IMPLEMENTING SECURITY POLICY IN A LARGE DEFENCE PROCUREMENT[1]

M. J. Nash* and Wg Cdr R. J. Kennett RAF**

***Gamma Secure Systems Limited**
Diamond House, 149 Frimley Road, Camberley, Surrey, GU15 2PS, United Kingdom

****Headquarters Logistics Command**
Royal Air Force Brampton, Huntingdon, Cambs PE18 8QL, United Kingdom

ABSTRACT

At the 1993 ACSAC conference a previous paper was presented describing the security policy developed for a large, integrated defence procurement, the United Kingdom Royal Air Force Logistics Information Technology System (LITS). The current paper describes some of the practical difficulties encountered in implementing that security policy during subsequent stages of the LITS system development. Issues discussed include the difficulties of "future proofing" a security infrastructure in the real world where user security requirements can and do change in ways that were not anticipated, the tension between security policy requirements and cost effective security solutions, and the conflict between labelling data and the use of untrusted applications.

INTRODUCTION

The Royal Air Force (RAF) Logistics Information Technology System (LITS) is a ten year United Kingdom (UK) procurement programme to provide the RAF with a fully integrated Information Technology (IT) system covering its Supply and Engineering functions. Some of the information held is protectively marked (current UK terminology for what is commonly called classified information, but also including Unclassified But Sensitive - in the remainder of this paper we use classified as the more commonly familiar term). A previous paper [1], presented at the 1993 Computer Security Applications Conference, described the security policy developed and the IT security problems encountered within the LITS procurement, up to the point where a Requirements Study of the first tranche (ie. group) of applications had been completed, and a selection process for a contractor to implement the system, a Prime Systems Integrator (PSI), had been initiated. This paper presents progress since that time, covering completion of the requirements studies and appointment of the PSI, through initial system implementation, and up to initial delivery to the RAF as the customer. Related papers [2,3] have looked at the management and contracting problems associated with LITS Information Security.

The LITS procurement is managed by the RAF Directorate of Logistics Information Systems (DLIS(RAF)). This combined team of RAF personnel and civil servant procurement and contracts specialists, supported by additional contractor management and technical support consultants, is based at the PSI's major development location. IT security within the DLIS(RAF) team is the responsibility of the LITS Security Policy Branch, which is headed by an RAF Wing Commander (equivalent to a Lieutenant Colonel) and has a further staff of a Squadron Leader (equivalent to a Major) and two full-time and one part-time consultants.

THE LITS MISSION

The LITS development has taken place in a period of significant and fundamental change to the planning and organisation of the entire Royal Air Force. The need for an integrated RAF logistics system was first

[1] PUBLISHED AT THE TWELFTH ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, SAN DIEGO, CALIFORNIA, 9-13 DECEMBER 1996. (pp. 15-23)
© British Crown Copyright / MOD 1996. Reproduced with the permission of the Controller of Her Majesty's Stationery Office under Ministry of Defence Crown Copyright Web Site License WSL043. PERMITTED USES: This material may be accessed and downloaded onto electronic, magnetic, optical or similar storage media, provided that such activities are for private research, study or in-house use only. RESTRICTED USES: This material must not be copied, distributed, published or sold without the permission of the Controller of HMSO.

identified in the mid-1980s. At that time the world situation was very different. When LITS was conceived, the primary function of the RAF was to protect the United Kingdom and its allies from air attack by Warsaw Pact forces, as part of a flexible NATO response to aggression within a northern European context. The existing supply and engineering systems had been developed to match this mission, where assets were primarily serviced and maintained in peacetime from established bases in Britain and West Germany and hostile operations were of relatively short duration and mounted from the established bases.

This scenario and mission is no longer realistic. The RAF's forward operational presence in Germany has been substantially reduced and will terminate before the year 2000. On the other hand, the Gulf War and support to UN operations in the former Yugoslavia have shown the need for the RAF to be able to sustain prolonged overseas operations in an unpredictable, flexible and responsive manner. The RAF needs to be able to participate in rapid reaction forces, flexible joint or multi-national operations, and extended remote deployments. This has changed the requirements for logistics support. Engineering and supply functions may be required in remote locations for extended periods, far away from the remaining established bases. In addition, there have been fundamental changes to UK national security philosophy. Both of these factors have had a major impact on LITS security policy.

THE PSI SELECTION PROCESS

In the previous paper [1], we described the process whereby a Full Study Contractor (FSC) was appointed to prepare a comprehensive requirements specification for LITS Tranche 1, the first group of LITS business applications to be implemented. This included the preparation of a Tranche 1 System Security Policy (SSP), the key IT security requirements document required under UK Information Security doctrine as set out by the Communications-Electronics Security Group (CESG), the UK national technical authority for IT security [4, 5]. The next major contracting activity was to select a PSI, a development and implementation contractor to supply a turn-key system satisfying the requirements specification, including the security requirements in the SSP.

The LITS PSI was selected using the open European Union procurement process used for all large UK Government purchases. This process started with the issue of a Statement of Programme Requirement. Approximately 110 companies expressed an interest, of which 64 were subjected to a pre-qualification process covering corporate capability and capacity, relevant experience, and management practices. Included within this experience assessment was previous experience of the UK security evaluation and certification process, although relevant experience elsewhere, such as with the US DOD National Computer Security Center or with the German Evaluation and Certification Scheme, was acceptable as equivalent.

After this pre-qualification process, a Statement of Requirement (SOR) was issued to 10 qualified companies and groups of companies, providing a broad statement of the LITS PSI requirement. The SOR contained a brief section on IT security, indicating the need for the system to be evaluated against the European Information Technology Security Evaluation Criteria (ITSEC) [6]. Seven companies responded to the SOR, from which four were subsequently selected to bid against a detailed Operational Requirement (OR), prepared by DLIS(RAF) and the FSC. The OR required the PSI to implement the first of three tranches of LITS applications, based on the detailed requirements specification produced by the FSC. In addition, the PSI had to propose and provide a supportive technical infrastructure that could subsequently be extended to support the subsequent tranches of applications. The FSC was contracted to prepare the requirements specification of these two further tranches in parallel with the process of PSI selection.

The security requirements for the infrastructure and Tranche 1 were contained in the Tranche 1 SSP prepared by the FSC. However, the main contracting document, the OR, contained a limited number of additional security requirements relating to the infrastructure that were not essential to support Tranche 1 business functions. These additional requirements were likely to have a significant impact on possible technical solutions. It was considered that without these additions, a bidder could propose a low-cost solution that met the requirements for Tranche 1, but which would then be impossible or at best extremely difficult to extend to meet known security requirements for later tranches. These additions fell into two major areas: constraining user access to data outside their particular business area, and data labelling.

CONES OF VISIBILITY

One major long-term objective of the integrated LITS system was to enable users to have greater ease and flexibility in obtaining the data needed to perform their work functions efficiently and effectively, and in particular to obtain information about related logistics assets held by other organisations or at other locations. There are security problems, however, in giving all users the ability to see a "big picture". An RAF-wide view of the status of a particular type of aircraft or equipment may well be more sensitive than the status of a single item. Other types of aggregated views or summary analyses give similar problems.

The possible increase in classification of aggregated data over its constituent elements is a potential problem for any system storing large quantities of data. In a complex database, it is difficult to determine the correct classification of arbitrary views purely from the classification of their constituent elements. The conservative approach to such views would classify them as having the highest possible classification. In most cases, this will be overly restrictive and cause operational inefficiency and user access problems. More seriously, if data update is permitted within such global views, correct grading of the updated constituent data is very difficult to determine, leading to unnecessary escalation of classification levels over time.

Representatives from the user areas confirmed to us that these were real problems. Fortunately, they were also able to come up with a method of solution based on a user understanding of actual data usage. They called this solution "cones of visibility". For each LITS user role, the user representatives defined a conceptual cone of data, within which the users could perform data analysis without risk of escalating the classification of the overall results. These cones permitted access to all the non-local data relevant to performing the relevant job function under normal circumstances. In some cases these cones were geographically based, in others weapon system or function based. However, in all cases the user representatives devised rules to keep queries within the permitted cone. We imposed the cones concept as a mandatory requirement within the OR.

DATA LABELLING

A second major area of concern was the correct marking of output data, whether on hard copy, or passed electronically to other systems. Any logistics system, however integrated and widespread, generates large quantities of paper. Particularly in Tranche 2, it was known that there would be a requirement for hard-copy labelling of printed output according to content. Without internal trustworthy classification labels, all printed output would have to be visibly marked at a conservative system-high level. This was seen as a huge usability and management problem as it was expected that up to 90 per cent of output would actually be unclassified. Downgrading printed output would require access to persons of sufficient rank or grade to authorise the downgrading, and would generate problems of storage and disposal of over-marked output.

It was also anticipated that there would be Tranche 2 business requirements to exchange data with external IT systems supporting labelled data. This would be simpler if LITS could automatically supply accurate labels when transmitting data to such systems.

It was therefore decided to impose an OR requirement for MAC-type labels on data, which could be then used by output functions to apply an accurate label on output, rather than forcing a conservative system-high operating level label. The degree and form of labelling was not mandated.

The Tranche 1 SSP without the cones of visibility and labelling requirements might have provided adequate security for Tranche 1 applications. However, it was strongly believed that applications in future tranches could not be implemented without them. It was therefore decided by the LITS Security Policy Branch that it was necessary to mandate their inclusion within the initial infrastructure, as a form of "future proofing" to ensure suitability for the later tranches.

The Tranche 1 SSP and the OR were requirements specifications, they did not impose a technical architecture or a security architecture. It was left open to the PSI bidders to propose architectures that they believed could satisfy the requirements in the most cost-effective way possible. In the two areas where non-functional requirements were mandated, the method of solution was still left open.

A Multi-Level Secure (MLS) architectural solution could have met all security requirements, but multi-level operation was not necessary to support the identified business functions as defined in the OR, and was consequently not mandated as the technical approach to be followed. We did not prohibit MLS solutions being proposed.

RESPONSES TO THE OR

All four bidders against the OR offered similar security architectures. In each case, the bidder proposed a geographically distributed client-server technical solution, with servers located at all major RAF sites and a distributed database spread across many servers.

All bidders proposed two logical networks, running at System High Restricted and System High Secret respectively (Restricted is a UK hierarchical security classification level, between Unclassified and Confidential). These logical networks are referred to within the LITS Programme as “tiers”. Every client and server would be part of one of these two tiers. Each site was to have a pair of Local Area Networks (LANs) running Restricted High and Secret High. The Restricted High LANs were to be linked by one Wide Area Network (WAN), the Secret High LANs by a different and distinct WAN. Inter-site traffic was to pass exclusively from servers to servers on the same tier - with the single exception that some very small RAF sites might have only client terminals, linked by the WAN to servers on a fixed larger site, and treated architecturally as remote local clients.

Each bidder proposed that the two system high tiers would be linked via a limited number of inter-tier secure gateways, that would act as Guard processors on the inter-tier traffic (ie. “firewalls”). There would also be links to other RAF and UK Ministry of Defence systems using a variety of means, from batch magnetic tape transfer to on-line real-time electronic links protected by other secure gateways. A typical architecture is shown in Figure 1.

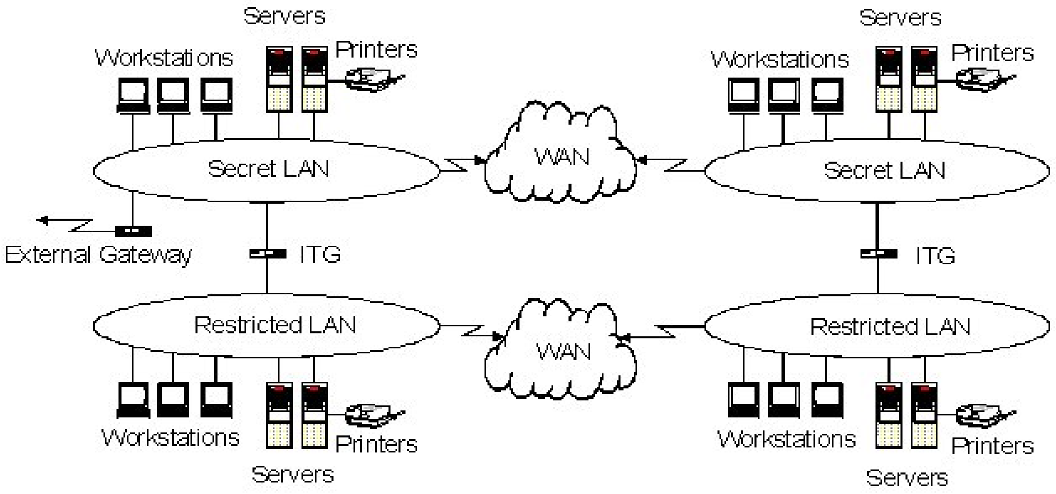

Figure 1 - A Typical Architecture

All bidders offered processors - servers, clients, gateways - with operating systems that had already been security evaluated, or were currently undergoing evaluation, and hence would be product certified at the required assurance level for their LITS use before live operation started. All data was to be stored within a distributed, replicated relational database, accessed through a Relational Database Management System (RDBMS), also product certified at the required assurance level prior to live LITS use. All application code was to be treated as untrusted, and based for the most part on existing Commercial Off The Shelf (COTS) packages.

At the time these proposals were submitted, the Tranche 1 SSP stated that all the potential system users were either cleared to Restricted, or to Secret. The vast majority of logistics data is classified as either Unclassified, Unclassified But Sensitive (UBS), or Restricted. Under the UK national security rules applicable at the time, UBS had to be protected as if classified Restricted. Given these business characteristics, the similarities in the four proposed architectures are perhaps not surprising. As already stated, the business requirement could probably also have been met by a single multi-level secure network approach, for example using Compartmented Mode Workstations (CMWs) for client terminals. However, with an envisaged total of perhaps 35,000 users, of which less than five per cent would ever need to process data above Restricted, this seems to have been discounted on cost-effectiveness grounds by all four bidders.

The FSC had identified a third possible architectural solution, three tiers running at Unclassified, Restricted High and Secret High. This was also apparently unattractive as a technical solution. Although there were a number of unclassified business areas, no significant user community entitled only to work at the Unclassified level had been identified. Thus there would be few apparent benefits but probably significant additional hardware and maintenance costs associated with the provision of a third distinct tier. Again, such a solution was not offered by any of the bidders.

There were some significant architectural variations between the four bids, particularly with respect to inter-tier communication and external gateways. One bidder believed that with appropriate design, the information flow between tiers could be restricted to flow exclusively from Restricted High to Secret High: this greatly simplified the functionality of his inter-tier Guards. Another bidder proposed to combine the functions of an inter-tier Guard and a LITS to external system secure electronic gateway into a single generic Guard system linked to both tiers and the external systems. This offered the potential for savings in hardware costs by reducing the number of inter-system connections and architectural variations.

A short-listing exercise reduced the four OR bidders down to a final short-list of two that were invited to prepare final costed tenders. From a security viewpoint, although we could rank the four bidders in a order of preference, the difference from first to last was not significant. We believed that all four bidders would have some problems with their proposed security solutions, but none of the problems provided a major differentiator, and we believed that all the problems could be overcome. Thus IT security did not play a major role in the short-listing.

SYSTEM PROCUREMENT STUDIES

As a risk reduction exercise before the PSI contract was awarded, the two surviving bidders were paid to perform a number of studies, called System Procurement Studies (SPSs), covering critical aspects of each of their proposed technical solutions. It was felt by DLIS(RAF) that these studies would make it easier to compare the two proposed approaches, and would enable a more informed view to be taken of the perceived areas of high risk. For both bidders, IT security featured in two of the study areas. Technical architecture studies expanded the overall technical design solutions put forward by the two bidders, and in both cases produced further, more detailed, security architecture specifications. In separate IT security studies, both short-listed bidders were paid to demonstrate the ability of their security architecture to satisfy the System Security Policy for Tranche 1 and the additional OR security requirements. This was achieved by getting each bidder to develop a System Electronic Information System Policy (SEISP) based on the Tranche 1 SSP and their proposed security architecture. The SEISP is a more detailed level of IT security documentation, following on from the SSP, and required under the standard UK approach (see [7]). It contains an overview of the security architecture of the system, and then defines how those security requirements that are to be satisfied by technical means will be implemented as trusted hardware or software measures within the system. The development of the SEISPs thus provided an elegant way to validate the security architectures being proposed in the technical architecture studies, and then to compare the two approaches to technical security measures.

Both remaining bidders completed these studies without difficulty, and were able to deliver acceptable detailed security architectures and SEISPs. One unexpected finding from this work was that a number of other study areas, which had appeared to have little IT security relevance, produced results which had significant implications for the security architecture. Often the relevant security team were unaware of these implications. For example, one bidder had difficulties with his proposed data migration approach from the existing mainframe-based supply system, due to the need for reverse data transfer back from LITS to the mainframe system over a period where some locations had migrated to LITS whilst other locations were still connected only to the mainframe system. This could only be supported by a major last-minute modification to the associated security architecture.

With hindsight, the SPS process was very helpful in assessing the successful implementation of the LITS security policy. It provided the LITS Security Policy Branch with an opportunity to work with the two security teams and assess their strengths and weaknesses, before a final selection decision was made. We were able to get both teams to concentrate on the weak areas in their security proposals, before full development work started and poor decisions became cast in stone. The security architecture documents were of genuine practical use, the SEISPs less so. Normally, when following CESG guidance, the SEISP is not produced until after development contract award. In a study-only phase, the necessary level of technical detail was not always available, and both SEISPs were somewhat incomplete in consequence.

Nevertheless, we were able to advise that both bidders were capable of meeting the security requirements, and could offer a secure solution.

TRUSTED GATEWAYS

The SPS process exposed one major problem, which affected both bidders equally. This concerned the assurance level and functionality required for the inter-tier and external gateways. Guidance [5] on appropriate assurance levels for UK Government systems is not designed for application to gateway Guards or firewalls. Both system designs were such that remote log-on (eg. rlogin), user formulated remote SQL enquiries and user initiated file transfer were not needed to support any cross-tier business processes. The Guards would connect servers on different tiers or systems, with the traffic passing through them restricted to server-to-server, low-level database table access and update requests and replies. This made the Guard functionality straight forward. However, the normal factors used to determine a minimum required assurance level (such as number of users, clearance/classification distance) became almost meaningless in this context. Both security teams found it difficult to construct a meaningful assurance level assessment according to [5], and in consequence, the LITS Security Policy Branch took the lead to construct an interpretation of [5] that was valid for both architectures and which could then be used to prepare an assurance level derivation that could be jointly presented to CESG and the system accreditor.

In the end, we determined that the only way we could sensibly apply [5] to this type of gateway was to identify all the types of failure within a server (whether by deliberate hacking or system error) that could initiate an improper data flow across a gateway, and then identify where such a flow would be detected and blocked. The most interesting case was that of an error causing highly classified data to be incorrectly labelled before being transmitted to the gateway. The gateway Guard could implement a classification-based security policy to block data flows above Restricted from the Secret High tier. However, The Guard could have no independent means of establishing the correct classification of internal RDBMS data. It would have to trust the label presented by the RDBMS server. If this label was in error, a Guard could pass information from the Secret tier to the Restricted tier that was actually classified above Restricted. However, the RDBMS database designs were such that on the Restricted tier, either the table which the data was intended to update would not exist or the mislabelled data would fail a master key integrity check. This required that all SQL table inserts were locally generated, which fortunately correctly reflected the business requirements. Provided that we had sufficient assurance in the RDBMS running on the Restricted tier that in these circumstances the data would be destroyed on receipt, there was no way that a user of the Restricted tier could access it. Furthermore, there was a very low level of probability that a sequence of events creating such a mislabelled and misrouted message would occur in practice, either by accident or malicious intent, and of course such a major database processing error could then be alarmed and audited on receipt by the Restricted RDBMS server. Thus we were able to accept the proposed architectures.

Paradoxically, this meant that the Guard would not be trusted to enforce the flow control policy between the tiers in all possible circumstances. This would be done by the two RDBMS servers. The security function of the Guard would be to limit inter-tier traffic to legitimate routings, namely those between RDBMS servers. One architecture connected the Guards directly to the RDBMS servers, thus elegantly eliminating the possibility of network misrouting.

SYSTEM DEVELOPMENT

The PSI contract was awarded to a consortium headed by IBM (UK) Ltd in June 1995. At the time of preparation of this paper, the initial implementation of LITS - a subset of Tranche 1, limited to a few aircraft of a single type located at a single site - was in Factory Acceptance Testing.

As should be expected, there have been many minor difficulties in implementing our IT security policy, during the development phase. The PSI's strategic approach to supplying LITS is based on maximising the use of Commercial Off The Shelf (COTS) products, with the minimum of LITS-specific application development. For example, our major logistics package is already used by the South African Air Force. However, this inevitably means that the majority of application code is not security-aware and cannot easily be modified to make it so. This has led to many minor problems, primarily because it is difficult to provide security features within user transactions when security functionality is only implemented by the trusted components of the architecture.

In an ideal world, all the requirements documents relating to a large system development, including the SSP, would be fixed before the start of the development phase, and then not changed during implementation. This has not been possible within LITS. As in most large projects, the requirements specification has needed clarification and refinement. During development, the PSI has wanted to change the way certain security features are provided, resulting in changes to the definition of technical security measures in the SEISP. Both the SSP and SEISP have been through a number of iterations, requiring formal acceptance by the RAF since they are contractual documents.

THE SECRET TIER

During the development phase a number of security-related problems have been encountered that have been of more major significance.

The first of these problems concerned the size of the proposed Secret High tier. During the LITS strategy study in 1988, it had been identified that the data and outputs from some applications, primarily in the areas of weapons and fuels, were generally classified above Restricted. Other application areas, although based on logistics data that was generally Unclassified or Restricted, generated a limited number of reports, and dealt with limited instances of data items, that were classified Confidential or higher. As a rule of thumb, it was estimated that no more than ten per cent of IT processing would involve data classified above Restricted, although the actual ratio would be dependent on the application design and the system architecture. The FSC's requirement studies had not provided a more accurate estimate of this figure. Because of the need for the study work to remain solution-independent, this had been seen as unfortunate but necessary. In fact, it became highly significant.

One of the activities performed by both SPS bidders was to undertake a detailed site survey of an actual RAF base, one that was likely to be an early candidate to have LITS installed. These studies looked into the physical locations across the base where access to LITS applications would be required, so as to estimate accurately the number of terminals and printers needed. The two consortia looked at different sites. Both surveys produced an identical and unexpected result. There appeared to be no requirement, at least within areas addressed by Tranche 1 applications, for Secret tier terminals! A number of site-specific explanations relating to the nature of the two bases examined and the types of aircraft flown could be advanced to explain this result. In particular, the Tranche 1 applications did not include the weapons and fuels application groups that were known to have a substantial above Restricted component. However, later studies looking at other sites produced very similar results. Most Tranche 1 data that was classified Confidential or above turned out to be peripheral to the main business functions, and in many cases did not need to be held on the computer system as it was purely reference data.

In parallel, a wide-ranging review of UK national security philosophy was taking place. This review caused major changes to national policy. For example, the concept of Government UBS was abolished. Instead, classifications were generalised to become “protective markings”, containing a descriptor to explain why the material had to be protected if not for national security. The clearance procedures for personnel were also reformed, and the basic checks on all RAF and civil servants now permitted them access to Confidential material as well as Restricted. These reforms naturally had an impact on LITS. A review of RAF classification policy established that much of the weapons and fuels logistics data could now be treated much more in line with general stores items, and in consequence they were potentially over classified.

The PSI proposed an aggressive approach to these changes. No current business requirements were identified where the provision of Secret-level processing accessible across all LITS sites was essential to performing the logistics business mission. If there was no such global Secret-level processing, there would be no need for a global Secret tier. If there was no such global Secret tier, there did not appear to be a need for inter-tier gateways and for the increased complexity in system architecture and database design to permit data replication across such gateways. The PSI’s proposal was that there was now no demonstrated LITS requirement for an integrated system handling Secret or Confidential data. Any areas where Secret data was found to be needed could be handled through the provision of isolated “Islands of Secret Processing”. If a requirement to communicate between such islands at a level above Restricted was subsequently found, it could be addressed once its scope and nature was known. We are therefore likely to be provided with a single Restricted High tier infrastructure, with any processing above Restricted being dealt with on a case-by-case basis. This is a major change to the security architecture, although paradoxically the changes to the SSP and SEISP are relatively limited - the security requirements have not altered, only their proposed solution.

INTER-TIER DATA FLOWS

The PSI's technical architecture, as originally proposed, envisaged that some applications would need to be available on both tiers. Which tier should be used for a particular transaction would depend on factors such as aircraft type and operational mission. In these cases, when running on the Secret tier much of the data used would still be expected to be classified below Confidential and shared with users using the Restricted tier. Thus there would need to be significant data replication across the tiers, with update information passing between database servers through the inter-tier Guards. This was the only data flow through the Guards.

The PSI decided to suspend development of the generic inter-tier Guards. Although completing their design and development would probably not have been particularly difficult, their usefulness in the new architectural approach was limited. It was a classic example of where "design to meet a future possible general requirement" was forcing provision of complexity and functionality that might never be needed at the majority of sites. If in the future a particular site or a particular type of application requires Secret processing, it will still be provided, but with a case-by-case approach to identifying the necessary security measures.

DATA CLASSIFICATION AND LABELLING

An essential component of the LITS technical architecture is its large, replicated, distributed database of logistics data. In many ways, LITS is built around its database and the associated RDBMS. The security classification and handling of data within this database have given rise to a number of difficult technical challenges.

A naive approach to data classification states that the owner of data is responsible for setting its classification, and for amending it if needed. In the real world this can be unrealistic: the person that first occupied a particular job and set the classification policy has usually long since changed post. Data will normally be classified based on precedent - often with limited understanding or proper consideration of whether that precedent is still relevant and correct. In a transaction processing, relational database environment, even identifying who is the owner of a particular data element is difficult. A radical reassessment of classifications, such as that needed when moving to an integrated system like LITS, may be very difficult to obtain.

The introduction of multi-level relational database technology brings its own security problems. Within such a relational database, much of the sensitivity is contained in the relationship between data elements and not in the atomic elements themselves. Conventional labelling philosophies do not reflect this. To classify all user generated views of data at the most restrictive level for the whole RDBMS is unrealistic. However, it is equally naive to believe that correct classifications for user views can be derived from a simple content analysis. With the exception of a very few research initiatives, all current relational database management systems that support security classification do so through labels assigned at the row or table level. This causes problems when applications need to perform joins and select operations on rows to create the data views needed by their users. Any row labels generated automatically to go with such views are potentially overly conservative, being based on a "worst possible case" and, on update, may cause unnecessary upgrade of the row labels within the underlying tables. In turn this may cause a gradual escalation of the whole database contents towards the database-high level, unless automatic classification is overruled - which either requires the user to specify the correct label on a case-by-case basis, or for an application specific algorithm, built into the application code, to calculate it. In turn, this forces parts of the application code to be trusted, with additional costs of customisation and security evaluation.

Within the LITS development, those concerned with data classification found it difficult to establish consistent classification rules from observation of current systems and information obtained from current data owners. Often data seemed to be classified by the context in which it was used rather than on any inherent value or sensitivity. Furthermore, the changing nature of the security threat to RAF assets meant that many existing classifications were based on obsolete risk assessments and potentially higher than actually necessary. Attempts to obtain realistic classification policy through the normal liaison channels were not effective - what came back was what the existing rules were, rather than why they were that way. In the end, it was necessary to initiate a security classification study involving visits to the majority of user sites and user groups, in order to obtain a coherent and consistent view of data classifications.

One major objective of the OR decision to impose data labelling within the DBMS was to reduce the burden of downgrading printed output from the system high level at which it was printed to its correct level. If this could be done automatically based on internal DBMS labels, it would save an overbearing administrative burden. In theory, this can be achieved in a system high, secure RDBMS environment in one of two ways: either by using a F-B1 RDBMS and operating system with enforcement of the F-B1 Mandatory Access Control policy switched off in order to operate system high, or by using a F-C2 system with database labels added and the relevant processing evaluated as part of the system evaluation. It appears that both these approaches are technically feasible using major commercial RDBMS packages.

In practice, technical problems associated with the interaction between untrusted COTS applications and the trusted RDBMS and operating system made the design of such a labelling solution almost impossible. Using COTS, in general it is the application that collates the data and formats the output, whether this is for export to another system or printing. This collation and formatting is not controlled by the RDBMS or operating system as it is a new object that is being created. There are two possible options for the COTS application, either it can create and manipulate the trusted labels, or it cannot.

If the application can create or change labels, then it must be trustworthy or the value of the labels it generates is nullified. This means that it must be security evaluated. In the case of LITS, the COTS applications that were chosen had not previously been evaluated. Even if they had been, the necessary customisation to meet other LITS requirements would have nullified most of the value of any existing evaluation certificate. Thus either a large and therefore expensive system evaluation of application code would be required, or the labels would have to be treated as advisory only, negating their main value. If the application cannot handle labels, then having labels within the database serves no effective purpose since when data is extracted from the database by the application, the database labels are ignored when labelling output. Even if a suitable label manipulation Application Program Interface existed, the COTS product would need to be modified to call this function and the calling code either trusted or again the labels treated as advisory only. This is equally unacceptable.

In the end, we abandoned the approach to labelling output based on internal RDBMS labels. Other techniques, based for example on knowledge of the intended purpose of particular reports, were used instead. Unfortunately, this then removed much of the justification of the OR requirement to mandate labels on data.

CONCLUSIONS

As would be expected in a programme of this size, we have encountered many technical problems relating to IT security. It might be thought that the appointment of a PSI would release the LITS Security Policy Branch from responsibility for resolving security problems; in reality this is not the case. The role of the Air Force is changing, and in consequence the security environment and requirements are also changing. These changes are not under the control of the PSI.

The PSI has changed his technical solution in response to both changes in the RAF's requirements and also his developing understanding of the technical problems that he has to solve. DLIS(RAF) has to act as the point of interaction between the PSI and the rest of the Air Force. The Security Policy Branch must ensure not only that the PSI is not forced to implement obsolete policy requirements, but also that the PSI does not propose and implement changes to his technical solution that compromise the necessary and agreed security policy.

Our PSI has been responsive to change. However, contractual agreements for large projects make the agreement process for changes difficult and slow. Reaching agreement on changes, particularly fundamental changes of philosophy, has not always been easy. We have faced some harsh choices.

Within the UK Government approach to security within the large project lifecycle [7], the security requirements are documented in an SSP, a living document which is produced during project definition, but then updated and kept valid into live operation of the final system. This approach works well. Changes to the LITS SSP have had to be negotiated between the LITS Security Policy Branch and the PSI. It is in the PSI's interest to minimise changes to their proposed technical solution to meet changed policy requirements. Likewise, the LITS Security Policy Branch has to consider carefully changes to policy proposed by the PSI in order to facilitate secure implementation of the system. However, it has been possible to reach a mutually satisfactory agreement on most such issues.

The prospective demise of the Secret Tier is an area of uncertainty. Quite reasonably, the PSI is following an aggressive approach to a requirement which currently cannot be demonstrated or justified. Unfortunately, if in implementing later tranches, a requirement for integrated Secret-level processing is found, the infrastructure to support it may not exist.

The security policy of LITS had two components: the security requirements established by the Tranche 1 study work performed by the FSC, and additional architectural requirements imposed by DLIS(RAF) in an attempt to "future proof" the initial infrastructure so that it would be guaranteed to support the security requirements of later tranches. This attempt at "future proofing" has not been successful. Changes to national security rules, changes to the role of the RAF and unforeseen technical problems have caused much of this work to appear irrelevant. A probable moral is that designing for future requirements is always dangerous and may easily turn out to be wrong in practice.

A recent Air Officer Commanding RAF Logistics Command, Air Chief Marshal Sir Michael Alcock, wrote [9] "It behoves all of us to ensure that the Nation is provided with an affordable air force, which delivers air power in a cost-effective manner. My Command is deeply involved in this process, which presents a significant but fascinating management challenge." Implementing security policy within the LITS procurement is one aspect of this process, and has indeed provided many significant and fascinating challenges to resolve.

ACKNOWLEDGEMENTS

The authors would like to thank Sqn Ldr T Dowds RAF, Mr G Klein of Gamma and Mrs G Martin of CSC Europe who kindly commented on earlier drafts of this paper and provided valuable comments.

REFERENCES

[1] Security Policy in a Complex Logistics Procurement
M J Nash and R J Kennett, Proceedings Ninth Annual Computer Security Applications Conference, Orlando, Florida, 1993.

[2] Information Security in a Complex Defence System Procurement
R J Kennett and M J Nash, Proceedings Fifth Annual Canadian Computer Security Symposium, Ottawa, Canada, 1993.

[3] Managing Information Security in Large Defence Procurements: The Royal Air Force LITS Experience
R J Kennett and M J Nash, Proceedings Seventh Annual Canadian Computer Security Symposium, Ottawa, Canada, 1995.

[4] System Security Policies, CESG Infosec Memorandum No. 5
Communication-Electronics Security Group, Cheltenham, UK, Issue 3.0, July 1994.

[5] Minimum Computer Security Standards for HMG Information Handled by IT Systems, CESG Computer Security Memorandum No. 10
Communication-Electronics Security Group, Cheltenham, UK, Issue 2.1, November 1994.

[6] Information Technology Security Evaluation Criteria, ISBN 92-826-3004-8
Commission of the European Communities, Luxembourg, Version 1.2, June 1991.

[7] Infosec Policy Documentation - A Manager's Guide
Communication-Electronics Security Group, Cheltenham, UK, 1996.

[8] Description of Scheme, UKSP01
UK IT Security Evaluation and Certification Scheme, Cheltenham, UK, Issue 2.0, April 1994.

[9] The Royal Air Force 1995, Issue 7, Foreword
Royal Air Force Public Relations, Bracknell, UK, 1995.