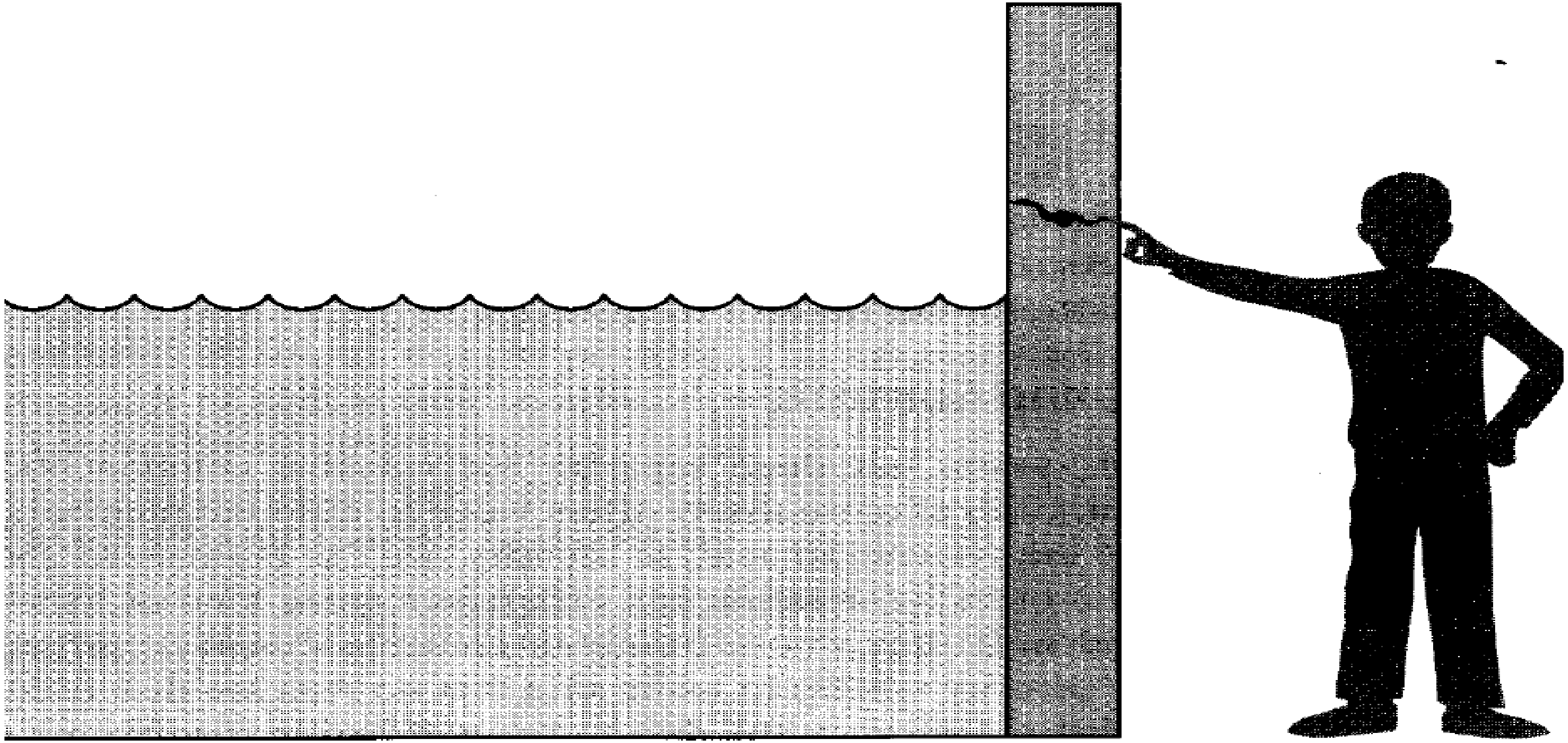
Threats

- Snooping
- Modification
- Spoofing
- Repudiation of origin
- Denial of receipt
- Delay
- Denial of service

Threats, Vulnerabilities, Controls



Pfleeger&Pfleeger, *Computing in Security*, 3rd Edition, Prentice Hall,2003

The Perpetrators

- Passers-by
- Script kiddies
- Systems administrators
- Career criminals
- Organised criminals
- Governmental organisations
- Insiders (“The Disgruntled Programmer”?)

Policy and Mechanism

Definition 1-1. A *security policy* is a statement of what is, and what is not, allowed.

Definition 1-2. A *security mechanism* is a method, tool, or procedure for enforcing a security policy.

Bishop, M. *Computer Security: Art and Science*, Addison-Wesley, 2004. p9.

Access Control Matrix Model

	file 1	*file 2*	*process 1*	*process 2*
process 1	read,write, own	read	read,write, execute,own	write
process 2	append	read, own	read	read, write, execute, own

The Generality of the AC Matrix

host names	*telegraph*	*nob*	*toadflax*
telegraph	own	ftp	ftp
nob		ftp, nfs, mail, own	ftp, nfs, mail
toadflax		ftp, mail	ftp, ftp, mail, own

	counter	*inc_ctr*	*dec_ctr*	*manager*
inc_ctr	+			
dec_ctr	-			
manager		call	call	call

Example of Bell-LaPadula

The Bell-LaPadula model can make formal statements about the security of systems that have ordering of security clearance levels, e.g.:

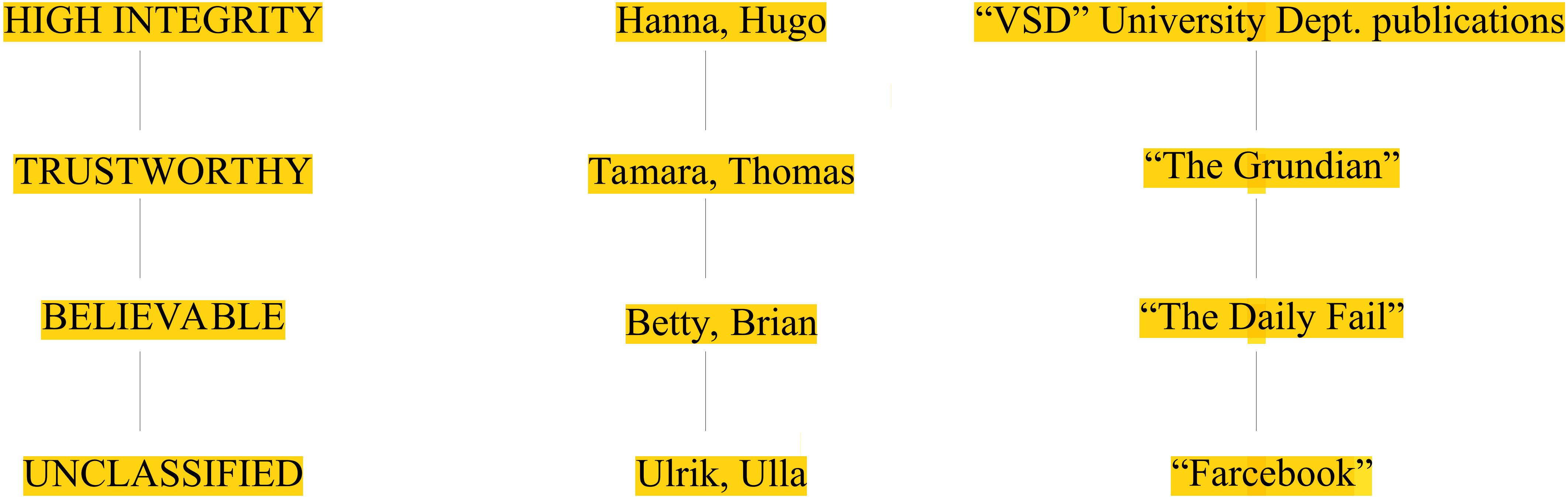
TOP SECRET (TS)	Tamara, Thomas	Personnel Files
SECRET (S)	Sally, Samuel	Electronic Mail Files
CONFIDENTIAL (C)	Claire, Clarence	Activity Log Files
UNCLASSIFIED (UC)	Ulaley, Ursula	Telephone List Files

Bell-LaPadula

- ***Simple Security Condition:*** *S* can read *O* if and only if $l_o \leq l_s$ and *S* has discretionary read access to *O*.
- ****-Property (Star Property), Preliminary Version:*** *S* can write *O* if and only if $l_s \leq l_o$ and *S* has discretionary write access to *O*.

Example of Biba

Biba works in a very similar way to Bell La Padula, but we should be careful about the differences



HIGH INTEGRITY	Hanna, Hugo	“VSD” University Dept. publications
TRUSTWORTHY	Tamara, Thomas	“The Grundian”
BELIEVABLE	Betty, Brian	“The Daily Fail”
UNCLASSIFIED	Ulrik, Ulla	“Farcebook”

N.B. The integrity classes here are examples and should it be understood that they are **not specified in Biba** (just as Top Secret, Confidential etc are not specified in Bell La Padula)

The Clark-Wilson Model

- Divides integrity requirements into
  - Internal consistency i.e. what the computer system can enforce
  - External consistency i.e. defines the relation between the internal state of the system to the real world
- With enforcement methods such as
  - Well-formed transactions
  - Separation of duties