

brightsight®

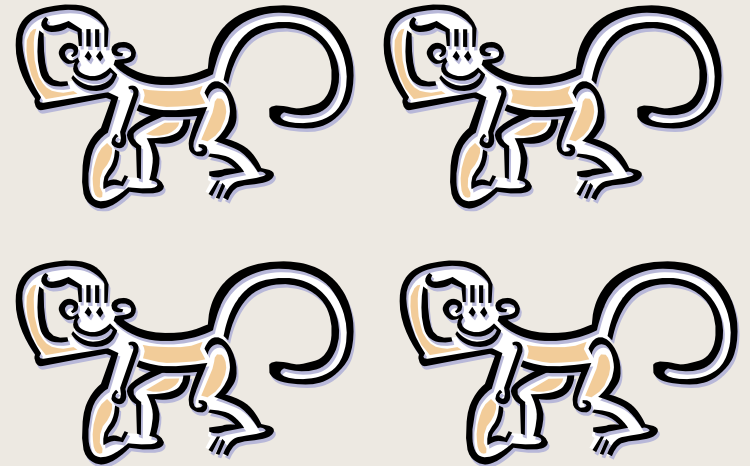
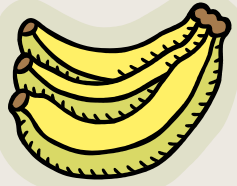


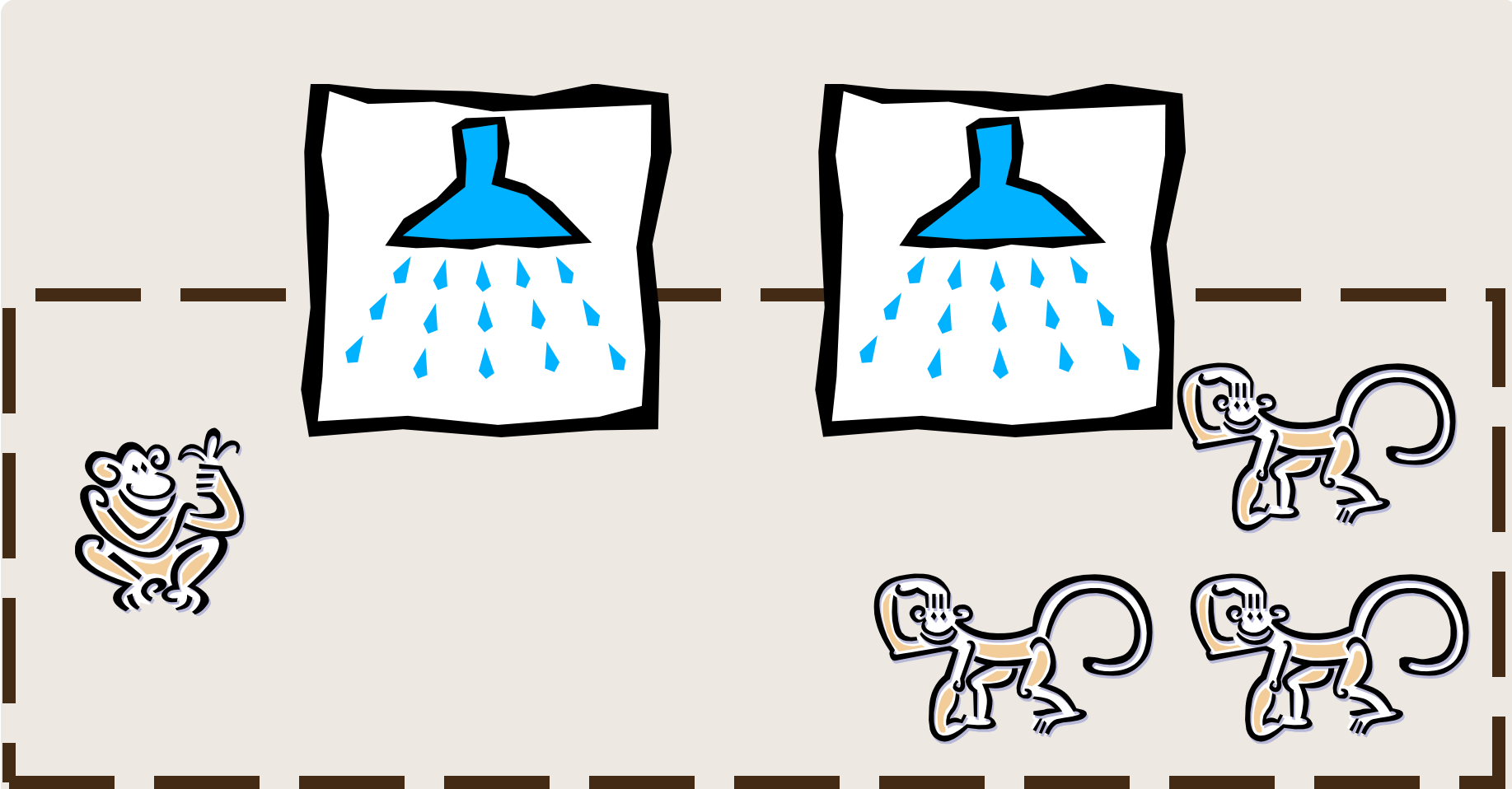
your
partner
in security
approval

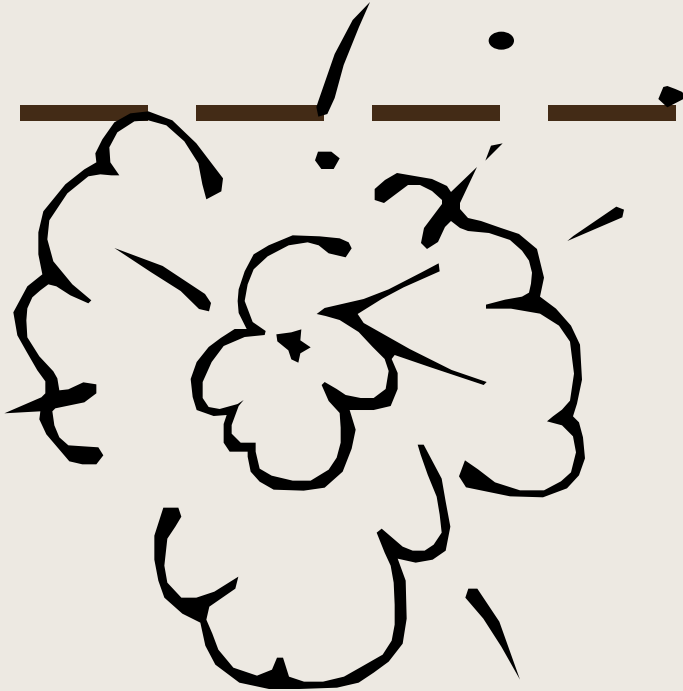
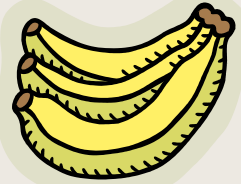


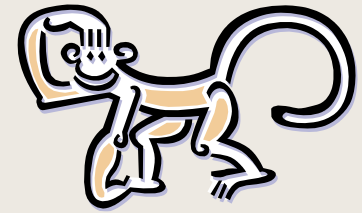
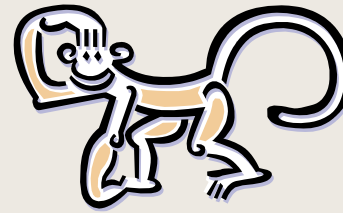
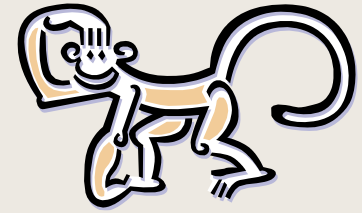
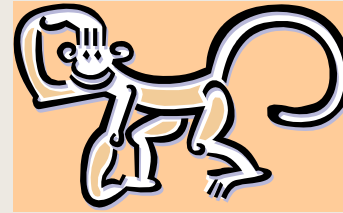
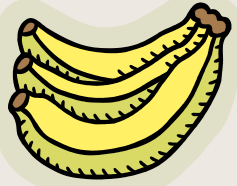
**A practical approach
to CC Part 2**

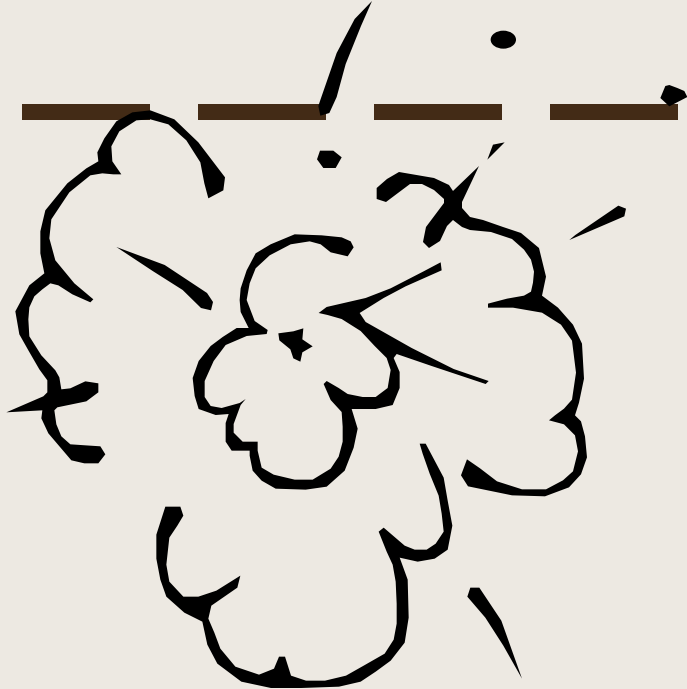
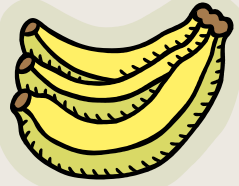
Dirk-Jan Out

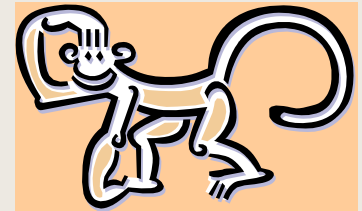
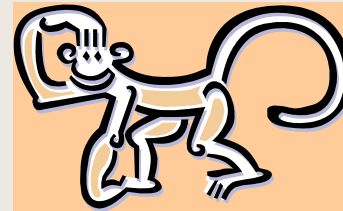
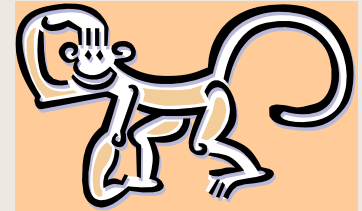
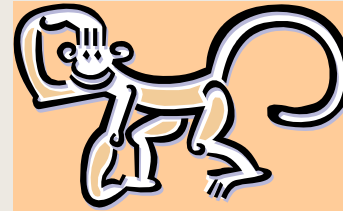
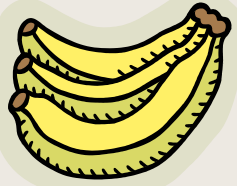




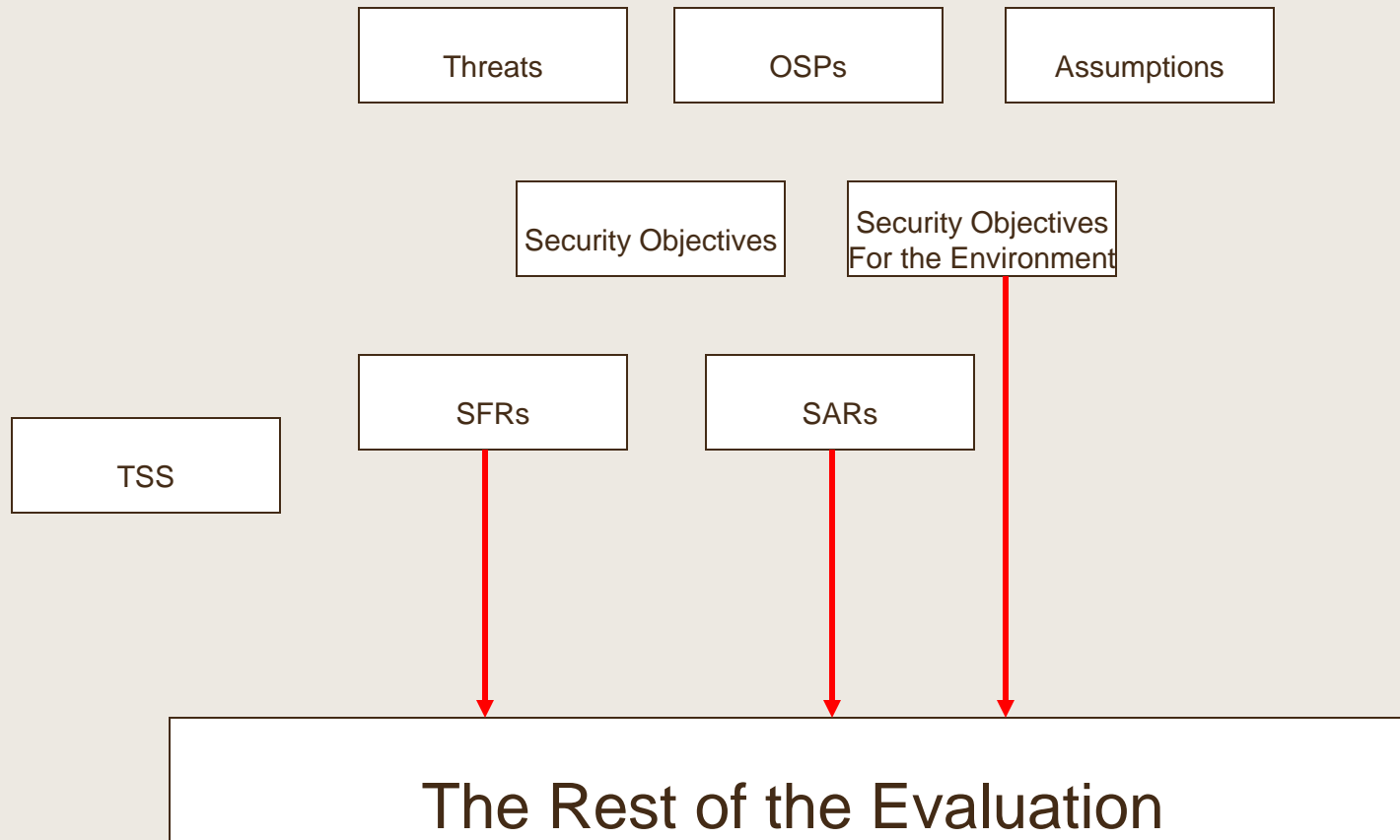








In CCv3 the SFRs are the sole defender



Why do we use Part 2?

Part 1, para 285

The CC requires [...] translation into a standardised language for several reasons:

1. **to allow comparison between two STs.** As different ST authors may use different terminology in describing their security objectives, the standardised language enforces using the same terminology and concepts. This allows easy comparison.
2. **to provide an exact description of what is to be evaluated.** As security objectives for the TOE are usually formulated in natural language, translation into a standardised language enforces a more exact description of the functionality of the TOE.

To allow comparison

If you are using a PP, the STs will (in general) be nearly identical.

Part 2 is not **necessary** to achieve comparability.

If you are not using a PP, Part 2 is not **sufficient** to achieve comparability, because:

- It is not clear which SFRs to use
- It is not clear whether it is required to use an SFR

To allow comparison: which SFRs to use

A “secure” connection between A and B

FCO_NRO: Non-repudiation of origin
FCO_NRR: Non-repudiation of receipt
FCS_COP: Cryptographic operation
FIA_UAU: User Authentication
FIA_UID: User Identification
FIA_USB: User Subject Binding
FDP_ACC: Access Control
FDP_ACF: Access Control Functions
FDP_ETC: Export from the TOE
FDP_IFC: Information Flow Control
FDP_IFF: Information Flow Functions
FDP_ITC: Import from outside of the TOE
FDP_ITT: Internal TOE transfer
FDP_UCT: Inter-TSF user data confidentiality transfer protection
FDP_UIT: Inter-TSF user data integrity transfer protection
FPR_ANO: Anonymity
FPR_UNO: Unobservability
FPT_ITC: Confidentiality of exported TSF data
FPT_ITT: Internal TOE TSF Data transfer
FPT_RPL: Replay detection
FPT_SSP: State synchrony protocol
FTP_TDC: Inter-TSF TSF data consistency
FTP_ITC: Inter-TSF trusted channel
FTP_TRP: Trusted Path



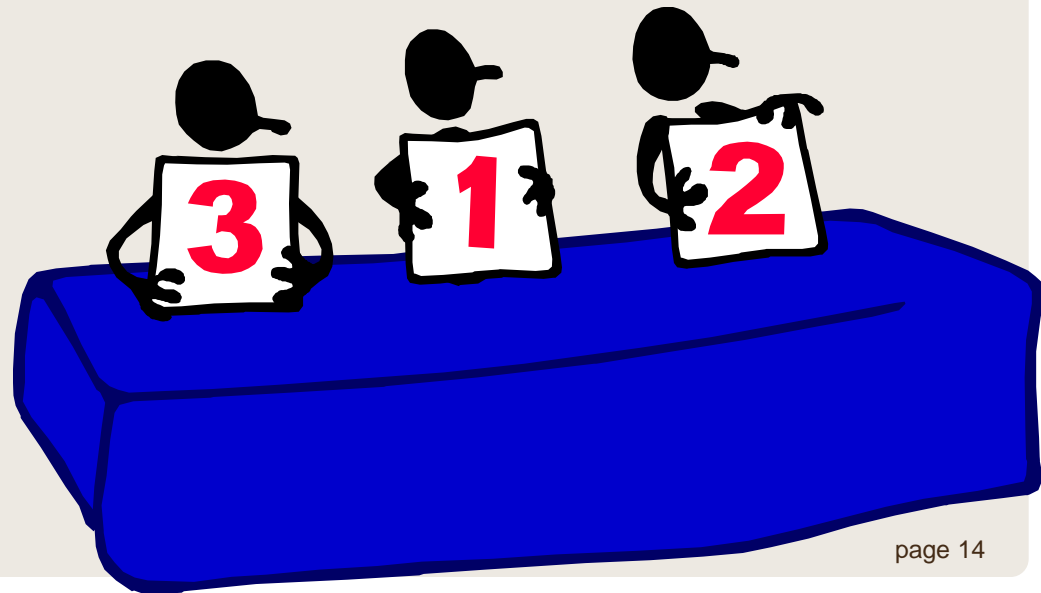
To allow comparison: whether to use an SFR?

What does it mean when a specific SFR is **NOT** included in an ST?

To allow comparison: when to use an SFR?

If FDP_ETC (Export of User Data) is NOT included then:

1. The TSF should prohibit export of any user data from the TOE
2. The TSF should allow all export of all user data from the TOE
3. The TSF should allow export except when it breaks other SFRs (it will come out in ARC or VAN)



Conclusion: Comparability and Part 2

- If you are using a PP, STs will be reasonably comparable. This would also be the case if Part 2 was not used
- If you are not using a PP, Part 2 will not ensure comparability. It doesn't work at all for current STs and PPs.

Why do we use Part 2?

Part 1, para 285

The CC requires [...] translation into a standardised language for several reasons:

1. **to allow comparison between two STs.** As different ST authors may use different terminology in describing their security objectives, the standardised language enforces using the same terminology and concepts. This allows easy comparison.
2. **to provide an exact description of what is to be evaluated.** As security objectives for the TOE are usually formulated in natural language, translation into a standardised language enforces a more exact description of the functionality of the TOE.

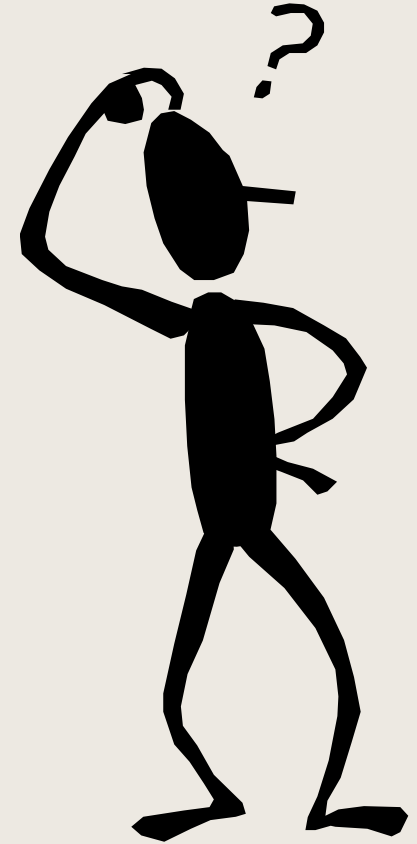
Does CC Part 2 provide an exact description?

There are similar problems as for comparison:

- When should you use SFRs?
- Which SFRs should be used?

There is no guidance that tells you how to do this:

- The CC itself does not contain examples
- Part 2 Annexes are useless
- ISO 15446 (PP/ST Guide) and BSI PP/ST Guide give some hints but lacks detail and examples



Theoretical work on Part 2 concentrates on difficult cases

Anonymous remailers

Multiparty voting systems

Composing a Javacard OS on an IC

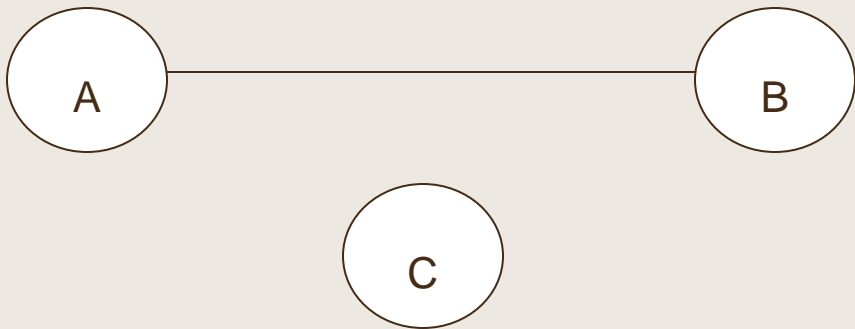
Biometrics

So.....let's concentrate on a **REALLY** difficult case



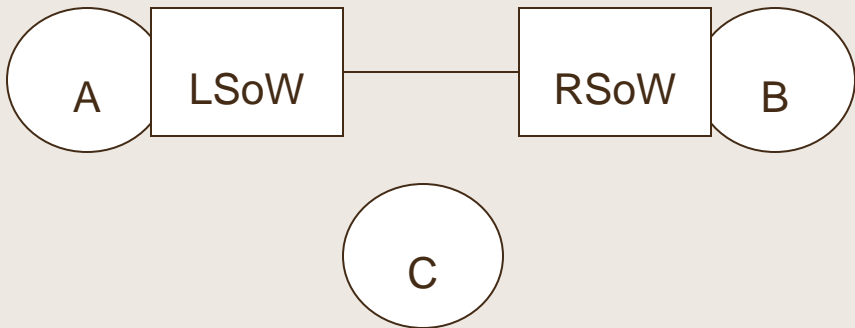
Modeling a wire

- A (outside the TOE) communicates with B (outside the TOE)
- C (outside the TOE) cannot listen in



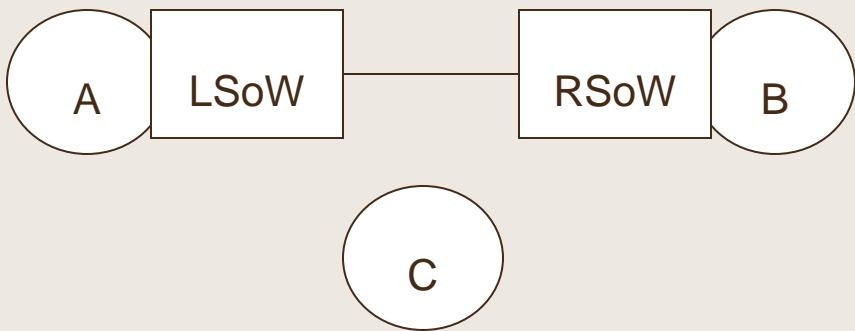
Modeling a wire II

- To use import and export of user data you need an access control policy
- Access control policies are defined on subjects (inside the TOE)
- A and B are outside the TOE and can therefore not be subjects



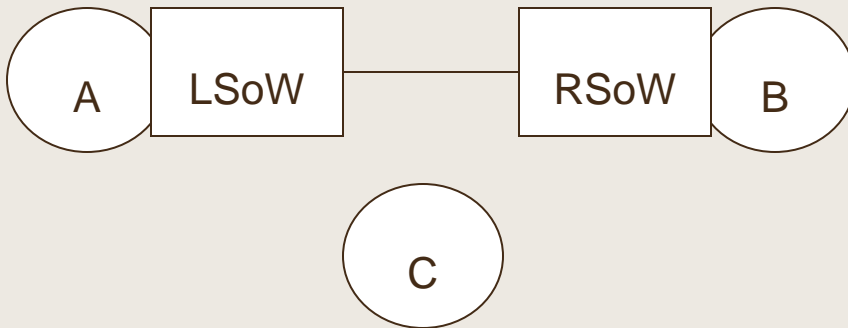
Modeling a wire III

- A is “the entity at the left”. Do you need identification (FIA_UID?).
- If not, how do you know it is not C?
- What do you write down?
- How are A and LSoW then actually associated? FIA_USB? If not, what else?



Modeling a wire IV

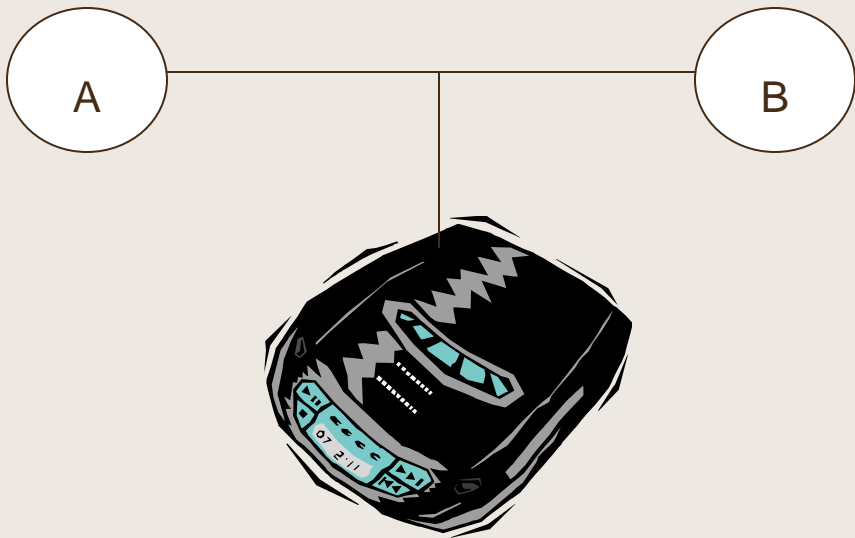
- Are the two “ends of the wire“ considered to be physically distributed?
(FDP_ITT)
- Does this depend on the length of the wire?



Modeling a wire VI-XIV were deleted to save time

Modeling a wire V

- Does a TOE consisting of a wire + a taperecorder meet the SFRs?
- If not, how do you model everything that you do not want?
- Must FDP_RIP then be a part of all TOEs?



Modeling a wire VI-XXIV were deleted to save time

For simple problems, Part 2 cannot hide that:

- It lacks a default model
- It lacks a standard conceptualisation of subjects/objects/users/interfaces
- It lacks a standard interaction model between users and TOE



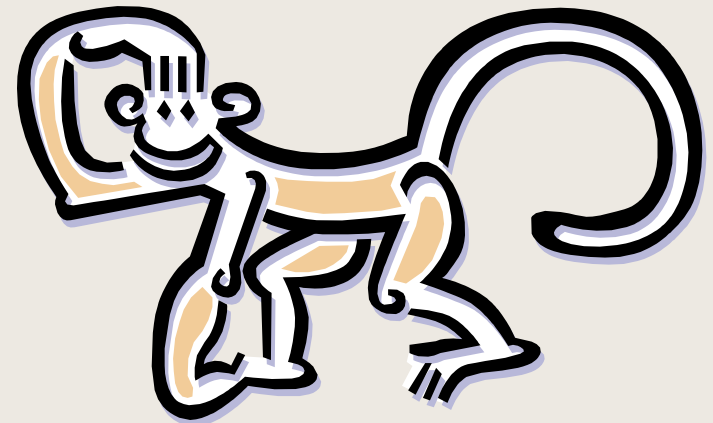
Thought

If I would propose a programming language that claims to be

- able to model almost all problems
- easily extendable for all other problems
- assist programmers in coming up with standard solutions
- claims that programs can now easily be compared
- has a whole suite of supporting libraries

But after ten years, it is still not clear how to print “Hello World”

Would you use it?



If it is far from obvious how to model a wire

How can you hope to adequately model a firewall?

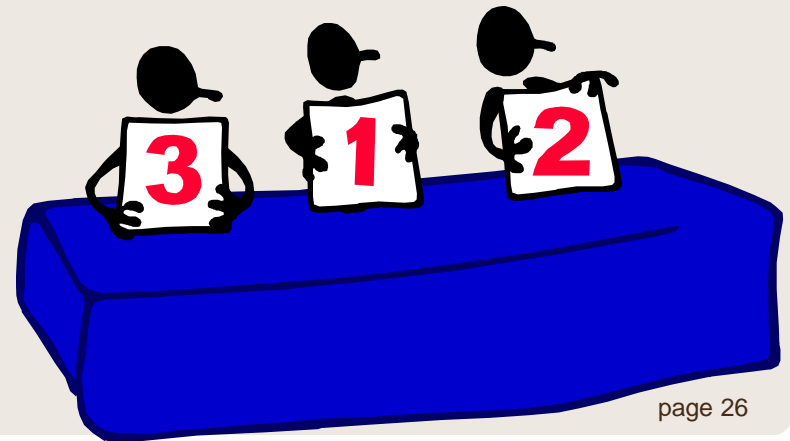
Or more complex systems?

How can you expect people to use this “language”?

If every PP or ST that is a superset of a wire models it differently

Why do you think anyone is using this “language” correctly now?

Does it really enforce a “more exact description”?



Why do we use Part 2?

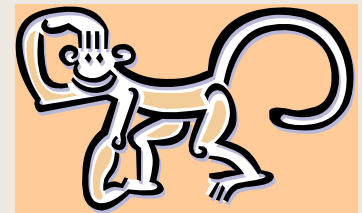
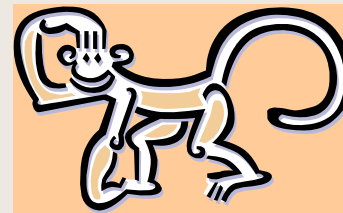
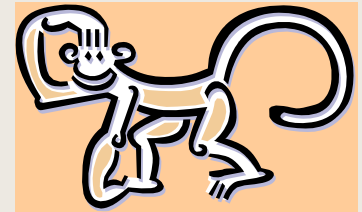
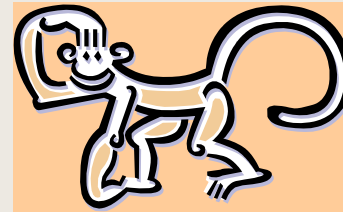
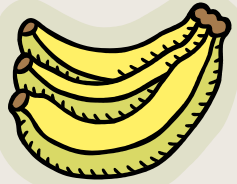
Part 1, para 285

The CC requires [...] translation into a standardised language for several reasons:

1. **to allow comparison between two STs.** As different ST authors may use different terminology in describing their security objectives, the standardised language enforces using the same terminology and concepts. This allows easy comparison.
2. **to provide an exact description of what is to be evaluated.** As security objectives for the TOE are usually formulated in natural language, translation into a standardised language enforces a **more exact description** of the functionality of the TOE.

So.....why do we use Part 2?

Why do we use Part 2?



How are we using Part 2 right now?

When writing a PP/ST

Find SFRs that seem to match many aspects of the security objectives and are not known troublemakers. Avoid extended requirements as they cause work.

Don't use too many SFRs. Reason away as many dependencies as possible as they cause work.

Tell the customer that it is too difficult for him to understand and he should not worry about it



When evaluating or certifying a PP/ST

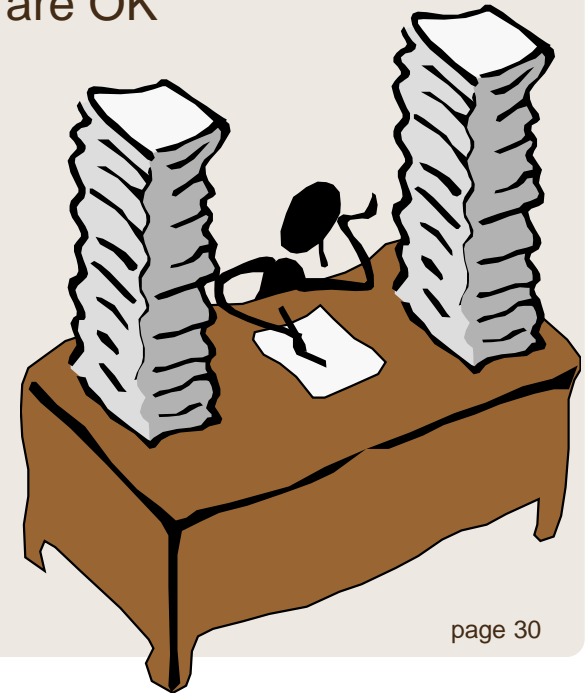
Worry only about:

- Are they complete and correct copies from Part 2?
- Are they bolded correctly?
- Are all operations OK?

And if there is no obvious mismatch conclude the SFRs are OK

The Pseudo-Achievement Syndrome

The Peter Principle, Peter & Hull, 1969



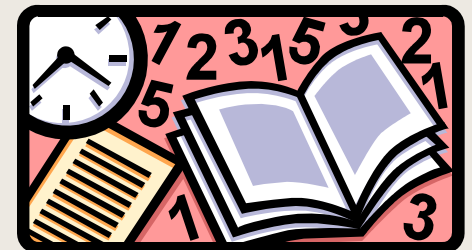
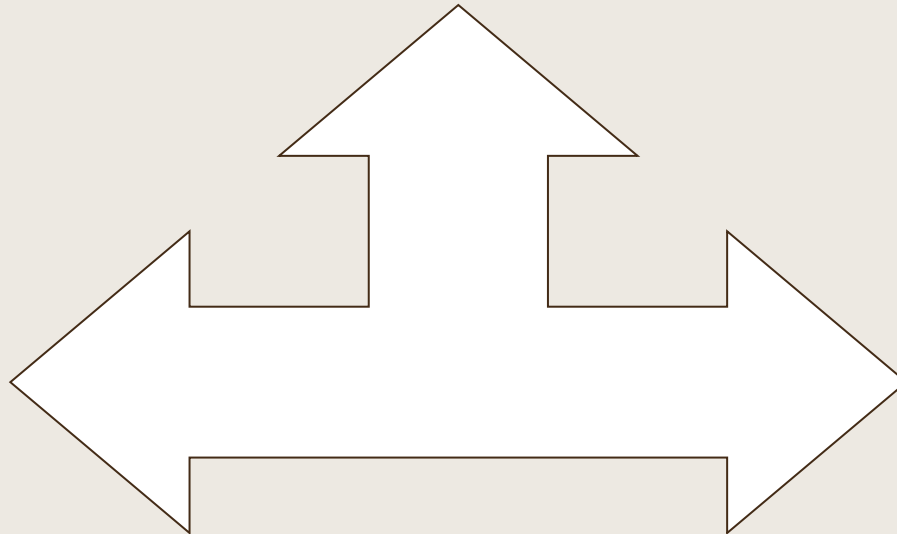
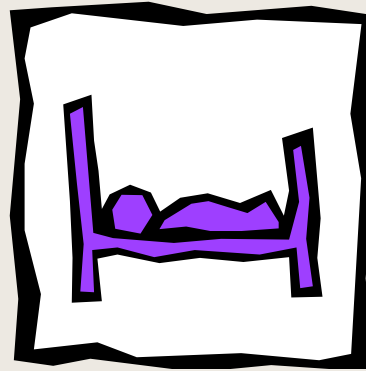
When doing the TOE evaluation

SFRs are an annoyance as they must be mapped against, the less SFRs you have, the less work you need to do

When determining whether something is a vulnerability, don't look at the SFRs. Err on the side of caution. Use professional judgment. Don't take on clients with a lot of lawyers.



So....Part 2 has problems, but we muddle through. Now what?



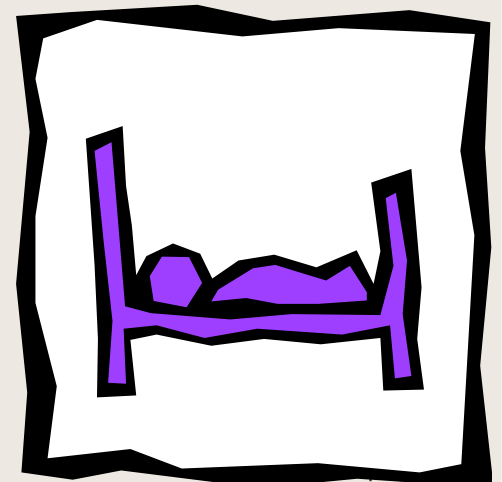
Do nothing

Some communities in the CC are moving towards EAL5+, EAL6+, EAL7+

So we spend ever more money to determine that the TOE meets the SFRs

But we are not so sure on what the SFRs mean

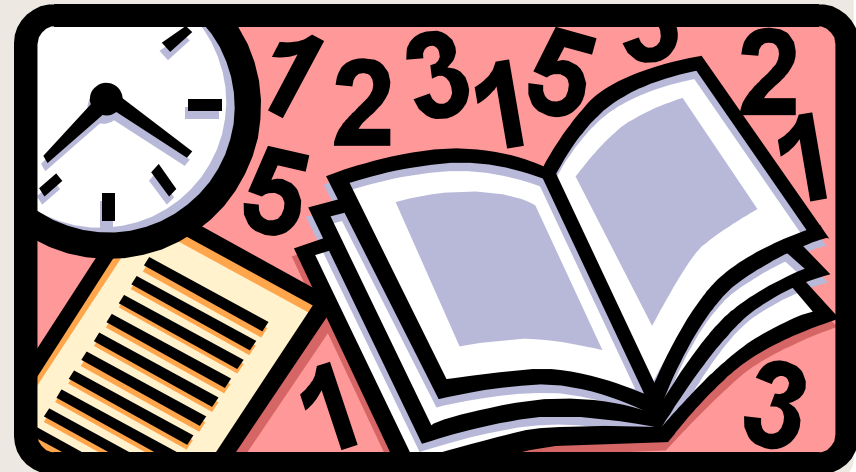
And therefore what a TOE that meets those SFRs actually is



Improving

Making a correct Part 2 that allows adequate modeling of a wire (something like CC Part 2 v3.0) will:

- Take significant time
- Lead to an even more abstract CC Part 2
- Would use a lot more SFRs
- May have little actual benefit
 - We are not really using Part 2 now
 - So apparently we can do without it





Removing it

We have semi-formalised something that we partially understand

However, I have learned a LOT from studying Part 2

Perhaps we should retain many of the concepts of:

- Objects, subjects, attributes, access control, information flow
- Users, identification, authentication
- Management, various flavors of auditing
- How these are tied together with dependencies

Apply a consistent terminology but use natural language and diagrams.

And replace CC Part 2 with a book on

- How to write good Security Policy Definitions
- How to write good Security Objectives

With as many examples (mini-PPs) as we can cram in and use a comply-or-explain paradigm to enforce re-use of the examples.

Evaluators and certifiers could then concentrate much more on whether the ST is clear and useful (and less on **bolding**)

So our clients, customers, end-users and all can also understand what they are requiring and getting



Summarising

There are big problems with CC Part 2

We solve these by ignoring them and muddling through

Repairing it in the “same style” may not be necessary: the semi-formalism does not bring us anything useful and prohibits understanding

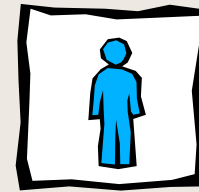
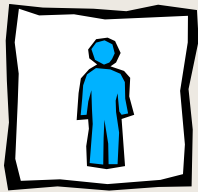
A natural language replacement would be much more valuable

If this is not possible, we should delete Part 2 entirely

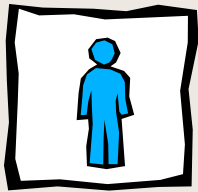
Questions?



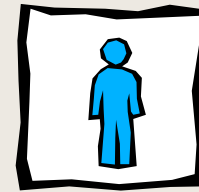
Divestiture Bias



Divestiture Bias



I'll sell for \$2.13



I'll buy for \$0.94



Divestiture Bias

Now that we have CC with this Part 2, deleting it is “too costly”

If we had a CC without this Part 2, adding it is “too costly”

