What is a Security Architecture?

Anthony Thorn, Tobias Christen, Beatrice Gruber, Roland Portman, Lukas Ruf

1   Introduction

This paper is one of the results of the Security Architecture working group of the Information Security Society of Switzerland.

In this paper we concern ourselves primarily with Security Architectures for organisations rather than for products or technologies (e.g. Java security architecture, GSS security architecture or CDMA) although most of this paper applies to all three types of security architecture.

A product security architecture will typically confine itself to the security properties of that product. Thus the Common Data Security Architecture (CDSA) describes how security services are provided in a layered model.

An enterprise security architecture needs to address applications, infrastructure, processes, as well as security management and operations.

An application security architecture lies between the two. It must address not only the security provided within the applications, but also the additional (compensating) controls which are required outside the application. The latter are sometimes more important and almost always harder, to specify and implement.

2   Definition

Although we all have an implicit understanding of the nature of a Security Architecture, we were unable to find an authoritative definition, furthermore we established that security architecture is interpreted very differently from organisation to organisation.

Traditionally security architecture is a document, which specifies which security services are provided how and where, in a layered model. Originally the model typically referred to OSI layers and specified the security elements or services (IS 7498-2 (superseded by IS 10745)) and the mechanisms used to provide them.

Our understanding of Security elements has expanded to include for example Vulnerability management, Patch management, Identity Management and many more. In addition many organisations do not have a Security Architecture in the form of a single document.

Our definition is:

A Security Architecture is a cohesive security **design**, which addresses the requirements (e.g. authentication, authorisation, etc.) – and in particular the risks of a particular environment/scenario, and specifies what security controls are to be applied where. The design process should be reproducible.

Design principles will usually be stated explicitly. Detailed specifications of security controls are often documented in separate documents.

Properties

This definition is intended to specify only that, an architecture is a design, which has a structure and addresses the relationship between the components. In the next sections we define and explain certain important properties of a Security Architecture.

2. Relationships & Dependencies
3. Benefits
4. Form
5. Drivers
6. The appendix lists some references and examples

3 Relationships & Dependencies

The scenario/requirements addressed by, a security architecture includes the relevant IT architecture. In this section we use the term "Reference Architecture" to identify the idealised model from which the "Solution Architectures" are derived.

In this diagram RED text and lines denote IT SECURITY specific components.
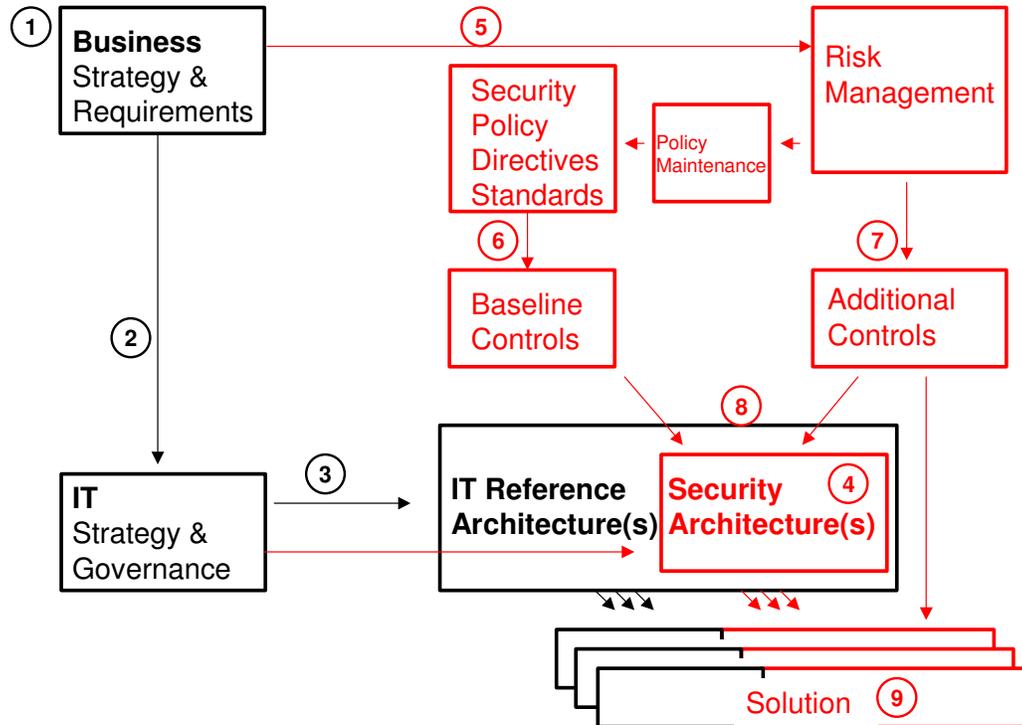
The diagram is intended to illustrate the following propositions (starting at the top-left):

1. Designing a security architecture should be a response to Business strategy and requirements.
2. The IT Strategy should be a response to the Business strategy and requirements.
3. The IT Reference Architecture(s) should be a response to the IT Strategy and Governance. The reference architecture will usually address multiple platforms.
4. The Reference Security Architecture(s) is part of the IT Architecture even if it is published as a separate document.
5. IT Security Risk Management, process and criteria. Are derived from the Business strategy and requirements.
6. A set of Baseline Controls is generated based on the Security Policy, Directives, Standards etc. By Baseline Controls we understand **mandatory minimum standards** for the organisation. Input comes from the legal/regulatory environment, Benchmarking and published security "good practice" etc. see section 5 below.
7. Additional controls are derived from the Risk management process.
8. The security Architecture is the embodiment of the baseline and the additional security controls. It can also be defined to include the policies, directives, standards and the risk management process.

9. Some organisations use the term solution architecture to refer to the specific implementations derived from the reference architecture.

This diagram reflects the different interpretations of Security Architecture identified by the members of our working group.

4 Benefits

Cost Effectiveness
The principal benefit of an enterprise security architecture is the same as an IT architecture, namely cost-effectiveness through standardisation[BG4].

The cost-effectiveness improvement stems from the re-use of the controls specified in the architecture, but this affects more than just the cost of implementation (1):
1. Easier, better cheaper implementation resulting from economies of scale
2. Re-use of skills of support staff, application developers, analysts, (and sometimes users).
3. Re-use of management interfaces
4. Easier, better, cheaper compliance checking
5. Easier, better cheaper effectiveness measurement (IS 27001).
6. Faster implementation of standard solutions
7. Fast Track approval
   In large organisations an IT security approval is required as part of project governance. Typically a "triage" will be performed in order to identify candidate projects for a detailed risk analysis, while for "harmless" projects a high-level analysis is sufficient.

   In such an organisation compliance with a security (and an IT) architecture will provide a "fast track" to security approval.

Re-use of standard modules is particularly important for security, because an excellent security control can be nullified by an apparently trivial implementation error.

Communication
In addition, particularly for a multi-national organisation, an architecture improves communication, and ensures that the specialists in different countries share a common understanding of terminology, requirements and solutions.

Similarly for a complex system a security architecture is essential to ensure that developers working on different sub-systems, understand the relationship of their contribution to the whole, and what security requirements their product must meet.

5 Form

As indicated in the above diagram, the security architecture is related to the IT architecture(s) but it can take various forms. It usually contains a catalogue of standard controls together with principles, relationship diagrams etc.   The details of the control implementation -preferably including measurement and testing standards- are often separate from the architecture document.

The security architecture may not be a standalone document, but could be a section/chapter of an IT architecture, or even a pervasive part of an IT architecture.

An undocumented security architecture, "a shared understanding of principles", does not meet the requirement of reproducibility.

6 Drivers

The security controls (as opposed to the IT and general business requirements) are derived in 4 ways.

1. Financial
2. Risk Management
3. Benchmarking & good practice
4. Legal and regulatory

Although more than one "driver" may be relevant in a particular case, one of these drivers is often sufficient.

6.1 Financial

The financial driver is "return on investment" (ROI) – although it may be measured as; NPV (Net Present Value), IRR (Internal Rate of Return), etc. Quite simply the cost after implementing the control is less than if the control had not been implemented.

Where the risk is included in the calculation – i.e. values for the risk with and without the control are used- this is called "ROSI". Some security controls can be cost effective even without taking the reduction of risk into account. e.g. less help desk calls as a result of a "self-service" password reset, included in an identity management project.

Note that this is not the same as risk management, although it is applied in the selection of controls in the risk management process.

6.2 Risk Management

Risk management is a process, which identifies risks and selects an appropriate treatment. The reason for managing risks is to make the total cost of adverse incidents predictable. Here total cost means the sum of the impact of the incident and the cost of controls intended to mitigate (or transfer) the risk.

Note that the priority in risk management is the (estimated) magnitude of the risk, and not the expected cost saving through treatment (see above). We may well be prepared to pay a premium over the annualised loss expectancy for this predictability.

This is the same reasoning for a private person buying accident insurance. Even though he expects the cost of insurance over the years to exceed the actuarial risk, he pays the premium for "peace of mind".

Note that detailed risk analyses are resource intensive, and where relevant actuarial/statistical information is not available the estimate degenerates to guesswork (also known as expert opinion!).

6.3 Benchmarking & Good Practice

Many controls are specified because they are included in (authoritative) published standards, or because peer organisations use them.

Again the specific controls may not be cost effective in the particular environment, but few security officers will want to expose themselves, as well as their organisations, by not implementing (or at least putting a tick in the box for) a control, which constitutes "recognised good practice".

This is also referred to as "due diligence" or famously by Schneier as "CYA" (cover your ass). However in fairness there is huge uncertainty about the magnitude of certain risks –especially the most improbable category- and so in certain cases it may be impossible to be sufficiently confident that a control is not justified.

6.4 Legal and Regulatory

Obviously we should all obey the law of the land, but this category also includes, for example, banking regulations, Federal Drug Authority requirements etc. as well as controls specified in contracts with suppliers or customers, e.g. to connect with their order and logistic systems.

For a multi-national organisation ensuring compliance in every country in which they operate is anything but straightforward. What ought to be the easiest decision ("just do it!") becomes a major challenge.

7   References and Examples

http://www.linux.com/articles/49803
Bruce Byfiel, d lists 9 principles of a (good) security architecture.

---

http://gita.state.az.us/enterprise_architecture/NEW/Security_Arch/
Provides this definition: "Security Architecture provides the framework and foundation to enable secure communication, protect agency business processes and information resources, and ensures that new methods for delivering service are secure."   and an example of a layered diagram which is a common expression of an architecture.

---

http://www.rites.uic.edu/csaw/
Computer Security Architecture Workshop call for papers provides this definition:
"Architectures, whether system or application, are composed of abstractions (interfaces) and their implementations. Security Architectures are architectures which enable implementations that are resilient to an appropriate and broad-based spectrum of threats. An evaluation of a Security Architecture requires understanding these threats; the tradeoffs between different system goals, including between security and non-security goals; the long-term appropriateness of its interfaces; and the implementations it allows. The best interfaces are those that capture the most important issues, enable different implementations, and are flexible enough to adapt (or be adapted) to different threats."

---

http://www.cl.cam.ac.uk/~mgk25/osi-faq.txt
IS7498-2 Provides a general description of security services and related mechanisms, which can be ensured by the Reference Model, and of the positions within the Reference Model where the services and mechanisms may be provided.

---

http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/026.pdf
The ISO 7498-2 Security Elements

---

http://www.sans.org/reading_room/whitepapers/auditing/1527.php

---

http://www.sans.org/reading_room/whitepapers/policyissues/504.php
This paper discusses an approach to Enterprise Security Architecture,… including a security policy, security domains, trust levels, tiered networks, and most importantly the relationships among them.

---

www.sabsa-institute.org
Example of a layered model of Operational Security Architecture

---

http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-711.pdf
Section 4.1 explains the need for a security architecture document for a complex system

---

Commercial publications which are not accessible to everyone have not been included in this list.