Disclaimers

- Personal views of authors
- Not necessarily official view of UK Ministry of Defence
- Experiences of a major user of evaluated products, not a product vendor
- Part of our experience relates to ITSEC, not CC
- We only distinguish ITSEC from CC where it mattered to us
Logistics Information Technology System (LITS)

Royal Air Force (RAF) Aircraft Engineering and Supply Functions
- also (at times) office automation and communications

Largest operational IT system in UK forces
- By an order of magnitude
Development history

- Development started 1990
- Initial operational capability 1996
- Development completed 2000
  - Development completed on time, under budget
- Final activity was Security Accreditation on 4th January 2001
  - Based on CESG System Certification S112 dated 30th November 2000
Real world

- In the real world, development work did not stop in 2000
- Reaccredited following major enhancements/changes
  - 7 May 2003
  - 2 July 2007
  - 15 April 2008
  - 1 June 2009
- Future will depend on UK Government’s current Strategic Defence and Security Review
Original vision

- Integrated air logistics approach paid for by efficiency savings
- 15,000 to 20,000 dedicated terminals worldwide with up to 25,000 users
- 24/7 service to users
- Better quality data, delivered more quickly
Today’s system

- Air Logistics Data Centre (ALDC)
- Integrated services
- 300 dedicated workstations; 6,000 direct users; multiple data feeds and sources
- Flexible real-time delivery of real-time data
- Major component of tri-service defence equipment and supply capability
User architecture

- Example: Asset Life Update
- AM Application component AT3610C
  - Functionality accepted 1995
  - Functionality unchanged today
- Implementations have changed, logic has not
System architecture

Key concepts in 1990:
- Distributed data and processing across 70+ locations
- Consistency based on OSI standards
- Networked communications based on X.25 packet switching
- Client/server with server nodes on the majority of RAF sites
- Intelligent terminals implementing secure protocols

Key concepts in 2010:
- Centralised data store
- Commercial product driven
- TCP/IP
- Centralised web servers and data feeds
- Access by secure browser session from any suitable MOD PC
Architectures in practice

In the Real World, architectures change

- First delivered architecture: dumb UNIX clients to local/remote UNIX servers
- Replaced by: Windows clients to local Windows servers to local/remote UNIX database servers
- Replaced by: Windows Citrix clients to local Windows Citrix/application servers to local/remote UNIX database servers
- Replaced by: Windows GUI Application to local Windows Citrix/application servers to local/remote UNIX database servers
- Replaced by: Vanilla Browser to remote Web Servers to application servers to virtualised database servers
- Augmented by: Data feed to XML proxy to application servers to virtualised database servers
LESSON ONE

Evaluation Strategies Matter
RAF originally contracted for a certified system

Obtaining certification was the Prime System Integrator (PSI)’s problem

First live deployment in 1996 was excused formal evaluation

- Experimental
- Small user community
- Low-risk functionality
- Limited lifetime

Evaluation work by CLEF did proceed in parallel but was always playing catch-up

PSI’s problem became our problem
API Review

- November 1997: Three initial system releases had shown that our agreed development strategy was ineffective
  - Evaluation lag was a minor problem compared to other issues
- UNIX was a dead-end for client platforms (primarily training costs, also stability issues)
- The users could never specify what they wanted until they had something that was not quite right
- Decision to change platform and delivery strategy
  - NT
  - No “big bang” deliveries, incremental packaging instead
- Evaluation had to fit in with this new approach
Evaluation strategy

- Evaluation strategy had always been flexible
  - *Had accommodated a change of DBMS without major upset*

- But suddenly a lot of completed evaluation documentation became irrelevant
  - *And a small proportion became very important in demonstrating that the new architecture could be secure*

- Some of the security functionality was built into applications
  - *Actually, application libraries*
  - *Stable, unchanged, already working*

- Other security functional requirements were unchanged but would be implemented by different COTS products
Pace of change

- During the late 1990s there were new system releases every three months.
- Under the UK ITSEC scheme, our system evaluation required a stable platform for at least 4 months to reach a certifiable state.
- It did not seem sensible to certify a system release that had already been replaced in live operation.
- However, some ITSEC evaluation activities did give useful results to the developers and assurance to management.
  - These activities were generally documentation-light.
Approval to operate

- CESG cautiously willing to accept product evaluation results in a system context without a system evaluation
- MOD cautiously willing to accept our application-level security as proven in practice
- Not enough confidence for formal approval
- Agreed decision to defer system evaluation until “development complete”
  - Approval to operate based on alternative assurances
  - Risk based arguments
  - Supported by independent vulnerability testing
System evaluation

- System evaluation (against ITSEC) performed in 2000
- All key LITS security products were already evaluated
  - CC was coming into use, but all infrastructure products used by LITS at that time were certified against ITSEC
- System evaluation assumed relevant evaluated products security functionality was implemented correctly
  - Security Target coverage was almost but not quite complete
- System was kept stable whilst evaluation work completed, written up and certified
Evaluation results

- Evaluation results were certifiable by CESG
- ITSEC Certificate issued
- System formally accredited in January 2001
- Very minor conditions and reservations
- Certification conditions were violated immediately
  - *NT clients and servers patched!*
- Recognition within LITS that the six month pause in development work in 2000 could never be repeated
New evaluation strategy

- Application level security functionality would have to be re-evaluated if changed
  - But evaluation not required if re-implemented and shown by testing to be functionally equivalent

- Product security functionality would not have to be re-evaluated in three cases:
  - Security functionality expressly covered by a valid product certification
  - Manufacturer patches to certified products
  - Approved later releases of certified products undergoing evaluation
Impact of new philosophy

- Application level functionality has never been a problem
  - If it’s a pure reimplementation, it must produce identical results to before
  - For all test suites, including the evaluation suite

- Patching certified products
  - Frequency and urgency of patching escalated after 2000
  - Responsible for some of security’s most pressing and difficult practical problems
  - Patching is more stable today than a few years ago
  - But always our most unsatisfactory evaluation risk
Later versions of products

- Important concession initially
  - Re-evaluation often slow, and different labs/targets often made it difficult to compare evaluation results

- Over time, the commitment by vendors to evaluation of new versions has become standard and customary

- Leading to inherent confidence that new versions will pass evaluation

- Under CC, compliance with standard Protection Profiles usually trivialises our reassessment
  - Major efficiency saving
  - We know which bits of CAPP we rely upon!
New products

Prior to 2000, key infrastructure products often lacked essential security functionality
- Let alone certified security functionality

Add-on security packages introduced their own integration vulnerabilities

In 2000, lack of alternative certified products was a major disincentive to changing infrastructure architectures
- ITSEC certified products were rarely directly comparable
The first time a new infrastructure product was shown from its Security Target to have all the security functionality we needed was 2004 (and from a CC target).

By 2006, we expected to find the information in the CC Target.

And for the Target to be available.

We now expect all infrastructure products with security functionality to be CC certified by the time LITS has completed a related development project.

Although, our development cycle is longer than in 2000, because of the inertia inherent from our user estate.
LESSON TWO

Evaluation Costs
Costs

- The cost of security evaluation was included in LITS costs from the start
- We spent money on early evaluation activities that was nugatory
  - Of course, we didn’t know in advance which bits would be vital in enabling us to change architectures and which would be irrelevant
- The actual cost to first certification was substantially lower than expected
  - The growth in certified COTS products was not anticipated
  - We over-estimated our dependence on secure applications
Operational security costs

- Maintaining an accredited system costs money
  - Including avoiding further security evaluations
- Initially, choosing certified products limited our product choice
  - Now rarely true, we find our preferred infrastructure products are either security certified or are not security relevant
- Still some compromises
  - Example: limiting remote management
- Certification maintenance costs are not popular
  - Fixing flaws that are found is even less so
- Maintaining application security has always been a minimal cost, and a non-issue
LESSON THREE

Evaluation cannot prove anything
Evaluation as a tool

- Product certification has no credibility with our infrastructure architects
  - *If it meant anything, why so many patches?*

- Architectural arguments convince
  - *No data flow, no data compromise*

- So does independent testing
  - *Whether as part of an evaluation or otherwise*
LESSON FOUR

Evaluation and Government Policy
UK Security Evaluation Policy

- UK Government Policy on security evaluation has been through multiple upheavals
- During LITS development, system evaluation was mandatory
- Now, system evaluation and use of evaluated products is only a recommendation
  - Risk assessment and risk management are mandatory
  - Evaluation recommended to help counter some risks
- LITS is likely to avoid security products not submitted for evaluation on risk grounds
  - Product evaluation is customary, why would a vendor not do it?
At one time UK Government policy specified an algorithm to calculate minimum CC EALs for products implementing security barriers

- The results of the relevant algorithm were achievable and intuitively reasonable when applied to LITS
- The algorithm could be subverted

Under current policy, recommended EALs are architecture independent

- Difficult for our infrastructure architects to accept
- Difficult for our financiers to ignore
Conclusions

- Evaluation and certification has always been an important part of our security strategy
- System evaluation was unrealistic
- Certified products give us assurance at little cost (to us)
- Product certification using CC has enabled us to change infrastructure components without changing our security requirements
- Our developers understand the need for a secure system but see little benefit from evaluation
- The ITSEC/CC evaluation and certification model was, and remains, unrealistic
Questions?
USING THE COMMON CRITERIA IN PRACTICE

Mike Nash
Gamma Secure Systems Limited
mnash@gammassl.co.uk

John Ford
Ministry of Defence