



Security Impacts of New Technical Trends

Jiří Ludvík

Introduction

Over the last few years, large tracts of media space have been used to describe the dire state of current enterprise security. Even more has been used to describe various potential remedies for the perceived problems. People speak of defence-in-depth, de-perimeterisation, identity-centric solutions and so forth, the list of 'answers' seems endless.

The one area of agreement amongst the discontent is that not everything is currently right. However, the breadth of solutions proposed merely serves to demonstrate the lack of consensus over both the nature of the problem and which of the trends currently dogging enterprise security are significant.

Given this, it would be futile to simply add more fuel to the technical arguments. Instead this paper takes a business-based view. It examines trends capable of generating substantive economic drivers across industry, sufficient to turn the direction of technical security practice. It uses these to predict which security services will be brought into prominence. Finally it outlines actions security departments could take that are likely to provide the most effective solutions.

The author understands that effective security is not and cannot be a pure technology play. However for clarity in this article he intends to stand back from the process and procedural aspects of the discipline, limiting discussion just to the technology and those requirements which can be implemented as technical solutions.

Setting the Scene

Most of today's security is actually implemented using mechanisms provided by operating system or network technology. Application-level security does exist, but it is typically implemented in more fragmented manner. That was good enough for a while but is ceasing to be so; not because of security threats or vulnerabilities, but because of changes in business requirements, for example:

- Increased focus on business-to-business interactions. This often requires extension of internal systems to external customers and business partners;
- Integration of organisations and their information technology alongside business processes instead of around functional boundaries;
- Increased stringency of management controls to meet requirements of new regulatory regimes;
- Lowering the long-term cost of information technology.

ENTERPRISE SECURITY

Security Service	Application Layer Implementation	System and Network Layer Implementation
Authentication	Widespread use of password authentication, but due to technical limitations and interoperability issues, implementation often local to applications.	Widespread and consistent use of desktop user authentication across organisation or business unit. Selective use of two-factor authentication in high-risk areas.
Authorisation	Widespread but local to applications or application platform.	Widespread and consistent use of authorisation capabilities provided by operating system and networking technology.
Audit	Limited and selective use of application infrastructure capabilities. Support often poor, requires substantial configuration, or custom development. Implementation local to application.	Widespread but selective use. Network intrusion detection and platform logging typically used in high risk areas. Problems with efficiency of processing of captured data and acting upon it.
Secure Channel	Widespread and consistent for Internet web-based applications but rare for internal and legacy applications.	Widespread use of virtual private network capabilities provided by platform or networking technology.
Platform Integrity	Limited and selective use of application hardening in high-risk areas.	Widespread and consistent use of firewall, anti-virus; selective use of platform hardening in high-risk areas.

Table 1 – Application and Infrastructure Security Practice

The fundamentals of the response to these new requirements will inevitably include:

- Increasing the use of application-level security mechanisms to complement system and network security;
- Developing and using common components used consistently across the enterprise to increase consistency and efficiency of authentication, authorisation and audit in a manner integrated with the overall architecture;
- Identifying the right set of technical and architecture security standards and making sure they are used.

To achieve this, security departments need to upgrade their capability and re-focus their activities, aligning them with enterprise architecture and system development processes. Payoff for those who manage this is an opportunity to fix some old problems and avoid other fundamental future ones.

Current Technical Security Practice

These new trends are challenging the core activities traditionally carried out by security departments. Therefore, to understand their impact, it is useful to stop to reflect on what we do, to help understand why we do it.

As the content of security standards such as BS7799 or the Common Criteria Protection Profiles suggest, a large part of today's technical security is implemented using technologies for authentication, authorisation, audit, secure channels and platform integrity protection services either within the infrastructure platform, or as part of applications.

Obviously, the selection of controls to provide comprehensive protection should be wider. However, it can be argued that it makes sense to pay special attention to a select few: those that implement foundational security mechanisms, have the biggest impact on users or are the most expensive. Once implemented, it is likely the organisation adopting these technologies will have to rely on protection provided by them for one or more software generation upgrade cycles. Therefore decisions about their implementation cannot be taken lightly.

As was stated earlier, most of today's 'security' is actually focussed on the implementation of security services by operating system or network technology. Although the importance of security controls in business logic and application infrastructure is accepted, there is much less attention paid to it by both internal security departments and the industry press.

It is quite telling to examine quantitative and qualitative aspects of implementations – to look

at how they are implemented based on anecdotal evidence. This was gathered whilst working for approximately 10 medium to large organisations across manufacturing, services and government sectors. As Table 1 summarises, the use of system and network security measures across these organisations is widespread and baseline infrastructure security measures are generally implemented in a consistent and integrated manner. What stands out in comparison to system and network security, is how selective, inconsistent and localised, implementations of application security measures are.

Yesterday's Business

Which and how security mechanisms are implemented depends on two classes of requirements: business-based security requirements for granting and controlling access to sensitive data and regulatory, audit and control requirements. These are generally well known and documented in general, industry or country-specific, codes of practice and standards.

Yet although widely documented, most practitioners would point out that adopting such guidance is no guarantee that the result is free of issues. Even those companies implementing baseline security codes of practice, can still suffer from problems, such as,

- Poor usability, due to multiple user accounts and credentials;
- Increased operating costs, due to the need to support multiple disparate systems, the need the use skilled resources for routine work, or the cost of password reset helpdesk activities;
- Poor service levels caused by the lack of centralised management and hence misaligned processes involving a number of operational support groups and systems;
- Insufficient ability to identify and react to security incidents due to disparate and inaccessible audit logs;
- Insufficient flexibility to support business change, due mainly to the complexity of the infrastructure and its static nature;
- Vulnerability due to the low implementation quality of fragmented security mechanisms or their decentralised management.

The frequency with which these problems arise implies that they are essentially risks that have been deemed acceptable by management against the backdrop of constraints that security is operating against, such as:

- Enterprise off-the-shelf software that does not have sufficient capabilities to address the above issues easily;

- Constraints of the typical security budget – traditionally this has been 1-4% of the overall IT budget (and the need to prioritise its use).

In summary, it can be said that existing technical security solutions did respond to yesterday's business requirements, mainly because expectations were low and the cost of solutions to meet higher expectations was high. Although they were leaving a trail of issues behind them, these were deemed to be 'acceptable' risks.

Good Enough for Tomorrow?

It can be argued that changes in business priorities and the improving capabilities of security products mean that technical solutions which were good enough yesterday are less acceptable today and will be even less so tomorrow. There are several reasons for this, such as:

- Current security practices are not capable of meeting today's more stringent legal and regulatory requirements affecting some industries and regions (e.g. Sarbanes-Oxley, Basel II, HIPPA and upcoming EU Regulation on the Application of International Accounting Standards or UK Operating and Financial Review regime). These can have direct financial impact on businesses, or legal consequences for executive management;
- External and internal business integration, one of the key priorities for enterprise IT departments (regardless of whether they fall under regulatory regimes or not). A pre-requisite for this is the integration of disjointed user-centric mechanisms;
- Systems are getting bigger and more complex. The flexibility and total cost of ownership is coming to the top of the agenda of IT decision-makers. A disjointed approach to security amplifies the situation in which IT is a barrier to business change. This is at a time when an organisation's capability to change is required to maintain its competitive advantage and hence it's very survival.

Interestingly enough, it is business and technical issues and priorities rather than security ones that make the current approach to security lose its acceptability. The common theme to all the examples above is that deficiencies of security solutions not so much pose a hypothetical security risk that could possibly materialise sometime in the future, although they do. No, the real issue is that they pose an imminent risk to the ability of enterprise information technology to support core business objectives. This makes the cause of technical security much more visible to the IT sponsors and so makes improvement of technical security solutions far easier to justify. Yet, existence of good business-justified reasons for an overhaul of technical security does not provide a blank cheque to fund any security initiative. Identifying the areas that require change

ENTERPRISE SECURITY

is as important a question as understanding what is driving it.

Reviewing the technical and operational requirements implied by the current wave of compliance, rationalisations, IT efficiency improvements and business process integration initiatives, it can be argued that the focus will be threefold:

- Complementing system and network security mechanisms by application layer security;
- Developing and using common security components to deliver security services, where technically feasible; and
- Promoting the use of technical and architecture standards.

The Rise of Application Security

Analysing the technical implications of business integration trends, it becomes apparent that the security discipline of tomorrow will be much more preoccupied with application measures.

External integration results in the increased activity of users. This in turn results in increased volumes of application traffic across organisation boundaries. As the frequency and volume of access across the enterprise boundary grows, the difference between trusted and untrusted becomes blurred. Access control then becomes more a matter of what the user's privileges are and what services he or she needs to access.

Looking first at authorisation, firewalls, although they do contribute to the overall protection, are ultimately badly equipped to enforce access control with the granularity required by application end-points. Intrusion detection does not necessarily cope better. There are currently many smart people trying to resolve this, but it is not clear how successful they are going to be. The problem actually lies in the fact that both were originally designed as network devices. Although network level devices may need to be aware of what kind of traffic they support, they were designed only to differentiate between application protocols and possibly, understand the syntax of these protocols. What they were not designed to do is understand what the data represents and means, which is exactly what is required to carry out granular authorisation.

Similarly, system-level policy enforcement points do understand the resources managed by the operating system – processes, memory, disk access – but they cannot necessarily cope with database views, business objects or transactions.

In theory, it is possible to de-couple the authorisation policy enforcement point; see for instance [1]. In practice though, performance limitations, coupled with both the difficulty of externalising application-specific resource types and the access constraints they entail, mean that much of application-bound security mechanisms

will be tightly coupled with the applications they are protecting in the foreseeable future.

For audit, the situation is similar to authorisation. The requirements for monitoring of access to sensitive personal data, which are inherent to many privacy protection requirements, or those for fraud detection, require audit to be enforced at a per-function, per-transaction or per-data view level of granularity. Whereas system or network devices are not really capable of capturing that type of data, application, database or transaction monitors should become much easier to configure or customise to provide required information.

As for authentication, it is one of the services that can, to a certain extent, be de-coupled from the application. But this has other consequences. Either the application owner has to accept limited content of application audit trails, which may be questionable – or the identity of a user initiating a transaction has to be propagated from the authentication system to the application. This is not always an option with application-agnostic software. All this does not necessarily mean that perimeter and system security measures will suddenly become obsolete. They will still be effective against threats such as malware or external hacking attempts. It simply means that ignoring the layer of security mechanisms operating on top of the system layer, including authentication, authorisation and audit, will become more dangerous than it is today.

Common Components

The second discernible trend is towards the more frequent use of common security components. This trend is driven by long-term cost management and in some cases compliance regimes.

It is not difficult to conclude that both enforcement and management aspects of security functionality will become more consistent across systems; witness the number of account provisioning systems implemented as a result of Basel II requirements or the weight paid to identity management by the current wave of service oriented architecture initiatives. It is hard to imagine consistency of automated policy enforcement across with concurrent local definition, storage and management of these policies without common or integrated components.

As the term 'component' suffers from general overuse, which could potentially lead to misunderstanding, let us digress for a moment to define what we mean by it. In this paper, the term is used in the rather loose sense, not necessarily having the same meaning as components in components-based development approaches or objects in object-oriented programming methods. For the purposes of this paper a 'common component' is deemed to be a piece of infrastructure that (a) provides common security

functionality used across a number of systems and applications, that (b) enables enforcement of common policy over these systems or that (c) enables centralised management of distributed security mechanisms. In other words, rather than a piece of technology implementing a single mechanism used by a single system, it is more of a container for a number of mechanisms, methods and interfaces whose purpose is to unify the enforcement of security policy across several systems.

So what is new about that? A range of measures – firewalls, security information management systems, and some implementations of public key infrastructure may pass as common security components. Rather than being an entirely new concept, they implement secondary attributes, such as consistency, that have become relevant only recently under a circumstance of scale, complexity, heterogeneity and the distributed nature of the systems they protect.

Coming back to the core of the argument, why common components will become more important, consider the implications of the localised implementation of authentication or user management on the ongoing cost of operating and changing an application. Fragmented mechanisms do not support the growing importance of controlling the long-term costs of information technology. It has been pointed out [2] that the current focus on the long-term costs of information technology often translates into consolidation, rationalisation and centralisation. Use of common security components makes sense in this respect. It is cheaper to change security configurations or upgrade security functionality if they reside centrally, in one place rather than scattered around dozens of systems. This also supports other requirements creeping into long-term plans of IT departments; infrastructure flexibility and reduction of lead time to implement changes.

With that in mind, which security services are, or can be, provided by common security components? It would seem tempting to argue that as the world is moving towards utility computing and service orientation, all security services should be provided as utilities through common components. As a general rule this does not make much sense. As previously discussed in a slightly different context, all these proposals would require some degree of externalisation. Externalising some logical security services, for instance authorisation and audit, is not practical because of performance implications. For other services, such as platform or data integrity, or secure channels, it is technically infeasible unless disabling inherent security mechanisms as a form of externalisation is considered.

Of the high-impact security services outlined earlier, this leaves the trinity of authentication, authorisation and audit as prime services that can be partially or fully externalised using com-

mon components. Furthering the level of detail, table 2 shows the types of requirements driven by the trends identified earlier. It also provides examples of common components that enable implementation of those requirements.

To sum up, business-driven requirements for integration, centralisation and consistency lead to the re-invention of common security components. The rising importance of application security functionality means that these will be mostly, though not exclusively, application-focussed and primarily supporting authentication, authorisation and audit security services.

A Word on Standards

The third distinct area that will be made prominent by the current wave of business-driven IT initiatives are technical standards, in particular those standards that enable consistency and commonality in within heterogeneous distributed systems.

Standards provide a crucial ingredient of interoperability and facilitate interoperation of security mechanisms when implemented in heterogeneous systems. Correct use of technical standards lowers costs and improves the technical feasibility of integration. This is true with or without the existence of common components. Lack of standards in larger-scale environments, by contrast, almost inevitably leads to untranslatable data formats, proprietary interfaces and incompatible implementation of security mechanisms. These can make the cost of integration prohibitive.

Hence, it would seem self-obvious that standards, especially open ones, are a good thing, that that they should be adopted as broadly and quickly as possible. In principle this is true but there are some qualifiers that ought to be attached to the statement. To make sure that standards bring the desired results, care needs to be taken to ensure that the right standards are chosen and that they are used in areas where benefits accrue.

Which are the right technical security specifications? There is a running joke about general technical standards, which also applies to security standards: the good thing about them is that there are so many to choose from. Indeed, even looking at just basic security services, the number of headlines under which individual standards can be grouped is more than a dozen:

- There is http and TLS for web authentication, Windows integrated logon and Kerberos for single sign-on, LDAP and SQL for access to authentication back-end; COM+, .NET or JAAS for authorisation, TLS and S-MIME for secure channels;
- There is DCE and CORBA and an assortment of mainframe specific protocols defining

Security Service	Emerging Requirements	Common Components and Products
Authentication	Single or simplified sign-on integrated across multiple applications internal or external to the organisation; Improved time to set up new users; Consistency on removal of user access.	Authentication servers and single sign-on gateways; EAI hubs, Metadirectory and password synchronisation products; Account provisioning systems.
Authorisation	Requirement for complete externalisation and centralised management is currently technically achievable; Consistency of authorisation across systems; Improved time to grant and revoke access to system resources.	Account provisioning products strengthening use of local systems and application authorisation capabilities; Identity management or service desk workflow products.
Audit	Timely and quality audit information for fraud or privacy violation purposes; Centralisation of audit data storage for evidential purposes; Self-service for business managers of data subjects.	Specialised solutions supporting audit log collection, event correlation and filtering and dissemination of audit information complementing use of audit capabilities inherent to applications or systems.

Table 2 – Typical Common Components

de-facto standards for authentication and authorisation in legacy applications;

- And finally, there are emerging standards for the XML and web services world SAML, Web Services Security, Liberty Alliance's Identity Federation and OASIS and W3C managed XML Security standards and even the odd standard from IETF.

The number of standards is staggering. As if that was not enough, to add complexity, both the standards themselves and the products developed using them continually evolve. This creates a shifting sand where any general-purpose comparison is of very limited use – it becomes obsolete as soon as it is published.

This complexity is further deepened by the way that standards are used by product vendors to control and extend market share. Standards are used either as a means of locking-in customers or as a weapon in competitive standard wars. Thus use of both *de jure*, and (more so) *de facto*, standards become unsafe for general use. Users are forced into evaluation of both the standards themselves and their implementation.

Therefore, rather than a detailed evaluation and comparison of individual specifications it is better to provide a general health warning for safer use of these standards.

- The first question to ask is who controls the specification? 'De facto' standards developed by vendors or groups of vendors can be as good as de jure standards. Unfortunately they are often used to lock customers in to the vendor's product set. But at least the motives of vendors are more or less transparent.

- If the standard is managed by a standard making body then the question is what type of a body is it and what track record it has in preventing misuse of the standard making process by interest groups. The situation with standard making can be complicated. Some standard making bodies, e.g. ISO, W3C, or national ones like IEEE or ECMA can be taken as independent, yet they are hardly at the forefront of technology progress. Others, such as OASIS are decidedly more leading edge, but there is a greater danger that they may be driven by vendors or interest groups. Yet other so called 'standard making' bodies are in fact vendor special groups furthering the special interests of vendors in a particular niche. In reality things get even more complex. Some specifications, such as WS-Security, are developed by a vendor, but subsequently passed onto a standard making body to become a standard. Vendors then associate proprietary specifications complementary to the standardised one as 'the standard'.
- Consider the purpose for which a standard was originally drafted. Standards generally build on technology that already exists. Therefore, as off-the-wall as it may seem, it makes sense to look at operational and technical characteristics such as performance and scalability. For instance, standards focussed on intranet authentication may not be fully suitable for extranet use and vice versa.
- The next question is: how widely adopted is the standard? The history of the technology industry is littered with standards that may have been theoretically influential, but which were, for all practical purposes, irrelevant. Al-

though vendors and standard making bodies should know better, the current wave of web services standards demonstrates that this is not necessarily the case. The thing to keep in mind is that although there may be some benefits from internal adoption of standards, full benefits are achieved only when standards are adopted by a critical mass of relevant users and off-the-shelf products.

- Another question arises when a number of standards are chosen: whether the standards are mutually compatible. A frequent problem in large organisations is that the size of the estate introduces considerable technological variety. This in turn leads to coexistence of standards. The problem is that in some cases standards that do work as part of point solutions, cease to work when used with other standards.
- Moving on to products developed in accordance with standards, it is worth noting that even a product developed in accordance with a standard may not guarantee interoperability. A brief look at any standard reveals that they often include a number of attributes or components that are optional or that can be used to customise behaviour. This can be used to devise what is, essentially, a proprietary implementation of an open standard. Microsoft's version of the Kerberos authentication protocol is a good case study of this.
- Finally, a point to keep in mind is that standards are not a guarantee of success. Unless a technical solution works, it is irrelevant whether it is secure or not. It is quite feasible that interoperable security standards may still result in a solution that cannot be made to perform against the requirements defined by the users.

Despite these qualifications, the conclusion from this should not be that technical standards are worthless or that agreement on a set of interoperable standards is not a goal worth pursuing. Rather it is that identifying which standards are the right fit for a particular organisation and particular context may be more difficult than one would first imagine.

Keeping Up With Technology

The practice of implementing technical security solutions is taking yet another major turn, re-inventing some of the concepts that appeared fifteen or twenty years ago.

To keep up with business requirements, many organisations are now starting to consolidate and integrate an assortment of point solutions that they acquired during the boom years. This generates new types of issues, but then again it also provides us with opportunities. It creates the opportunity to actually improve the strength of some security mechanisms, to ensure consis-

tency across systems, improve flexibility and reduce costs. It also presents a unique opportunity to make security part of the solution right from the beginning rather than as an add-on.

Yet achieving this is not automatic; to make use of this opportunity both processes and people have to be able to keep up with changes in technology. For this, we need to take up new activities, which we may not have been doing in the past, such as:

- Promoting the re-use of common security components through technology standards compliance processes;
- Building incentives for re-use of common components into budgeting rules for new projects;
- Ensuring total cost of ownership is considered spanning both implementation and operations stages in the security technology life cycle;
- Integrating security into the software implementation process from the beginning;
- Shifting the focus of security management from compliance to architecture management and from operations to development.

In order to seize the opportunity, we need to upgrade our capabilities in parallel to upgrading the technical infrastructures. People, their skills and mind sets are significant prerequisites necessary for the technical change to take place. The brave new world of application security, common components and standards requires that security specialists, architects and managers acquire a new range of skills, or that they are capable of applying some older ones in new contexts:

- The ability to understand and manage end-to-end cost efficiency;
- An understanding of applications and application infrastructure technology in order to be able to define and implement security at the application layer;
- The ability to understand the enterprise architecture management process to ensure security solutions and architectures are aligned across departments and applications;
- An understanding of the development process and its cultural specifics, or at least talking to infrastructure and application architects sufficient to influence the implementation process.

As some are pointing out [3], the role of security and the security department in enterprise IT is changing. Considering the importance of business trends, the extent to which security departments are able to update their capabilities to address topics discussed in this paper, will affect their credibility and signpost the road to the future.

Conclusions

It is becoming apparent that the current approach to security is slowly becoming less than acceptable, yet there is no consensus about which methods and tools will be effective to provide protection in the future. It is argued that the development of technical security in the next several years will be driven by the combination of business and enterprise IT management trends rather than changes in the threat landscape.

These trends will increase the importance of application security, and will drive more frequent adoption of common enterprise security components, primarily delivering authentication, authorisation and audit services. Secondary requirements for interoperability and integration will bring attention to technical standards.

This will pose new challenges for security departments. These will have to acquire a new set of capabilities, such as awareness of total cost of ownership issues, understanding of enterprise architecture and application development life cycles, and the capability to collaborate with other departments to make security happen.

This may be challenging, but it presents a major opportunity to fix some old problems whilst building a secure grounding for the next wave of IT initiatives.

References

- [1] Various, *Security Design Patterns*, The Open Group, April 2004
<http://www.opengroup.org/security/gsp.html>
- [2] Gartner issues, *10 CIO resolutions for 2005*, Computerworld, December 2004
<http://www.computerworld.com/managementtopics/management/story/0,10801,98326,00.html>
- [3] Andrew Briney, *Endangered species: Information security officers*, in *Information Security Magazine*, September 2004
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci1027324,00.html

About the Author

Jiří Ludvík is a senior technical architect with Capgemini in the UK. Jiří has worked in the IT industry for 10 years, most of the time in the security arena. In recent years, he has worked as a technical architect, lead security architect or security manager on several large-scale e-business, ERP and infrastructure rollout projects in the transport, legal and government sectors.

Before that Jiří was a security consultant specialised in risk analysis, security policy development and security audit. He is one of the co-authors of the Czech translation of ISO 17799.

Jiří holds a Masters degree in IT and management from the University of Economics in Prague, Czech Republic and is Certified Information Systems Security Professional.

There is *only* one way to get all issues of
Information Security Bulletin:

SUBSCRIBING!

Please use the form in the journal, or visit
<http://www.isb-online.net>