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

Joe Loughry

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

HST'13
Boston, 12–14 November 2013

Outline

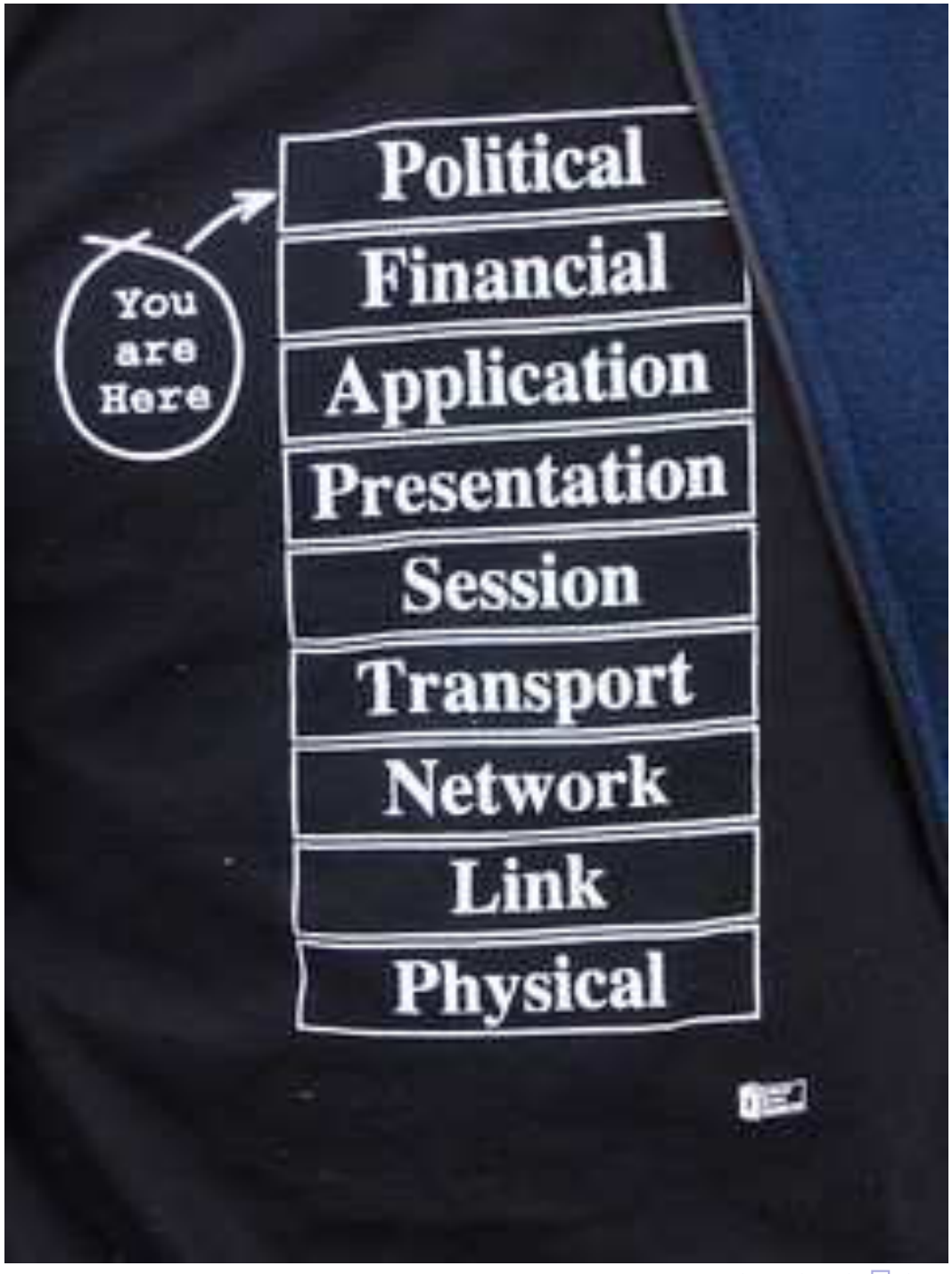
- Introduction
- Definitions
- Methodology
- Assumptions
- Findings and New Results
- Future Work
- Conclusion

Introduction

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

Definitions

- Cross Domain Solution (CDS)
  - Synonymous with *guard* or *controlled interface*
  - Not the same thing as a firewall
- Cross Domain System (CDS)
  - Together with its connected networks, is built from one or more cross domain solutions.


You are Here
Political
Financial
Application
Presentation
Session
Transport
Network
Link
Physical

Definitions

- Certification
  - Certification Test and Evaluation (CT&E) phase
  - Is performed by a *certifier* or *certification authority*.
- Accreditation
  - Security Test and Evaluation (ST&E) phase
  - Is performed by an *accreditor* or Designated Approving Authority (DAA).
- Re-certification event
- Accreditation Maintenance phase

Methodology

- I used a grounded theory methodology to discover what interesting things could be found in the data.
  - This is especially suitable for software engineering investigations where controlled experiments are difficult and expensive to replicate.

Assumptions

- Cross Domain Systems are always installed in an adversarial environment.
  - Data owners do not trust one another.
  - Accreditors represent data owners.
- Accreditors have security clearance only to the necessary level.
  - For example, some accreditors are cleared only for SECRET information and others have TOP SECRET security clearance.

Findings and New Results

1. Model of inter-accreditor communication
   - It satisfies the criteria of Spence and Akerlof for reliable signals in the presence of asymmetric information.
2. Method for predicting behaviour of accreditors
   - Some undesirable information flows are forced.
   - Some desirable information flows are inhibited.
   - If Bell–LaPadula rules are followed, the security policy must be violated under some conditions.
3. Method for controlling the behaviour of certifiers
   - The software developer of a CDS can exert some measure of control on the schedule of certification.

Future Work

- The presence of asymmetric information leads to arbitrage opportunities.
- Is there a market for risk?
- New tool: *nihil obstat*

Conclusion

- The accreditor behaviour model is theoretically sound.
- It is possible to predict certain types of accreditor communication.
- The software developer has some control over the certification testing process.

Merci

- Thank you for inviting me here.