# Safety & Security in Computer Based Systems

Brian Gladman

# Talk Outline

- Compare and contrast the approach to safety and security in computer based systems
- Consider the impact of politics on the provision of  security in commercial market computer systems
- Consider security models for UK government systems handling citizen owned data

# Computer Systems Safety Examples

- Nuclear reactor monitoring & control
- Aircraft flight control
- Air traffic control
- Engine management & control
- Railway signalling
- Road traffic management
- Weapons fusing, arming & control
- Nuclear weapons command & control

# Characteristics of the Safety Domain

- The safety requirement almost always dominates other requirements
- A mostly open community in which experience (good & bad) is shared
- No significant opposition to safety attainment
- Safety certification ‘owned’ by the community and based on best current practice

# Characteristics of the Security Domain

- Government (NSA, GCHQ) opposition to security technology deployment in open market systems
- Little sharing of practical experience, especially of security failures
- Radically different security models (open & closed) promoted by different ‘political’ interest groups
- Security certification  based on ideal requirements rather than best current practice; ‘imposed’ by minority (defence) customers in an attempt to drive the  market

# Computer Security & The Civil Market

- Security historically of low priority but large IT suppliers are now showing an increased interest in providing security
- The Trusted Computing Group (was TCPA) is now leading an industry effort to improve computer systems security
- But is this a genuine effort to improve end user security or an attempt to support the licensing & digital rights management (DRM) needs of content and software suppliers?
- Putting high grade security capabilities in the hands of novice end users could provide ideal exploitable capabilities for those with nefarious objectives (crypto viruses, bot-nets, …)
- There are hence serious concerns among technologists that improved computer security won’t serve end user interests (but I don’t think this will stop these developments)

# Security Models

- The Closed Systems Security Model:
  - Security through obscurity
  - Historically almost universal within UK government (even when inappropriate)
  - Widely used by many commercial suppliers
- The Open Systems Security Model:
  - Open publication of specifications, design & implementation
  - Applied by the open source community and some commercial companies
- Technical analysis of these models is limited but what exists suggests that one is not necessarily better than the other

# Government IT Systems That Process Citizen Owned Information

- Principle:
  - The person (or persons) who carry the risks of security failures (i.e. the citizens)  have the right to determine for themselves whether the security provided is sufficient for their purposes
- The Closed Security Model might assist security but it might equally hide insecurity --- citizens have no way of knowing which applies
- Hence only the Open Security Model meets the above principle
- While the government applies the closed security model in its citizen facing IT systems, we cannot have confidence in their security
- Will the Home Office openly publish full details of the procedural, technical and operational mechanisms that will be used to protect seized keys BEFORE the GAK provisions are bought into force?

# Security, Functionality and Scale

- The more people who share a secret the less likely it is to remain secret
- The promotion of data sharing across systems is hence in direct conflict with good security and privacy principles
- Government IT systems holding citizen owned data should hold only that data needed to meet their immediate purpose
- At the current ‘state of the art’ such computer systems can only be built to provide two of the following three properties:
  - Security
  - Functionality
  - Scale
- Security will remain elusive while the government insists that it must have all three properties in such systems

# My Conclusions

- The security community lacks cohesion and is driven by conflicting political and economic forces that hamper technical developments
- Government information systems holding data on which the safety,  security and privacy of individual citizens may depend must adopt the Open Security Model
- Now (and for the foreseeable future) such systems can provide only two of the three properties of scale, functionality & security
- Traditionally security has lost out but we now need to reduce either scale or functionality in order to provide effective safety, security and privacy
- In particular, limiting systems functionality will be essential if we are to achieve effective, affordable and reasonably secure citizen facing government IT systems