A Model of Certifier and Accreditor Risk Calculation for Multi-Level Systems

Joe Loughry
mailto:joe.loughry@stx.ox.ac.uk

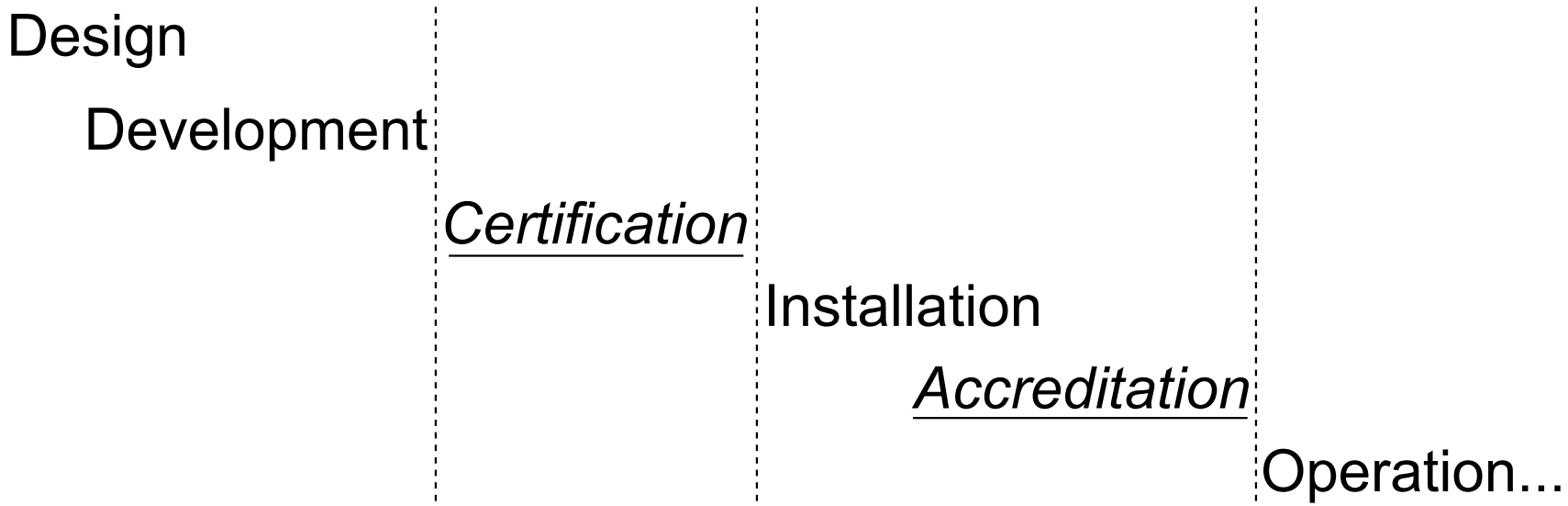
Department of Computer Science, University of Oxford
Wolfson Building, Parks Road, Oxford, OX1 3QD, UK

IEEE HST'13
Boston, 12–14 Nov. 2013

Topics

1. C&A in 60 Seconds
2. Where all this data came from
3. Findings
4. Summary and Conclusion

C&A in 60 Seconds



Where this data came from

- Grateful acknowledgement is given to Lockheed Martin for access to project records and data:
  - . . . from an unsuccessful Common Criteria (CC) security evaluation in 2006
  - . . . and from the *successful* DIACAP security certification of a similar product in 2010
  - . . . as well as from a previous CC validation of an earlier version of the same product in 1999.

- Methodology: participant observation, grounded theory.

Findings

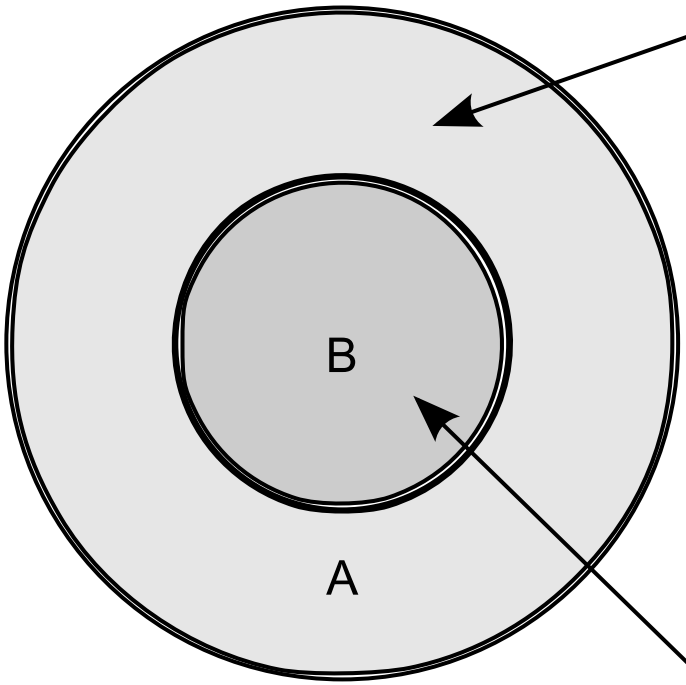
- Certifier model (observational)
- Accreditor model (analytical)
- Grounded theory of implicit and explicit communication channels in C&A
- Proof that channels exist and are reliable
- Paradox in security rules

Assumptions, applicability, and practical applications.

Assumptions

1. Accreditors have appropriate security clearances for their jobs.
2. Every cross domain system has exactly $n = 2$ accreditors.

This is Accreditor #1's view of the situation.



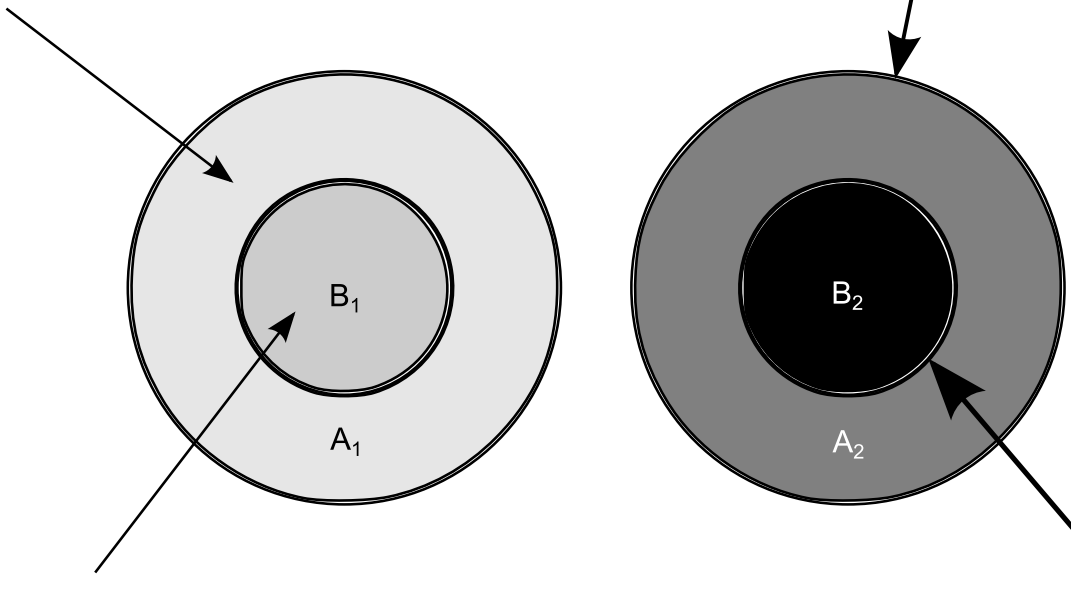
A: threats that are known

B: mitigations that are feasible

Accreditor #2 has a different, equally valid perspective.

threats known to accreditor #1

threats known to accreditor #2



mitigations thought to be feasible by accreditor #1

mitigations thought to be feasible by accreditor #2

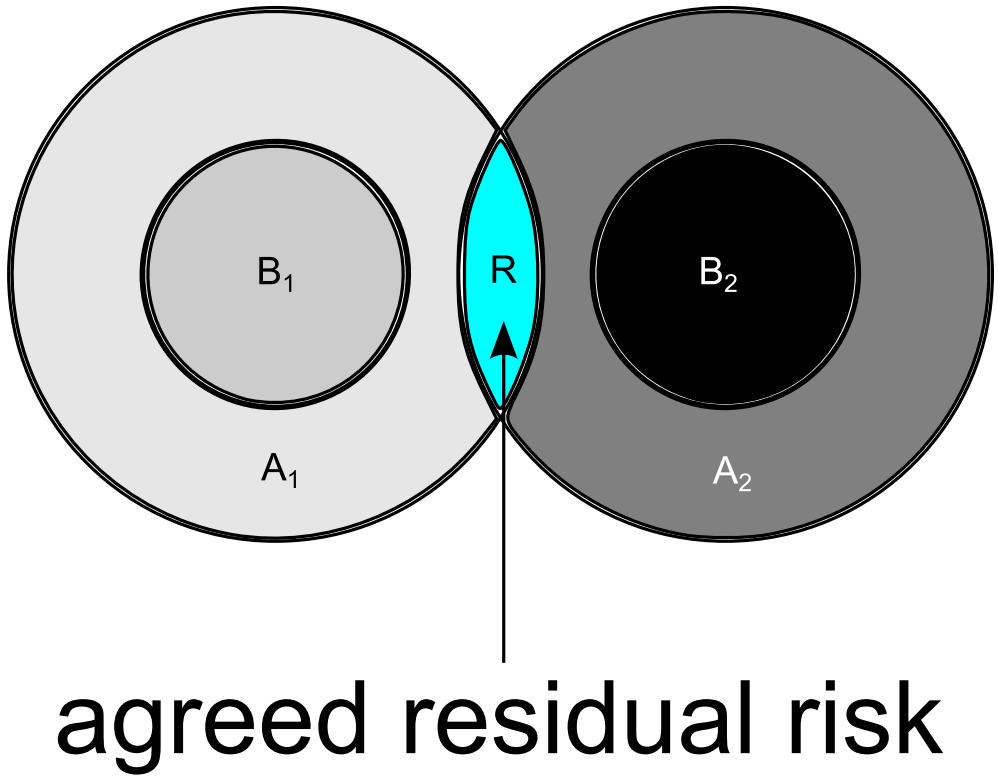
High-side known threats

High-side risk mitigations

Low-side risk mitigations

Low-side known threats

Public information



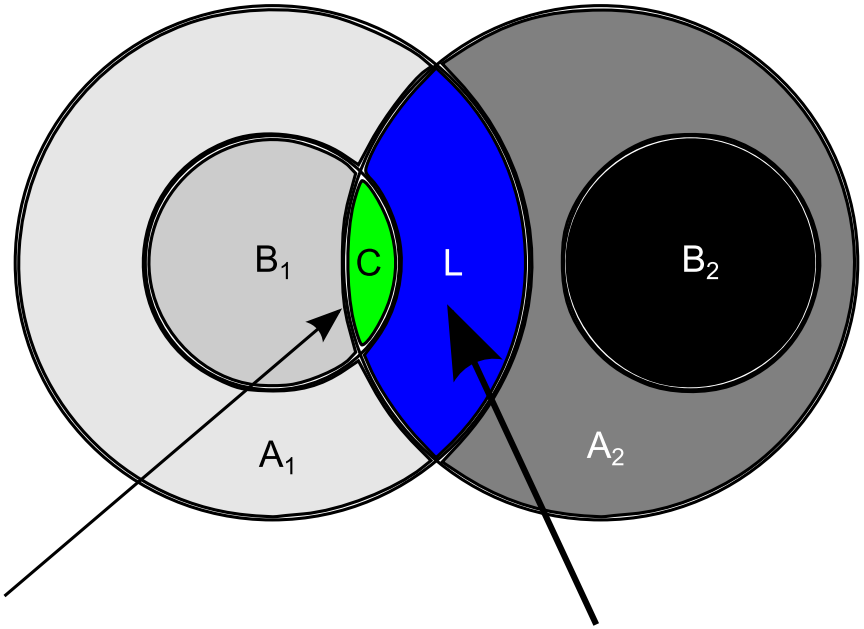
High-side known threats

High-side risk mitigations

Low-side risk mitigations

Low-side known threats

Classified information with risk of information leakage



area of consensus on safety

first risk of information leakage

High-side known threats

High-side risk mitigations

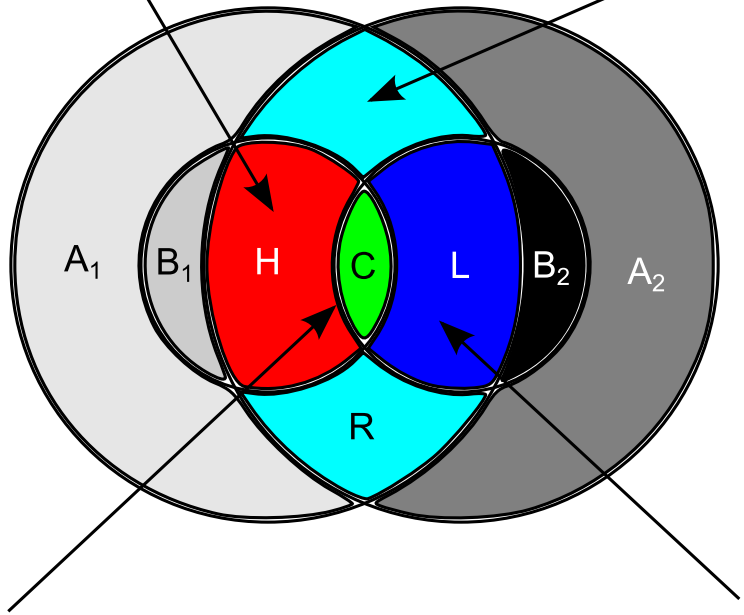
Low-side risk mitigations

Low-side known threats

Personal risk to Accreditor #2

hazardous area

agreement on residual risk



area of consensus on safety

continued risk of information leakage

High-side

High-side

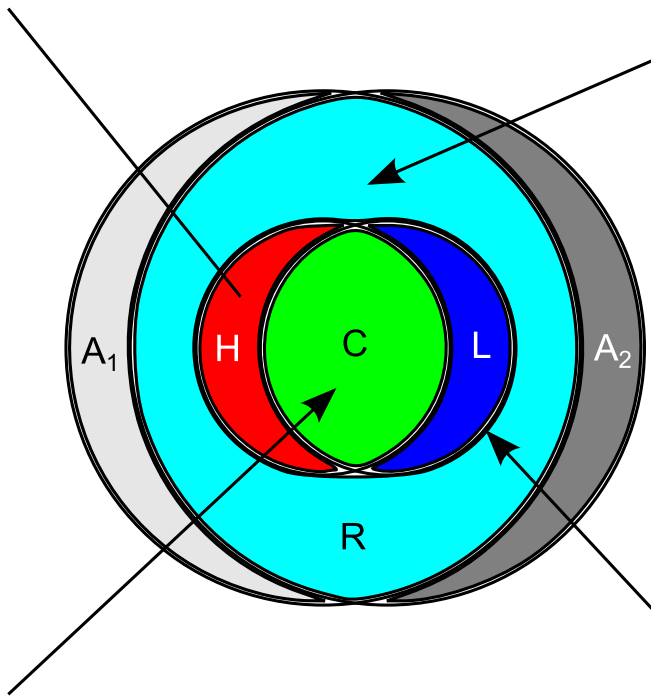
Low-side

Low-side

As the situation approaches a pure collateral. . .

hazardous area shrinks

agreement on residual risk grows



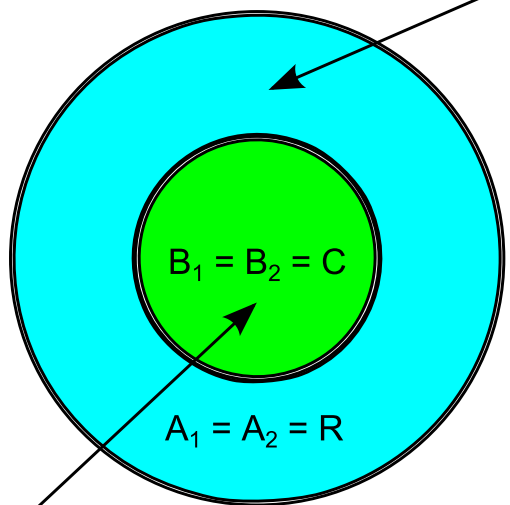
area of consensus on safety growing

lessening risk of information leakage

High-side High-side Low-side Low-side

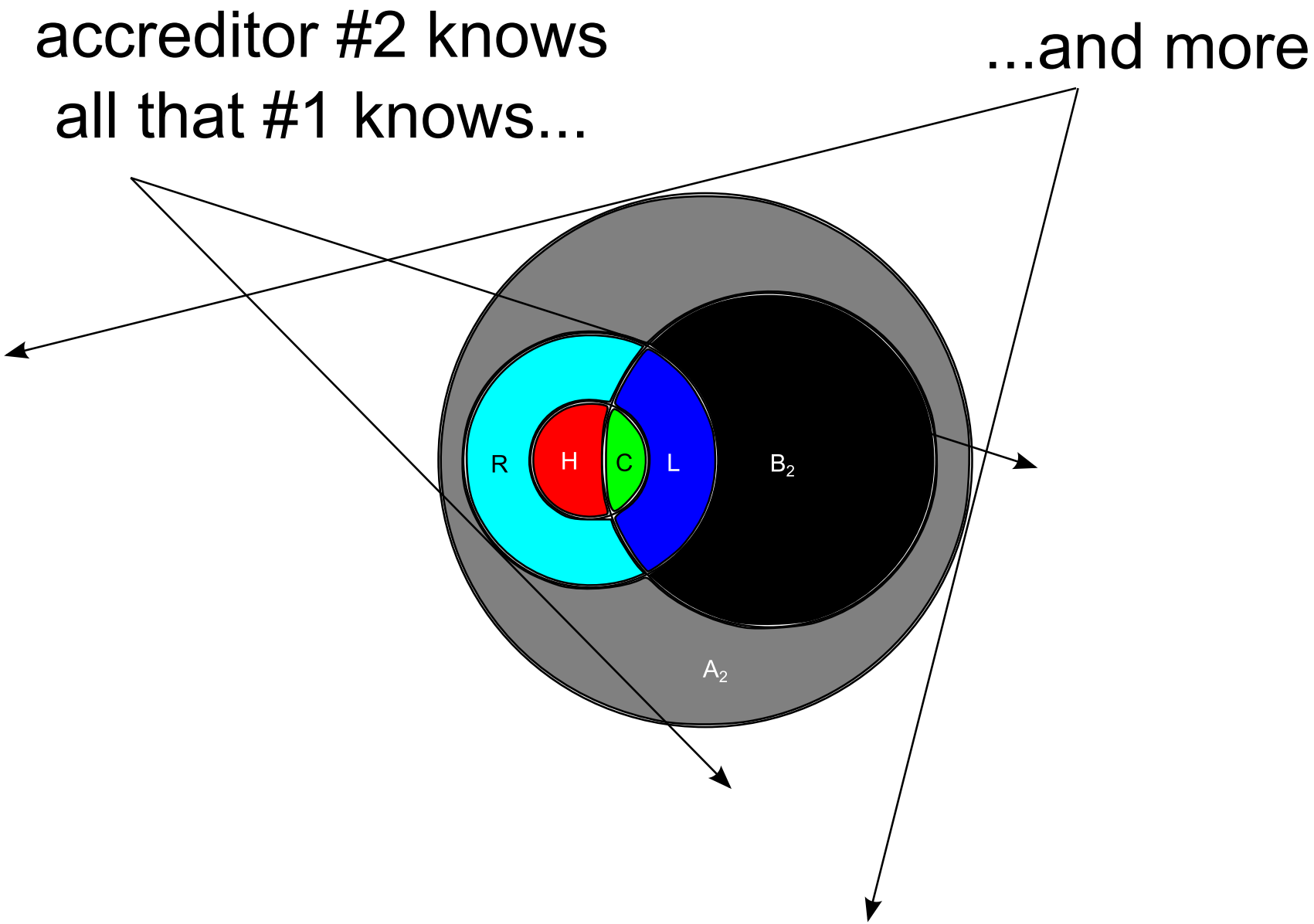
. . . degenerate situation. . .

complete agreement
on residual risk

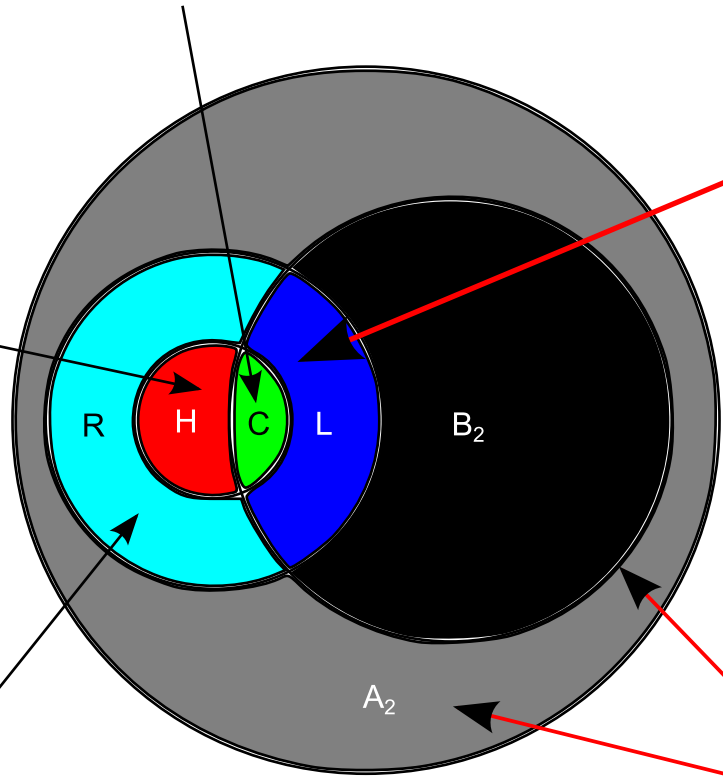


complete
consensus on safety

Collateral with different security clearances



Security paradox!



both still agree
this area is safe

zone of
information
leakage

guilty
knowledge

still agreement on
residual risk here

here be
dragons

Summary and Conclusion

1. Some desirable information flows are inhibited by security policy.
2. Some *undesirable* information flows are forced.
3. The paradox of looser security rules.
4. It is possible, within limits, to predict the duration of accreditation.
5. Developer can exert a measure of control over certification schedule.

mailto:joe.loughry@stx.ox.ac.uk