

Ministry of Defence

Multi Level Security, 3½ decades later

Capt Erik Muller (E.Muller.01@NLDA.nl)

Erik Poll (E.Poll@cs.ru.nl)

Tim Grant (TJ.Grant@NLDA.nl)

Netherlands Defence Academy - **Faculty of Military Sciences**
Radboud University Nijmegen - **Science Dept.**

Overview

Goal of presentation:

- Is there a problem?
- How far are we in solving the problem?
- New directions for research?
- Conclusion

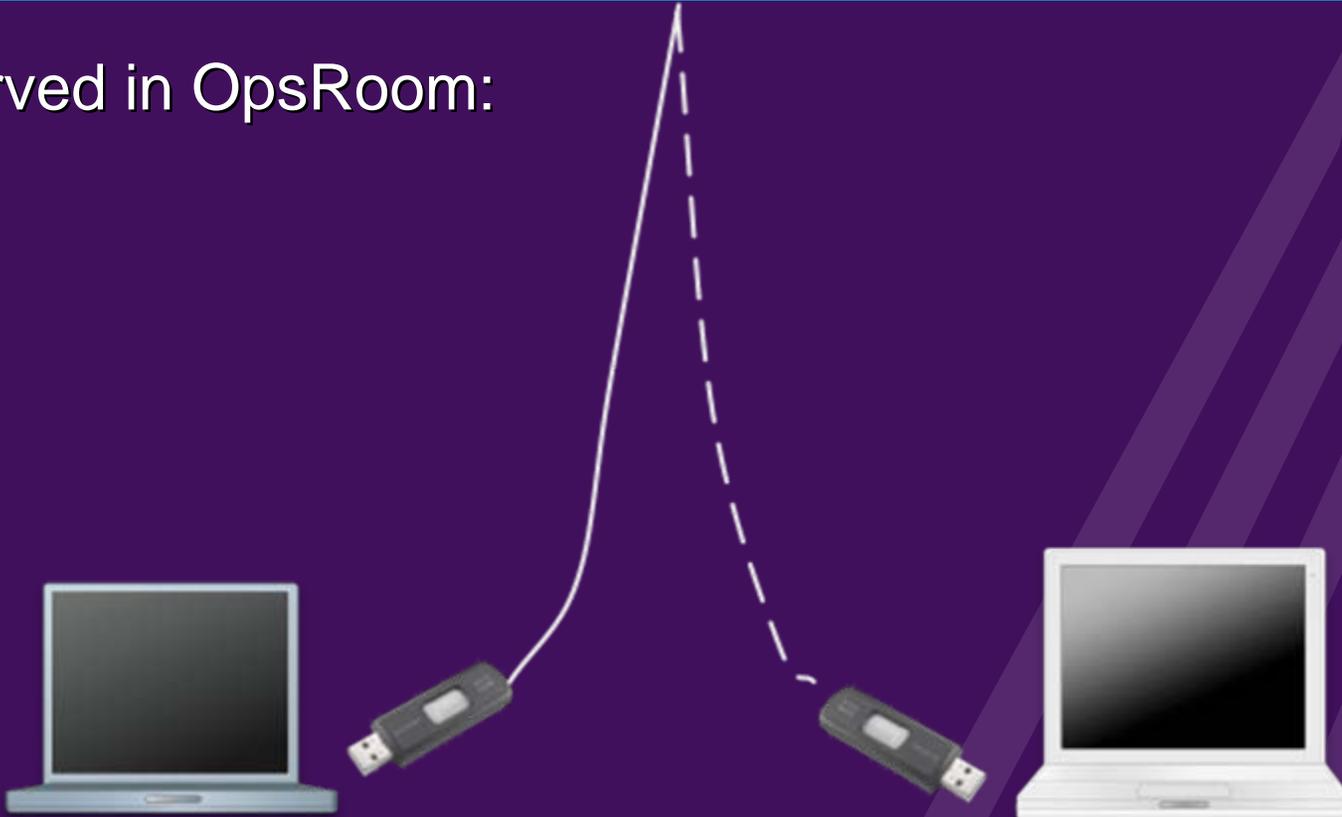
My experience Tarin Kowt (FOB Ripley, Afgh)

July 2006 - Jan 2007:

- 10 Different networks (2007)
- Physically separated
- Data-exchange not possible
- 'Risky' copying of data using USB storage devices
- Unworkable

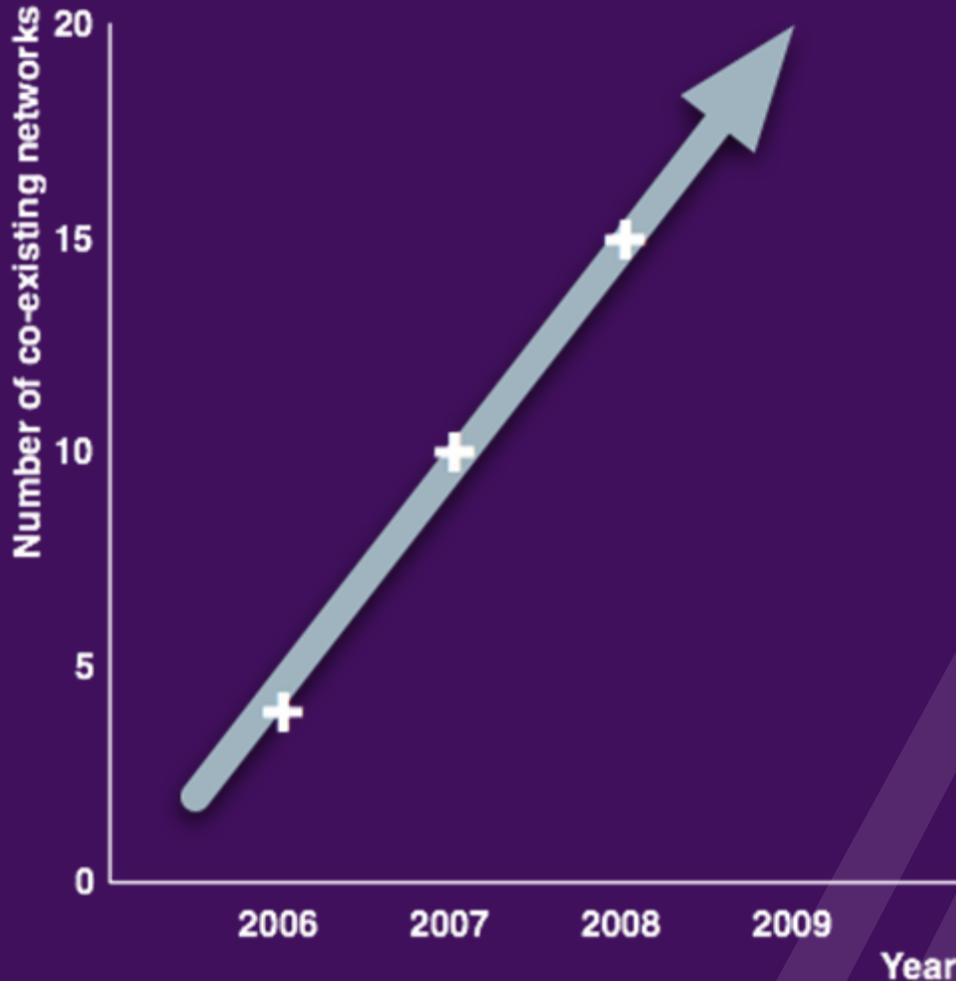
Is there a problem?

Observed in OpsRoom:



2 Networks connected by a thumb drive
attached to the ceiling by a rubber band

Growth in number of networks



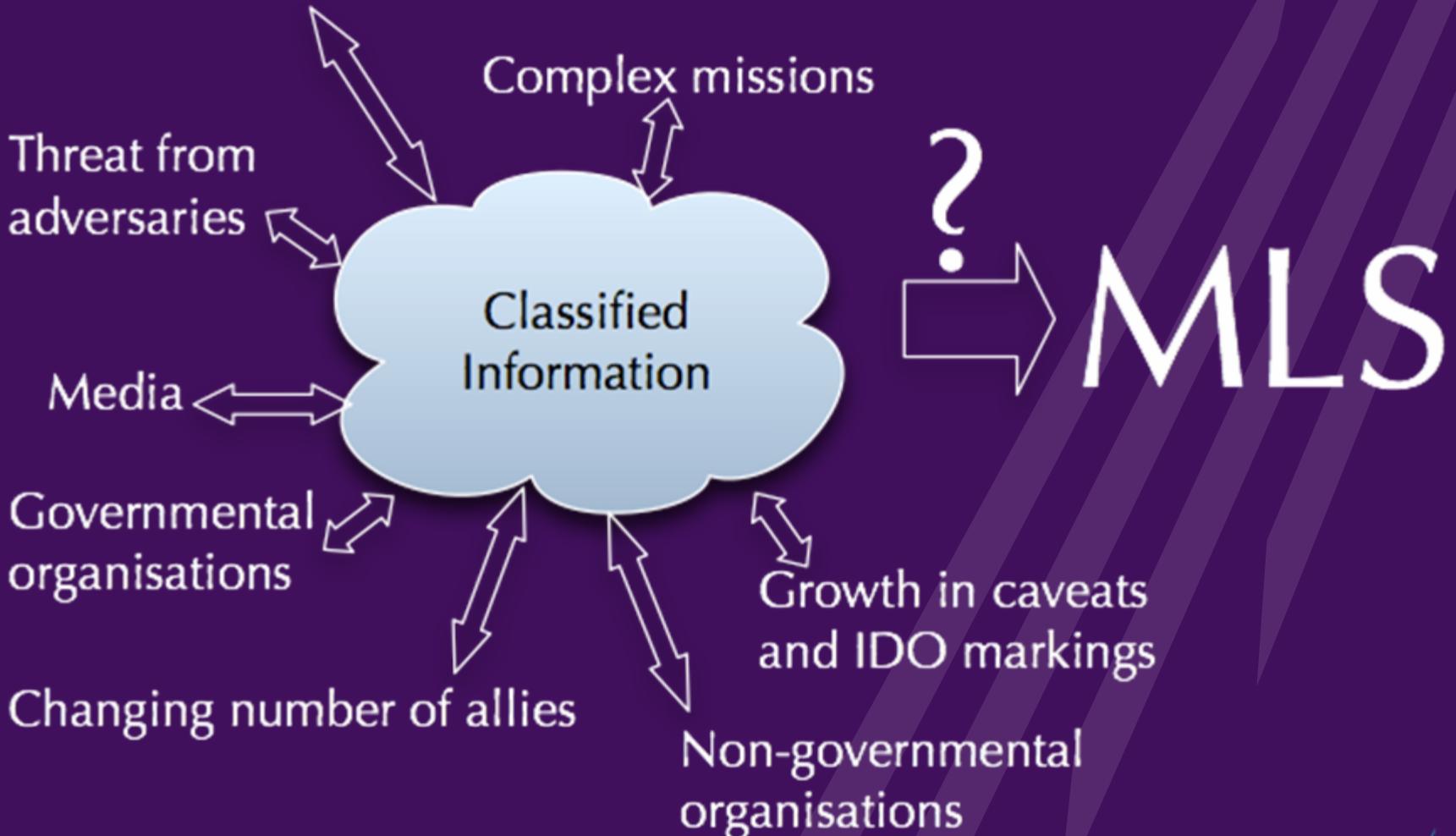
- NLD Secret
- NLD/AUS Mission Secret
- SIPR
- Centrixs
- ISAF Secret
- NATO Secret
- NLD restricted
- AUS Secret
- Mil Internet
- Welfare internet
- etc.

Characteristics

- Increase of the use of digital information
- More information sharing between military units, GOs, NGOs, media, repair organisations and suppliers
- C2 decision time needs to speed up to respond more quickly to dynamic situations
- Adversaries become increasingly keen on intercepting classified information

Characteristics (2)

Growth in digital information



Multi-Level Security (1970s)

Definition Multi-Level Security:

“a class of systems containing information with different sensitivities that simultaneously permits access by users with different security without risk of compromise”

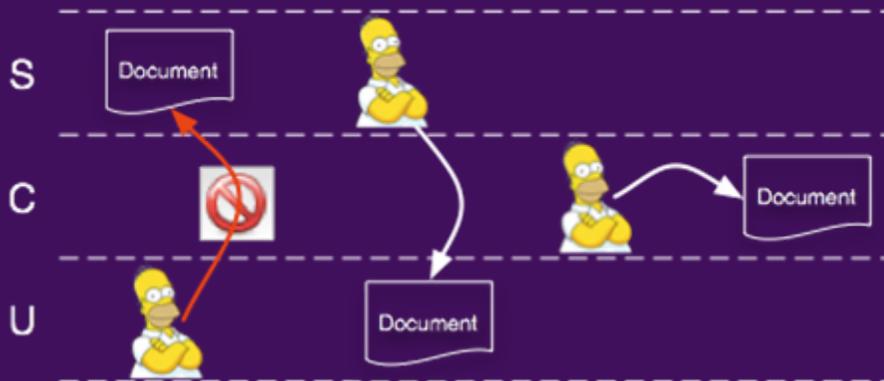
Source: “Orange Book”, Trusted Computer System Evaluation Criteria. Published by the National Computer Security Center (NCSC) in 1983, revised & released 1985

Why haven't we yet achieved true MLS?

Most effort went into implementing Bell-LaPadula

- The Bell-LaPadula model is one of the first models that was created to control access to data
- Developed in 1973 to formalise the US DoD multilevel security policy
- Focuses on the confidentiality of classified information

No Read Up - Simple Security Property



No Write Down - *-Property



- BLP offers protection against Trojans and illiterate

Multi Level Security, 3½ decades later - Erik Muller

users!

Why haven't we yet achieved true MLS? (cont'd)

- Large effort spend on developing and building true MLS systems has led to several failed systems
- Changed economical and political situation over past 2 decades has led to budget cuts whilst the use and exchange of classified information has intensified tremendously
- Governments have been drawn towards low-cost, low-security solutions ever since

➔ No viable MLS products based on BLP

Simplified 'MLS' models

Failure to implement 'true MLS' models has led to systems based on simplified MLS-models:

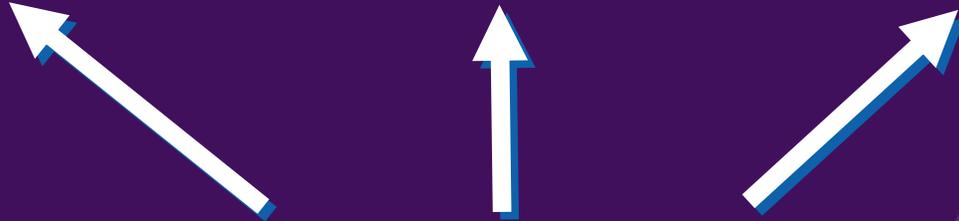
- High Watermark
- System High

➔ Lead eventually to the same (original) problem

Where lies the real problem concerning MLS?

Models provide a perfect theoretical solution!

Implementation = BLP-model + Additional security measures



Where does it go wrong?

- ➔ Do we have a technical problem?
- ➔ Are we implementing wrong or outdated security policies?
- ➔ Is there another (unknown) issue?

What can we do?

- Question the BLP model?
- Question additional policies?
- Work on new / better implementation techniques?
- Something else...?

Further research

Possible directions for further research

- Replacing security levels by a gradual scale
- Redefining (military) definitions
- Using virtualization techniques
- Abandoning BLP as true MLS model
- Cryptographic techniques for tagging
- Redefining classification levels to automatic declassification (in time)
- Dedicated Operating Systems (TCB)
- Secure database storage of information
- Introducing risk management (redefining risks)
- Research into covert channels

Conclusion

- We (still) have a problem
- Research has been ongoing, but has not led to viable MLS products over the long term
- Where do we go from here?



Ministry of Defence

Suggestions?

Erik Muller (E.Muller.01@nlda.nl)
Netherlands Defence Academy
Faculty of Military Sciences