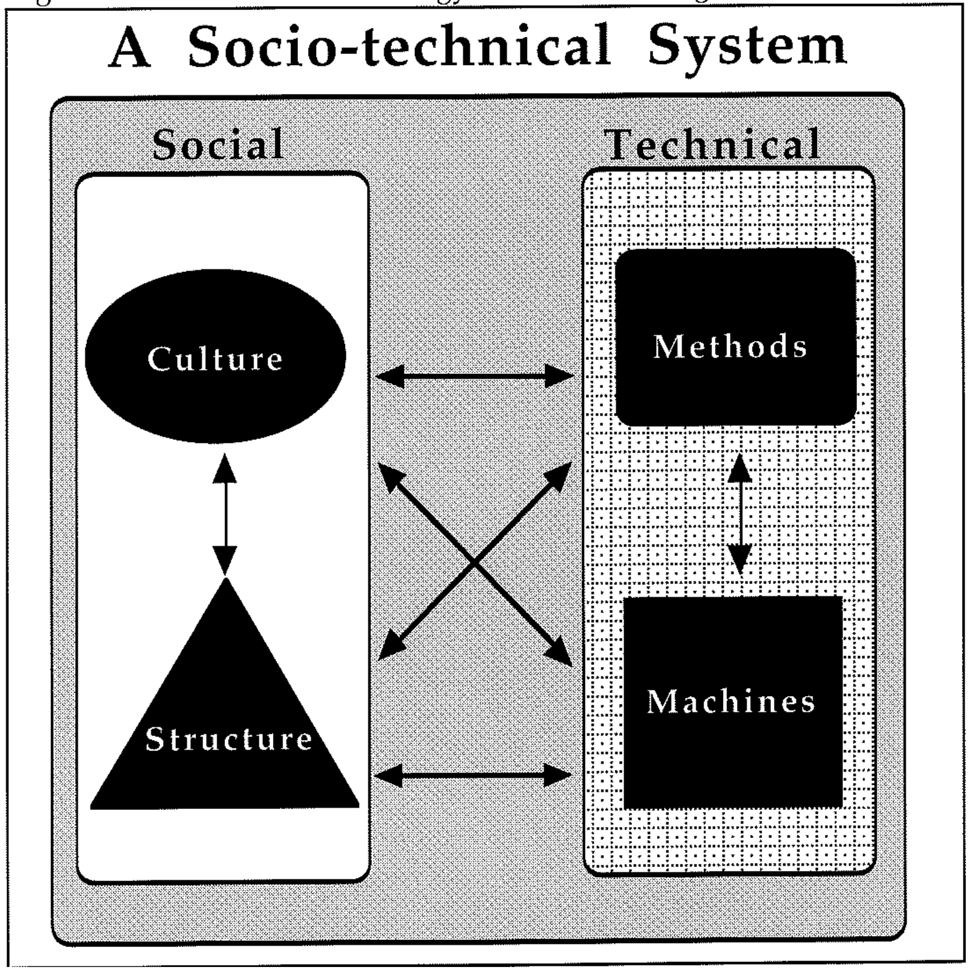
Semantics Syntax

TECHNICAL MECHANISMS

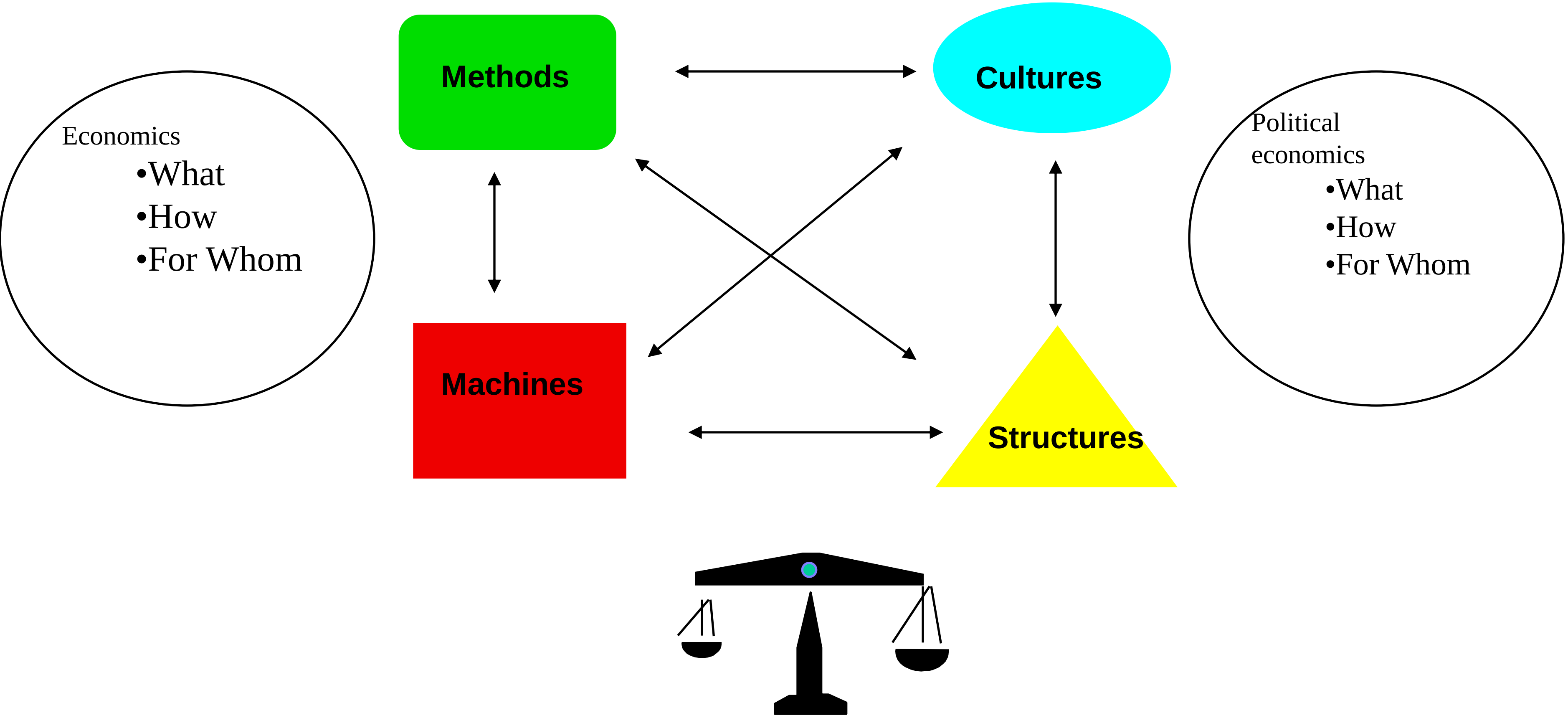
Syntax Semantics

Model Systems
K.I.S.S.
Keep it simple Stewart

Figure 1.5 A Model of Technology and Social Change



The Model of the Century.-)
Common identifiable and observable characteristics of <u>any human organization!</u>



Methods

Cultures

Machines

Structures

Economics

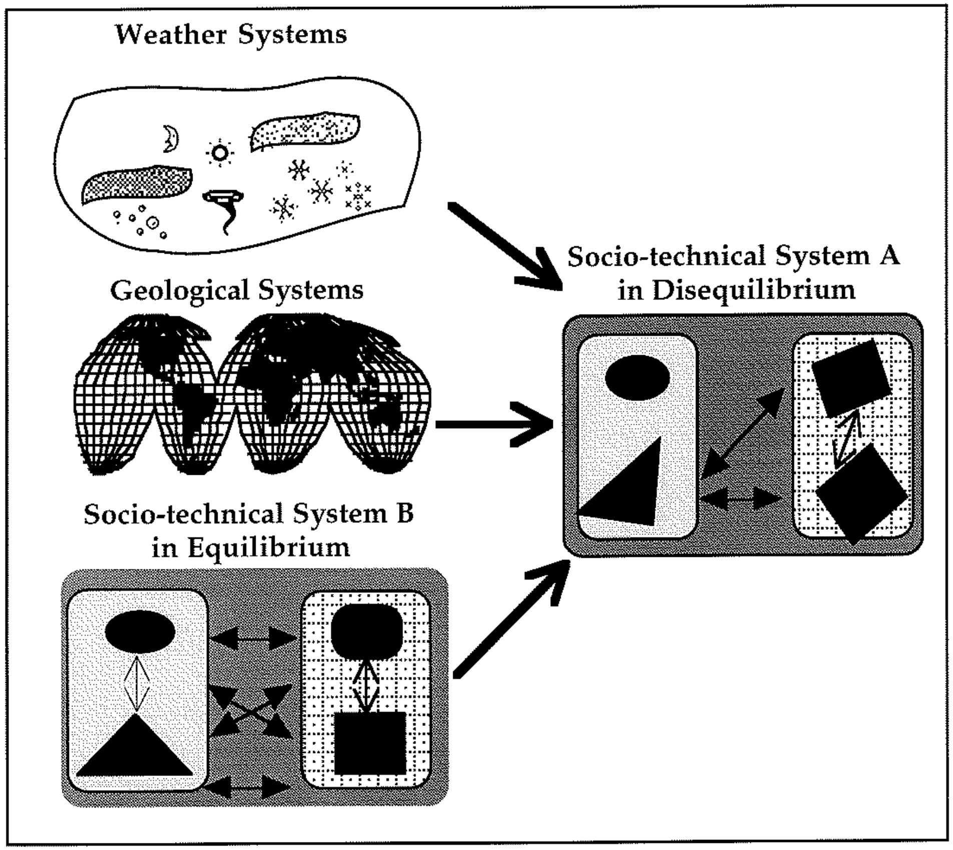
- What
- How
- For Whom

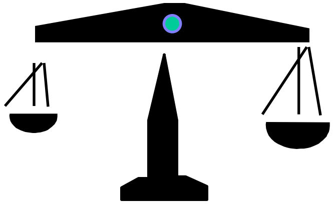
Political economics

- What
- How
- For Whom

Concrete-Abstract
(Secuirty = Balance=Homestisis

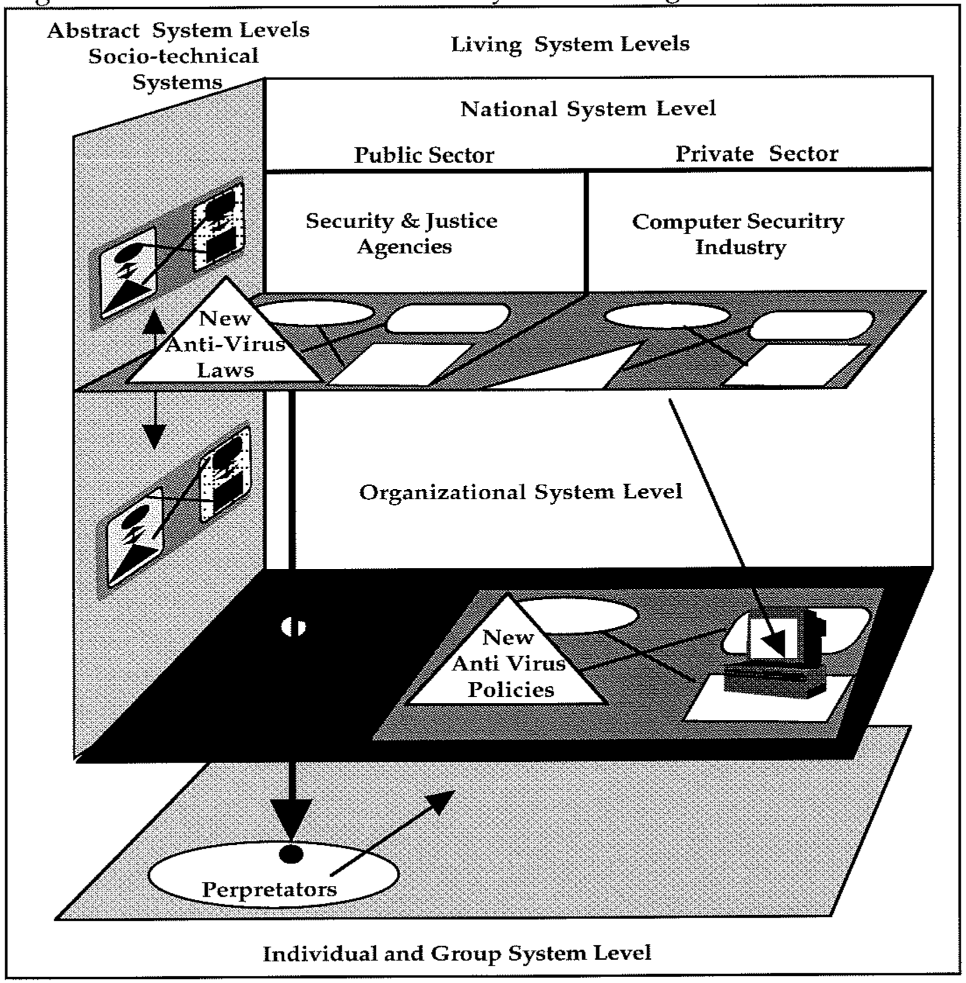
Figure 1.6 Social-Technical System: Subject to Influences from the Environment

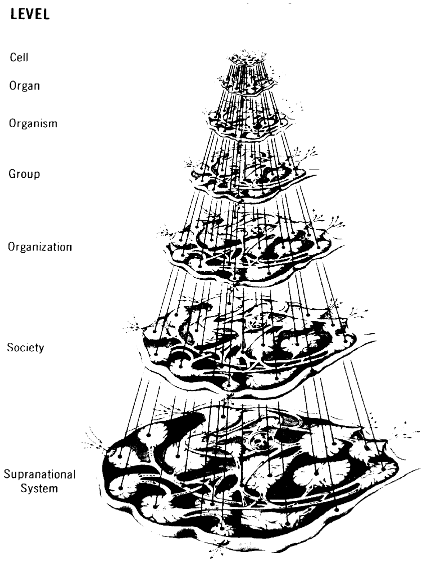

Weather Systems
Geological Systems
Socio-technical System A in Disequilibrium
Socio-technical System B in Equilibrium

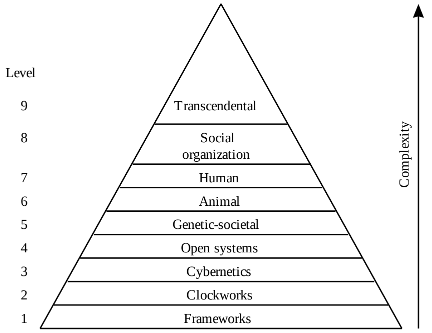


Make it Complicated

Figure 1.7 Socio-technical IT Security Measure Against Virus Threat

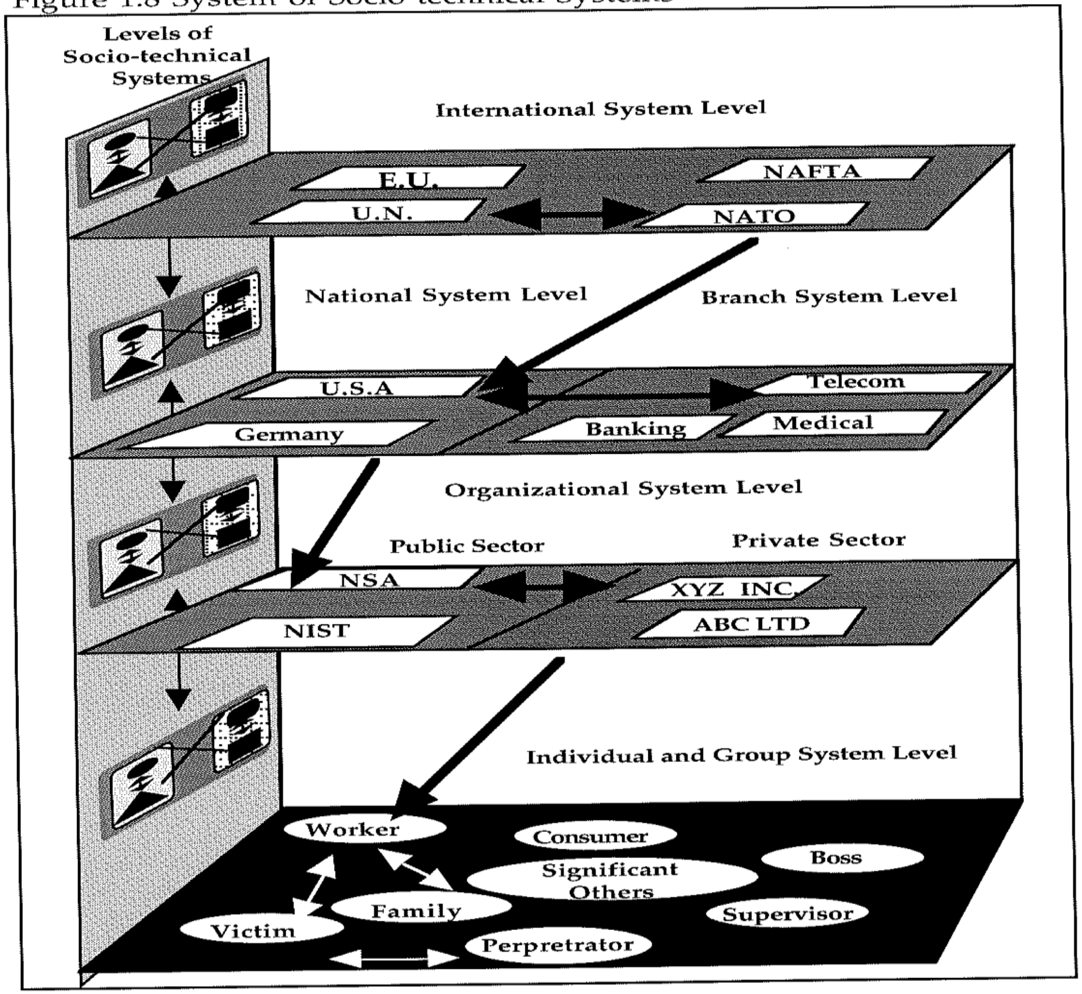


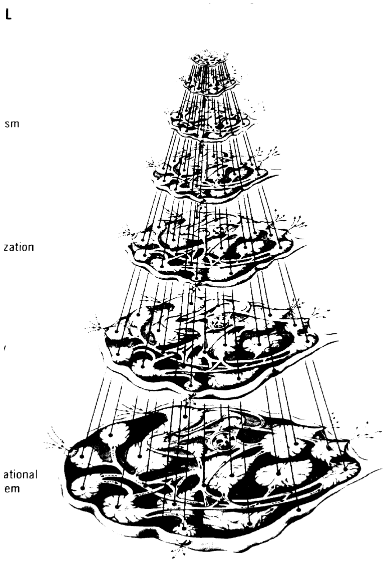


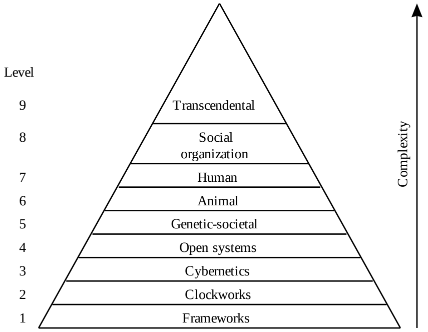


Make it Complicated

Figure 1.8 System of Socio-technical Systems






Level

9 Transcendental

8 Social organization

7 Human

6 Animal

5 Genetic-societal

4 Open systems

3 Cybernetics

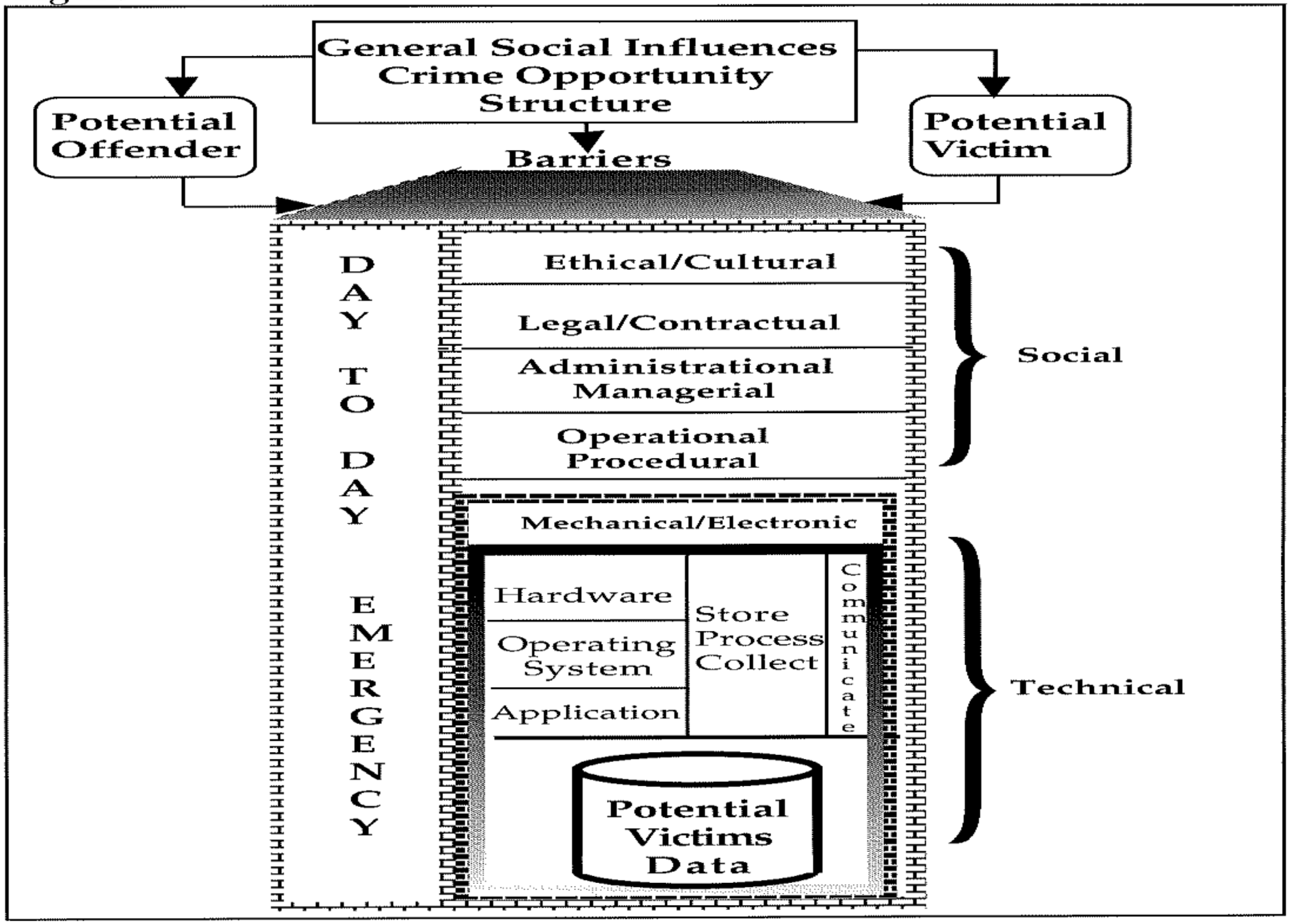
2 Clockworks

1 Frameworks

Complexity

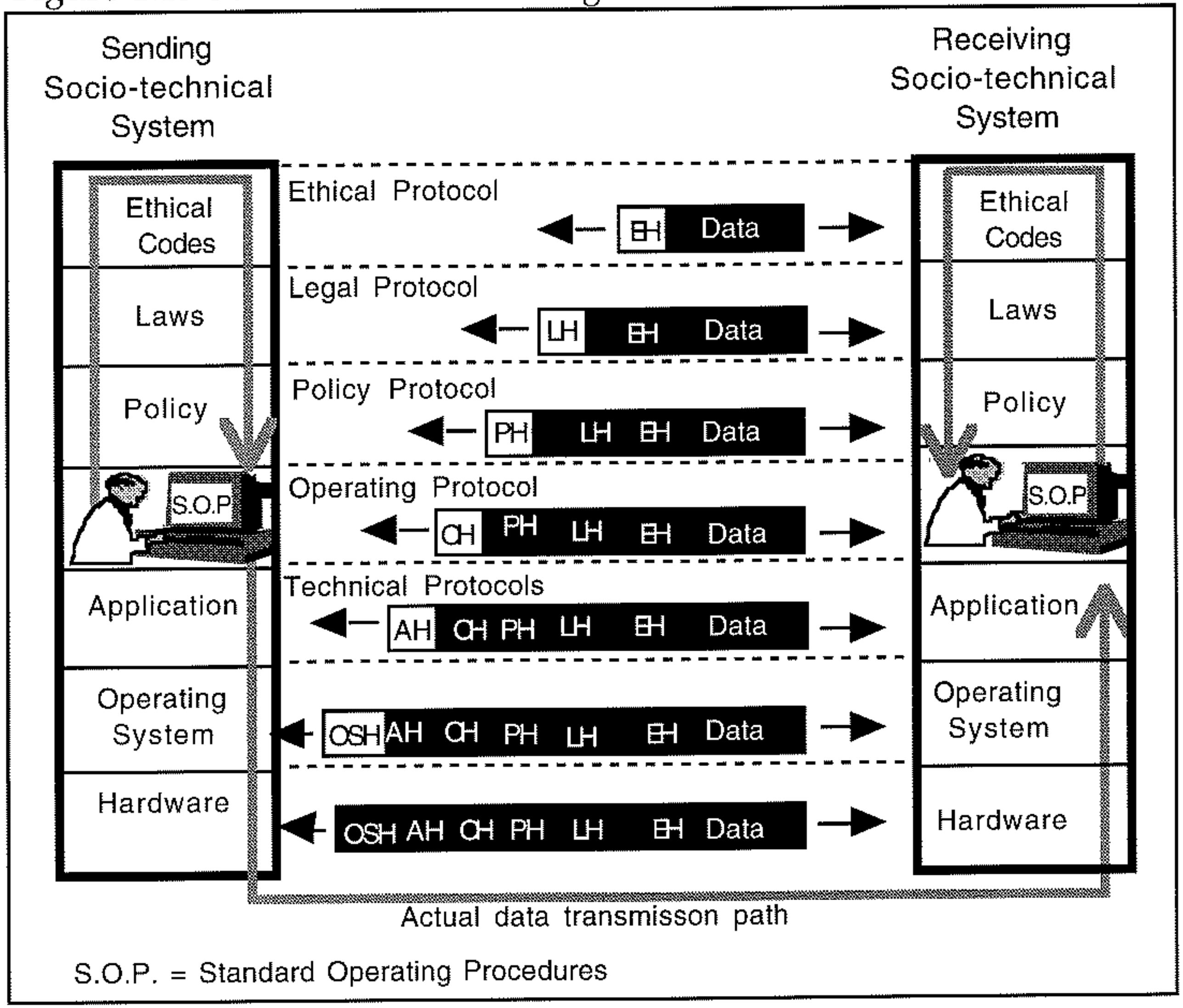
Concrete abstract living Mental Model

Figure 13.3. SBC Framework



Living-Abstract-Concrete

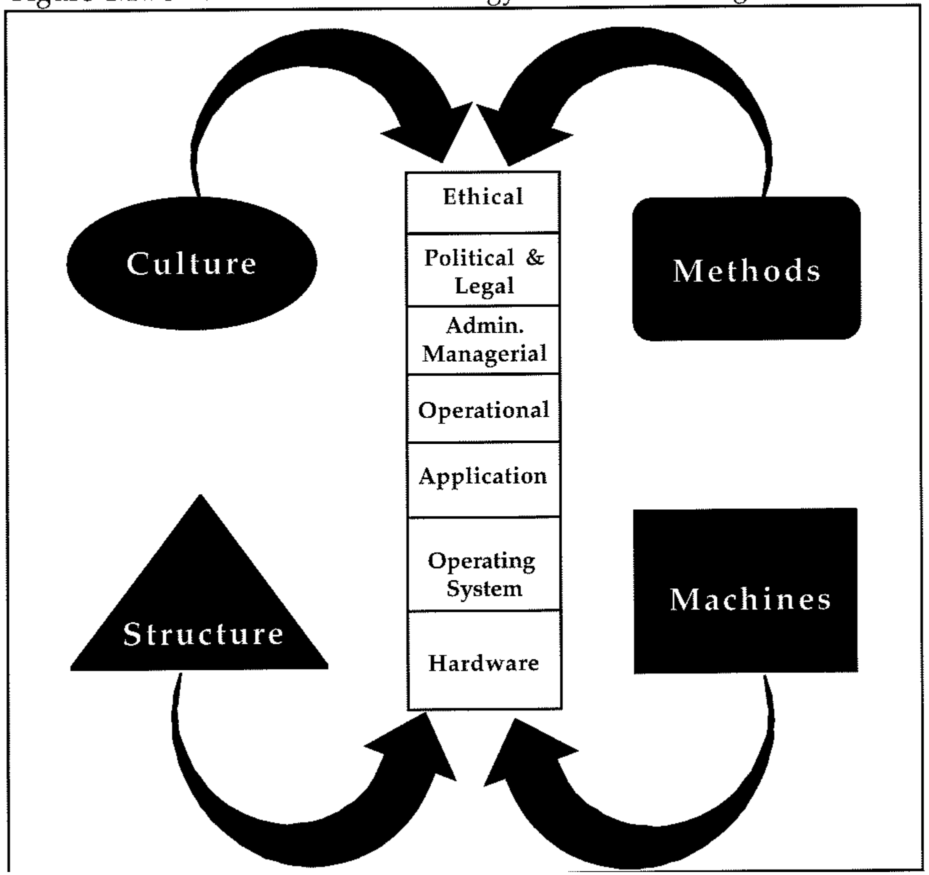
Figure 1.13 Socio-technical Labeling

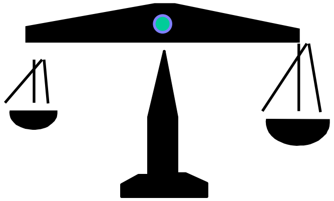


S.O.P. = Standard Operating Procedures

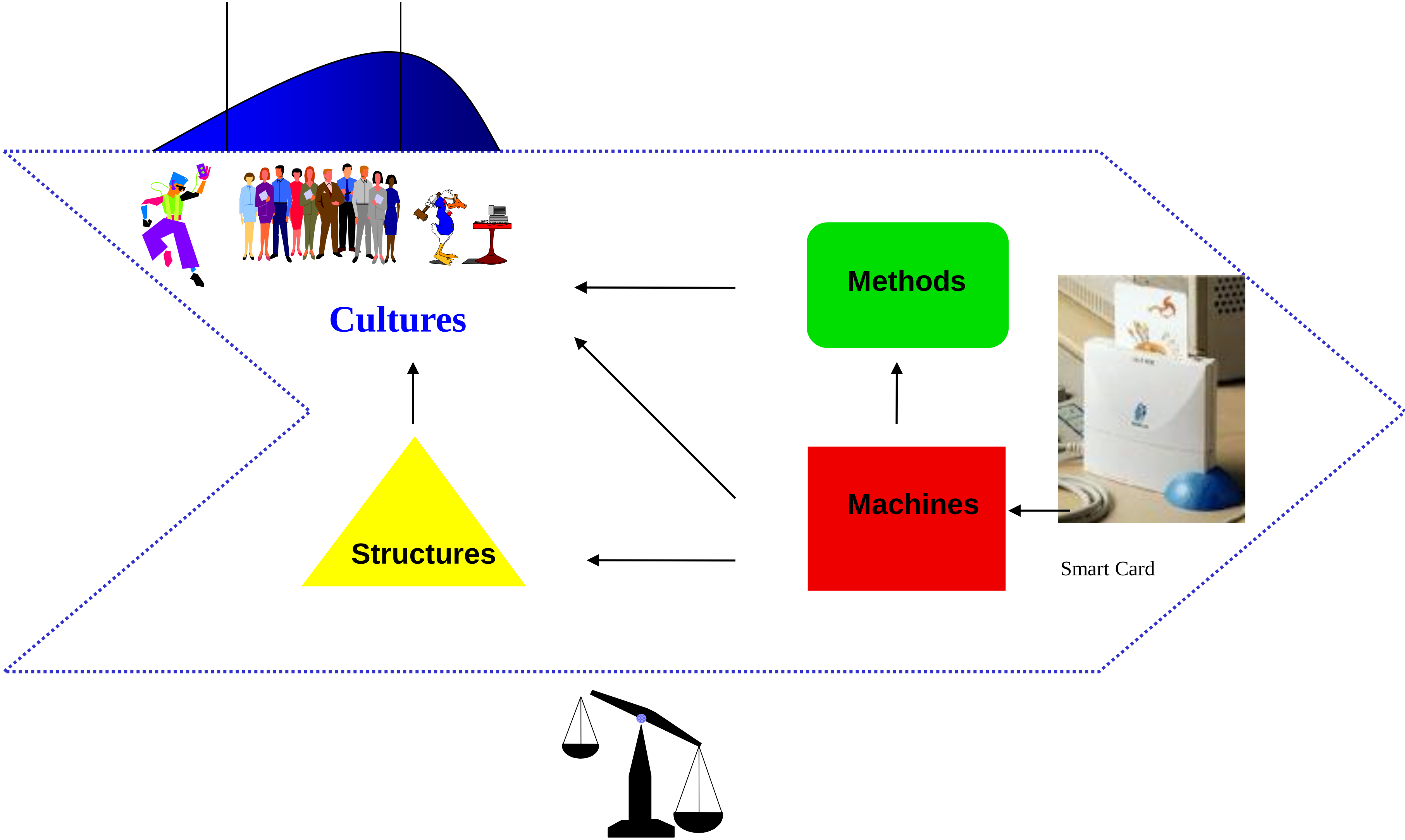
Keep it Simply Secure

Figure 1.14 SBC Model and Technology and Social Change

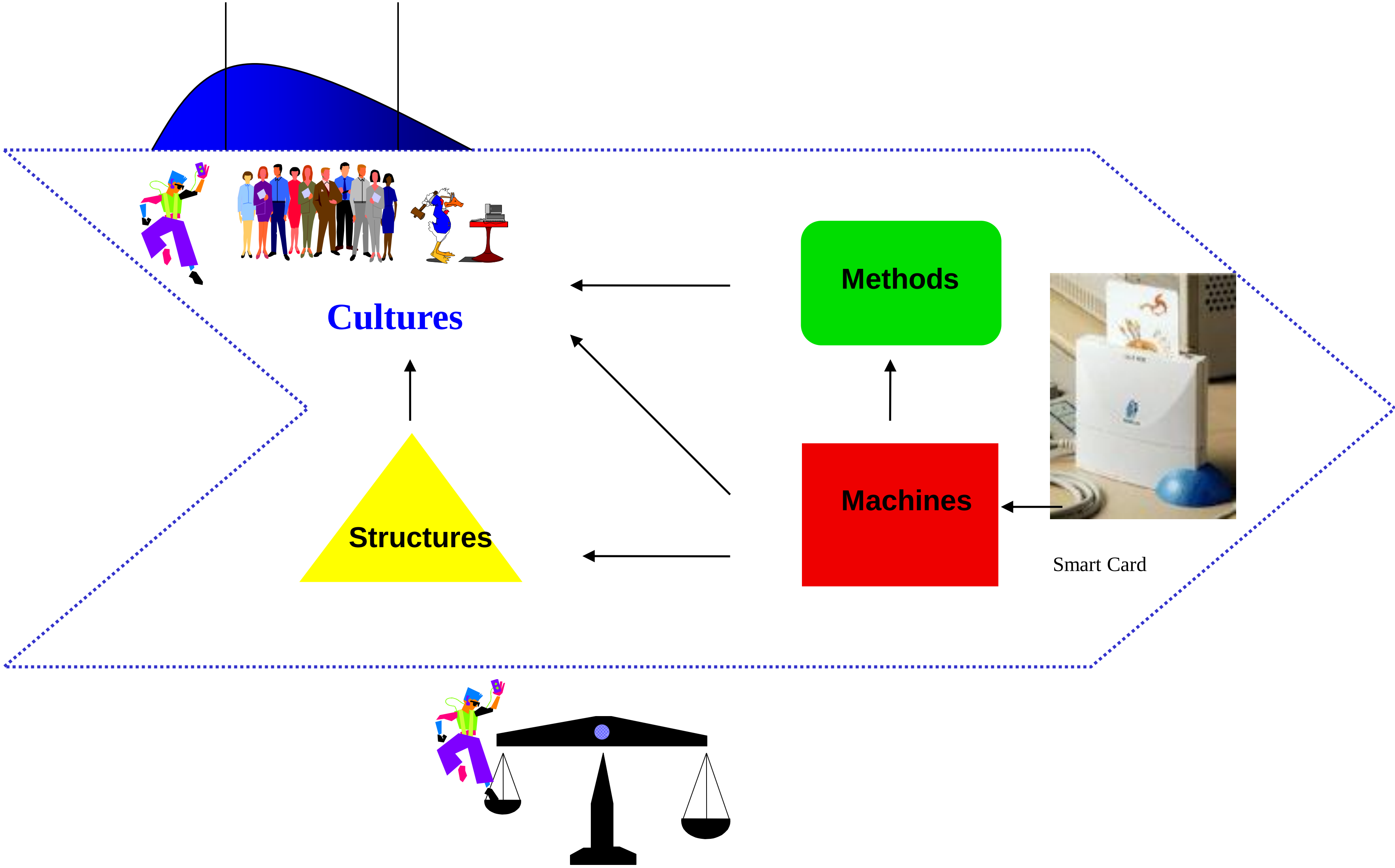




An Insecure Socio-technical System



A (s)ecure Socio-technical System



Cultures

Methods

Machines

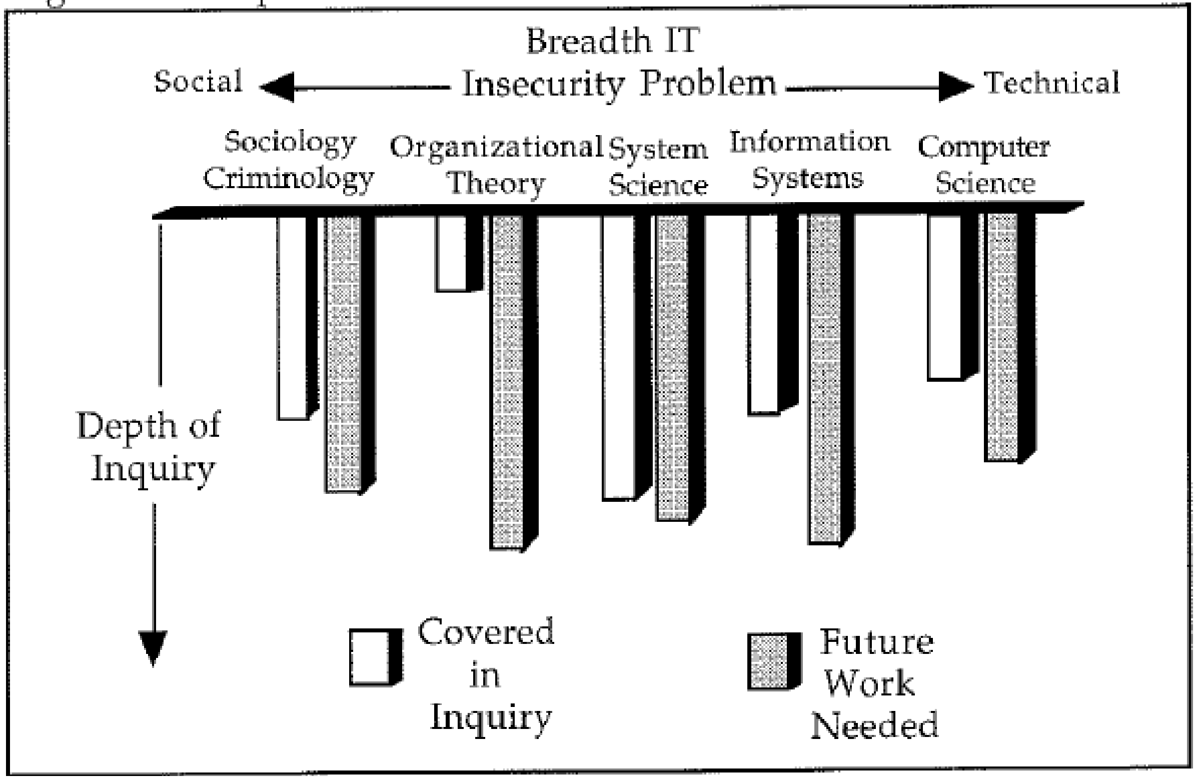
Structures

Smart Card

Chapter 1

- Class room or home work* active. Discuss with your neighbor where

Figure 1.17 Depth and Breadth of Present and Future Work



* For those of you studying off campus , either find someone to discuss this with, it could be a friend or a spouce. If this does not work you can book a skype meeting with me to discuss it.

Chapter 1

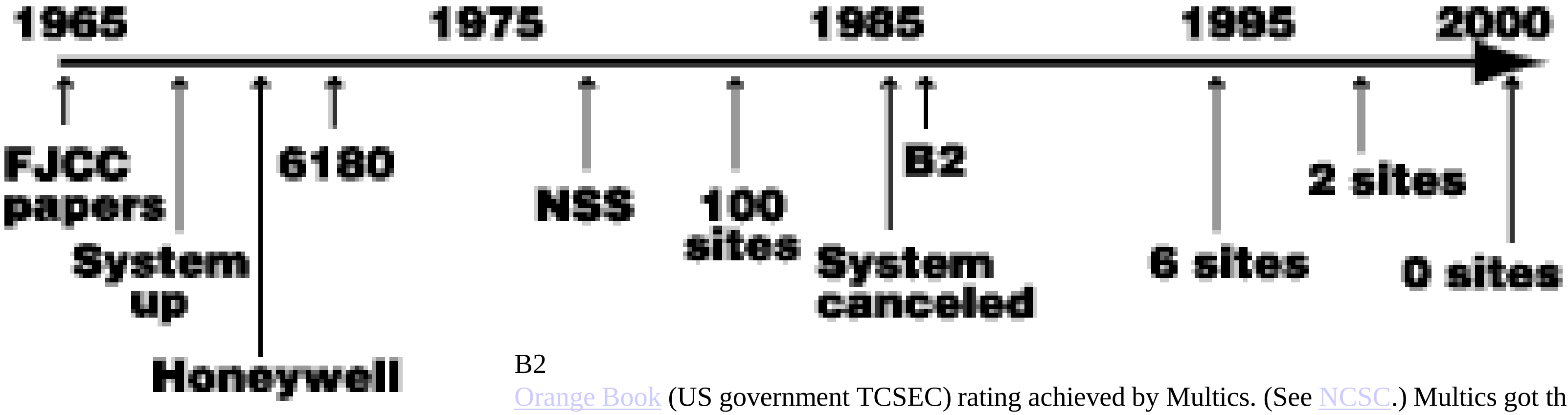
- Problem Formulation (Historical Context)
  - Paradigm Crisis in formal modeling computer security end of the 80’s
    - Death of secure Multics (see next slide)
    - Biba, Bell-LaPadula (Mathemtical 70’s)
    - Clark-Wilson (Mathematical-Business Accounting) 80’s
  - «We in the [computer] security community give very little attention to the task of defining our subject matter; yet we spend a great deal of our time constructing supposed models of security comparing them with one another, and building systems based on them. The study of formal models is important, but focusing only on model building may blind us to the fact that we're attempting to build secure systems, where security has essential empirical content quite apart from our formal manipulations [YOUN 89 p 47]. Towards a Foundation of Security

Chapter 1

- Problem Formulation (Historical Context)
    - – 1. Striving to represent a complex socio-technical system by replicating it in a mathematical format (for example, simulation using a large scale, computerised, albeit severely constrained, model),
    - – 2. seeking abstract models to serve as thinking aids, revealing possible clues or illuminating some aspect of system behaviour in a different way (usually such models are simple enough to abandon without regret, occasionally elegant enough to cherish) [LINS 84 p 14].

Brief History MULTICS

- Joint project between MIT, Bell Labs, and GE
- Bell labs withdrew in 1969
- GE Sold its computer business to Honeywell in 1970 who sold Multics as a commercial product

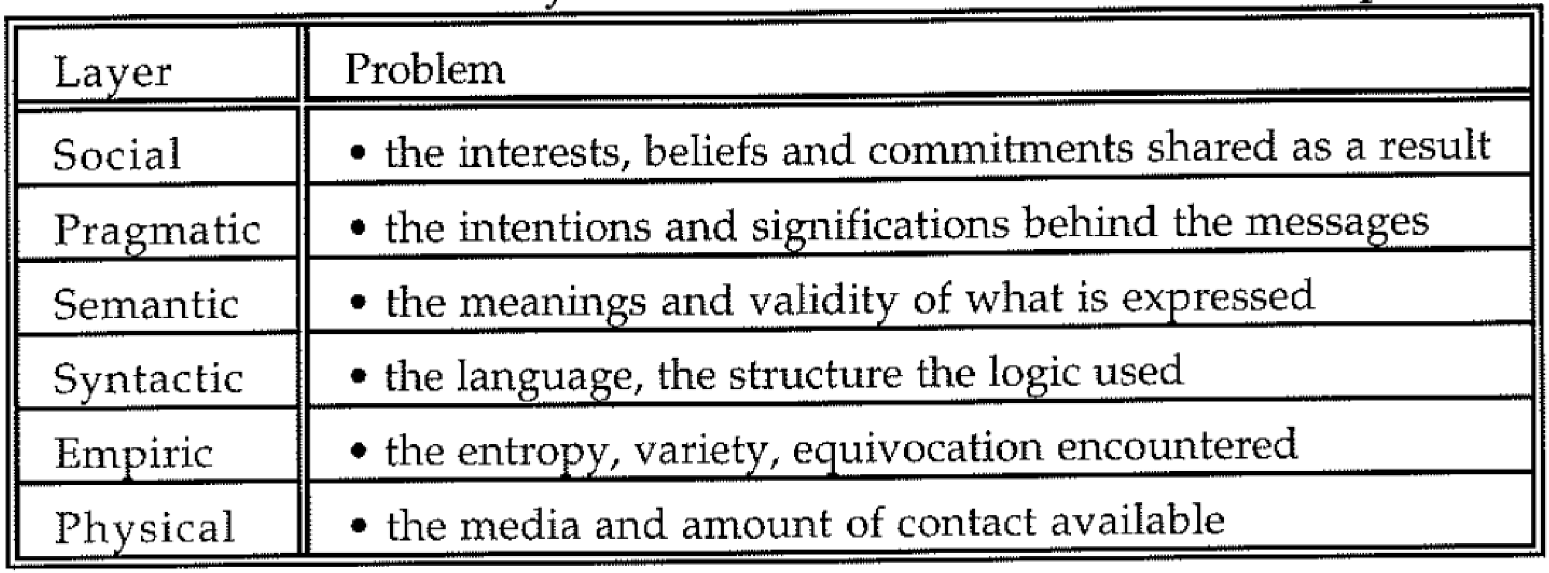


B2
Orange Book (US government TCSEC) rating achieved by Multics. (See NCSC.) Multics got the first B2 rating, in August, 1985, and had the only B2 for many years. A rating at the B level indicates support for mandatory access control as well as a relatively high level of security assurance. See AIM. Official letter: [page 1] [page 2]

Chapter 1

- Problem Formulation (Historical Context)
  - Computer where starting to be more networked so we need a networking

Table 1.2 Problem Layers in Communication [FALK 90 p 9]



Layer	Problem
Social	• the interests, beliefs and commitments shared as a result
Pragmatic	• the intentions and significations behind the messages
Semantic	• the meanings and validity of what is expressed
Syntactic	• the language, the structure the logic used
Empiric	• the entropy, variety, equivocation encountered
Physical	• the media and amount of contact available

Chapter 1

- Problem Formulation (Historical Context)
  - Computer where starting to be more networked so we need a networking

Figure 1.11 SBC Model as Framework for Secure IT Communication

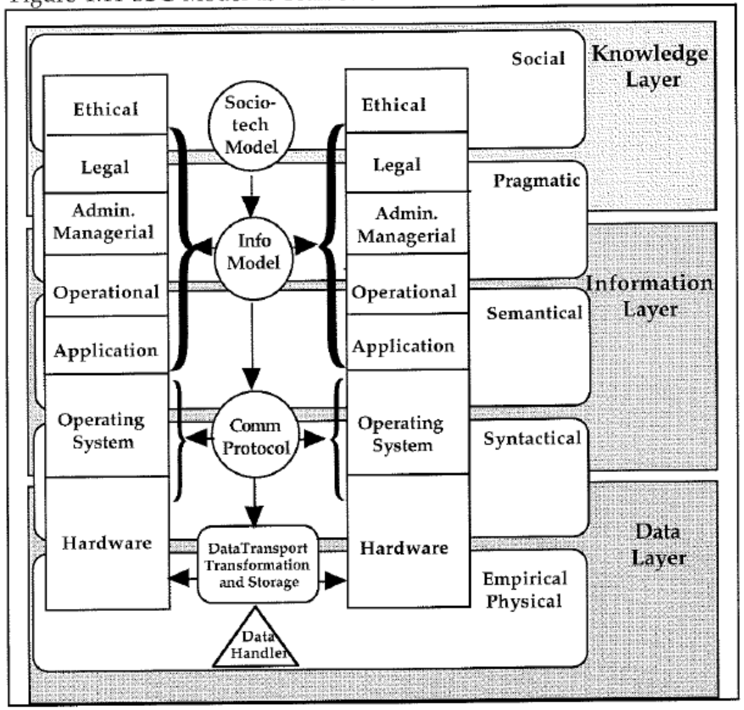
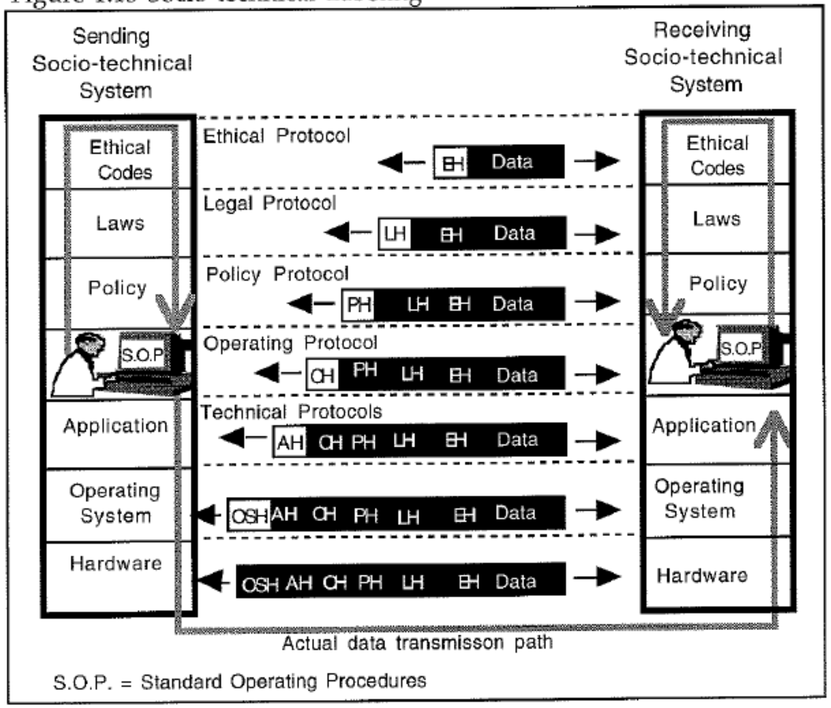
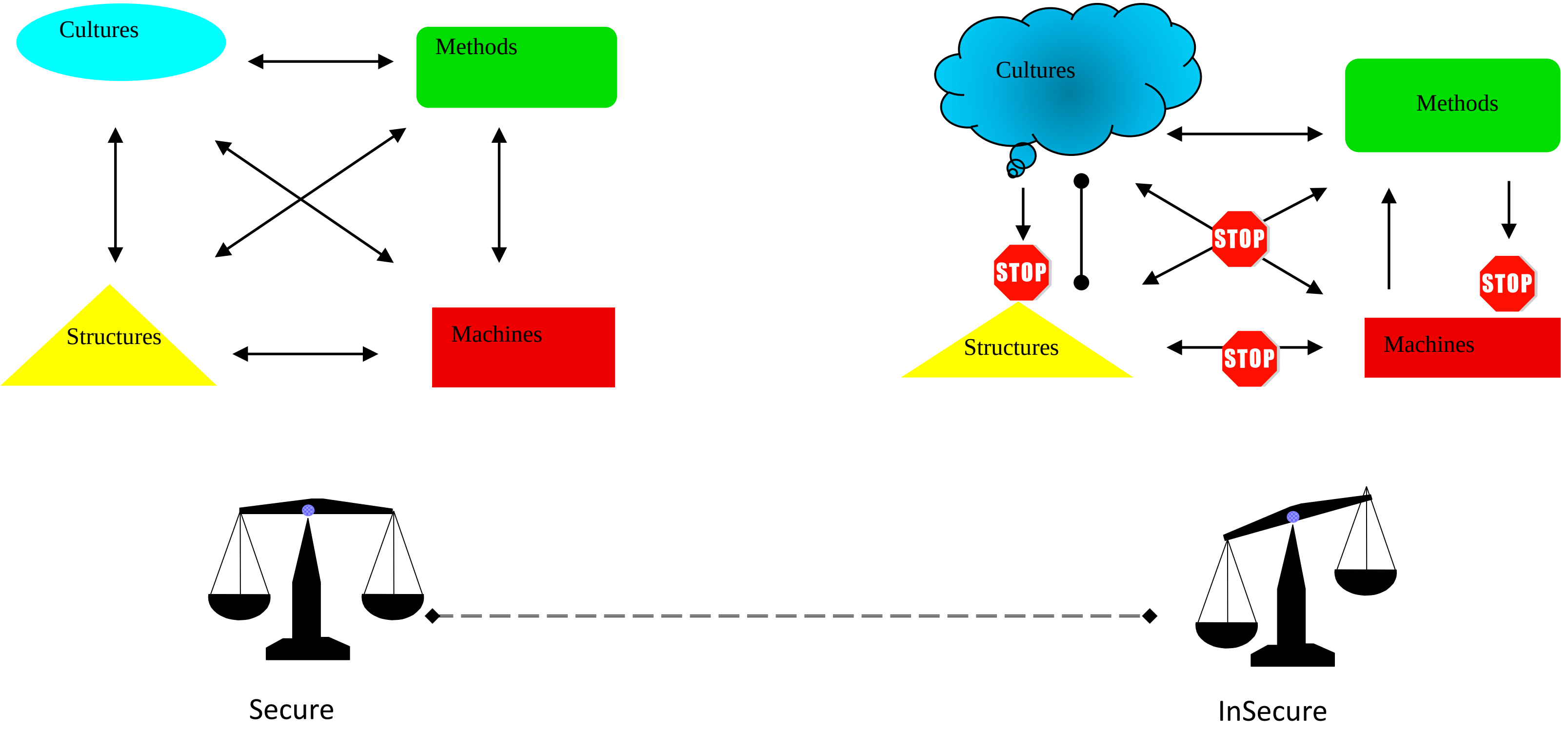


Figure 1.13 Socio-technical Labeling



Chapter 1

- Problem Formulation
  - Dynamics of socio-technical change and insecurity



Chapter 1

- Problem Formulation
  - Use security framework to put the system back in

Figure 1.11 SBC Model as Framework for Secure IT Communication

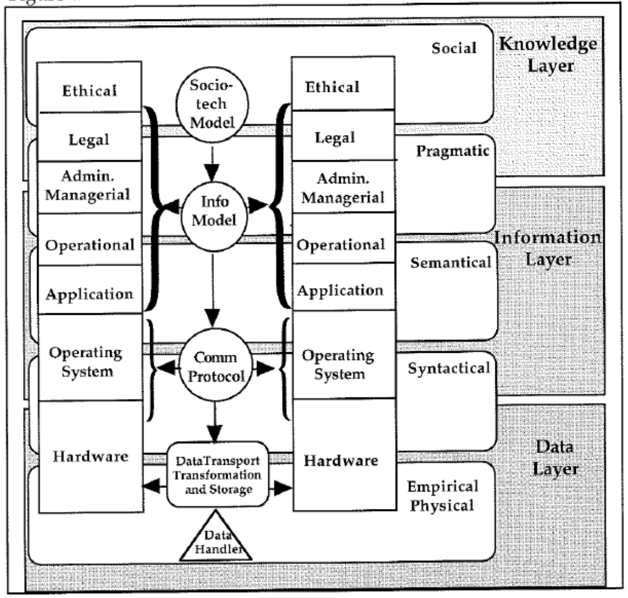
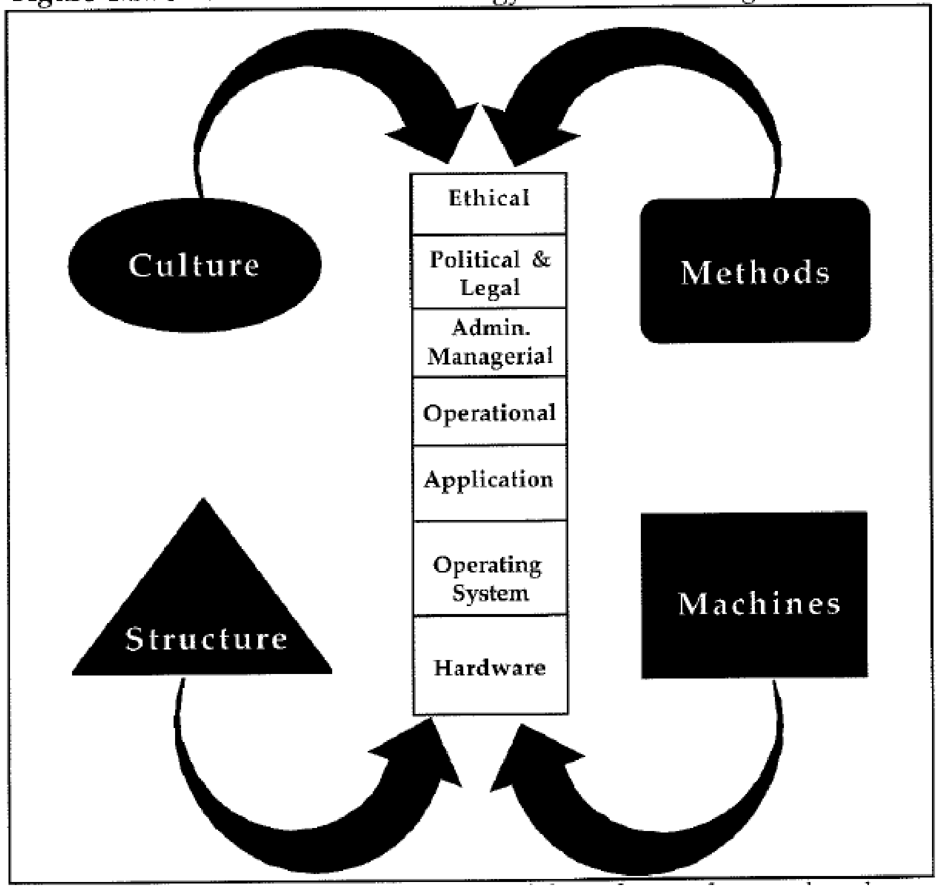


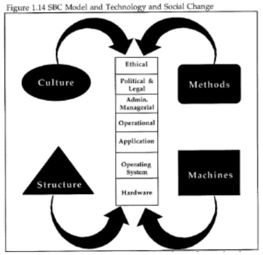
Figure 1.14 SBC Model and Technology and Social Change



Chapter 1

- Problem Formulation
  - The organization needs apply a SBC analysis to bring back in balance

Figure 1.14 SBC Model and Technology and Social Change



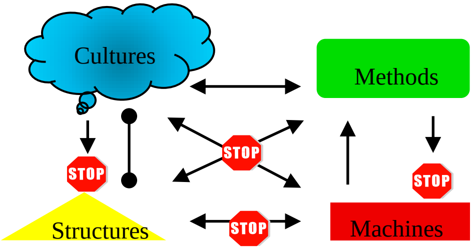
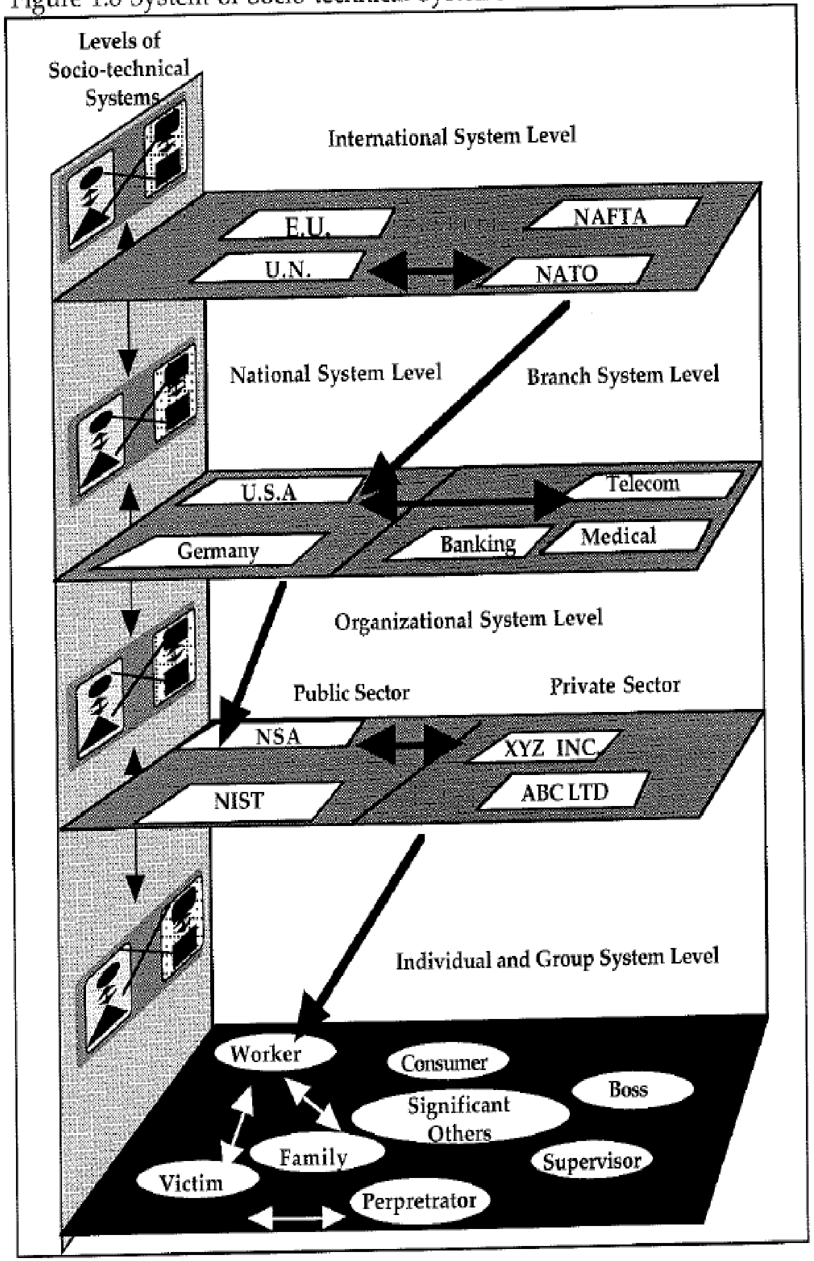
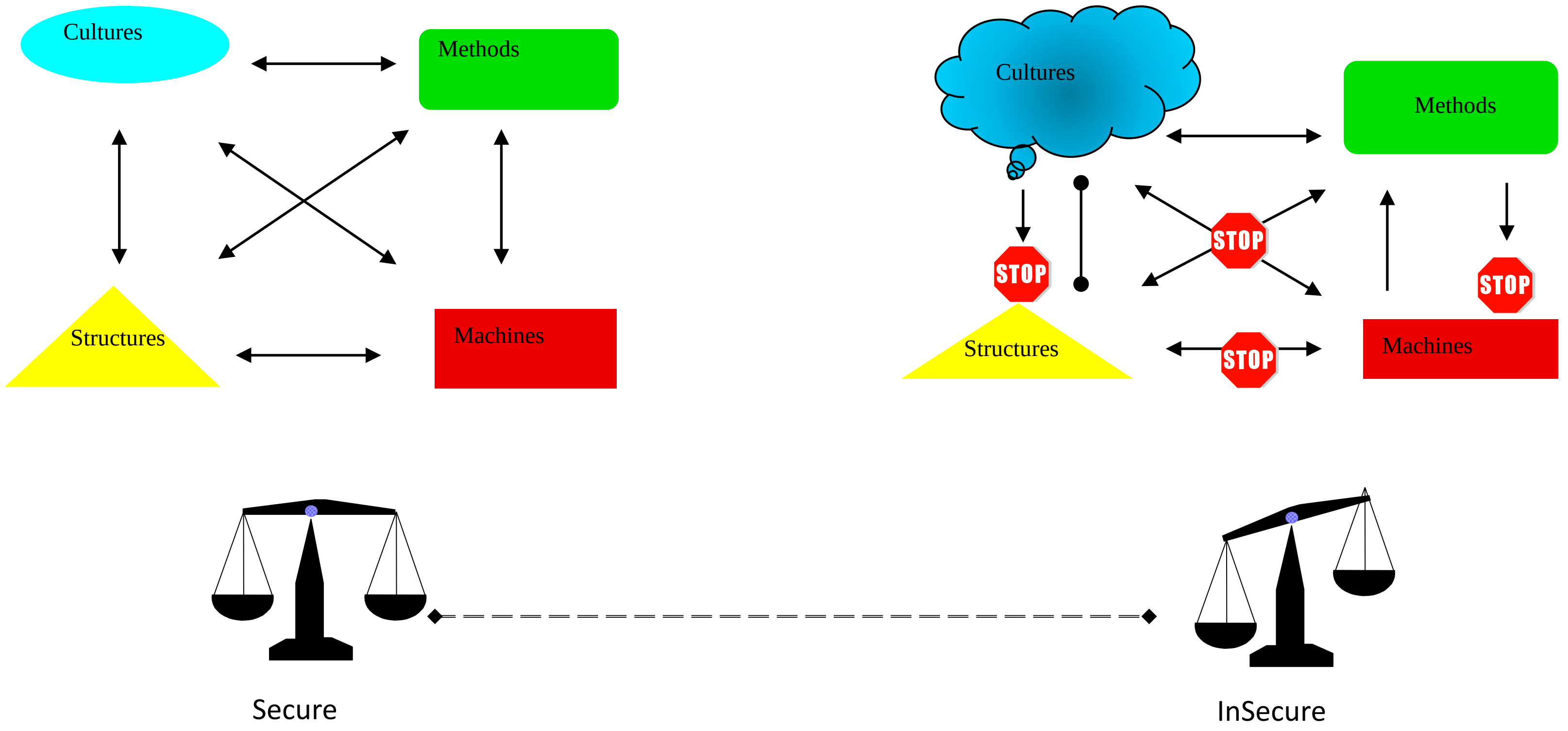


Figure 1.8 System of Socio-technical Systems



Chapter 1

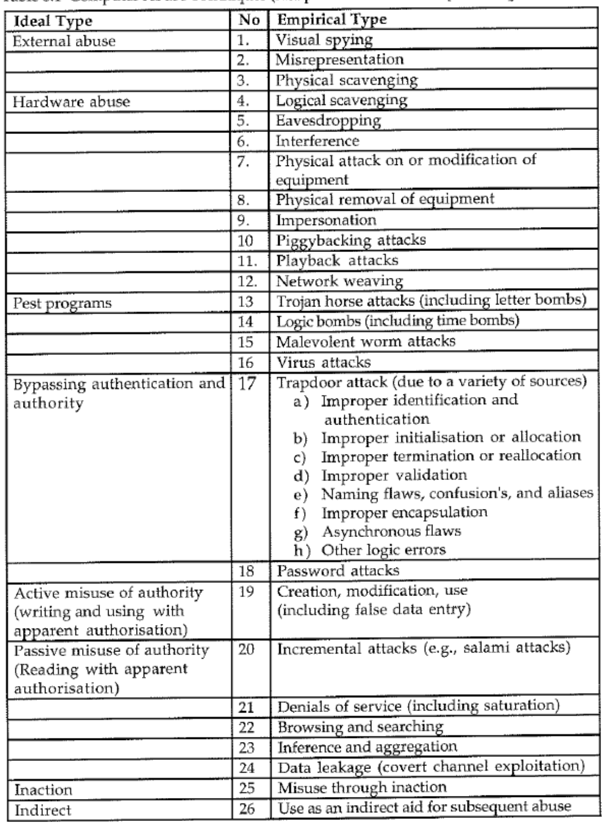
- Problem Formulation
  - Dynamics of socio-technical change and insecurity



2013-05-03

Chapter 6 Modeling Abuse and Collecting Emperical Data

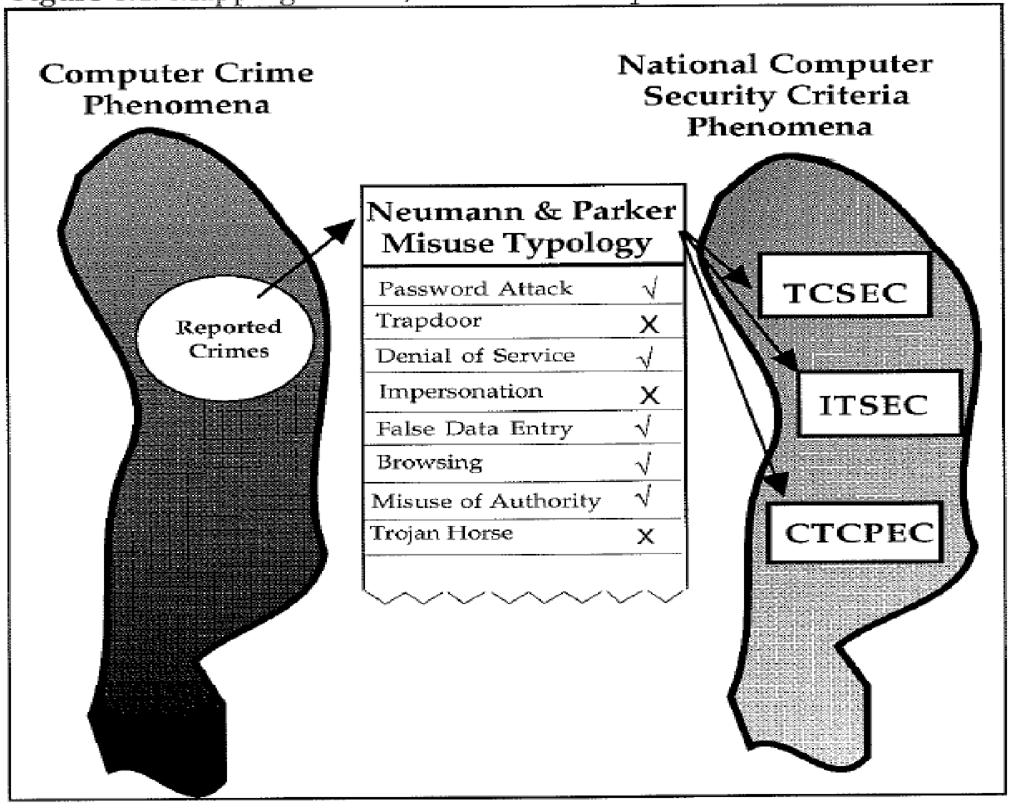
Table 6.1 Computer Abuse Techniques (Adapted from Neumann [NEUM90]).



Ideal Type	No	Empirical Type
External abuse	1.	Visual spying
	2.	Misrepresentation
	3.	Physical scavenging
Hardware abuse	4.	Logical scavenging
	5.	Eavesdropping
	6.	Interference
	7.	Physical attack on or modification of equipment
	8.	Physical removal of equipment
	9.	Impersonation
	10	Piggybacking attacks
	11.	Playback attacks
	12.	Network weaving
Pest programs	13	Trojan horse attacks (including letter bombs)
	14	Logic bombs (including time bombs)
	15	Malevolent worm attacks
	16	Virus attacks
Bypassing authentication and authority	17	Trapdoor attack (due to a variety of sources) a) Improper identification and authentication b) Improper initialisation or allocation c) Improper termination or reallocation d) Improper validation e) Naming flaws, confusion's, and aliases f) Improper encapsulation g) Asynchronous flaws h) Other logic errors
	18	Password attacks
Active misuse of authority (writing and using with apparent authorisation)	19	Creation, modification, use (including false data entry)
Passive misuse of authority (Reading with apparent authorisation)	20	Incremental attacks (e.g., salami attacks)
	21	Denials of service (including saturation)
	22	Browsing and searching
	23	Inference and aggregation
	24	Data leakage (covert channel exploitation)
Inaction	25	Misuse through inaction
Indirect	26	Use as an indirect aid for subsequent abuse

Chapter 6 Modeling Abuse and Collecting Emperical Data

Figure 6.4. Mapping Crimes, Misuse Techniques and Criteria



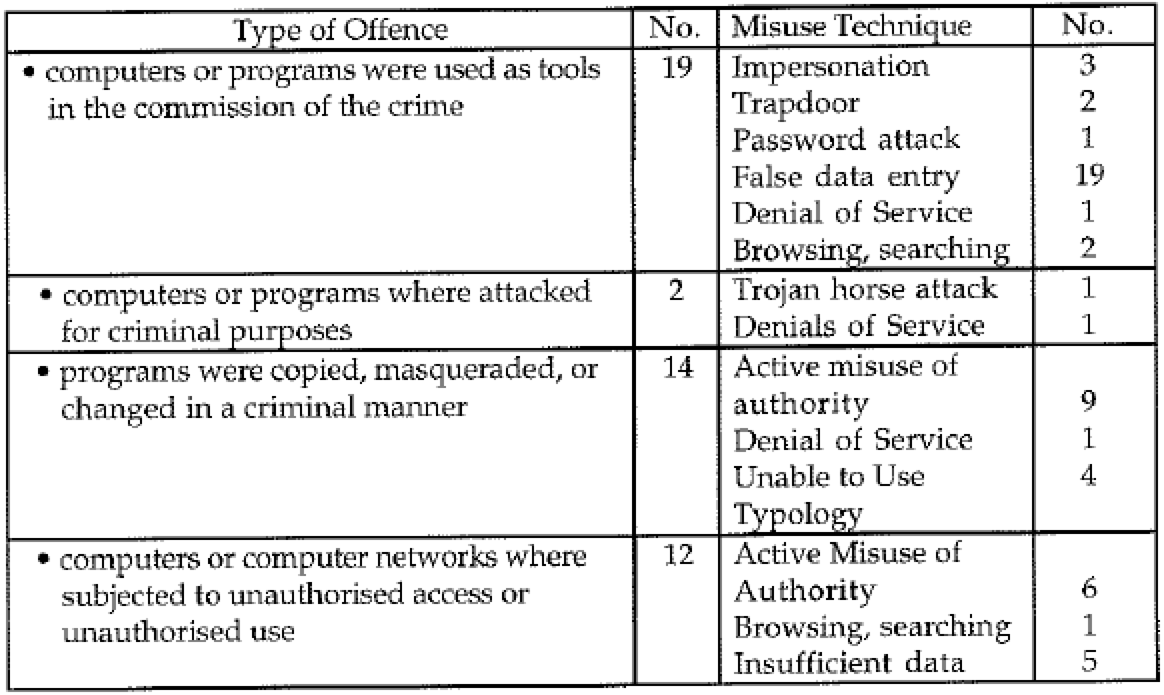
Neumann & Parker Misuse Typology	
Password Attack	√
Trapdoor	X
Denial of Service	√
Impersonation	X
False Data Entry	√
Browsing	√
Misuse of Authority	√
Trojan Horse	X

TCSEC - American Orange book

ITSEC- European CTCPEC- Canadain

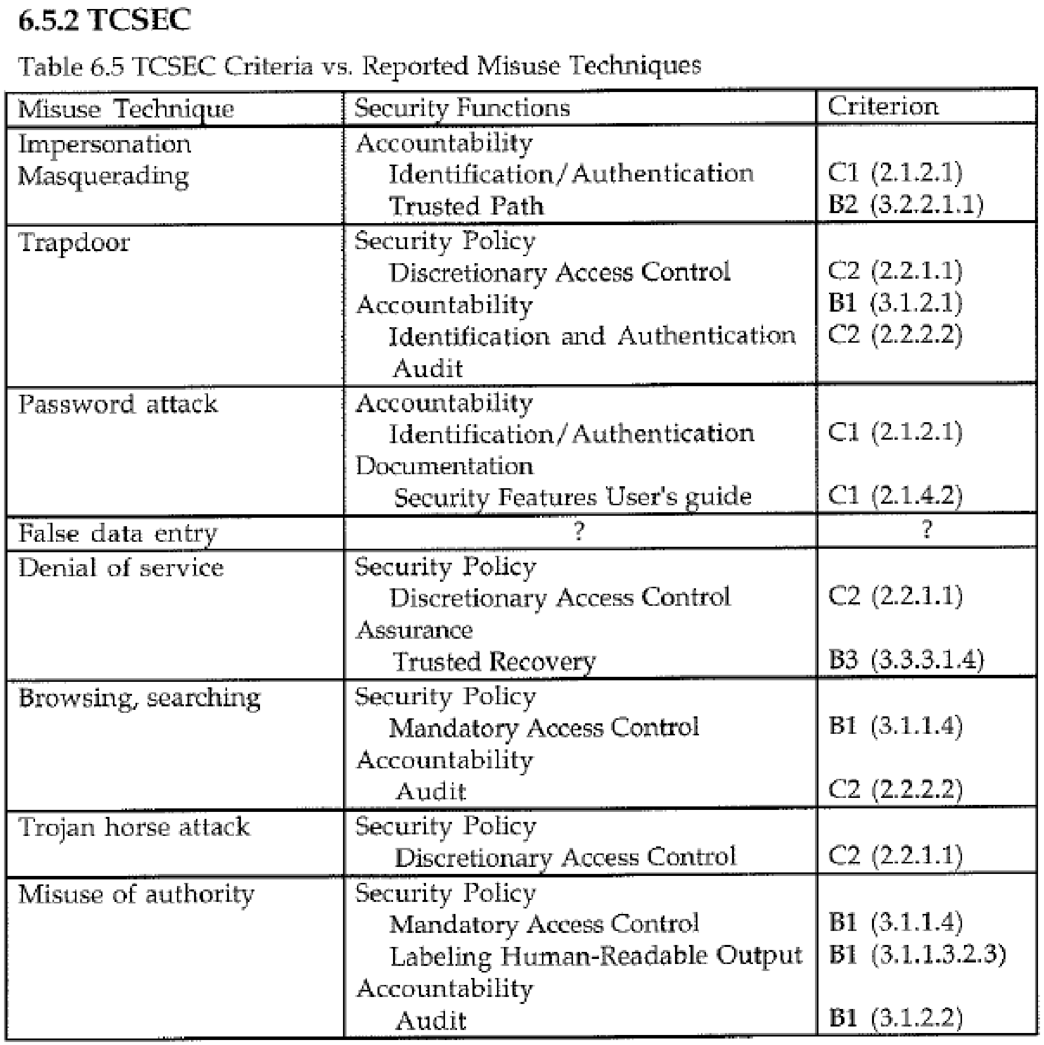
Chapter 6 Modeling Abuse and Collecting Emperical Data

Table 6.4 Cases Reported Mapped to Misuse Typology



Type of Offence	No.	Misuse Technique	No.
• computers or programs were used as tools in the commission of the crime	19	Impersonation Trapdoor Password attack False data entry Denial of Service Browsing, searching	3 2 1 19 1 2
• computers or programs where attacked for criminal purposes	2	Trojan horse attack Denials of Service	1 1
• programs were copied, masqueraded, or changed in a criminal manner	14	Active misuse of authority Denial of Service Unable to Use Typology	9 1 4
• computers or computer networks where subjected to unauthorised access or unauthorised use	12	Active Misuse of Authority Browsing, searching Insufficient data	6 1 5

Chapter 6 Modeling Abuse and Collecting Emperical Data



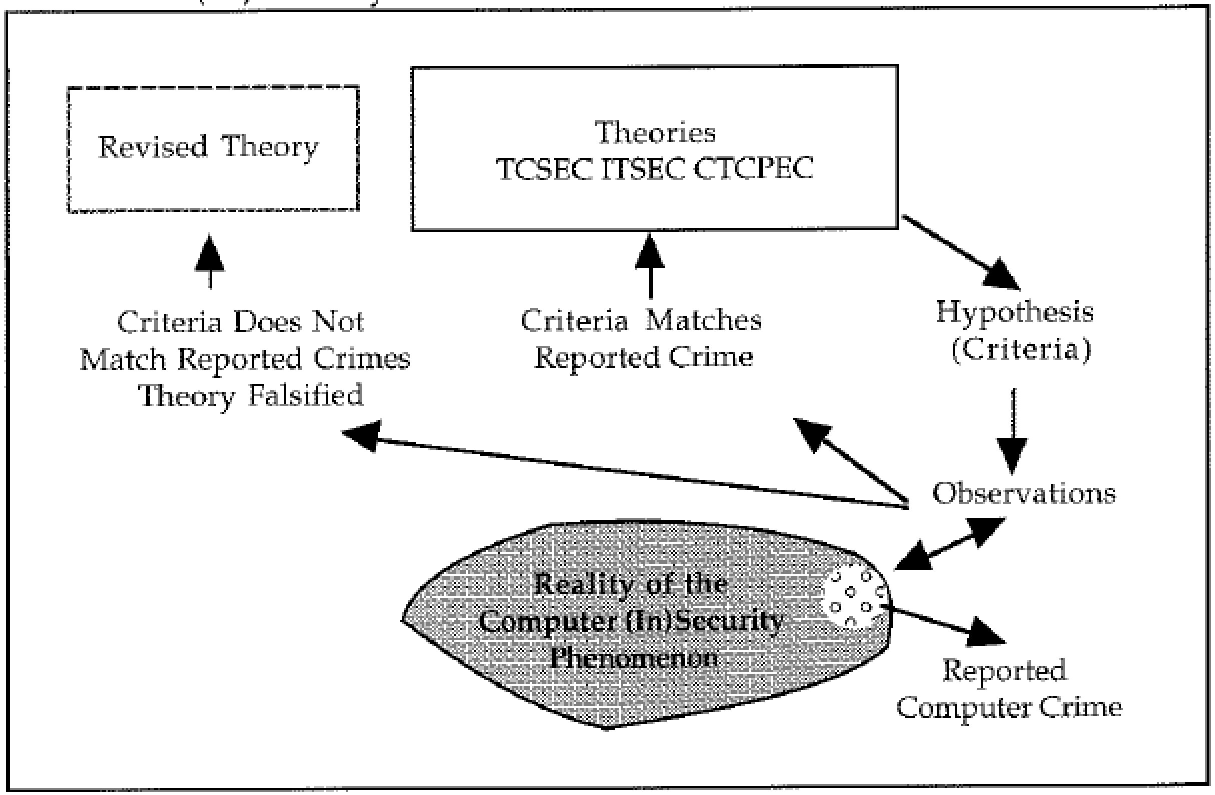
6.5.2 TCSEC

Table 6.5 TCSEC Criteria vs. Reported Misuse Techniques

Misuse Technique	Security Functions	Criterion
Impersonation Masquerading	Accountability Identification/Authentication Trusted Path	C1 (2.1.2.1) B2 (3.2.2.1.1)
Trapdoor	Security Policy Discretionary Access Control Accountability Identification and Authentication Audit	C2 (2.2.1.1) B1 (3.1.2.1) C2 (2.2.2.2)
Password attack	Accountability Identification/Authentication Documentation Security Features User's guide	C1 (2.1.2.1) C1 (2.1.4.2)
False data entry	?	?
Denial of service	Security Policy Discretionary Access Control Assurance Trusted Recovery	C2 (2.2.1.1) B3 (3.3.3.1.4)
Browsing, searching	Security Policy Mandatory Access Control Accountability Audit	B1 (3.1.1.4) C2 (2.2.2.2)
Trojan horse attack	Security Policy Discretionary Access Control	C2 (2.2.1.1)
Misuse of authority	Security Policy Mandatory Access Control Labeling Human-Readable Output Accountability Audit	B1 (3.1.1.4) B1 (3.1.1.3.2.3) B1 (3.1.2.2)

Chapter 6 Conclusion

Figure 6.5 Computer (In)security Theories and the Computer (In)security Phenomenon



Chapter 11-12 Using the SBC Modeling the World, From ideal to actual!!

Ideal

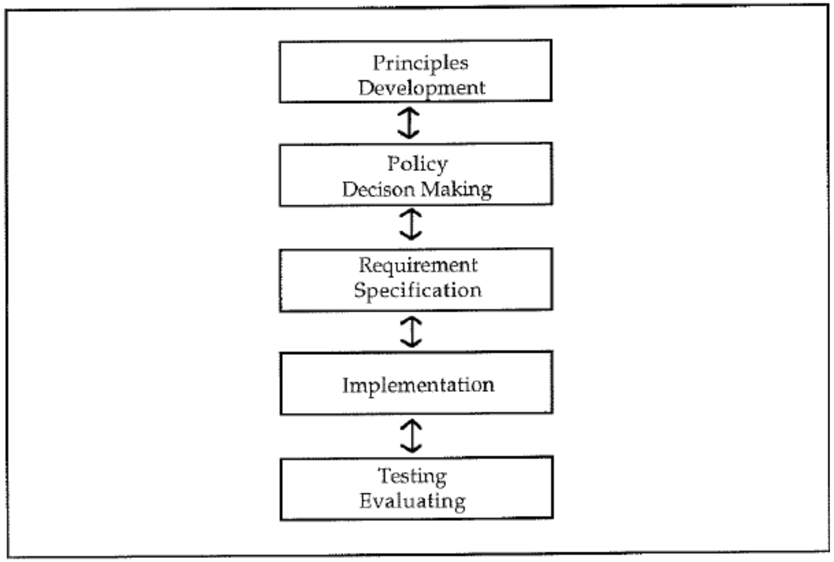
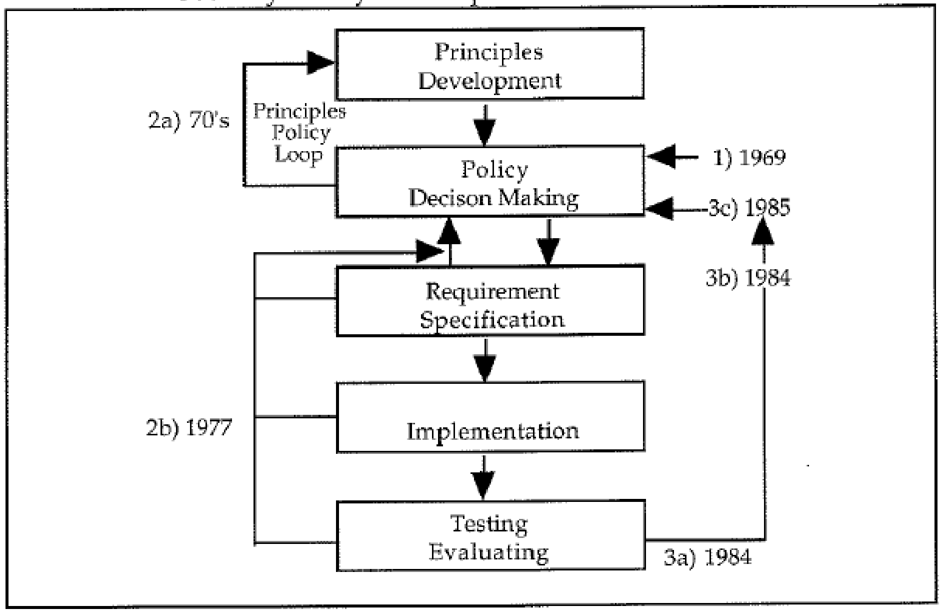
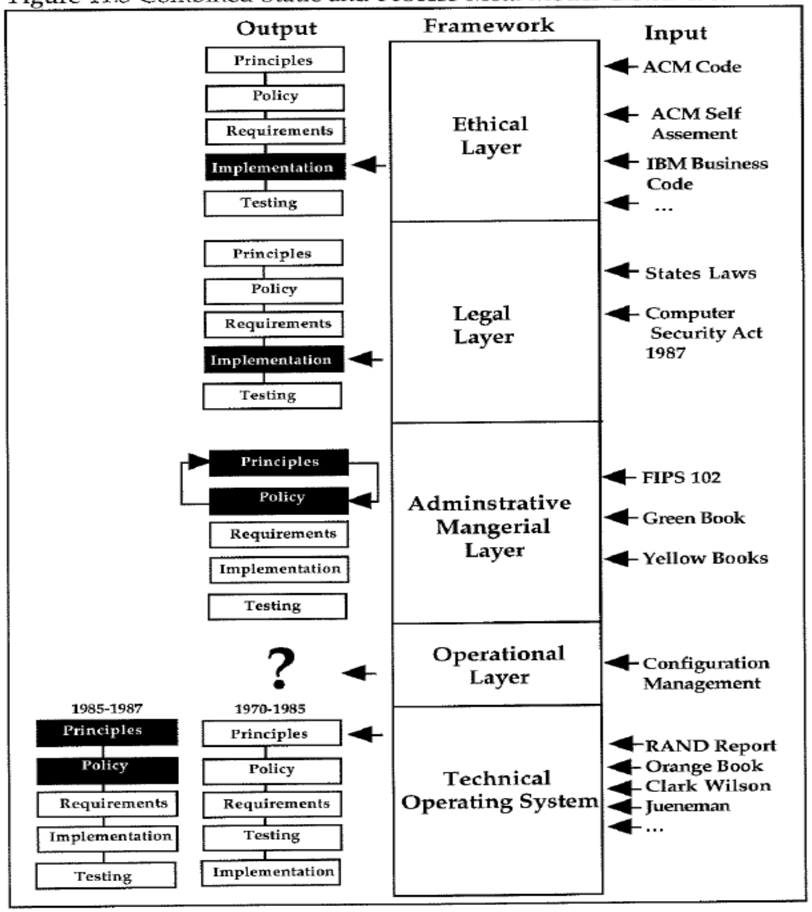


Figure 11.2 Process Meta Model of the U.S.A National Computer Security Policy Development 1969-1985



Chapter 11-12 Using the SBC Modeling the World, From ideal to actual!!

Figure 11.5 Combined Static and Process Meta Model U.S.A. 1989



Chapter 11-12 Using the SBC Modeling the World, From ideal to actual!!

Figure 12.3 SBC Flow Diagram Ethical Subsystem

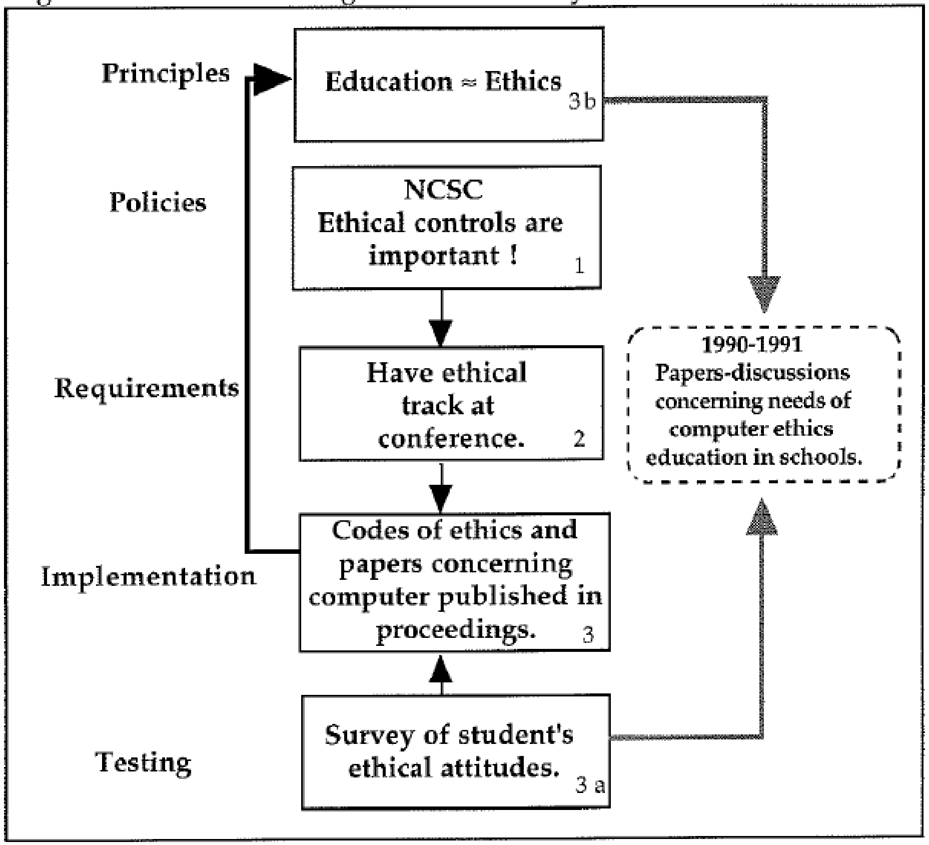
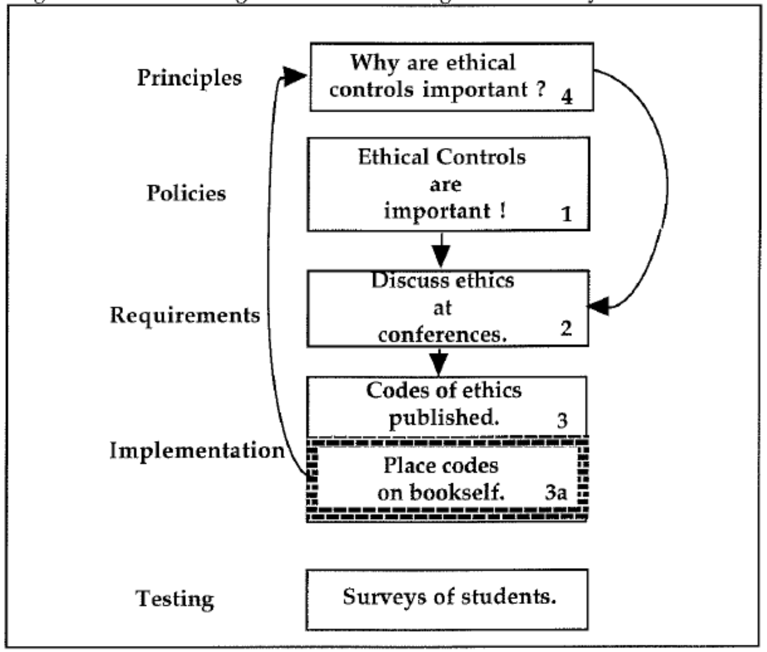

Principles
Policies
Requirements
Implementation
Testing
Education ≈ Ethics 3b
NCSC
Ethical controls are important ! 1
Have ethical track at conference. 2
Codes of ethics and papers concerning computer published in proceedings. 3
Survey of student's ethical attitudes. 3 a
1990-1991
Papers-discussions concerning needs of computer ethics education in schools.

Figure 12.4 Flow Diagram Disfunctioning Ethical Subsystem


Principles
Policies
Requirements
Implementation
Testing
Why are ethical controls important ? 4
Ethical Controls are important ! 1
Discuss ethics at conferences. 2
Codes of ethics published. 3
Place codes on bookself. 3a
Surveys of students.

Chapter 11-12 Using the SBC Modeling the World, From ideal to actual!!

Figure 12.5 Flow Diagram Political Legal Subsystem

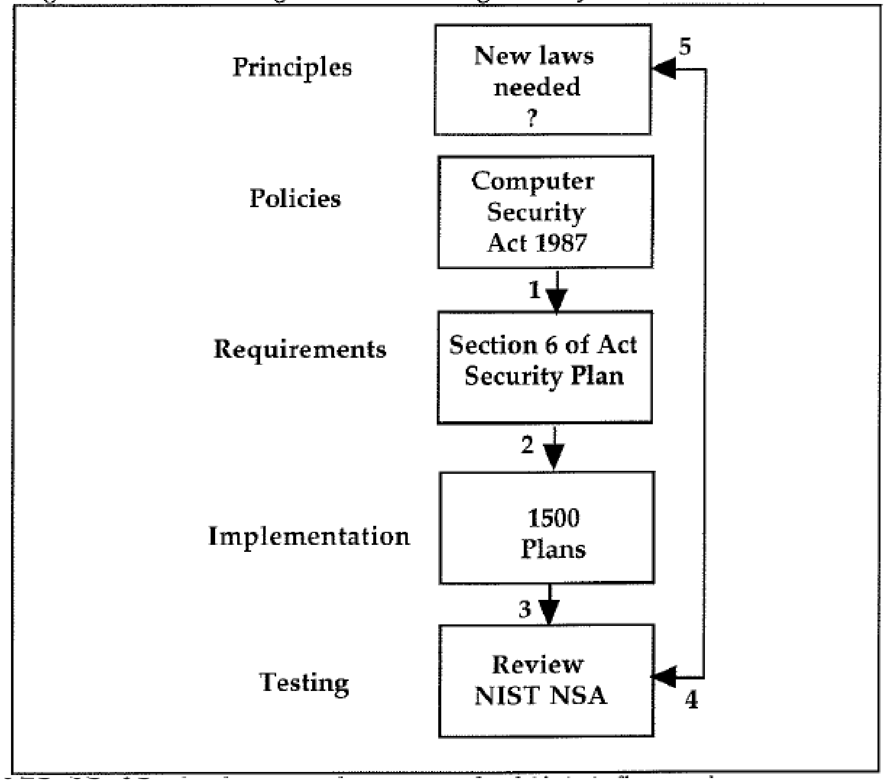
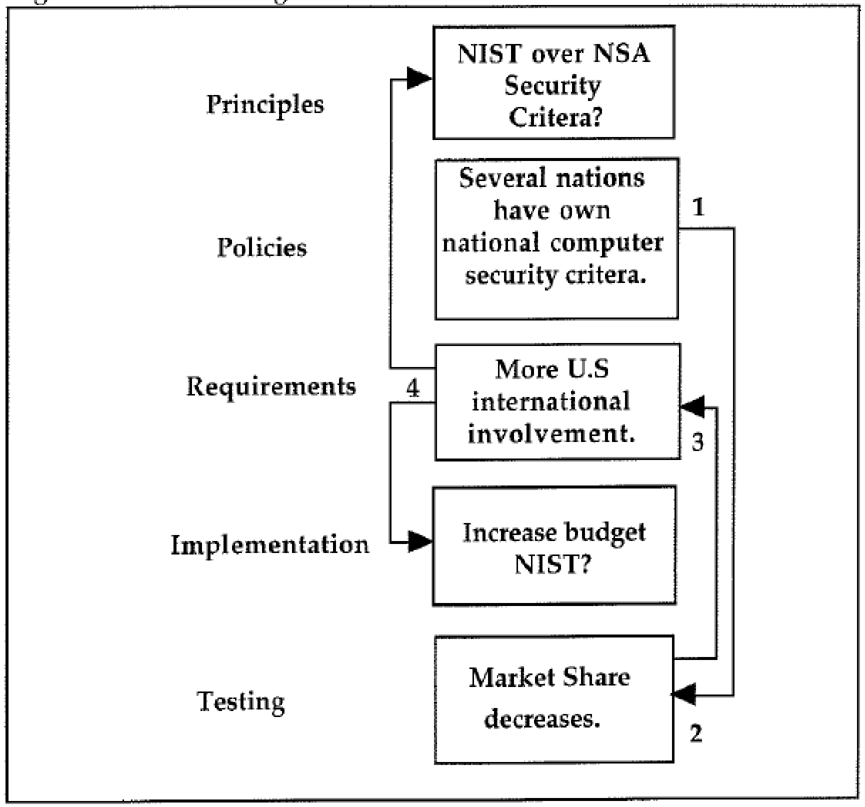


Figure 12.6 Flow Diagram of a Possible Future Political Situation


Principles
Policies
Requirements
Implementation
Testing
NIST over NSA Security Critera?
Several nations have own national computer security critera.
More U.S international involvement.
Increase budget NIST?
Market Share decreases.
1
2
3
4

Chapter 11-12 Using the SBC Modeling the World, From ideal to actual!!

Figure 12.8 Flow Diagram Disfunctioning Operational Subsystem.

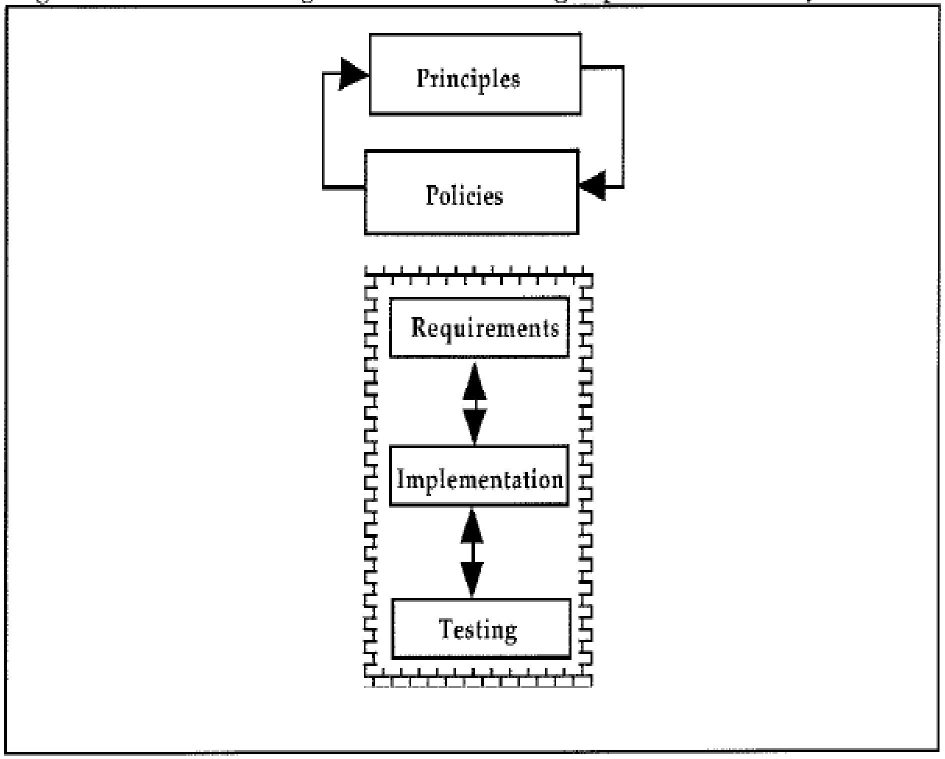
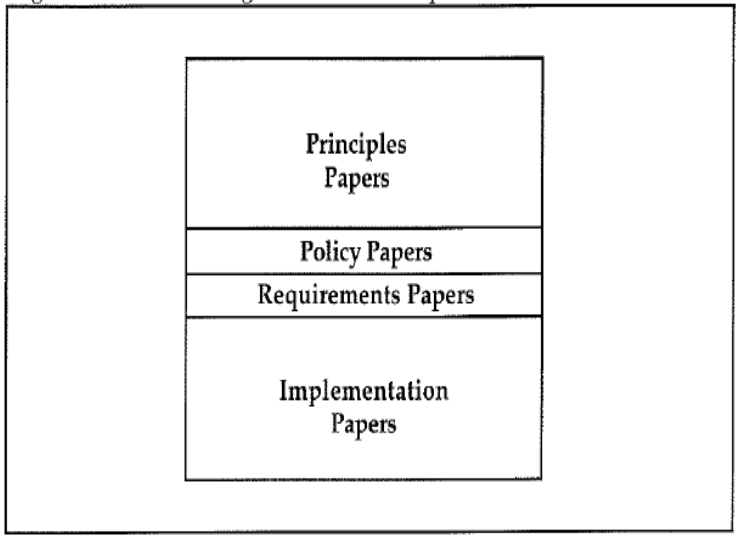


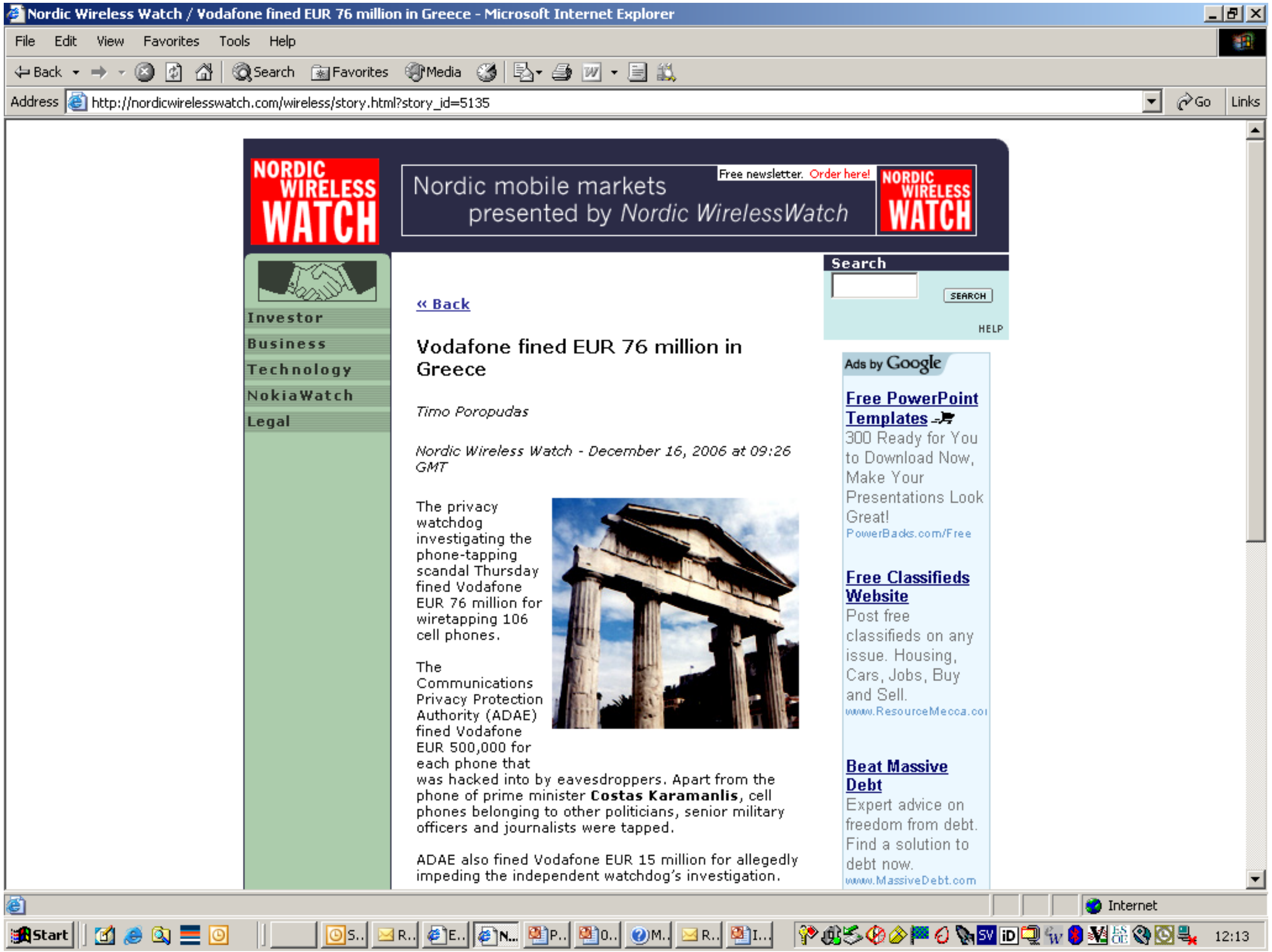
Figure 12.9 Block Diagram Technical Papers



Outline

- Background War Stories
  - Why I am Jaded!
- A Naïve inductivist
  - Why I use a socio-technical systems approach to deal with information security, past and present
- Practise and Standard choose for certification
  - “All is not quite on the Western/Eastern Front!”
  - Past and Present experience with using common criteria

1989-2002



Nordic Wireless Watch / Vodafone fined EUR 76 million in Greece - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://nordicwirelesswatch.com/wireless/story.html?story_id=5135
Go Links
NORDIC WIRELESS WATCH
Nordic mobile markets presented by Nordic WirelessWatch
Free newsletter. Order here!
Investor
Business
Technology
NokiaWatch
Legal
Search
SEARCH
HELP
Internet
Start
12:13

« Back

Vodafone fined EUR 76 million in Greece

Timo Poropudas

Nordic Wireless Watch - December 16, 2006 at 09:26 GMT

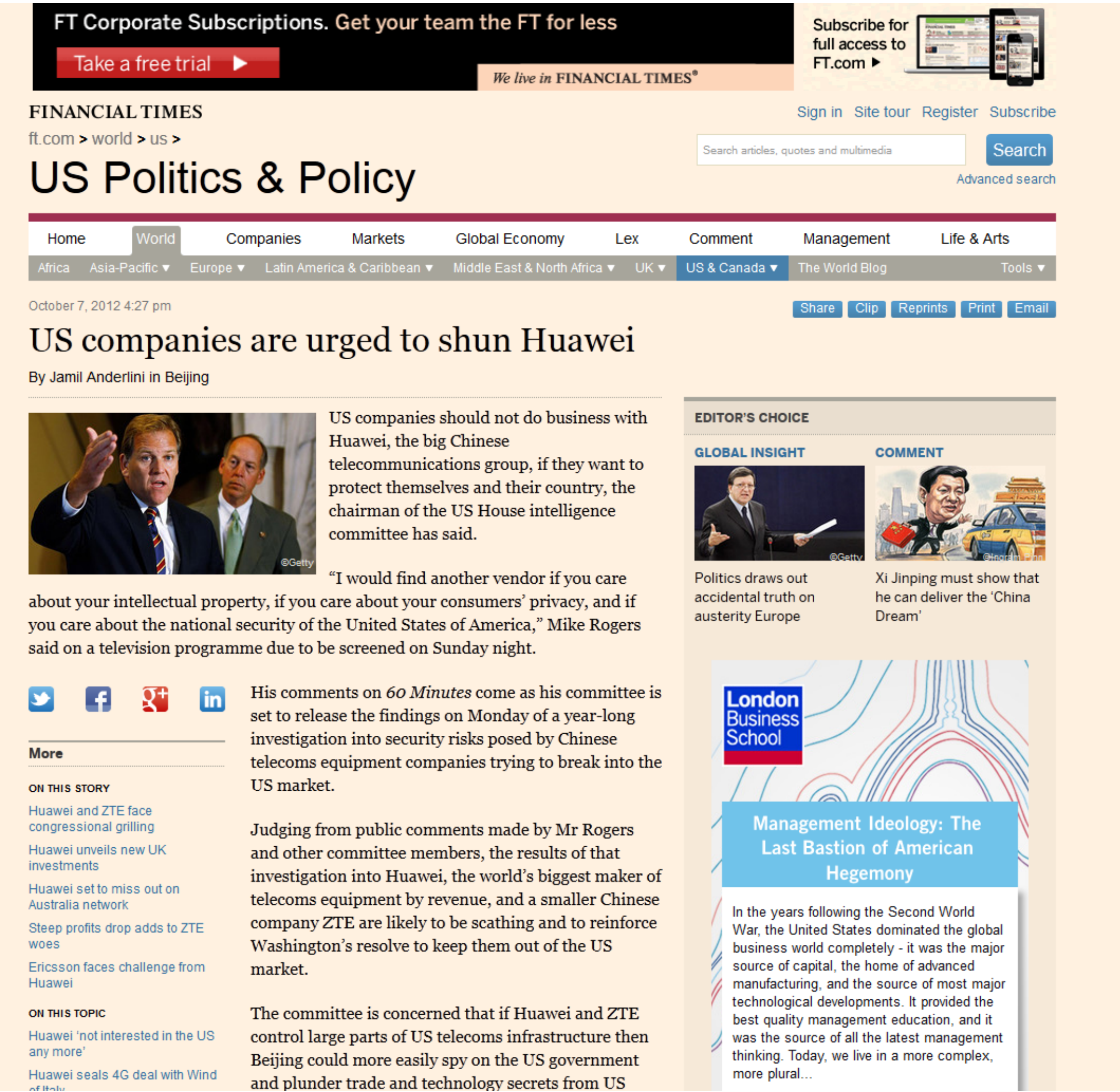
The privacy watchdog investigating the phone-tapping scandal Thursday fined Vodafone EUR 76 million for wiretapping 106 cell phones.

The Communications Privacy Protection Authority (ADAE) fined Vodafone EUR 500,000 for each phone that was hacked into by eavesdroppers. Apart from the phone of prime minister **Costas Karamanlis**, cell phones belonging to other politicians, senior military officers and journalists were tapped.

ADAE also fined Vodafone EUR 15 million for allegedly impeding the independent watchdog's investigation.

Wikipedia

New Worries
Standards War



FINANCIAL TIMES

US Politics & Policy

October 7, 2012 4:27 pm

US companies are urged to shun Huawei

By Jamil Anderlini in Beijing

©Getty

US companies should not do business with Huawei, the big Chinese telecommunications group, if they want to protect themselves and their country, the chairman of the US House intelligence committee has said.

"I would find another vendor if you care about your intellectual property, if you care about your consumers' privacy, and if you care about the national security of the United States of America," Mike Rogers said on a television programme due to be screened on Sunday night.

His comments on *60 Minutes* come as his committee is set to release the findings on Monday of a year-long investigation into security risks posed by Chinese telecoms equipment companies trying to break into the US market.

Judging from public comments made by Mr Rogers and other committee members, the results of that investigation into Huawei, the world's biggest maker of telecoms equipment by revenue, and a smaller Chinese company ZTE are likely to be scathing and to reinforce Washington's resolve to keep them out of the US market.

The committee is concerned that if Huawei and ZTE control large parts of US telecoms infrastructure then Beijing could more easily spy on the US government and plunder trade and technology secrets from US

More

ON THIS STORY

- Huawei and ZTE face congressional grilling
- Huawei unveils new UK investments
- Huawei set to miss out on Australia network
- Steep profits drop adds to ZTE woes
- Ericsson faces challenge from Huawei

ON THIS TOPIC

- Huawei 'not interested in the US any more'
- Huawei seals 4G deal with Wind of Italy

EDITOR'S CHOICE

GLOBAL INSIGHT

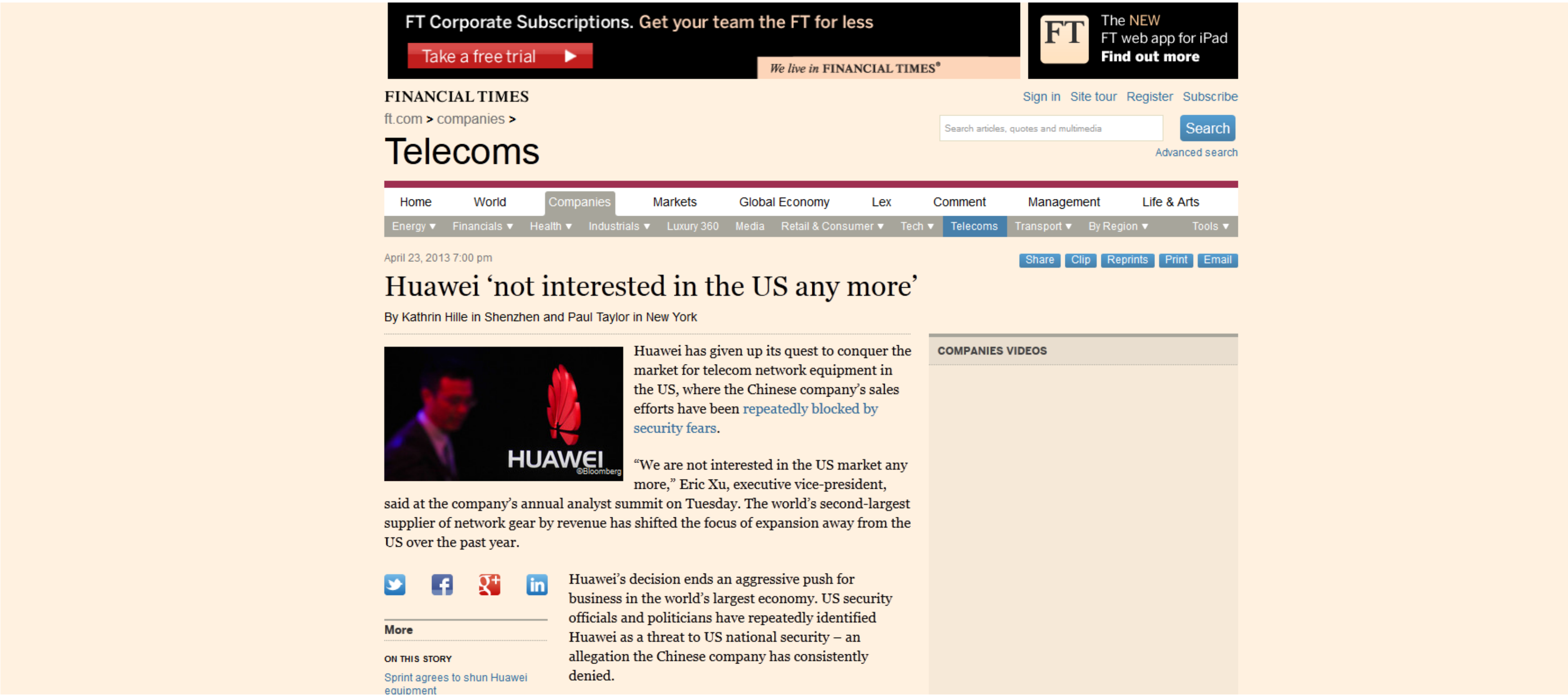
©Getty

Politics draws out accidental truth on austerity Europe

COMMENT

Xi Jinping must show that he can deliver the 'China Dream'

Breaking News



FINANCIAL TIMES

ft.com > companies >

Telecoms

April 23, 2013 7:00 pm

Huawei 'not interested in the US any more'

By Kathrin Hille in Shenzhen and Paul Taylor in New York

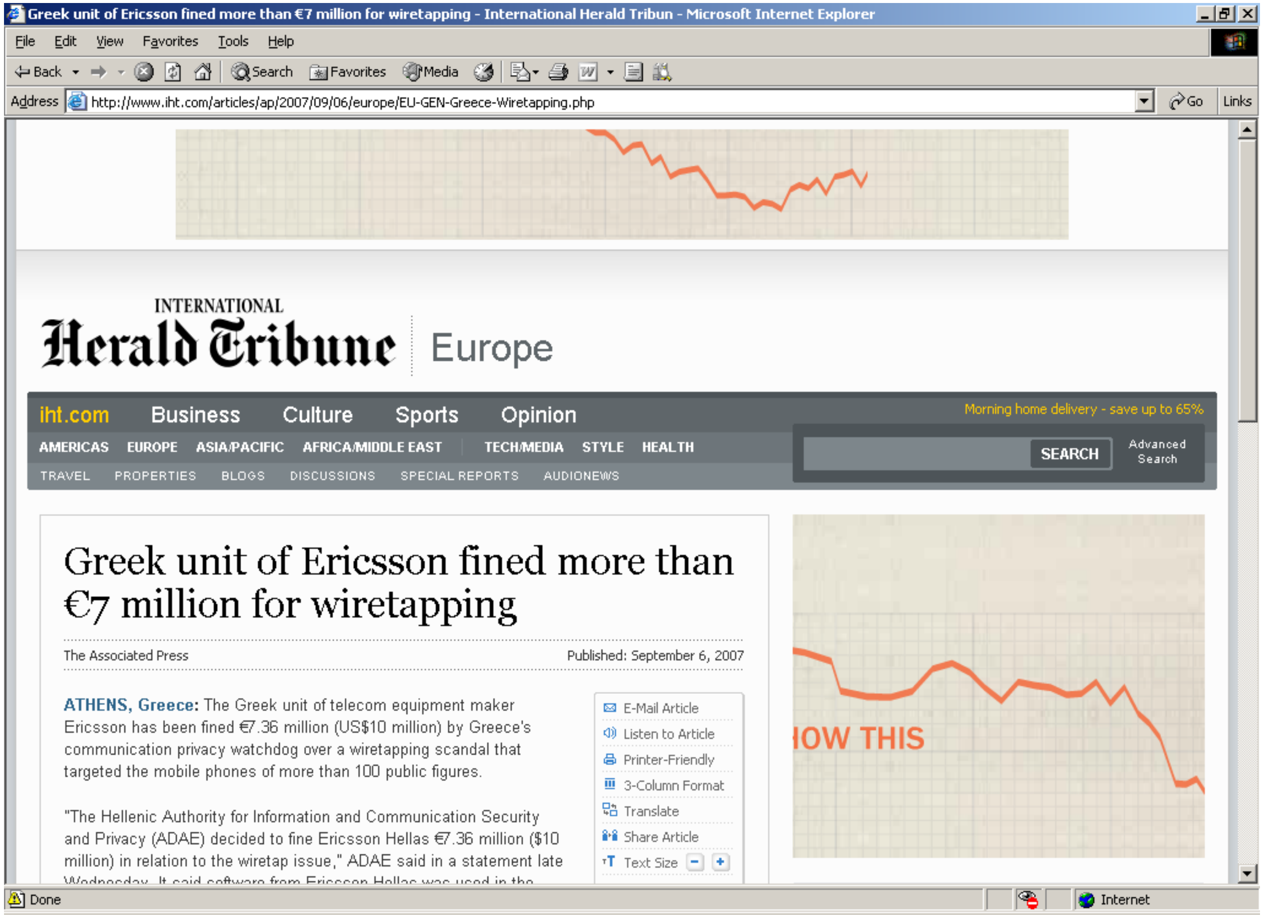
Huawei has given up its quest to conquer the market for telecom network equipment in the US, where the Chinese company's sales efforts have been repeatedly blocked by security fears.

"We are not interested in the US market any more," Eric Xu, executive vice-president, said at the company's annual analyst summit on Tuesday. The world's second-largest supplier of network gear by revenue has shifted the focus of expansion away from the US over the past year.

Huawei's decision ends an aggressive push for business in the world's largest economy. US security officials and politicians have repeatedly identified Huawei as a threat to US national security – an allegation the Chinese company has consistently denied.

Sprint agrees to shun Huawei equipment

Ericsson has beened fined


Greek unit of Ericsson fined more than €7 million for wiretapping - International Herald Tribun - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://www.iht.com/articles/ap/2007/09/06/europe/EU-GEN-Greece-Wiretapping.php
Go Links
iht.com Business Culture Sports Opinion
Morning home delivery - save up to 65%
AMERICAS EUROPE ASIA/PACIFIC AFRICA/MIDDLE EAST TECH/MEDIA STYLE HEALTH
TRAVEL PROPERTIES BLOGS DISCUSSIONS SPECIAL REPORTS AUDIONEWS
SEARCH
Advanced Search
E-Mail Article
Listen to Article
Printer-Friendly
3-Column Format
Translate
Share Article
Text Size
IOW THIS
Done
Internet

INTERNATIONAL Herald Tribune | Europe

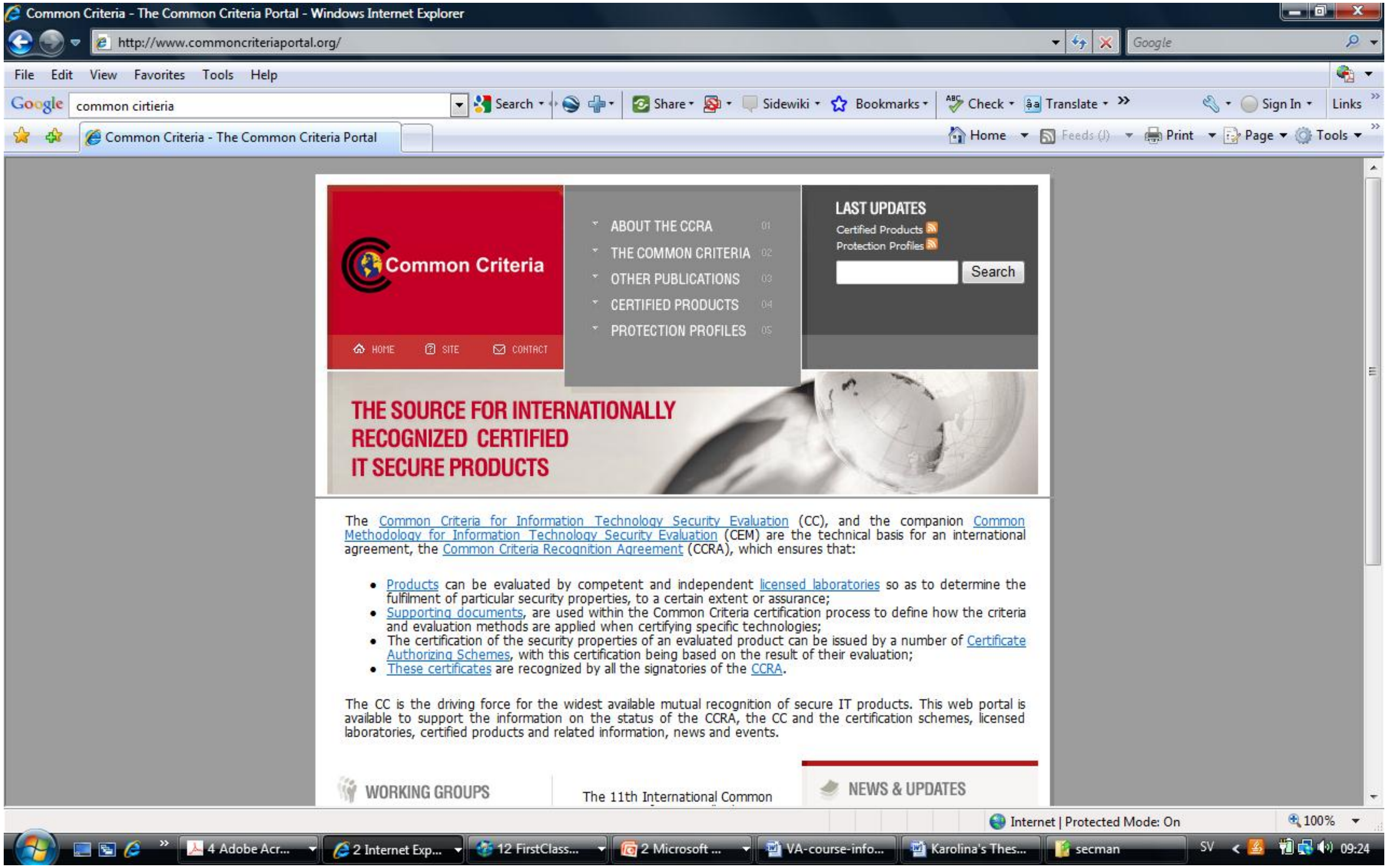
Greek unit of Ericsson fined more than €7 million for wiretapping

The Associated Press — Published: September 6, 2007

ATHENS, Greece: The Greek unit of telecom equipment maker Ericsson has been fined €7.36 million (US$10 million) by Greece's communication privacy watchdog over a wiretapping scandal that targeted the mobile phones of more than 100 public figures.

"The Hellenic Authority for Information and Communication Security and Privacy (ADAE) decided to fine Ericsson Hellas €7.36 million ($10 million) in relation to the wiretap issue," ADAE said in a statement late Wednesday. It said software from Ericsson Hellas was used in the

The Portal



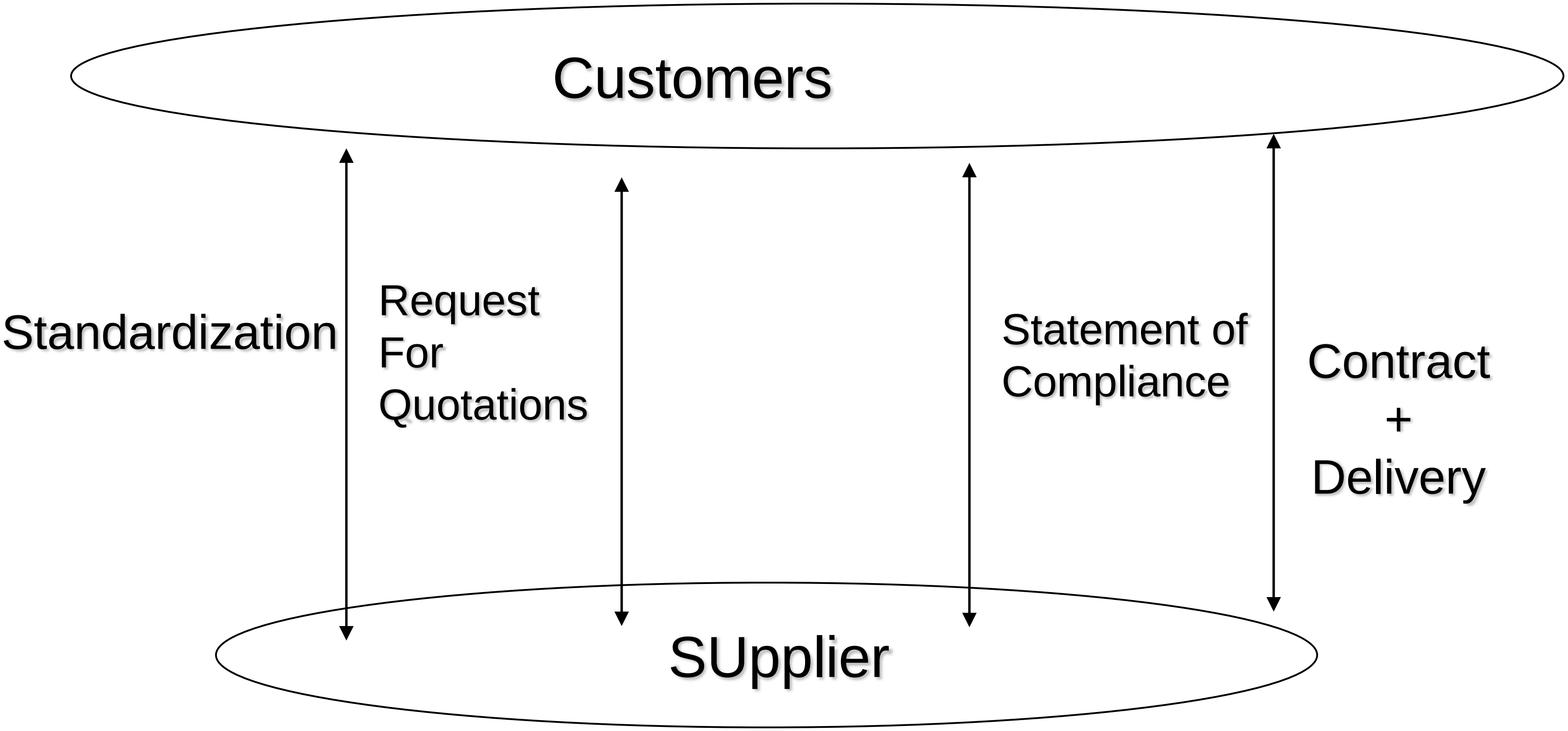
The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which ensures that:

- Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;
- These certificates are recognized by all the signatories of the CCRA.

The CC is the driving force for the widest available mutual recognition of secure IT products. This web portal is available to support the information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events.

The 11th International Common

B2B security not B2C



Customers

Standardization

Request
For
Quotations

Statement of
Compliance

Contract
+
Delivery

SUpplier

SIM Lock Security Standard

- Personalisation (3GPP -22022)

- 14 (e) ***It should be impractical to read or recover any of the control keys from the ME.***

- 14 (f) It should be impractical to ***alter or delete*** the values of the personalisation indicators, the control keys, the stored IMSI or the stored network operator, SP and corporate codes, other than by the defined personalisation and de-personalisation processes, ***without completely disabling the ME from working with any SIM/USIM.*** (Possible methods that might be used by criminals to alter or delete the values include freezing, baking, exposure to magnetic fields or UV light.)

- In all cases, ***secure arrangements*** shall be followed ***with the transfer and handling of the critical data such as the IMSI and the associated control keys***.

- In common with the normal de-personalisation processes, ***the manufacturer controlled processes should be secure and be key or password controlled***.

Request For Quotations (2002)

- The security is to be documented to the buyer.

- Such documentation may include security reviews and evaluation according to standardised criteria, such as those in [TCSEC], [ITSEC], [FIPS140], and [CC 15408], among others.

Background (Why)

Secure SIMLock

- X loses millions of euros every year through the breaking of SIMLock. Subsidised terminals are bought at a reduced price, the SIMLock broken and then the terminal sold at non-subsidised price. X does not therefore get the continued use from the user that is designed to recoup the subsidy.
- Many mechanisms for SIMLock have been tried by terminal manufacturers and virtually all to date have been broken. X therefore hopes that a terminal that has been designed with software and behaviour resilience in mind will provide the secure SIMLock that x seeks.

NESR Map to ISO 15408

Mapping from AWS NESR to Common Criteria

Italic blue text in brackets are assignments or selections added by the author
Red text are not one-to-one mappings, but introduces rules that might be used instead

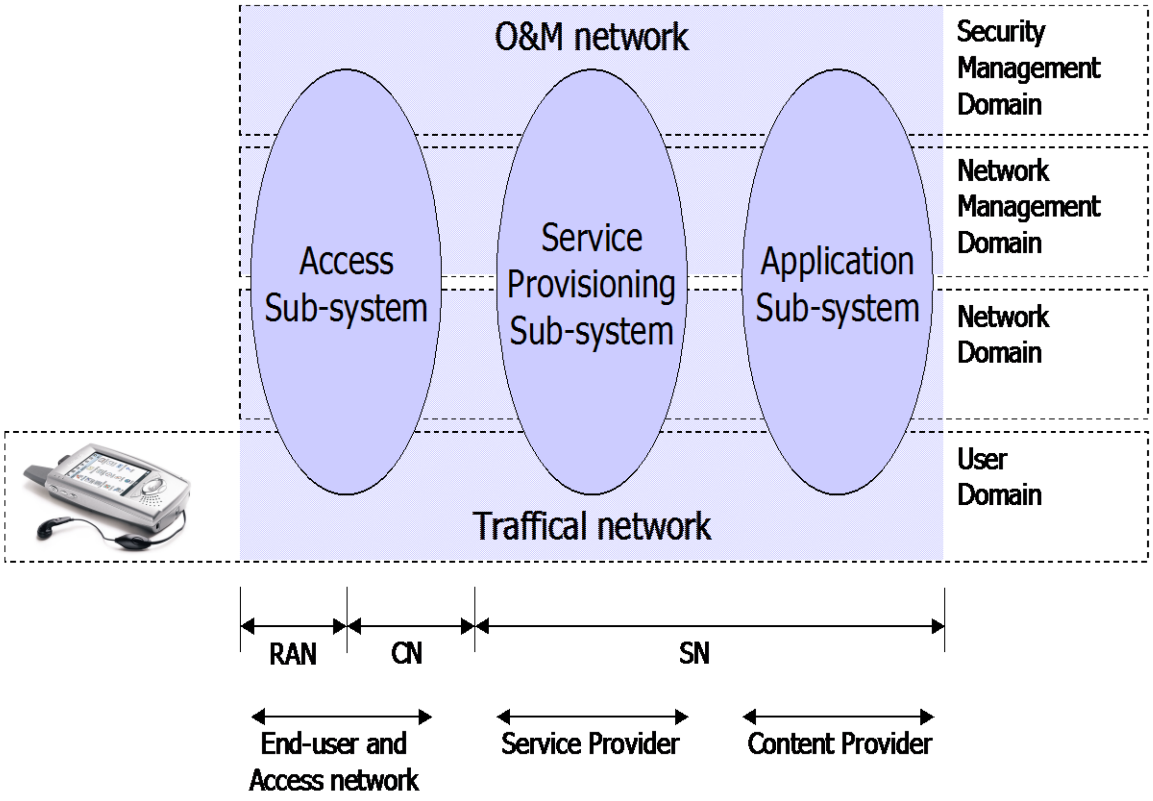
General Computing

NESR #	Description	CC Name	CC description / Comments
1.1.1	**Password/PIN complexity:** The password must be a min of 5 characters long and the construction must be complex enough (not words, names, birthdays etc).	FIA_SOS.1.1 FIA_SOS.2.1 FIA_SOS.2.1	The TSF shall provide a mechanism to verify that secrets [*are at least 5 characters long and complex enough*]. …generate secrets that meet… …enforce the use of generated secrets…
1.1.2	**Disabling inactive user IDs:** The password of a user whose ID has not been used for more than 45 days must be disabled	FDP_ACF.1.4	The TSF shall explicitly deny access to subjects [*whose ID has been inactive for more than 45 days*] (deny access not the same as disabling…)

!

Draft
PP/ST's

The 3G System Model for security

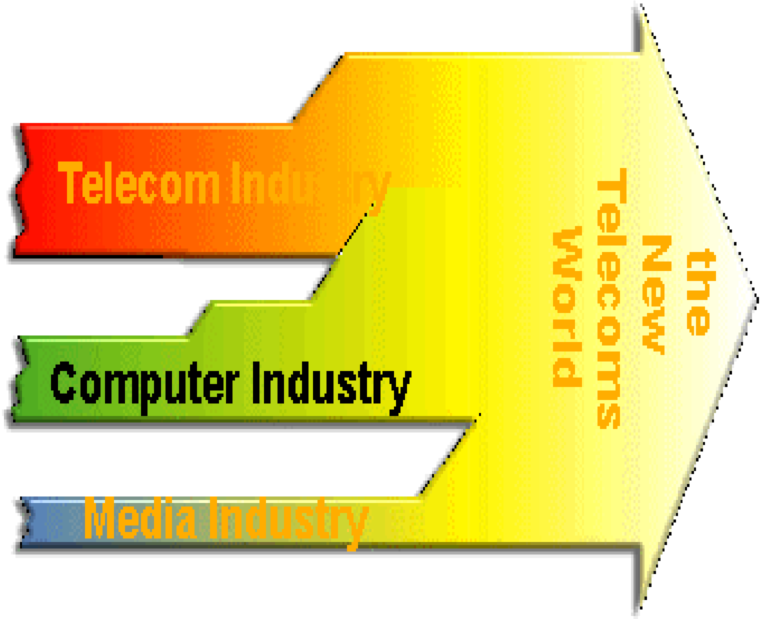


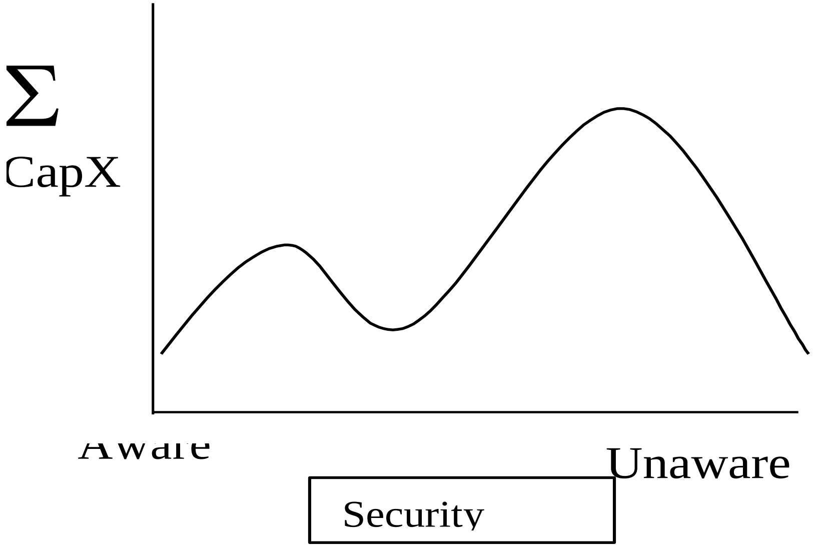
"Key Administration Center"

√ J-20 ST
Backbone Route PP

√ SIM-Lock
Function

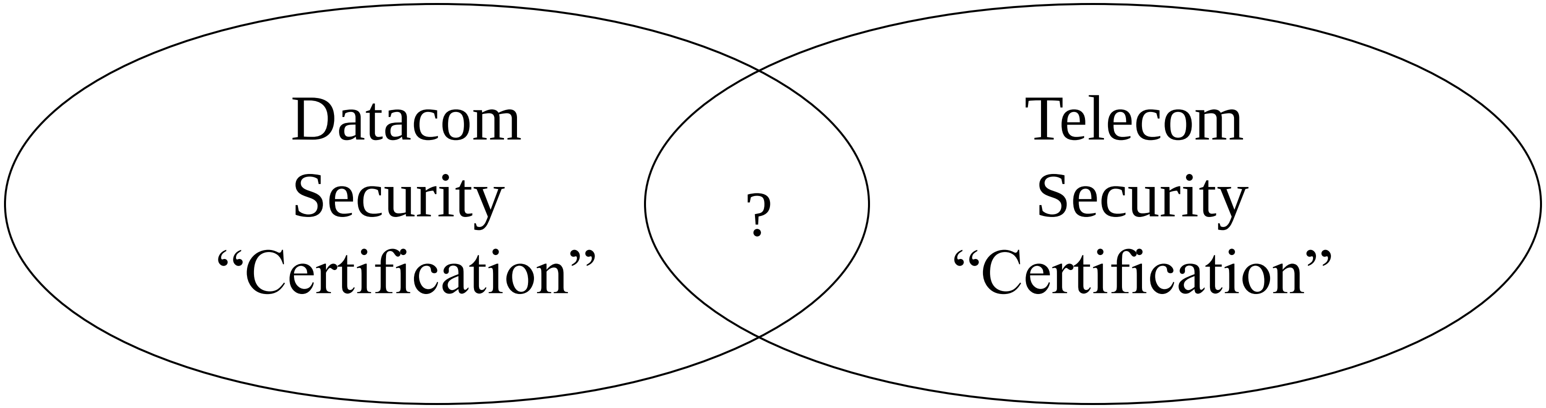
Background 7 years Ago
The Market?





Technical Background
: “State of the Union”

- Telecom Datacom Security
  - The 802.11b case



Datacom
Security
“Certification”

?

Telecom
Security
“Certification”

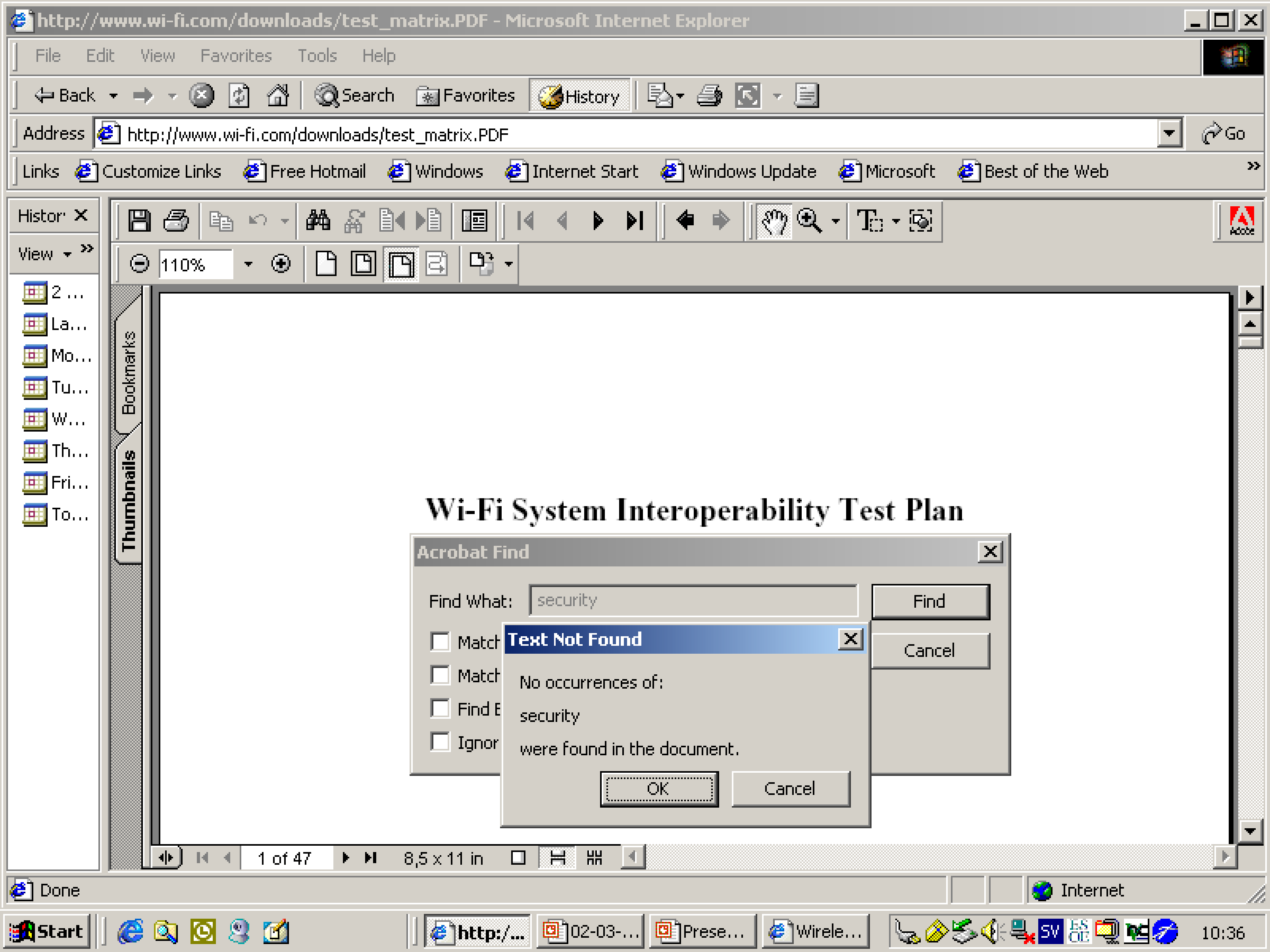
ASSUMED Secure

- “The standard ´IEEE 802-11b, Wi-FI´ was assumed to be adequate since no beta testing had been able to defeat WEP without a significant computing effort”.

United States National Infrastucture Protection Center

Wireless Ethernet Compatibility Alliance 802.11b Wired Equivalent Privacy (**WEP**) **Security** February 19, 2001

- The goal of **WEP** is to provide an equivalent level of privacy as is ordinarily present with an unsecured wired LAN.


http://www.wi-fi.com/downloads/test_matrix.PDF - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address
Go
Links Customize Links Free Hotmail Windows Internet Start Windows Update Microsoft Best of the Web
Histor
View
2 …
La…
Mo…
Tu…
W…
Th…
Fri…
To…
Bookmarks
Thumbnails
110%
1 of 47
8,5 x 11 in
Find
Cancel
Match
Match
Find E
Ignor
OK
Cancel
Done
Internet
Start
http:/…
02-03-…
Prese…
Wirele…
SV
10:36

Address: http://www.wi-fi.com/downloads/test_matrix.PDF

Wi-Fi System Interoperability Test Plan

Acrobat Find

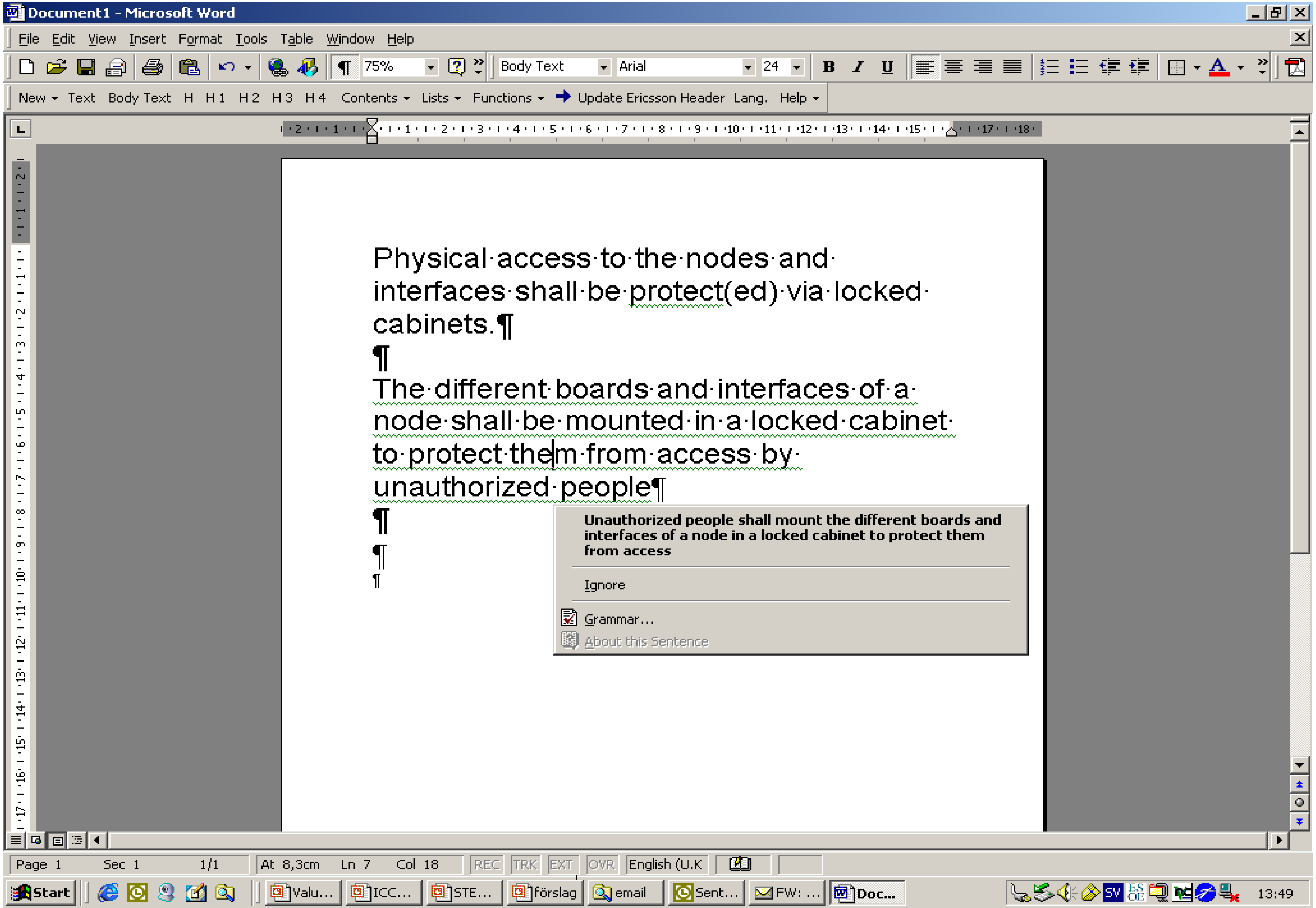
Find What: security

Text Not Found

No occurrences of:

security

were found in the document.



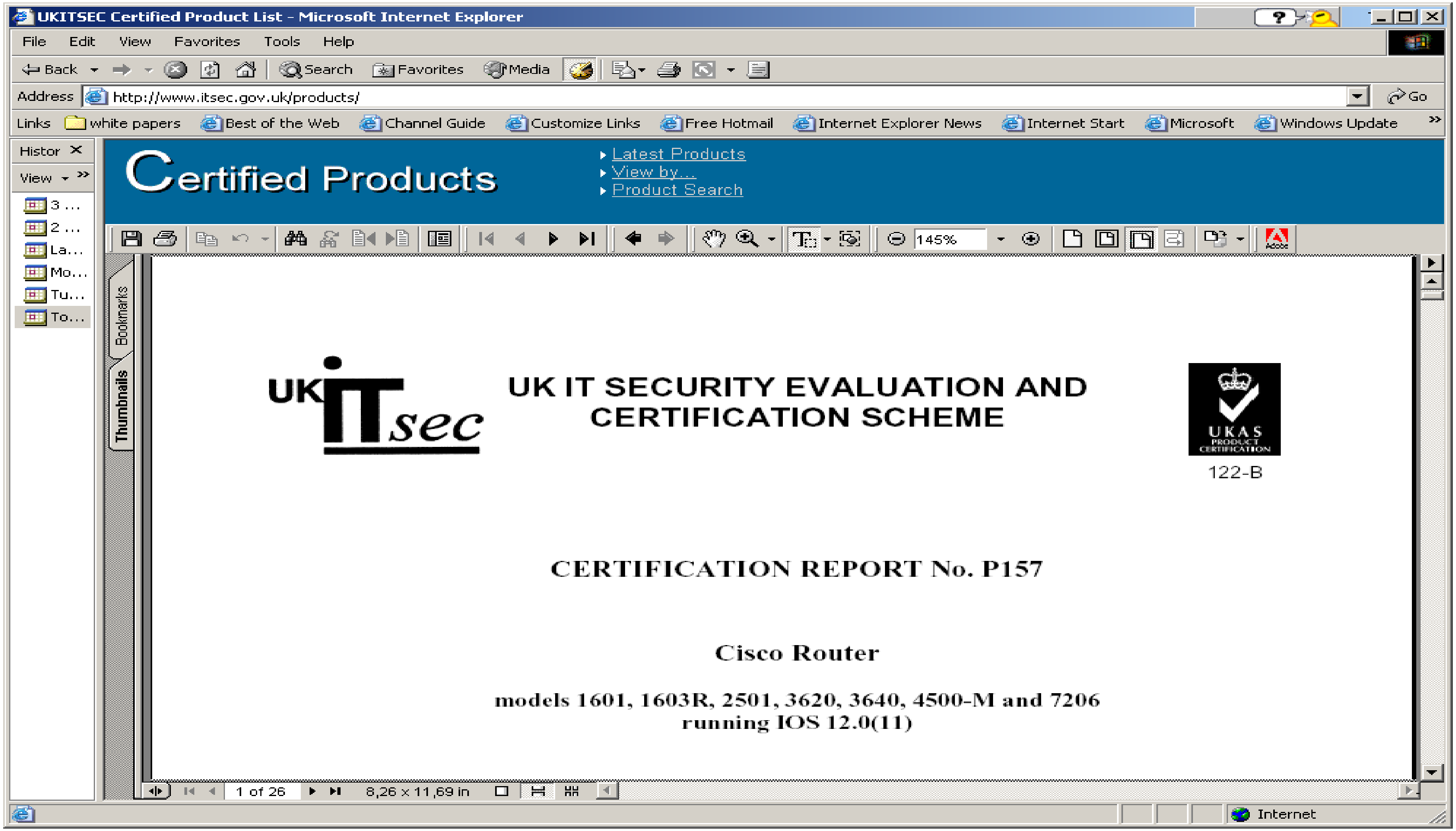
Physical access to the nodes and interfaces shall be protect(ed) via locked cabinets.

The different boards and interfaces of a node shall be mounted in a locked cabinet to protect them from access by unauthorized people

Unauthorized people shall mount the different boards and interfaces of a node in a locked cabinet to protect them from access

Document1 - Microsoft Word
File Edit View Insert Format Tools Table Window Help
75%
Body Text
Arial
24
New Text Body Text H H 1 H 2 H 3 H 4 Contents Lists Functions Update Ericsson Header Lang. Help
Ignore
Grammar...
About this Sentence
Page 1 Sec 1 1/1 At 8,3cm Ln 7 Col 18 REC TRK EXT OVR English (U.K
Start
Valu...
ICC...
STE...
förslag
email
Sent...
FW: ...
Doc...
SV
13:49

The Large Print Gives!



UK IT sec

UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

UKAS PRODUCT CERTIFICATION

122-B

CERTIFICATION REPORT No. P157

Cisco Router

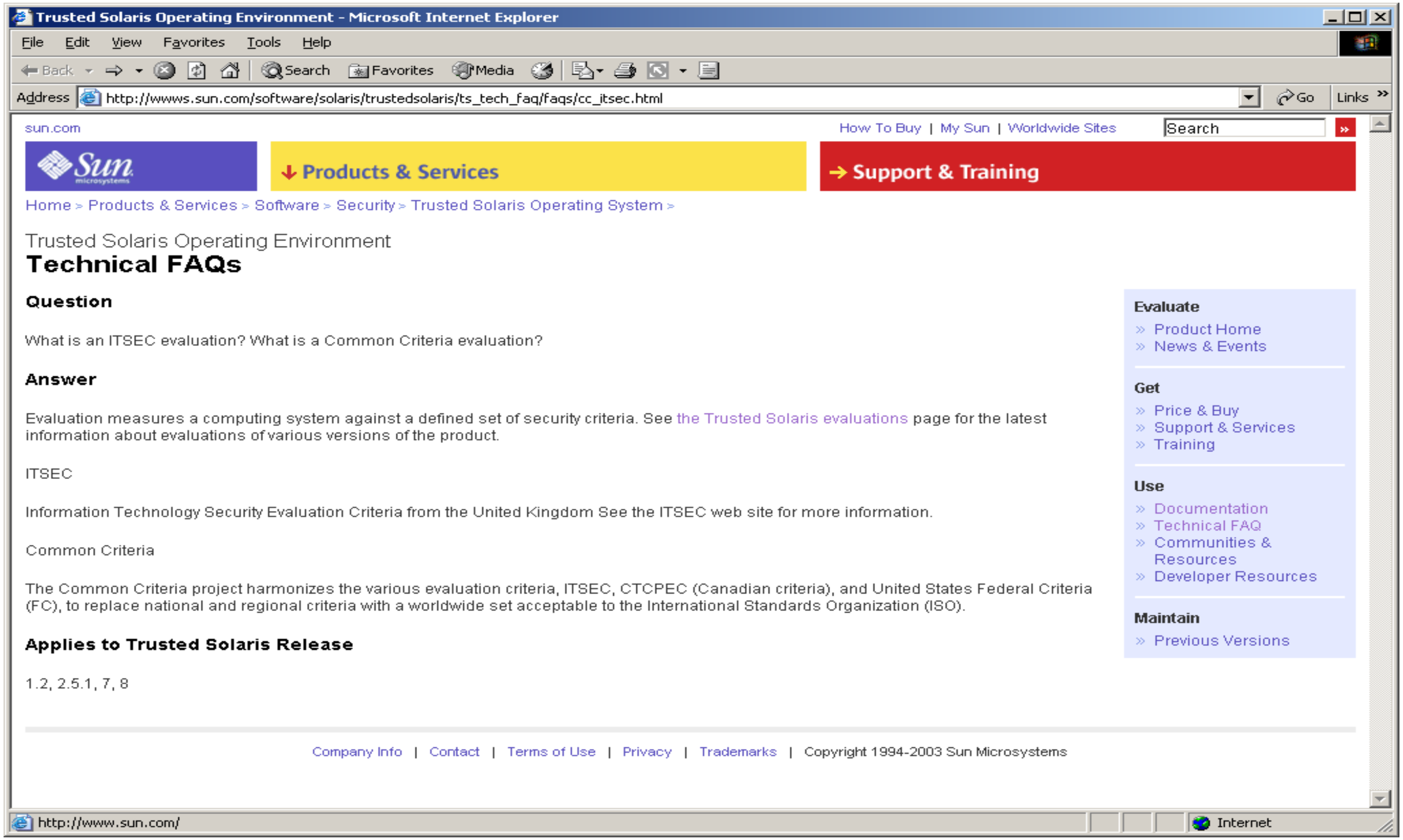
models 1601, 1603R, 2501, 3620, 3640, 4500-M and 7206
running IOS 12.0(11)

The Small Print Takes Back.

- Certification is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with higher assurance levels) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body’s view at the time of certification. Users (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether such patches have been evaluated and certified. Users are reminded of the security dangers inherent in downloading ‘hot-fixes’ where these are available, and that the UK Certification Body provides no assurance whatsoever for patches obtained in this manner.

- The issue of a Certification Report is not an endorsement of a product.

Trust Solaris



Trusted Solaris Operating Environment - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://wwws.sun.com/software/solaris/trustedsolaris/ts_tech_faq/faqs/cc_itsec.html
Go Links
sun.com
How To Buy | My Sun | Worldwide Sites
Search
Products & Services
Support & Training
Home > Products & Services > Software > Security > Trusted Solaris Operating System >

Trusted Solaris Operating Environment

Technical FAQs

Question

What is an ITSEC evaluation? What is a Common Criteria evaluation?

Answer

Evaluation measures a computing system against a defined set of security criteria. See the Trusted Solaris evaluations page for the latest information about evaluations of various versions of the product.

ITSEC

Information Technology Security Evaluation Criteria from the United Kingdom See the ITSEC web site for more information.

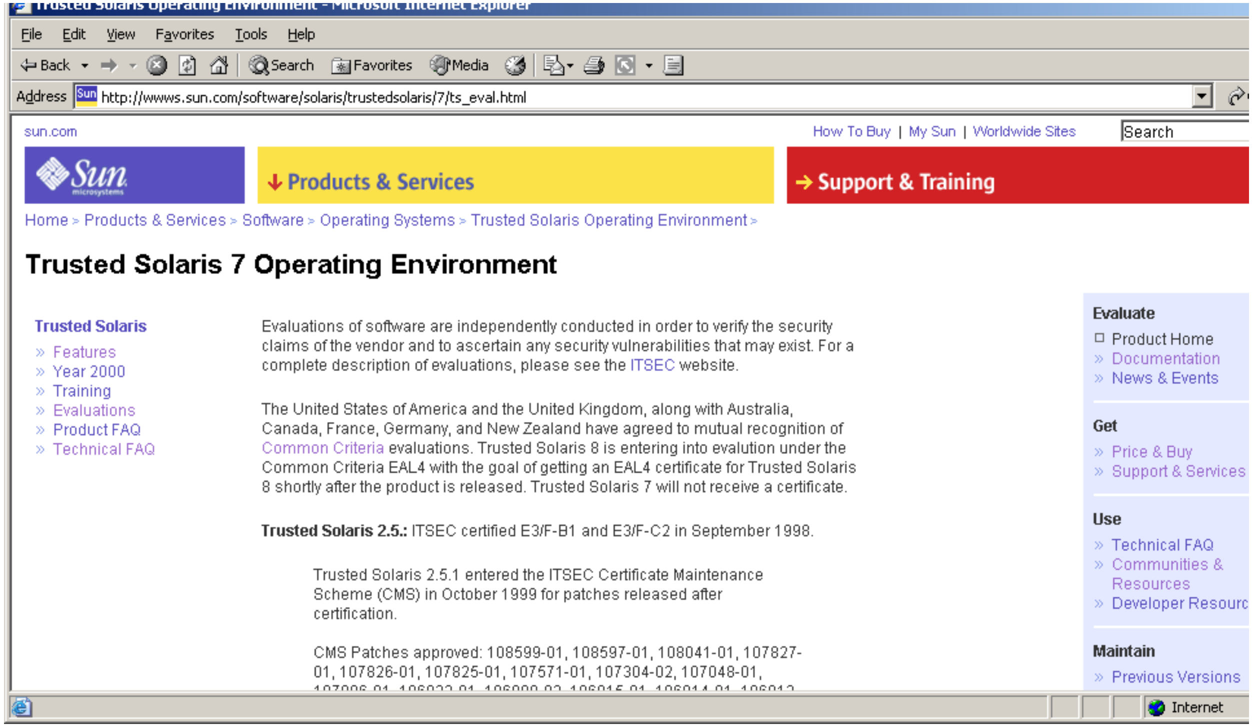
Common Criteria

The Common Criteria project harmonizes the various evaluation criteria, ITSEC, CTCPEC (Canadian criteria), and United States Federal Criteria (FC), to replace national and regional criteria with a worldwide set acceptable to the International Standards Organization (ISO).

Applies to Trusted Solaris Release

1.2, 2.5.1, 7, 8

I usually kill for money but since you are a friend a kill you for nothing!
2495$ vs 995


Trusted Solaris Operating Environment - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://wwws.sun.com/software/solaris/trustedsolaris/7/ts_eval.html
sun.com
How To Buy | My Sun | Worldwide Sites
Search
Sun microsystems
Products & Services
Support & Training
Internet

Home > Products & Services > Software > Operating Systems > Trusted Solaris Operating Environment >

Trusted Solaris 7 Operating Environment

Trusted Solaris

- Features
- Year 2000
- Training
- Evaluations
- Product FAQ
- Technical FAQ

Evaluations of software are independently conducted in order to verify the security claims of the vendor and to ascertain any security vulnerabilities that may exist. For a complete description of evaluations, please see the ITSEC website.

The United States of America and the United Kingdom, along with Australia, Canada, France, Germany, and New Zealand have agreed to mutual recognition of Common Criteria evaluations. Trusted Solaris 8 is entering into evalution under the Common Criteria EAL4 with the goal of getting an EAL4 certificate for Trusted Solaris 8 shortly after the product is released. Trusted Solaris 7 will not receive a certificate.

Trusted Solaris 2.5.: ITSEC certified E3/F-B1 and E3/F-C2 in September 1998.

> Trusted Solaris 2.5.1 entered the ITSEC Certificate Maintenance Scheme (CMS) in October 1999 for patches released after certification.
>
> CMS Patches approved: 108599-01, 108597-01, 108041-01, 107827-01, 107826-01, 107825-01, 107571-01, 107304-02, 107048-01, 107006-01, 106933-01, 106909-02, 106915-01, 106914-01, 106913

Evaluate

- □ Product Home
- Documentation
- News & Events

Get

- Price & Buy
- Support & Services

Use

- Technical FAQ
- Communities & Resources
- Developer Resourc

Maintain

- Previous Versions

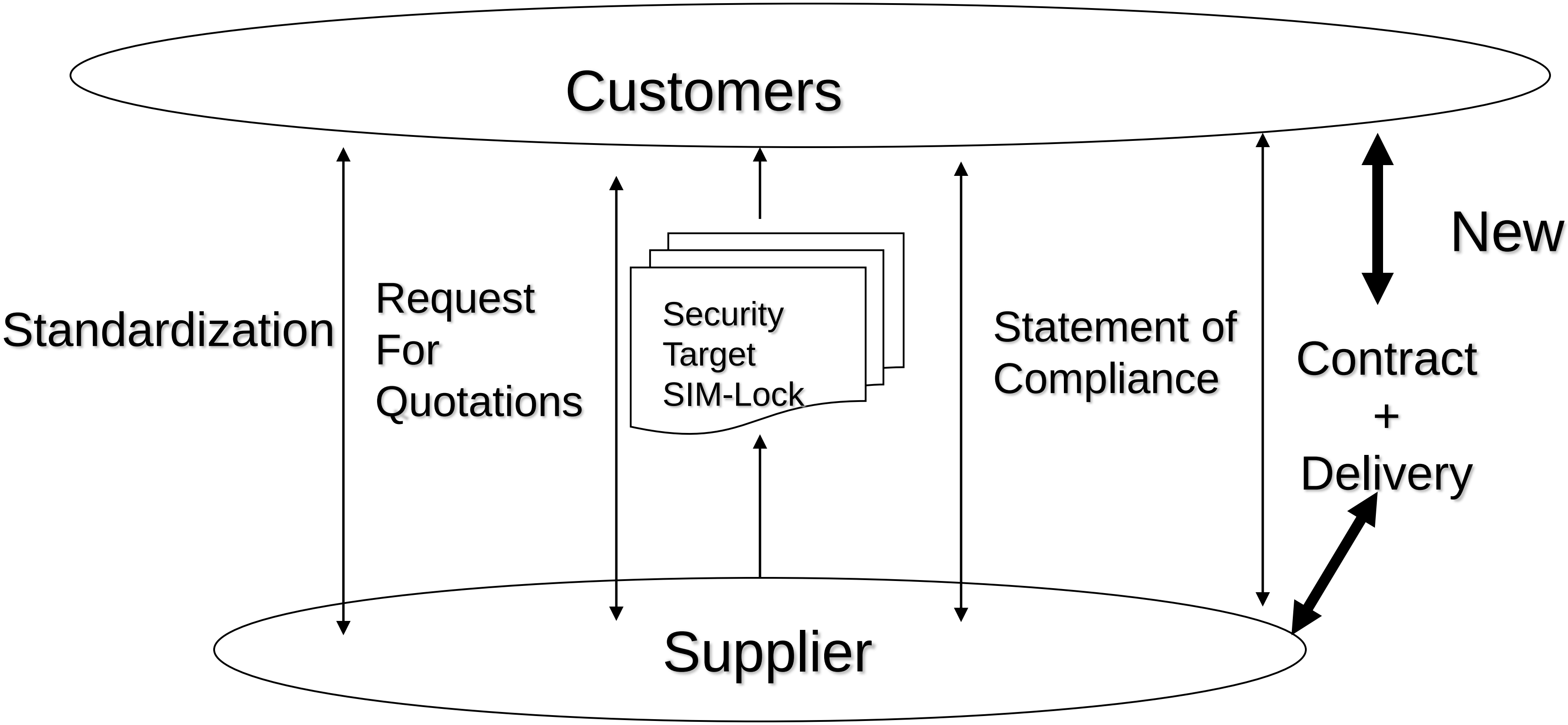
External Cost

- EAL2 100k-170k, 4-6 month
- EAL 3 130k-225k, 6-9 month
- EAL4 (medium complex) 175k-300k, 7-12 month
- EAL4 (complex, e g OS): 300K-750K 12-24 month
- + 10-20 Certification cost (1-3 mon)

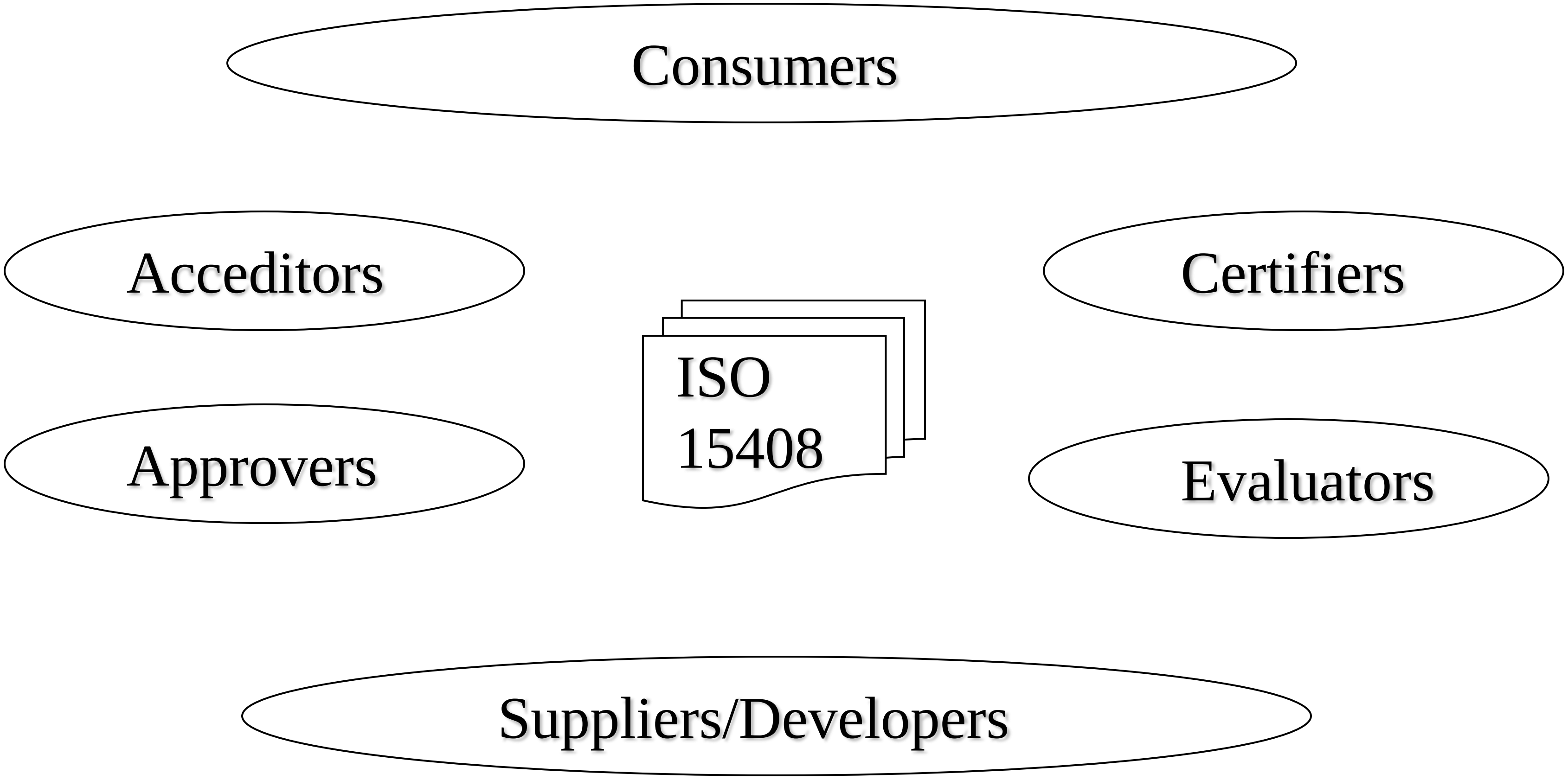
Dialog Process with Security Target

=

Renewed Contract



What is ISO 15408?



Consumers

Acceditors

Certifiers

ISO 15408

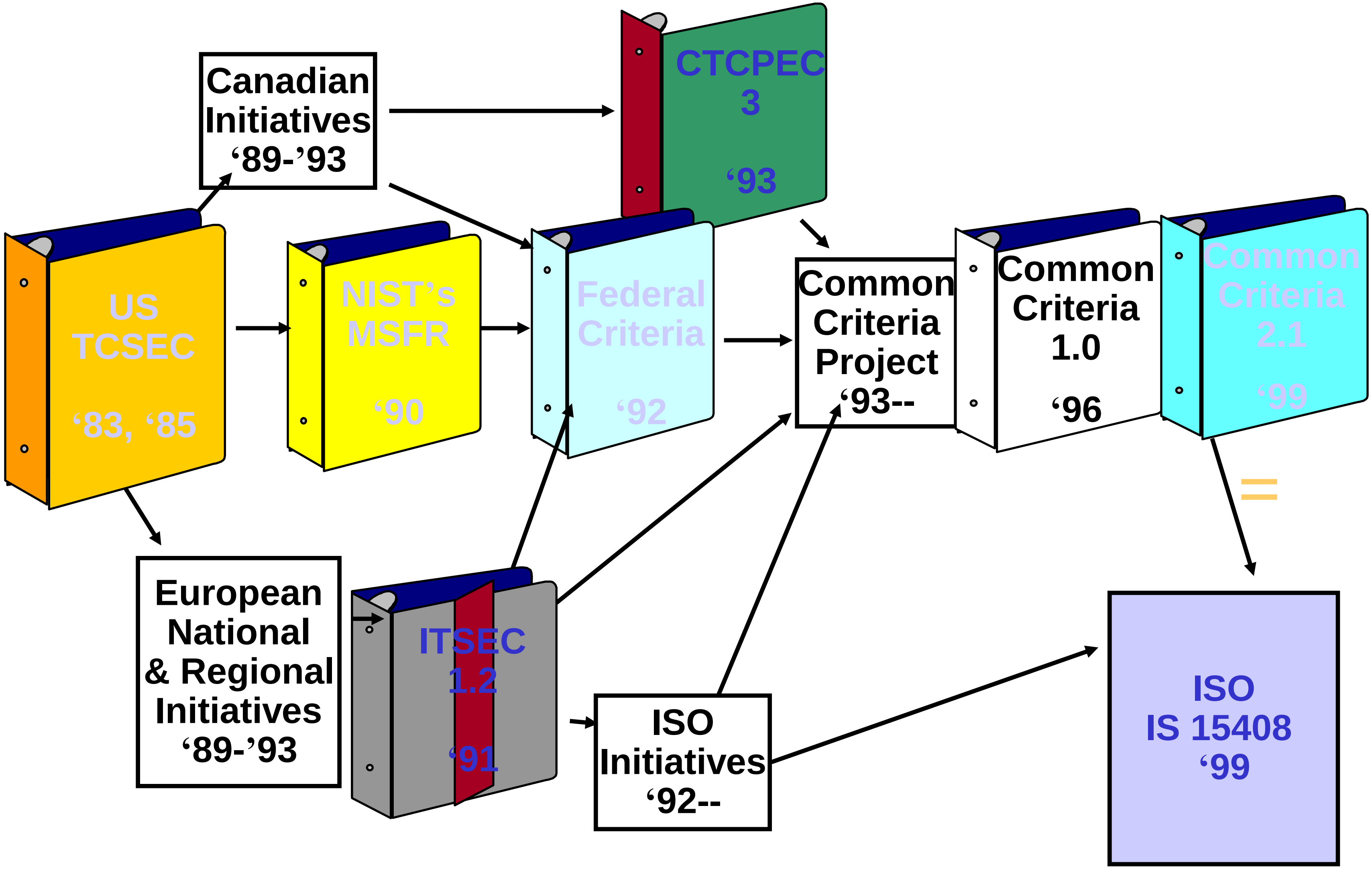
Approvers

Evaluators

Suppliers/Developers

Many Things to Many People!

History



Canadian Initiatives ‘89-’93

CTCPEC 3 ‘93

US TCSEC ‘83, ‘85

NIST’s MSFR ‘90

Federal Criteria ‘92

Common Criteria Project ‘93--

Common Criteria 1.0 ‘96

Common Criteria 2.1 ‘99

=

European National & Regional Initiatives ‘89-’93

ITSEC 1.2 ‘91

ISO Initiatives ‘92--

ISO IS 15408 ‘99

The Common Criteria (CC)

- The CC is a catalog of criteria and a framework for organizing a subset of the criteria into security specifications.

What is evaluation, certification and accreditation and what is it good for?

- Evaluation is the process when a product or system is assessed against specific security requirements.

- Certification is the formal approval of a product or a system, often based on an evaluation.

- Accreditation means approval for a specific purpose, e.g. a system for certain use and application. An accreditation may be based on a certification, but must be made by the organisation responsible for the application of the system.

What is the ISO 15408 to a Supplier?

- a dictionary/glossary
- a catalogue
- a marketing tool
- a process
    - etc

What is the ISO 15408 to a Supplier?

- a dictionary/glossary
- a catalogue
- a marketing tool
- a process
  - etc

Examples

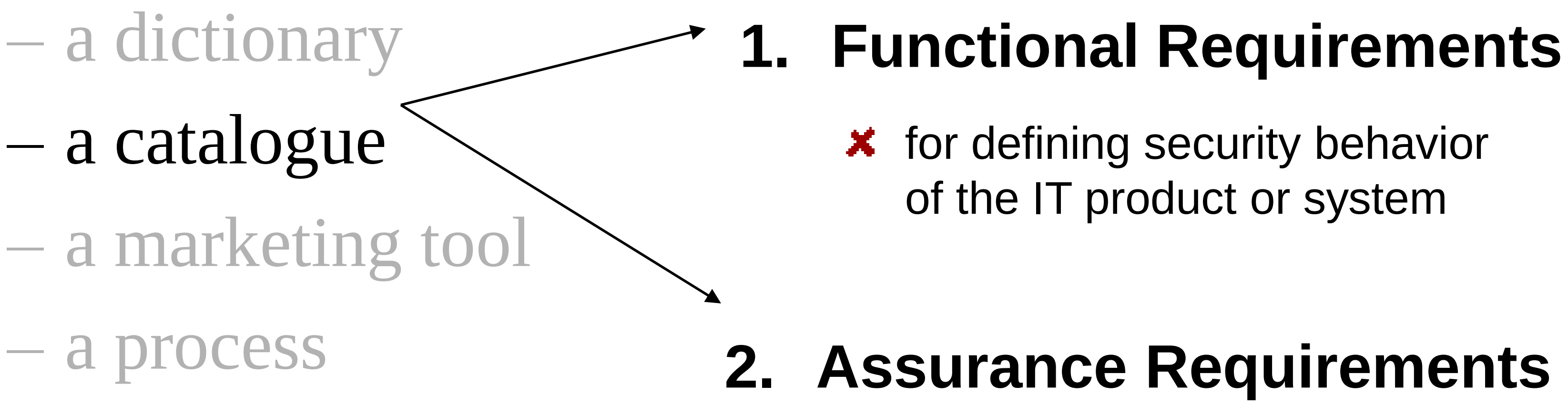
•TOE = Target of Evaluations

•TSF   = TOE Security Function

•SFP   = Security Function Policy

•etc

What is the ISO 15408 to Supplier



- – a dictionary
- – a catalogue
- – a marketing tool
- – a process

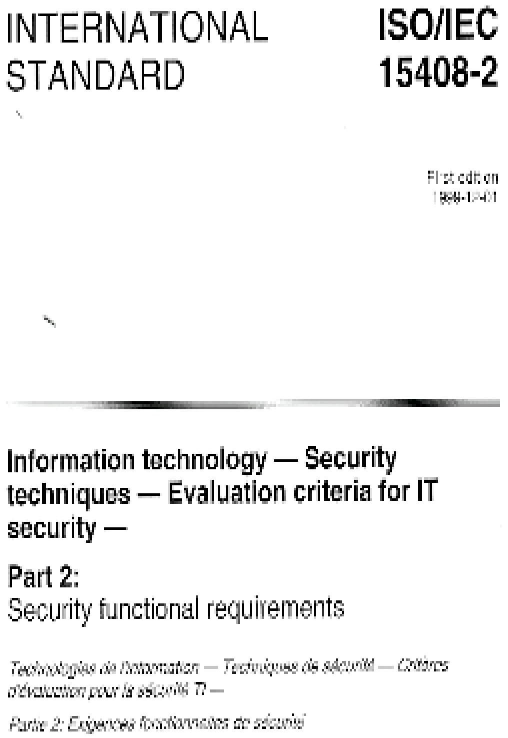
1. Functional Requirements

- for defining security behavior of the IT product or system

2. Assurance Requirements

- correctness of implementation
- effectiveness in satisfying objectives

Functional Requirments Catologue



INTERNATIONAL STANDARD

ISO/IEC 15408-2

First edition 1999-12-01

Information technology — Security techniques — Evaluation criteria for IT security —

Part 2:
Security functional requirements

Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI —

Partie 2: Exigences fonctionnelles de sécurité

Class	**Name**
FAU	**Audit**
FCO	**Communications**
FCS	**Cryptographic Support**
FDP	**User Data Protection**
FIA	**Identification & Authentication**
FMT	**Security Management**
FPR	**Privacy**
FPT	**Protection of TOE Security Functions**
FRU	**Resource Utilization**
FTA	**TOE Access**
FTP	**Trusted Path / Channels**

Use Data Protection (FDP) Information Flow Control Policy (IFC)

- **FDP_IFC.1.1 The TSF shall enforce the [*assignment: information flow control SFP*] on [*assignment: list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].**
- *** SFP Security Function Policy**
- *** TSF –TOE* Security Function**
- *** TOE-Target of Evaluation**

Re-Writing Requirment Specification (RS) Using 15408 Language

FDP_IFC.1.1 (CC)

- The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].

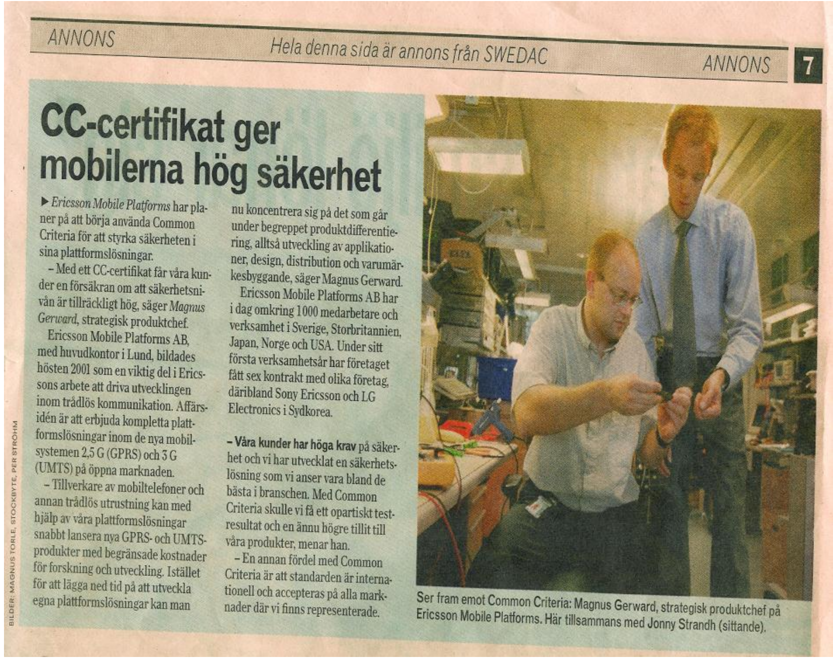
FDP_IFC.1.1 (RS)

The X shall enforce the *key import policy* on *the xxxx: the key is imported to the X module (which is part of the TOE) from the underlying hardware xxxxxxx (no additional import rules apply.)*

What is the ISO 15408 to A Supplier?

- – a dictionary
- – a catalogue
- – a marketing tool
- – a process

DI October 2002



ANNONS Hela denna sida är annons från SWEDAC ANNONS 7

CC-certifikat ger mobilerna hög säkerhet

▶ *Ericsson Mobile Platforms* har planer på att börja använda Common Criteria för att styrka säkerheten i sina plattformslösningar.

– Med ett CC-certifikat får våra kunder en försäkran om att säkerhetsnivån är tillräckligt hög, säger *Magnus Gerward*, strategisk produktchef.

Ericsson Mobile Platforms AB, med huvudkontor i Lund, bildades hösten 2001 som en viktig del i Ericssons arbete att driva utvecklingen inom trådlös kommunikation. Affärsidén är att erbjuda kompletta plattformslösningar inom de nya mobilsystemen 2,5 G (GPRS) och 3 G (UMTS) på öppna marknaden.

– Tillverkare av mobiltelefoner och annan trådlös utrustning kan med hjälp av våra plattformslösningar snabbt lansera nya GPRS- och UMTS-produkter med begränsade kostnader för forskning och utveckling. Istället för att lägga ned tid på att utveckla egna plattformslösningar kan man nu koncentrera sig på det som går under begreppet produktdifferentiering, alltså utveckling av applikationer, design, distribution och varumärkesbyggande, säger Magnus Gerward.

Ericsson Mobile Platforms AB har i dag omkring 1000 medarbetare och verksamhet i Sverige, Storbritannien, Japan, Norge och USA. Under sitt första verksamhetsår har företaget fått sex kontrakt med olika företag, däribland Sony Ericsson och LG Electronics i Sydkorea.

– Våra kunder har höga krav på säkerhet och vi har utvecklat en säkerhetslösning som vi anser vara bland de bästa i branschen. Med Common Criteria skulle vi få ett opartiskt testresultat och en ännu högre tillit till våra produkter, menar han.

– En annan fördel med Common Criteria är att standarden är internationell och accepteras på alla marknader där vi finns representerade.

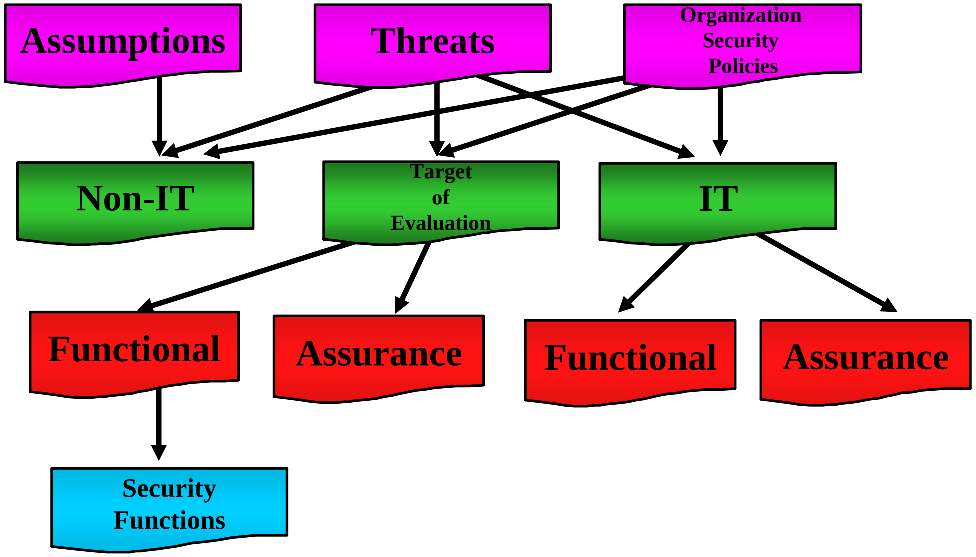
Ser fram emot Common Criteria: Magnus Gerward, strategisk produktchef på Ericsson Mobile Platforms. Här tillsammans med Jonny Strandh (sittande).

BILDER: MAGNUS TORLE, STOCKBYTE, PER STRÖHM

How Did We Use ISO 15408?

- – a dictionary
- – a catalogue
- – a marketing tool
- – a process map
  - to document security functionality
  - produce a security Target for the SIM-Lock function

ISO 15408 Process



Security Target

The structure of this document is as defined by [CC] Part 1 Annex C.

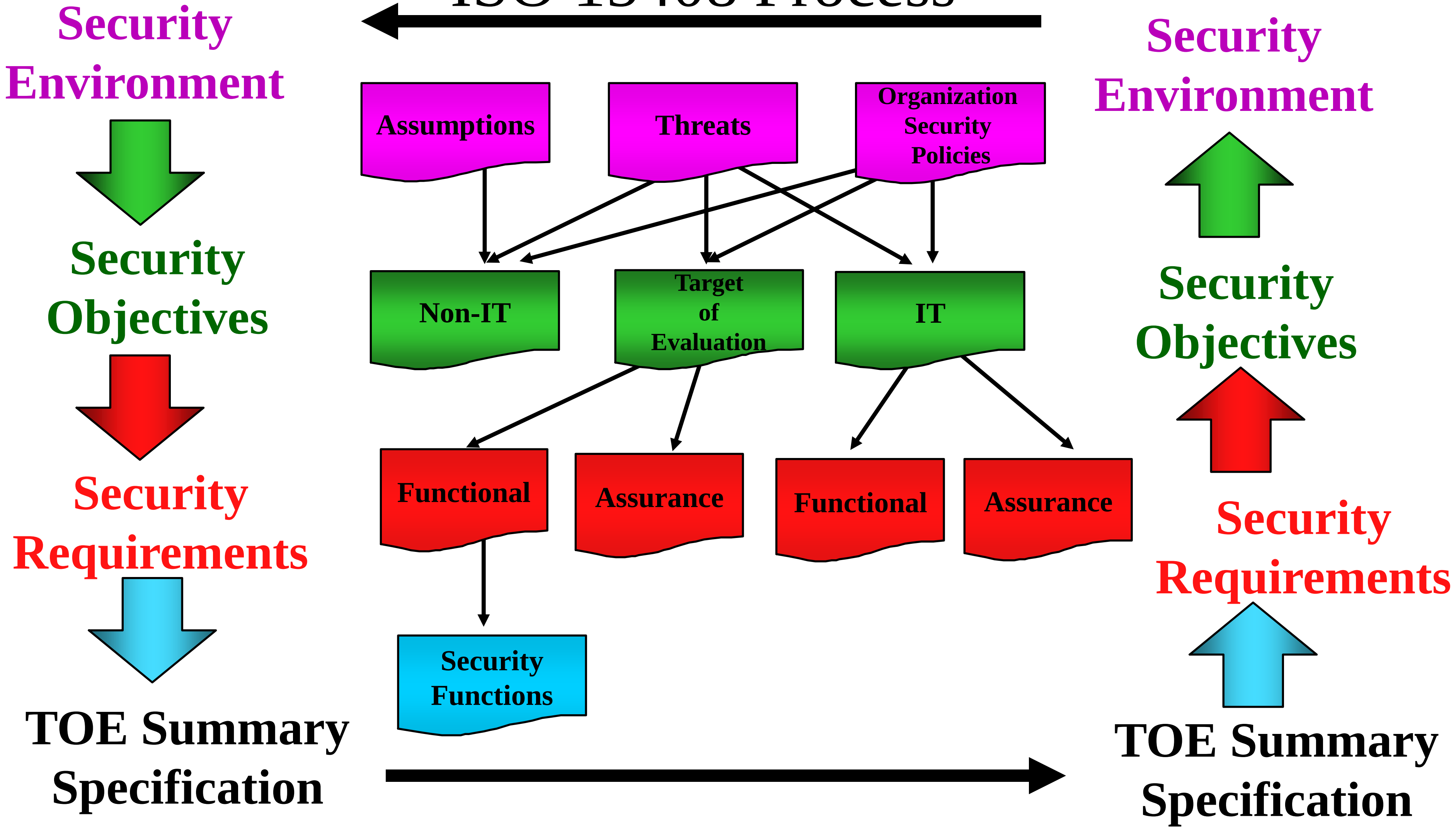
- Section 1 Introduction
- Section 2 is the TOE description.
- Section 3 provides the statement of TOE security environment.
- Section 4 provides the statement of security objectives.
- Section 5 provides the statement of IT security requirements.
- Section 6 provides the TOE summary specification, which includes the detailed specification of the IT Security Functions.
- Section 7 PP Claims (Optional)
- Section 8 provides the rationale for the security objectives, security requirements and TOE summary specification

TOE Description

Introduction to SIMLock

- The personalisation features work by storing information in the ME,(handset) which limits the SIMs with which it will operate, and by checking this information against the SIM whenever the ME is powered up or a SIM is inserted. If a check fails, the ME enters the “limited service state” in which only emergency calls can be attempted.

ISO 15408 Process



Security Environment

Security Objectives

Security Requirements

TOE Summary Specification

Assumptions

Threats

Organization Security Policies

Non-IT

Target of Evaluation

IT

Functional

Assurance

Functional

Assurance

Security Functions

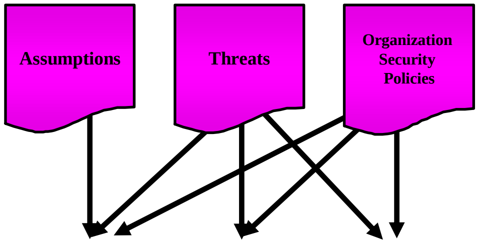
Security Environment

Security Objectives

Security Requirements

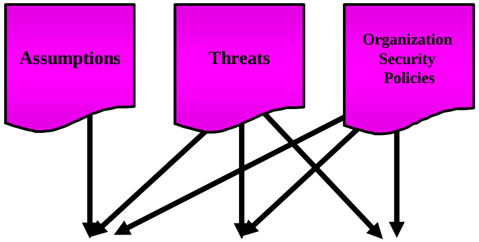
TOE Summary Specification

Assumption

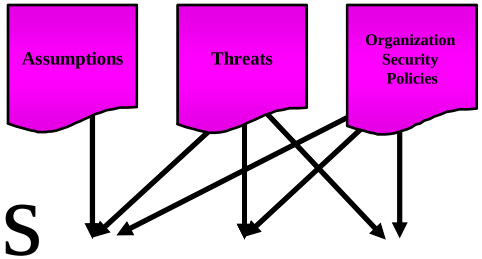


Type	Assumption	
Personnel	A.INTERNAL	Appropriate personnel and procedural measures (such as procedural two-person control) will be provided to ensure secure storage of SIM- Lock object and IMEI. Procedures shall exist to ensure that the database audit trail and/ or the audit trail for the underlying operating system and/or secure network services are regularly analysed and archived. In case of out sourcing, these requirements should be agreed upon and implemented within the third party.
Procedures and Routines	A.WHITELIST	White-, black or grey lists shall be handled in such a way that the information in these registers is not accessible to unauthorised personnel or outsiders. These registers must not be misused in any case.

Threat Table



Threat name and description	Security Objectives
T.ACCESS-KEYS: An unauthorised user may gain access to Control Keys in order to depersonalise the handset.	O.KNOWN O.ACCESS
T.MODIFY-KEYS AND IMEI: An accidental or deliberate unauthorised modification of IMEI and control keys. An unauthorised user might deliberately try to modify the control keys in order to de-personalise the handset.	O.INTEGRITY SSD



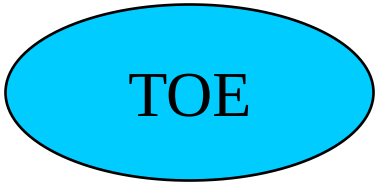
Security Policy examples

Organisational Security Policy
OSP.READ It should be impractical to read or recover any of the control keys from the ME.
OSP.ALTERATION It should be impractical to alter or delete the values of the personalisation indicators; the control keys, the stored IMSI or the stored network operator, SP and corporate codes, other than by the defined personalisation and de-personalisation process, without completely disabling the ME from working with any SIM/USIM.
OSP.DE-PERSONALISE For each de-personalisation procedure, there shall be a mechanism to prevent unauthorised attempts to de-personalise the ME. These may include blocking the ME if the number of failed attempt to de-personalise the ME exceeds a certain limit, or alternatively an increasing delay after each successive failed de-personalisation attempt. Other mechanisms may also be used.

Key Definitions- Security Target

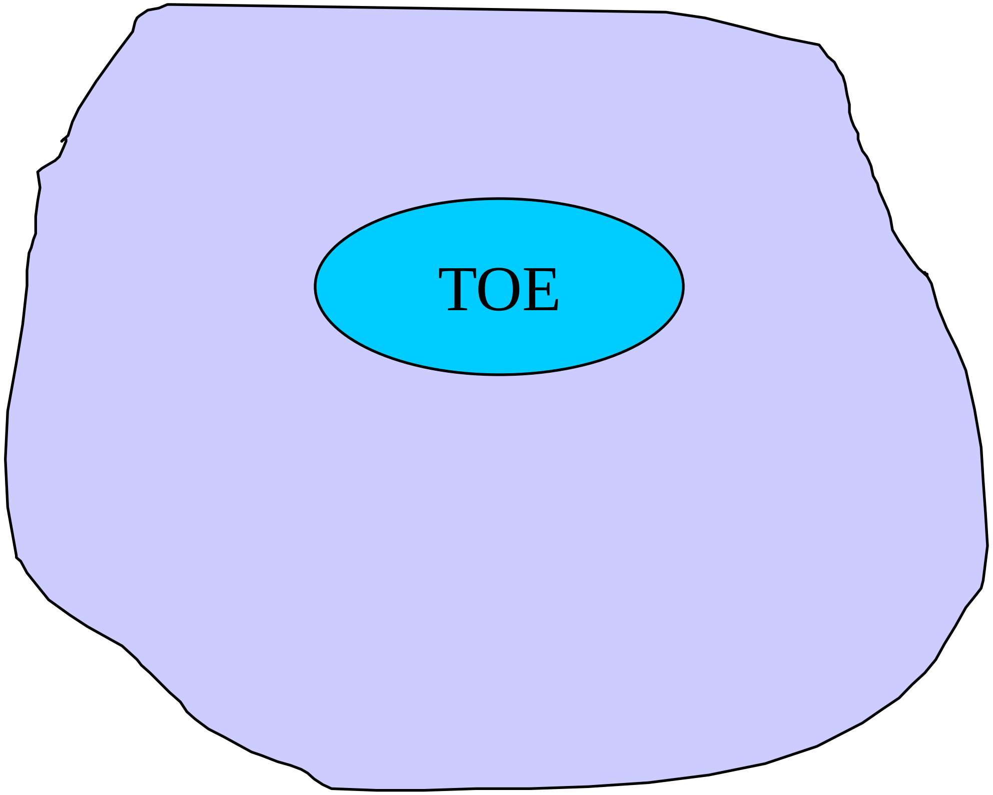
- Security Target (ST)
  - An implementation- dependent set of security requirements and specifications used as the basis for evaluation of the identified TOE
  - as- built specification
- Makes the statement: “This is what I have.”
- Vendors, developers write Security Targets

Key Definitions- TOE (Target of Evaluation)

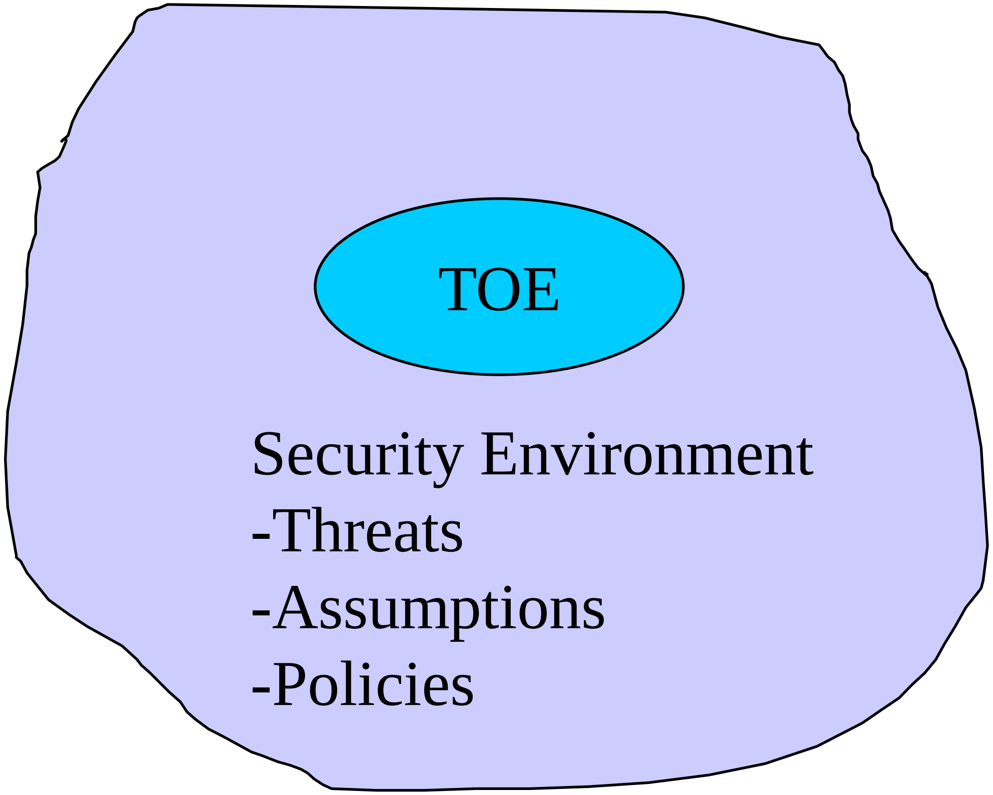


TOE

Key Definitions- TOE (Target of Evaluation)



Key Definitions- TOE (Target of Evaluation)



TOE

Security Environment

-Threats

-Assumptions

-Policies

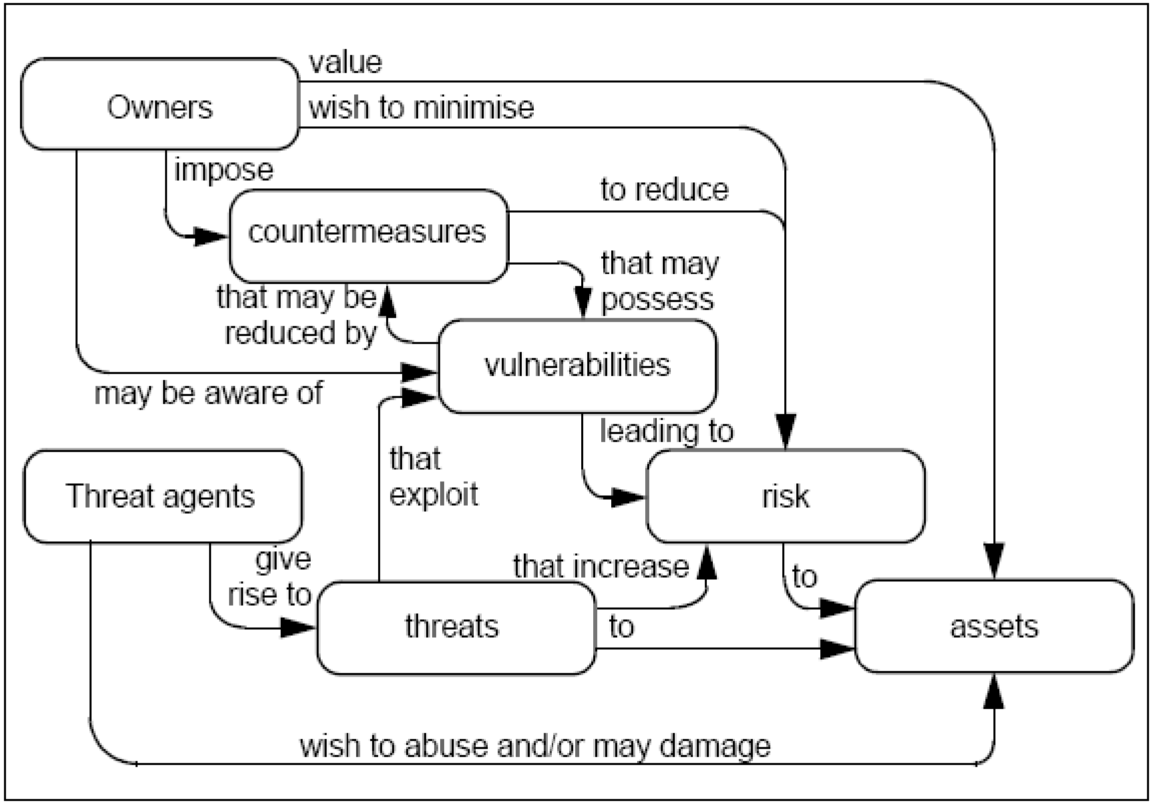
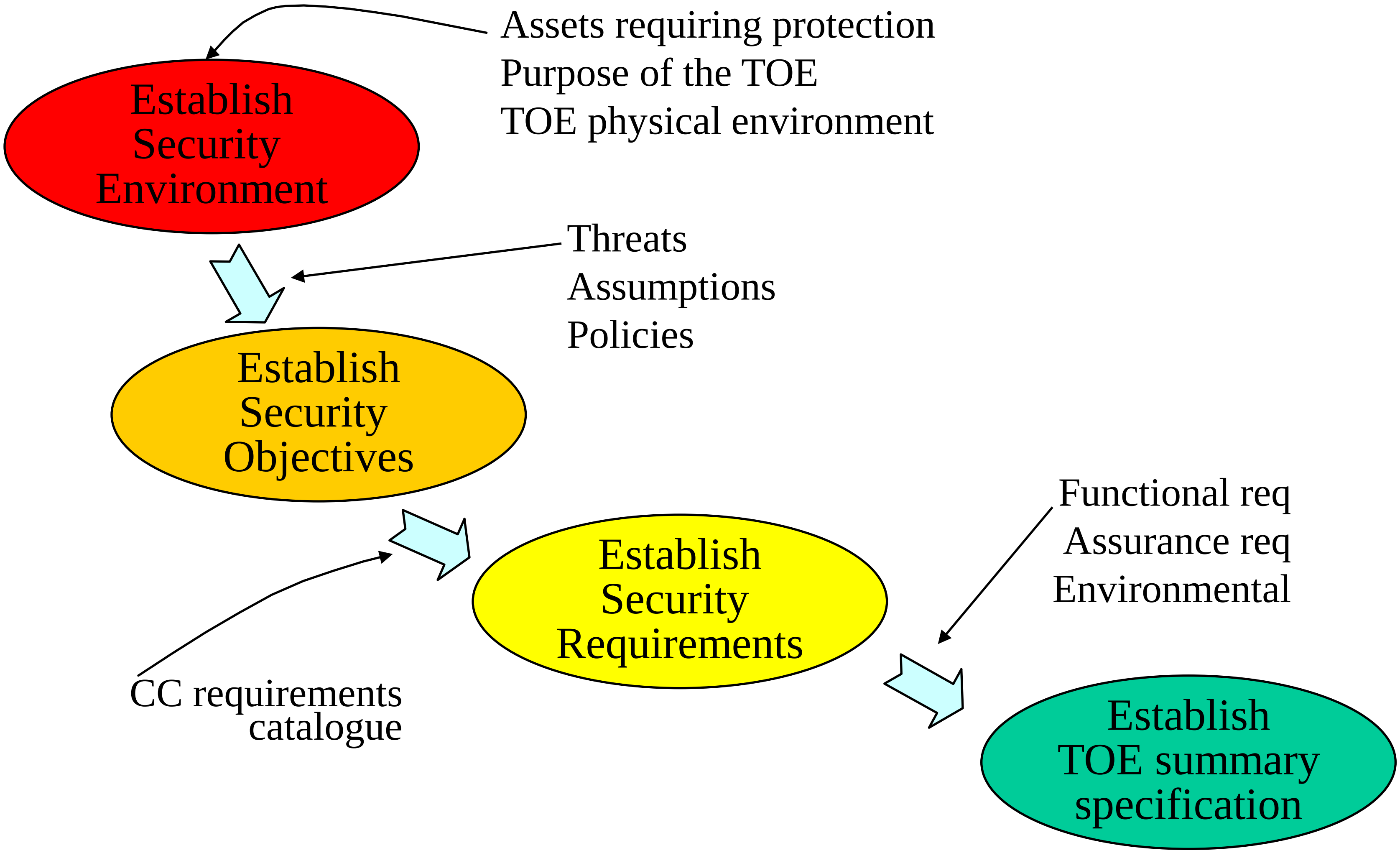


Figure 4.1 - Security concepts and relationships

How to develop a Security Target?



Establish Security Environment

Assets requiring protection
Purpose of the TOE
TOE physical environment

Establish Security Objectives

Threats
Assumptions
Policies

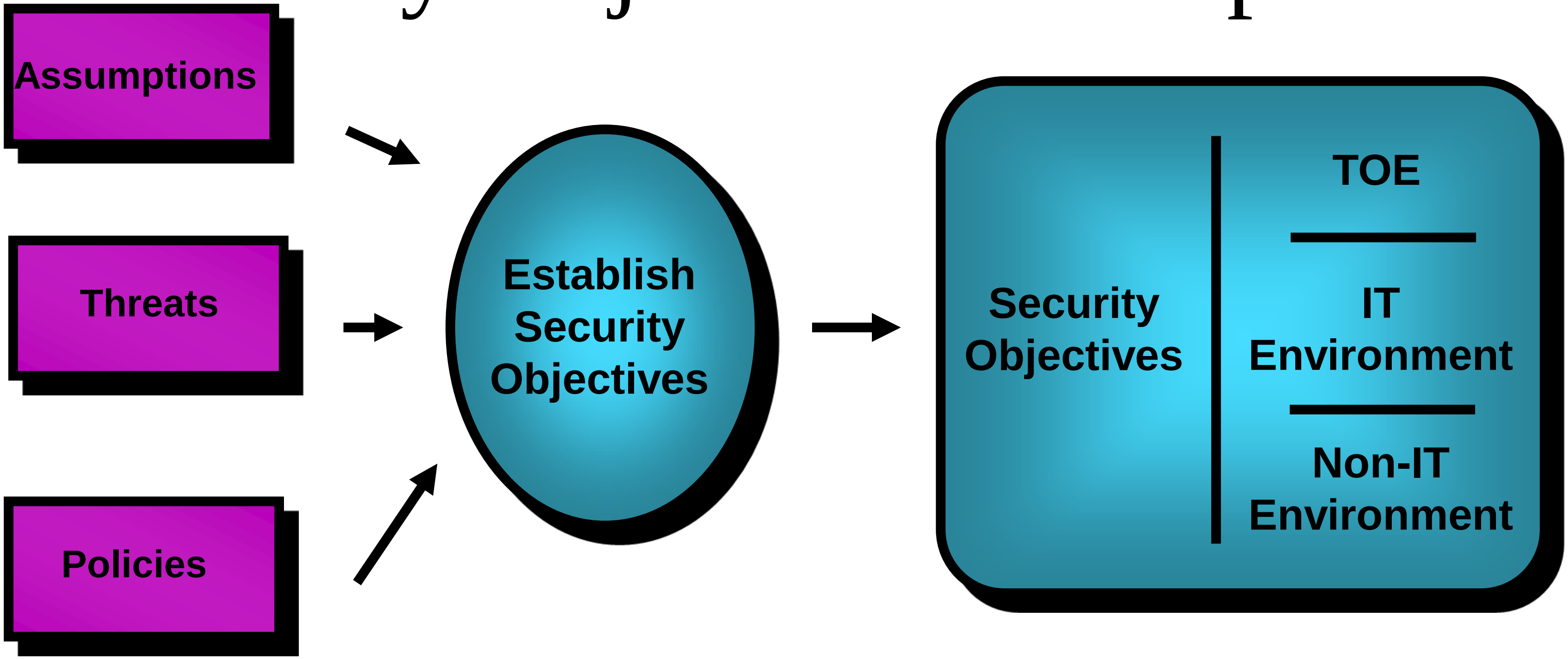
Establish Security Requirements

CC requirements catalogue

Establish TOE summary specification

Functional req
Assurance req
Environmental

Security Objective Development



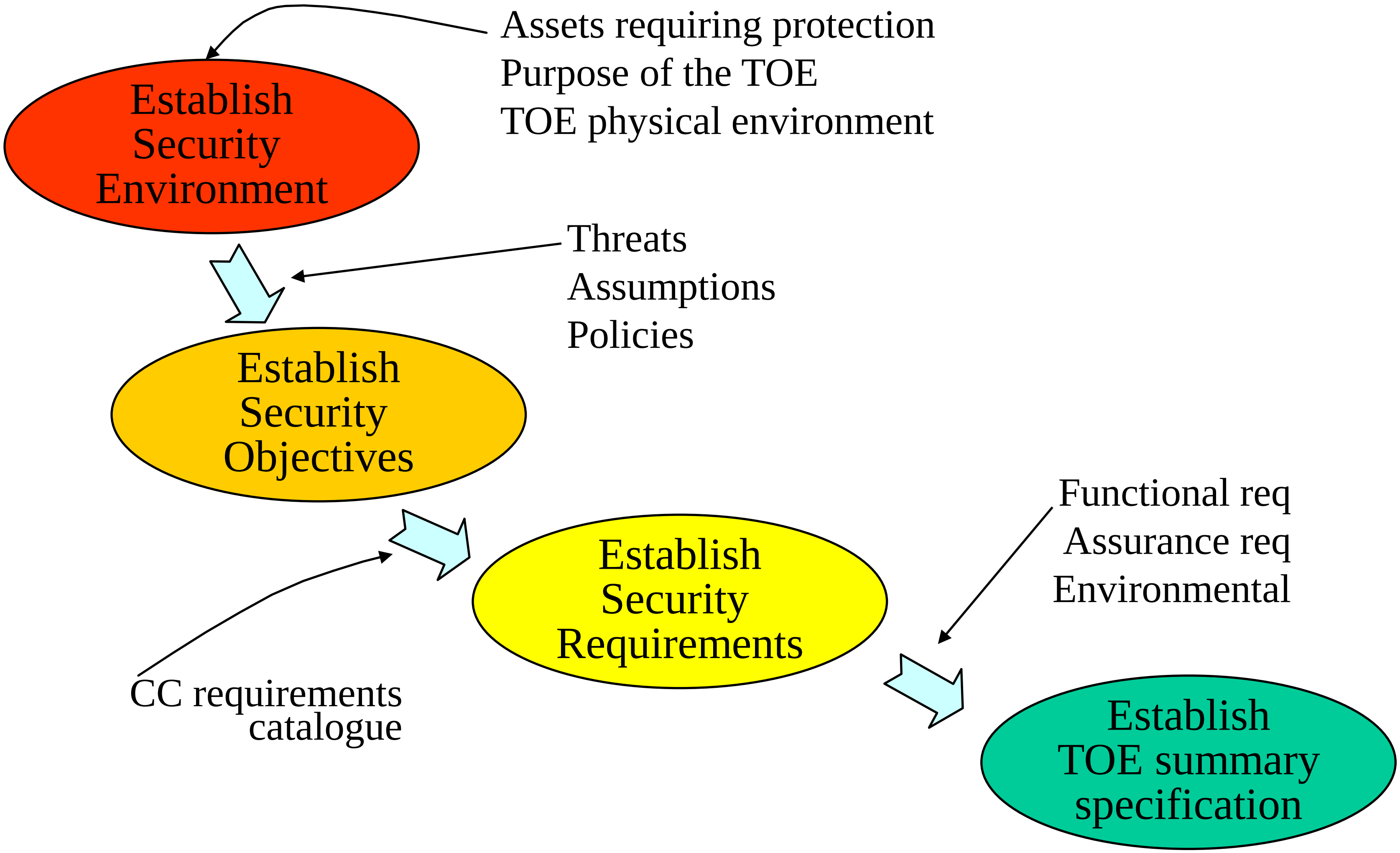
Security Objectives reflect the intent to counter identified threats and/or address any identified organizational security policies and/or assumptions.

Key Definitions- Security Objectives

- Security Objectives

  Security Objective= a statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions

How to develop a Security Target?



Establish Security Environment

Assets requiring protection
Purpose of the TOE
TOE physical environment

Establish Security Objectives

Threats
Assumptions
Policies

Establish Security Requirements

CC requirements catalogue

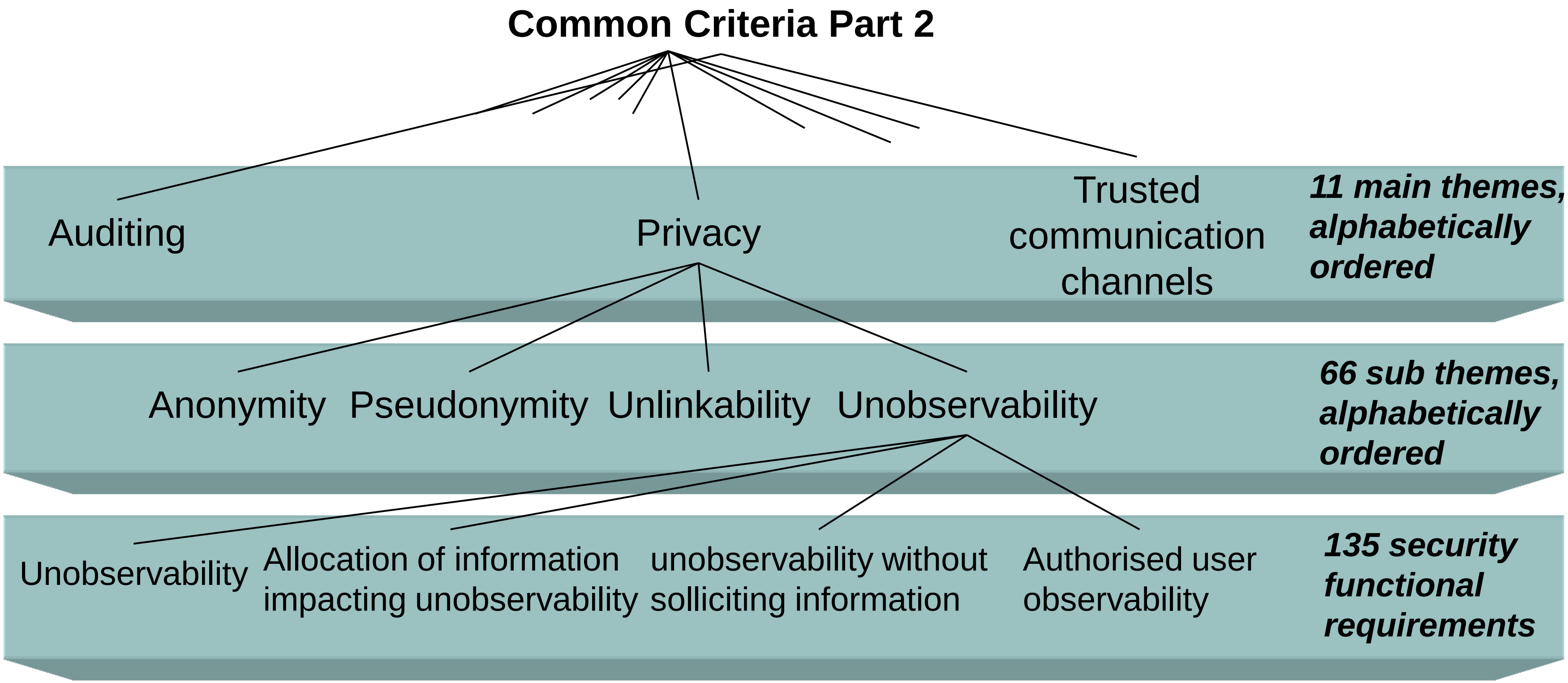
Establish TOE summary specification

Functional req
Assurance req
Environmental

Functional Requirements

- Audit (FAU)
- Communications (FCO)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Privacy (FPR)
- Protection of the Security Functions (FPT)
- Resource Utilisation (FRU)
- TOE Access (FTA)
- Trusted path/channels (FTP)

Security Functional Requirement



Common Criteria Part 2

Auditing

Privacy

Trusted communication channels

11 main themes, alphabetically ordered

Anonymity

Pseudonymity

Unlinkability

Unobservability

66 sub themes, alphabetically ordered

Unobservability

Allocation of information impacting unobservability

unobservability without solliciting information

Authorised user observability

135 security functional requirements

Key concept

Functional Requirements

- **for defining security behavior of the IT product or system**
- **implemented** requirements become security functions

(what the product does)

Assurance Requirements

- for establishing confidence in Security Functions
- correctness of implementation
- effectiveness in satisfying objectives

(is the product built well & does it meet the purpose)

Assurance requirements

- Configuration Management
- Delivery and Operation
- Development Documentation
- Guidance Documents
- Life- Cycle Support
- Testing (ATE)
- Vulnerability Assessment
- Maintenance of Assurance

Assurance- What is Assurance?

Common Criteria Definition:

Grounds for confidence that an IT product or system meets its security objectives.

Why Do We Care About Assurance?

Vulnerabilities can arise from….

- Requirements
  - – Insufficient or ineffective requirements
- Construction
  - – Incorrect design decisions
  - – Errors in implementation
- Operation
  - – Inadequate controls

How Do We Gain Assurance?

- Analysis of processes and procedures
- Checking that processes and procedures are being applied
- Analysis of the correspondence between TOE design representations
- Analysis of the TOE design representations against the requirements
- Verification of mathematical proofs
- Analysis of guidance documents
- Analysis of functional tests and results
- Independent functional testing
- Analysis for flaws
- Penetration testing

Security Assurance Classes

- Configuration Management
- Delivery and Operation
- *Development*
  - *Functional specification*
  - *High level design*
  - *Informal Correspondence*
- *Guidance Documentation*
- Life Cycle Support
- Maintenance of Assurance
- Tests
- *Vulnerability assessment*

Evaluation Assurance Levels (EAL)

CC	Description
EAL1	functionally tested
EAL2	structurally tested
EAL3	methodically tested and checked
EAL4	methodically design, tested & reviewed
EAL5	semiformally design and tested
EAL6	semiformally verified design and tested
EAL7	formally verified design and tested

7 predefined assurance packages, Evaluation Assurance Levels (EALs)

- **EAL1: Functionally Tested**. This where the applicable where threat to security is not serious, however some confidence in current operation is required. In the evaluation, there is assistance from TOE developer. The requirements are: Configuration Management, Delivery and Operation, Development, Guidance documents and Tests.
- **EAL2**: **Structurally Tested.** This assurance level is applicable where low to moderate level of independently assured security is required. Here, it requires some cooperation from the developer. It will definitely require no more than good vendor commercial practices. To add to the previous requirements are developer testing, vulnerability analysis, and more extensive independent testing.
- **EAL3**: **Methodically Tested and Checked**. It is applicable where moderate level of independently assured security is required. The cooperation from the developer is requires. It places additional requirements on testing, development environment controls and configuration management. The additional requirement is the Life Cycle support.
- **EAL4**: **Methodically Designed, Tested, and Reviewed**. This is applicable where moderate to high level of independently assured security is required. It is to ensure that there is some security engineering added to commercial development practices. This currently the highest level likely for retrofit of an existing product. There are additional requirements on design, implementation, vulnerability analysis, development and configuration management.
- **EAL5**: **Semiformally Designed and Tested**. It is applicable where high level of independently assured security is required. It requires rigorous commercial development practices and moderate use of specialist engineering techniques with additional requirements on specification, design, and their correspondence.
- **EAL6**: **Semiformally Verified Design and Tested**. This evaluation level is applicable where assets are valuable and risks are high and do requires a rigorous development environment. The additional requirements are on analysis, design, development, configuration management, and vulnerability/covert channel analysis.
- **EAL7**: **Formally Verified Design and Tested**. This is applicable where assets are highly valuable and risks are extremely high. However, practical use is functionally limited for amenability to formal analysis. The assurance is gained through application of formal methods. The additional requirements for these is testing and formal analysis.

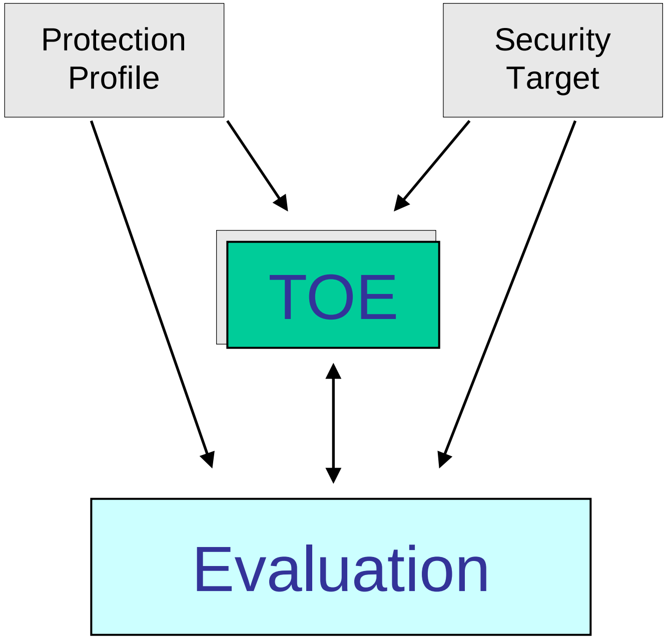
Assurance classes

Evaluation packages and EAL levels

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				**1**	1	**2**	2
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5
	ACM_SCP			**1**	**2**	**3**	3	3
Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**
	ADO_IGS	**1**	1	1	1	1	1	1
Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**
	ADV_IMP				**1**	**2**	**3**	3
	ADV_INT					**1**	**2**	**3**
	ADV_LLD				**1**	1	**2**	2
	ADV_RCR	**1**	1	1	1	**2**	2	**3**
	ADV_SPM				**1**	**3**	3	3
Guidance documents	AGD_ADM	**1**	1	1	1	1	1	1
	AGD_USR	**1**	1	1	1	1	1	1
Life cycle support	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD				**1**	**2**	2	**3**
	ALC_TAT				**1**	**2**	**3**	3
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**2**	2	**3**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_CCA					**1**	**2**	2
	AVA_MSU			**1**	**2**	2	**3**	3
	AVA_SOF		**1**	1	1	1	1	1
	AVA_VLA		**1**	1	**2**	**3**	**4**	**4**

Evaluation

The product (TOE) has to meet the requirements in the PP and ST.



The product (TOE), PP and ST are evaluated.

To Consider when Selecting an EAL (Evaluation Level EAL 1-7)

- Value of the “assets”
- Risk of the “assets” being compromised
- Current state of practice
- Development and maintenance cost
- Functional requirement dependencies
- Security Objectives

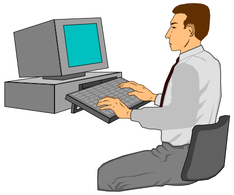
External Cost

- EAL2 100k-170k, 4-6 month
- EAL 3 130k-225k, 6-9 month
- EAL4 (medium complex) 175k-300k, 7-12 month
- EAL4 (complex, e g OS): 300K-750K 12-24 month
- + 10-20 Certification cost (1-3 mon)

The Common Criteria

- These security specifications serve

Consumers - as a guide for the **procurement** of products with IT security features

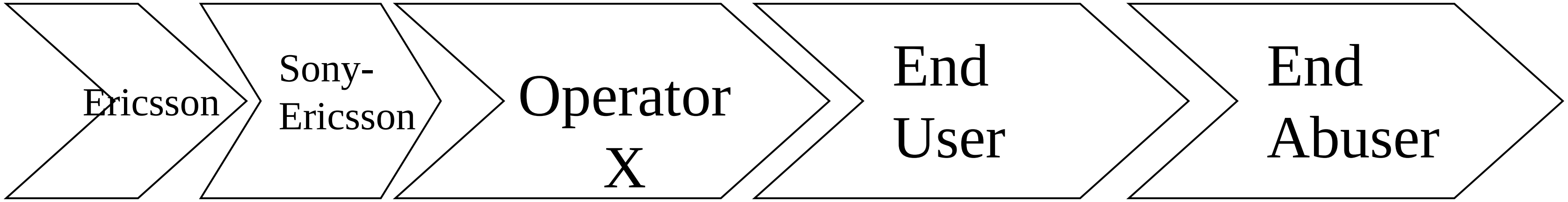


Product Developers and Integrators - as a basis for the **development** of products with IT security features

Evaluators - as the basis for the **evaluation** of IT security products

Auditors, Certifiers, Accreditors - to support their specific needs

Value Based Risk Analysis of a Stolen Handset



Ericsson

Sony-Ericsson

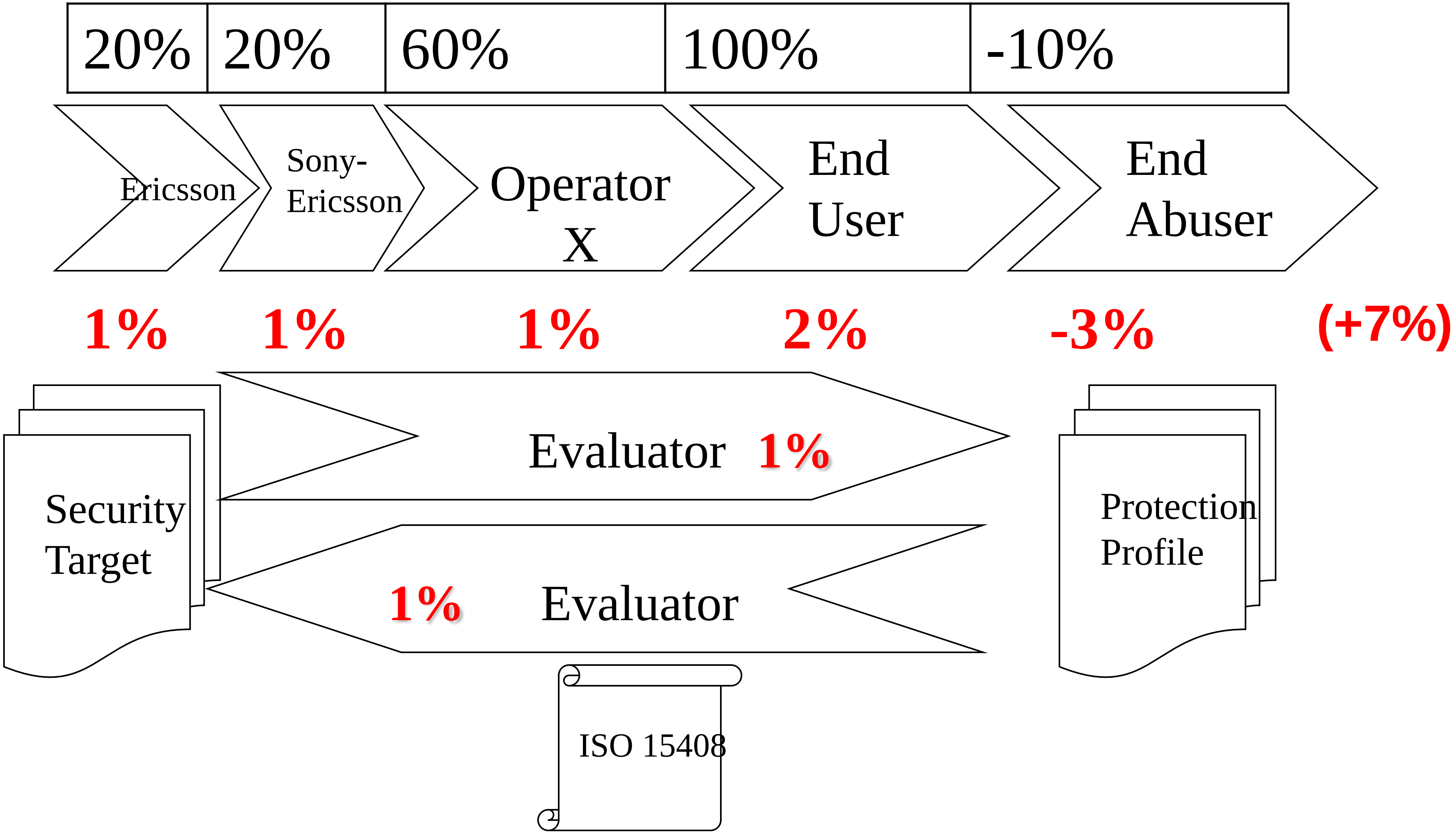
Operator X

End User

End Abuser

1.00	1.30	1.60	3.20	1.60
1.50	1.80	2.60	4.60	1.70
1.80	2.50	3.80	7.60	4.60

Valued Based Risk Analysis with ISO 15408 in the Chain



20%	20%	60%	100%	-10%

Ericsson

Sony-Ericsson

Operator X

End User

End Abuser

1% 1% 1% 2% -3% (+7%)

Security Target

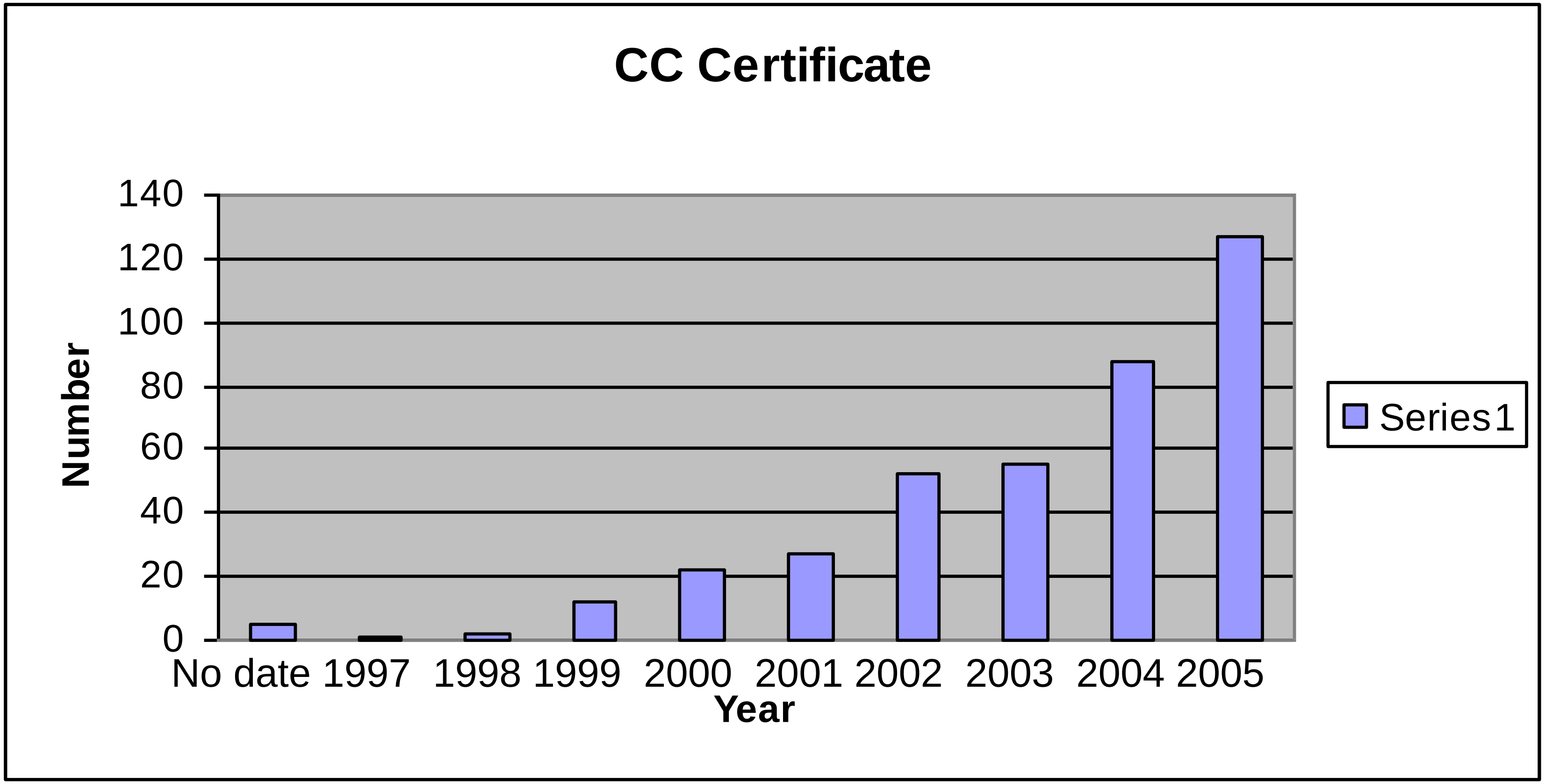
Evaluator 1%

1% Evaluator

Protection Profile

ISO 15408

Certified products



Certified PPs

- 47 in total

name				
Protection Profile – Secure Signature-Creation Device Type 1				
version	issue date	assurance level	certification report	protection profile
1.05	April 2002	EAL4+	pp0004a.pdf	pp0004b.pdf
name				
Protection Profile – Secure Signature-Creation Device Type 2				
version	issue date	assurance level	certification report	protection profile
1.04	April 2002	EAL4+	pp0005a.pdf	pp0005b.pdf

Certified products

Types:

EAL 1: Firewalls, VPN, crypto, card reader
EAL 2: Firewalls, Network, PKI, Smart Card, Multifunction (printers/copiers)

EAL 3: PKI, Firewalls, databases, Smart Card, Operative systems, crypto, Multifunction (printers/copiers)

EAL 4: Firewalls, crypto, Network, databases, Smart Card, Operative systems, PKI

EAL 5: Smart Cards

Example evaluated products

- Sun Solaris 8 Operating environment, EAL4
- Windows 2000 Professional, EAL4+
- Symantec Enterprise Firewall v7.0, EAL4
- Oracle 9i Release 9.2.0.1.0 (EAL4 in eval.)
- Nokia IPSO Version 3.5, (EAL4 in eval.)
- Sharp Multifunction (printer/copier)

How to look at a certified product:

name		
AR-FR11 VERSION M.20		
manufacturer	assurance level	certification date
Sharp Corporation	**EAL3**	**3 June 2005**
certification report	security target	
certification_report_c0026_000.pdf	security_target_c0026.pdf	

What to look for in Certificates and Certification/Validation Reports

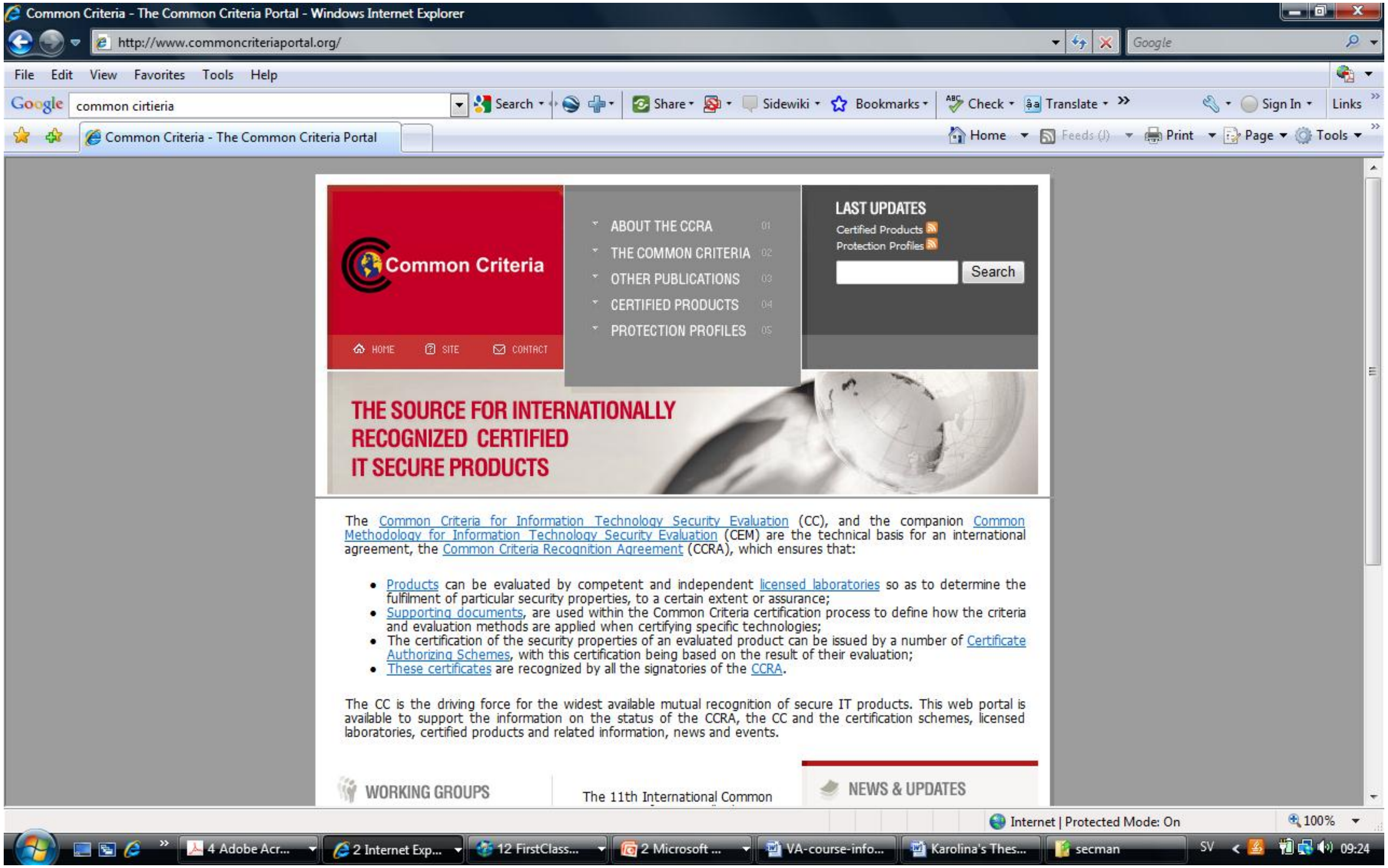
- A certificate should provide the following information:
- • Scheme identification
- • Product name and version
- • Hardware/software platform
- • Assurance package (EAL)
- • PP claims
- • Date certified/validated
- The Certification/Validation Report is the source of detailed security information about the product for any interested parties. It is intended to provide practical information to consumers. The contents of the report are specified in the Mutual Recognition Arrangement, as follows:
- • Executive summary
- • Identification of the product
- • Product security policy
- • Assumptions and scope of the evaluation
- • Architectural information
- • List of product documentation
- • Outline of testing approach and results
- • Description of the evaluated configuration
- • Results of the evaluation
- • Evaluator comments and recommendations
- • Security Target

How can/should we/you use the common criteria to make product more secure

- Document work better
- Work together with customers
- Drive the suppliers to delievry better products
- Raise the barrier for new entery
- Requirement reuse, steal with pride
- etc

The Portal

http://www.commoncriteriaportal.org/theccra.html



The Common Criteria for Information Technology Security Evaluation (CC), and the companion Common Methodology for Information Technology Security Evaluation (CEM) are the technical basis for an international agreement, the Common Criteria Recognition Agreement (CCRA), which ensures that:

- Products can be evaluated by competent and independent licensed laboratories so as to determine the fulfilment of particular security properties, to a certain extent or assurance;
- Supporting documents, are used within the Common Criteria certification process to define how the criteria and evaluation methods are applied when certifying specific technologies;
- The certification of the security properties of an evaluated product can be issued by a number of Certificate Authorizing Schemes, with this certification being based on the result of their evaluation;
- These certificates are recognized by all the signatories of the CCRA.

The CC is the driving force for the widest available mutual recognition of secure IT products. This web portal is available to support the information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events.

Best Practise

- Oracle
  - http://www.oracle.com/technology/deploy/security/seceval/index.html

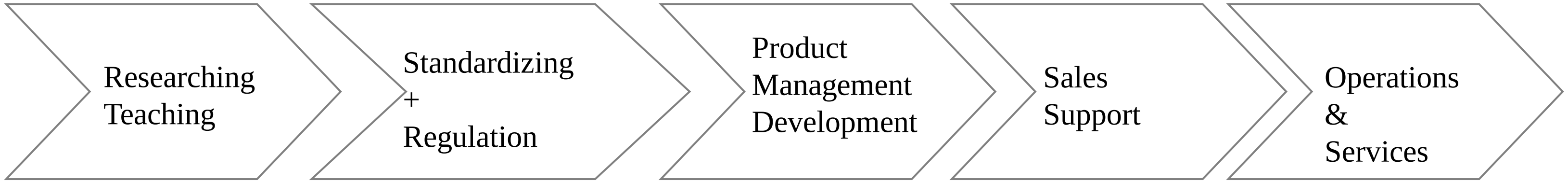
Outline

- Background War Stories
  - Why I am Jaded!
- A Naïve inductivist
  - Why I use a socio-technical systems approach to deal with information security, past and present
- Practise and Standard choose for certification
  - “All is not quite on the Western/Eastern Front!”
  - Past and Present experience with using common criteria

Goal of this Lecture

- Give you some background and history of security assurance problems and story from an industrial supplier and socio-technical systems security research perspective.
- Give you some back ground to the Common Criteria as a “security researcher”
- Encourage more “naïve“ inductivist” and empirical research in information security systems security
- Improve the strength of our common socio-technical security value chain.

How do you want to strength our common security value chain?



Researching
Teaching

Standardizing
+
Regulation

Product
Management
Development

Sales
Support

Operations
&
Services