Tribute to Michael Jackson

- **9:00** Welcome (Bashar Nuseibeh)
- 9:05 Pamela Zave – on Michael Jackson
- 9:15 Tony Hoare
- 9:45 Daniel Jackson
- 10:00 John Cameron
- **10:30** Break
- 11:00 Axel van Lamsweerde
- 11:30 Anthony Hall
- 12:00 Pamela Zave
- **12:30** Lunch
- 14:00 Cliff Jones
- 14:30 Bashar Nuseibeh
- 15:00 Daniel Jackson
- **15:30** Break
- 16:00 Michael Jackson responds
- 17:00 Discussion
- **17:30** Reception (**ends 19:00**)

Working with Michael Jackson

BASHAR NUSEIBEH

THE OPEN UNIVERSITY (OU), UK

Michael Jackson @ The OU

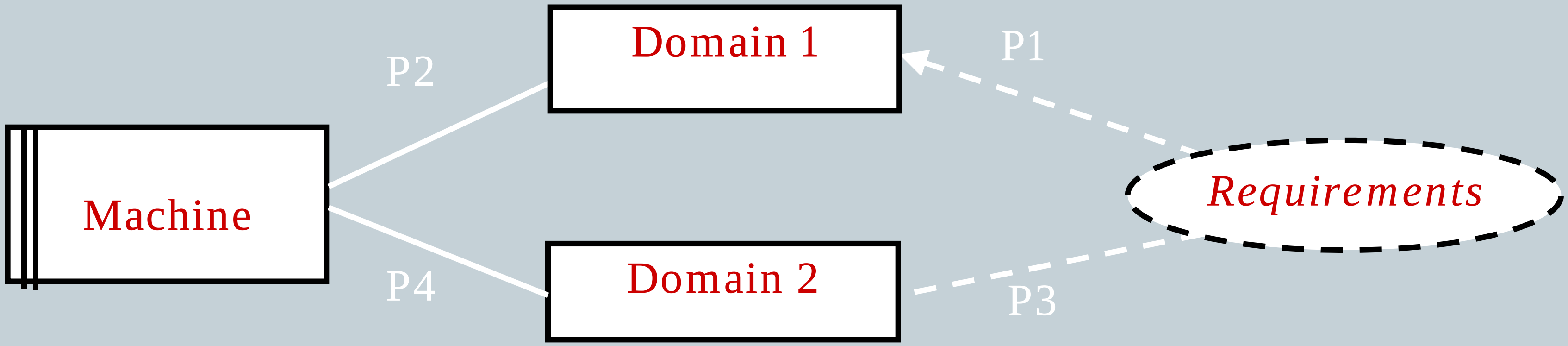
- Visiting Professor
- Colleague
- PhD Supervisor
- Confidant

If Software is the Solution, What is the Problem?

- The world and the machine
  - Requirements and design
  - Problem-orientation
  - Specialisation

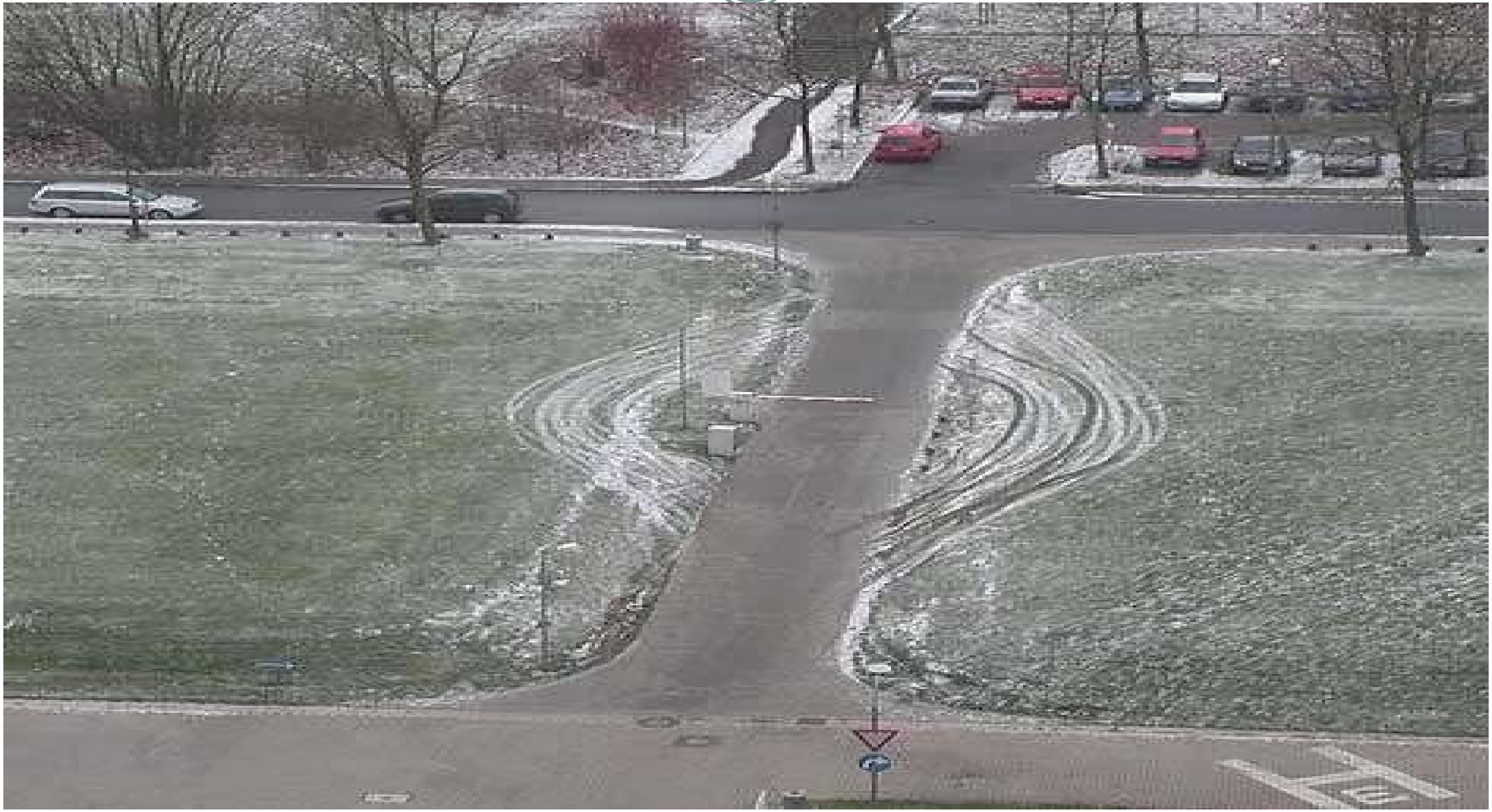
Problem Frames

- Articulate the separation between world and machine
  - Defining problem boundaries
  - Defining and scoping problem alphabet



- Define and organise recurring patterns

A security problem?



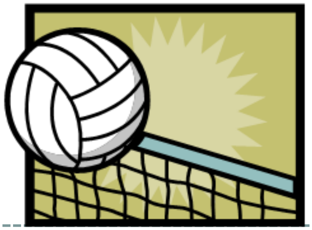
A wicked problem

- **Security is a ‘wicked problem’ [Rittel]**, for which there is no perfect solution;
  - security implementations are a trade-off between **cost** and effectiveness;
  - some **assets** are not worth protecting,
  - acceptable solutions vary from **stakeholder** to stakeholder,
  - the solution space is bounded by what the **customer** is willing to **spend** and what technology can provide.

Security goals – CIA … A

- **Confidentiality** – ensure that an asset is visible only to actors authorized to see it.
- **Integrity** – ensure that the asset is not corrupted.
- **Availability** – ensure that the asset is readily accessible to agents that need it, when they need it
- **Authentication** – ensure that the identity of the asset or actor is known.
    - **… accountability … non-repudiation … authorisation …**

Security is not football



- **Security is not a zero sum game**:
  - there is no exact equivalence between the losses incurred by the asset owner and the gains of the attacker.
- So, the evaluation of possible harm to an asset can sometimes be carried out without reference to particular attackers; and
- consideration of the goals of attackers cannot be used simply to arrive at the goals of a defender to prevent harm.

Problems of scope …

- This cash machine has been designed with the most sophisticated password encryption.
- Special precautions have been taken to ensure that only authorised users with valid smart cards can withdraw money.

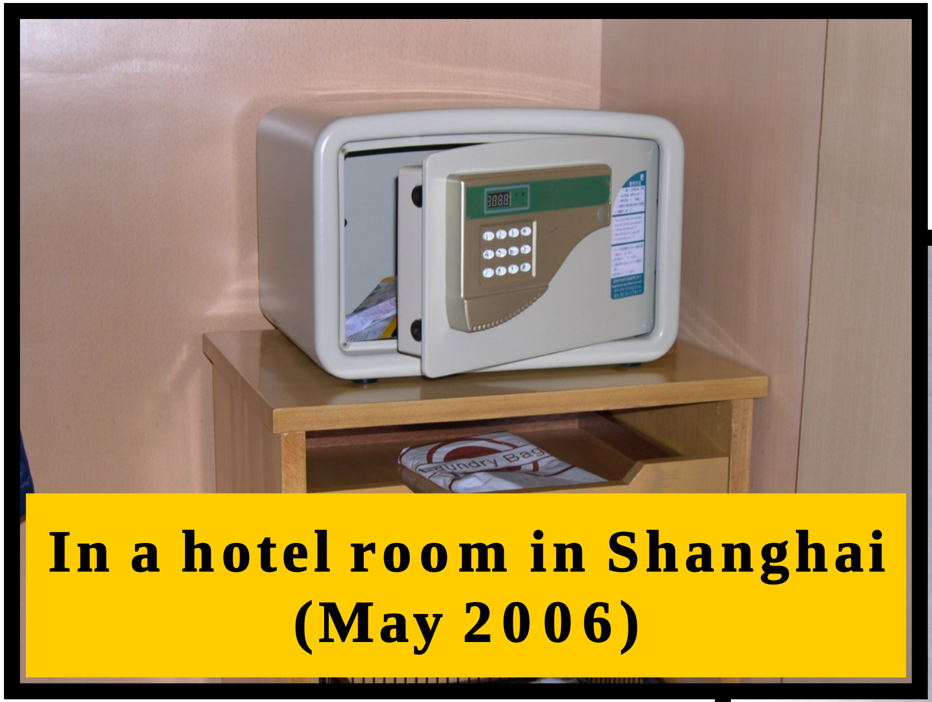
Problems of scope …

- Is it secure?

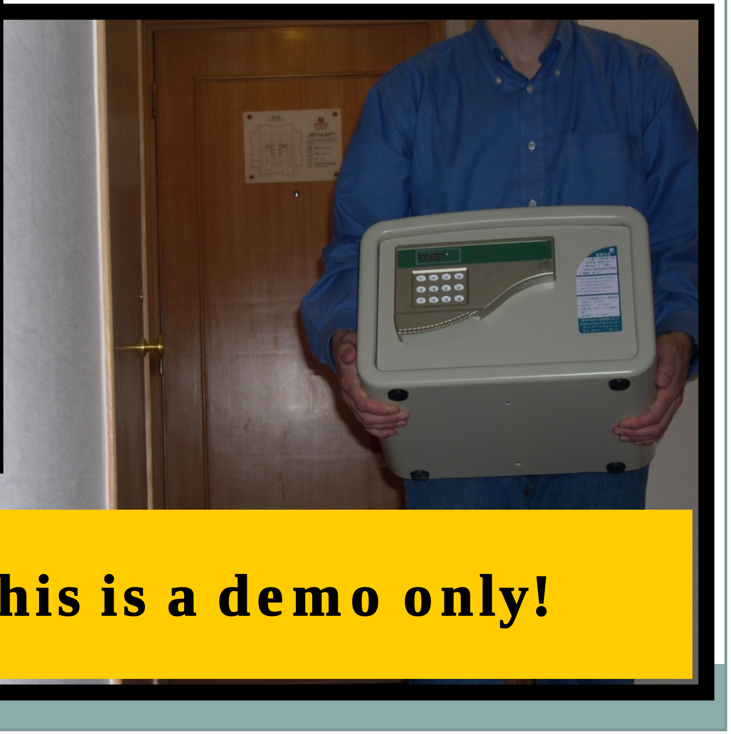
A Problem

- Not if the whole machine is stolen!

Not an isolated incident



In a hotel room in Shanghai (May 2006)



This is a demo only!

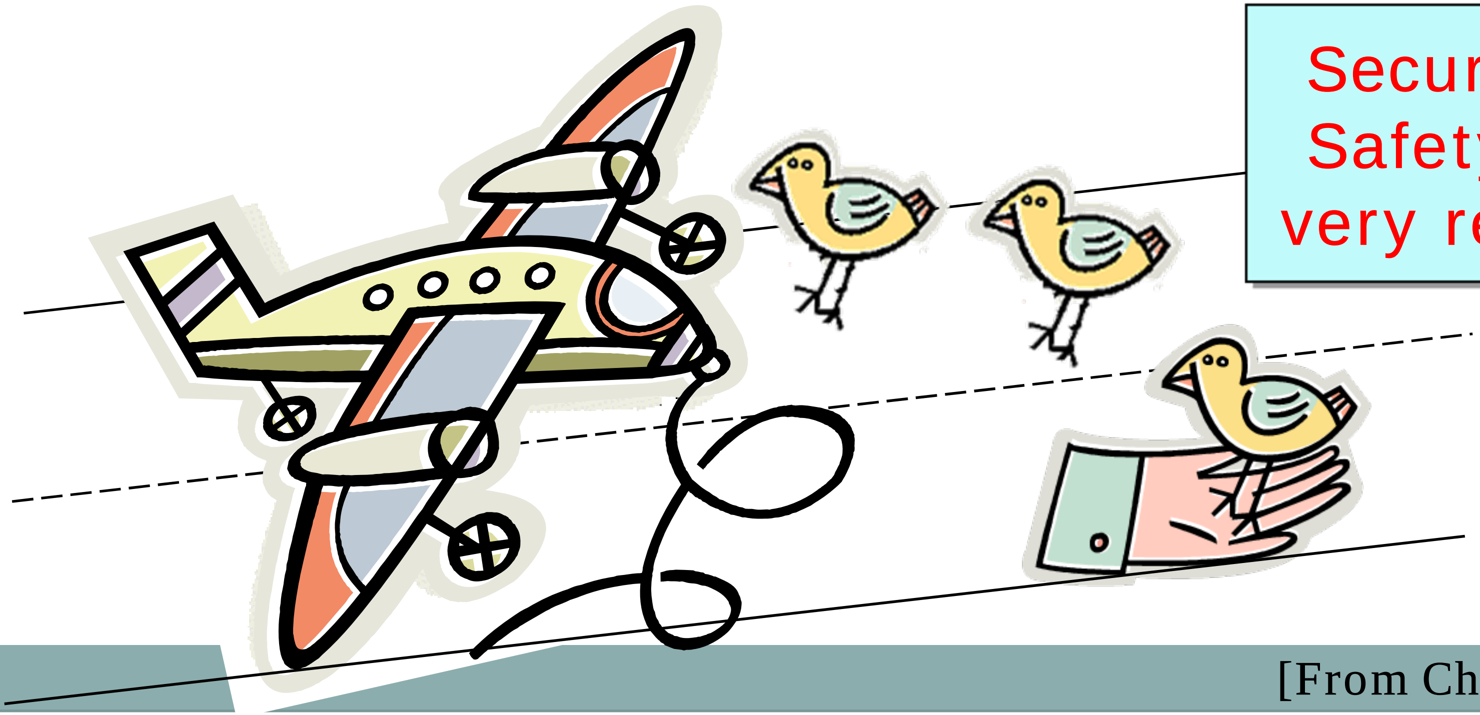
Anti-requirements

- We define an **anti-requirement** as the requirement of a **malicious** user that subverts an existing requirement.

- This is useful because:
  - If we can find circumstances in which both a requirements and an anti-requirement hold (compose), then we hypothesise that the conditions of composition identify a potential vulnerability in a system that implements both requirements.

Security & Safety

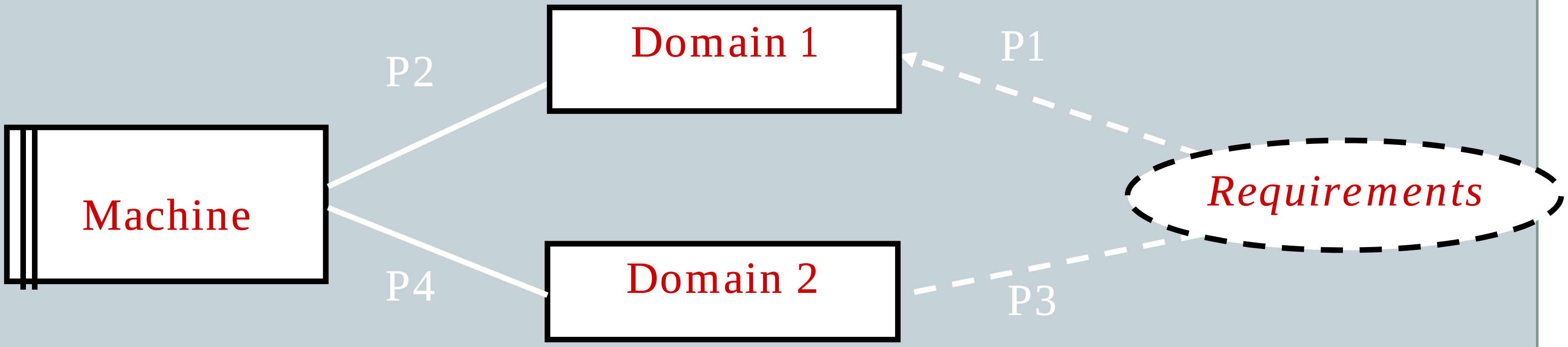
- **Security:** **incidents caused by intention**
- **Safety:** **incidents caused by accident**



Security & Safety are very related

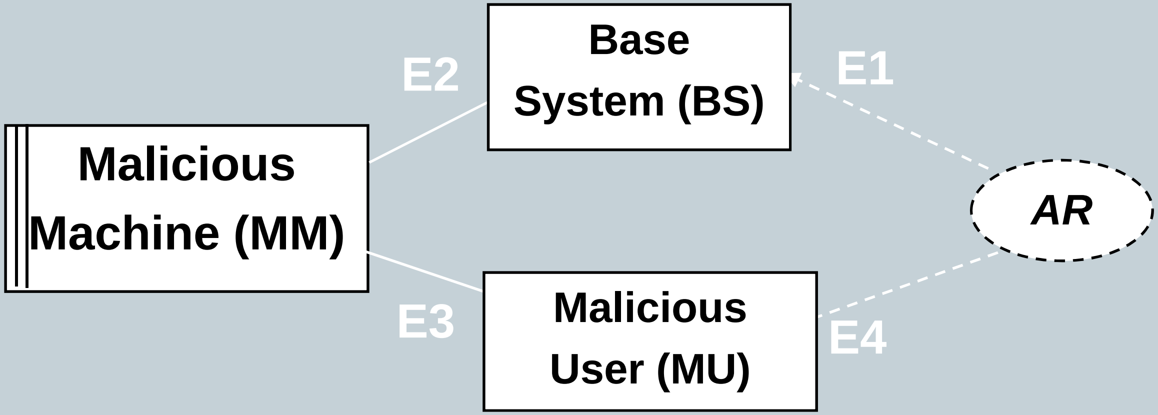
[From Charles Haley]

Problem Frames and Anti-requirements



- Consider an **anti-requirement (AR)** as the requirement of a **malicious** user that subverts an existing requirement.
  - It defines a set of undesirable **phenomenon** that will ultimately cause the system to reach a vulnerable state.

Abuse Frames



- The **Base System (BS)** is the system attacked.
- **The anti-requirement (AR)** specifies the undesirable phenomena in terms of *E1* in the Base System (BS).
- *E4* indicates that the Malicious User (MU) can interact with the *BS* through or unexpected phenomena.
- The specification of the *MM* describes the interface over the *E3* of the *MU* and the *E2* of the *BS* that will *existentially* satisfy the AR.

Threat analysis Using Abuse Frames

- **Scope the problem and identify the subproblems**
  - Describe the security concerns on the functionality to be achieved in each problem frame diagram.
- **Identify the threats and constructing abuse frames**
  - Identify the anti-requirements.
- **Identify security vulnerabilities**
  - Describe the domain properties.
- **Address security vulnerabilities**
  - New security requirements?
- **Iterate**

Abuse Frame Classes (Patterns)

- **Interception**
- **Modification**
- **Behavioural**

Patterns of attack:

- Embody known attack possibilities
- Help to reveal composition possibilities

Other security patterns

- Security patterns of base systems
  - Can embody avoidance of known failures
  - E.g., Single Point of Entry pattern
- General patterns of base systems
  - Help to focus on phenomena
  - Mandate explicit consideration of alphabets

Thank you, Michael Jackson, from …

- Leonor Barroca
- John Brier
- David Bush
- Jon Hall
- Charles Haley
- Robin Laney
- Zhi Li
- Armstrong Nhlabatsi
- Bashar Nuseibeh
- Jonathan Moffett
- Marian Petre
- Lucia Rapanotti
- Mohammed Salifu
- Pete Thomas
- Thein Than Tun
- Yijun Yu
- …

OU Research in Problem Frames

- Architecture Frames (AFrames)
  - Rapanotti et al.
- Composition Frames
  - Laney et al
- Change Frames
  - Brier et al.
- Coordination Frames
  - Barroca et al
- Abuse Frames
  - Lin et al.