Security Architecture and Design from a Business/Enterprise Driven Viewpoint

Introduction to Enterprise Security Architecture using the SABSA methodology, and design pattern examples

Robert Trapp, Perry Bryden
Presented at ISC2 Meeting, September 18, 2014
Agenda

- Introduction – What’s “Enterprise” Security Architecture and who cares

- Introduction to SABSA Methodology

- Logical Security Architecture - overview and example  
  (Adapted from 2013 COSAC conference presentation: Security Design Patterns at Logical Architecture Level)

- Physical Security Architecture - overview and example  
  (Adapted from 2013 COSAC conference presentation: Security Design Patterns at Physical Architecture Level)

- Presentation Wrap up

- Further Q&A… Discussion
Key Takeaways for Enterprise Security Architecture

• Framework to manage enterprise complexity

• Move from 100% Firefighting to Designed-in

• Business/Mission Perspective

• Prioritized investments

• Moving past compliance

• Address gaps in the NIST approach
What Enterprise Security Architecture is **NOT**

- Enterprise Security Architecture is NOT:
  - Typical Enterprise Architecture practice
    - Security is usually a lightweight afterthought
  - Technical Architecture (part of the picture, but not the main focus)
    - A network diagram with Firewalls, routers & other devices,
    - A diagram of the Active Directory design
    - Lacks traceability to Business needs and priorities
    - Lacks enterprise perspective, business drivers
  - Compliance
    - NIST, ISO, COBIT, PCI, etc.
    - Compliance treats all assets as if they have the same value
    - Compliance alone doesn’t produce security architecture and is not sufficient to produce secure systems
  - Product Driven
    - Vendor point solutions leave gaps
    - Lacks interoperability
    - Not Vendor neutral – leads to Vendor Lock-in
What IS ESA

• A holistic enterprise-wide view of security with principles, policies, models and standards for designing and building enterprise systems - with the aim of reducing risk

• ESA is Security Architecture from a business/enterprise viewpoint
  • Security decisions based on business need, top down
  • Starts with business processes not with IT products on hand or in the market
  • Provides traceability: All security designs and technology/products must have an explicitly traceable (i.e. auditable) path back to their business purpose (i.e. why they are used)

• ESA provides a framework for managing complexity of the huge array of architectural factors we need to track in a coherent way
  • Business process, assets, organizations, strategies, market environment and risk environment
  • Enterprise risk management based decision processes
  • Transition from high level to low level architectures and design, to components products & configurations
  • Methodical progression from business attributes to physical design
Why you should care about ESA

- We MUST move away from compliance-only driven thinking
  - Compliance alone does not create effective security
  - We have proof that it’s not effective. (e.g. Target, 100s of others)
- Top down engagement is necessary to prioritize and fund security investments
  - Security $$ should be tied to the business value of the asset
- Provides a common framework and language to enable meaningful dialogs at all levels of the organization about real security issues
  - Without this
    - Trust and access decisions made at a technical level are not apparent to business level but can have a business impact
    - Changes to the nature of a business partnership requires changes to access rules but are not easily implemented by the technical team due to prior inflexible design decisions
- ESA is not a silver bullet solution, but it is a necessary part of the solution
Why you should care about ESA

- Provides an approach to creating meaningful metrics to measure success and progress
  - Every level of the organization has a different focus
    - Business execs care about managing risk to business assets
      - They care little about the number of viruses/malware were detected or patches applied
      - Tell them how active threats are being identified and how risks are being managed
    - Show the layers of protection working together
      - The Web App scanner detected a vulnerability and the WAF enforced a mitigation until the patch can be implemented
    - Show dynamic processes for working at all layers of the organization and ESA - If an attacker gets past a layer of defense, immediately adapt the mechanism to compensate
Introduction to SABSA – Background

- Sherwood Applied Business Security Architecture (SABSA)
- Methodology for developing business-driven, risk and opportunity focused enterprise security & information assurance architectures, and for delivering security
- Comprises: framework with several integrated models, methods & processes

- Proven method, developed and evolved from experience not theory
- Most well developed methodology for architecting security
- Uses an enterprise architecture type framework for communications across different sets of stakeholders
- Infrastructure solutions that traceably support critical business initiatives
- Business driven approach
- Used internationally, adopted by many government and private organizations as standard for security architecture, recently TOGAF 9 adoption
- Coherent with ITIL
- Open source: although copyright protected, SABSA is free for use.
Introduction to SABSA – Background


- Can be applied flexibly:
  - Several scopes: enterprise, individual system, component
  - In whole or in part
  - Seamless security integration & alignment with other frameworks (e.g. NIST, TOGAF, ITIL, ISO27000 series, Zachman, DoDAF, CobIT)
  - Fills the gaps for security architecture and security service management left by other frameworks

- Comparing to NIST – SABSA has an enterprise perspective, NIST is very system centric. Would integrate well into NIST 800-39 RMF 1st & 2nd tier
Introduction to SABSA – The Framework

• SABSA comprised of:
  • Principles and approach
  • A series of integrated frameworks, models, methods, and processes
  • Two foundational frameworks: Master matrix and Services matrix

• 2 genuinely unique aspects of SABSA approach (Our opinion):
  • Reframing business security goals as NOT just CIA/CIAAA
  • The Business Attributes Profile
    • Method for requirements management and establishing measurable security
    • Crux of traceability

• SABSA covers the whole life cycle, but does not have any models or frameworks for the implementation phase, it recommends use of proven approaches like PMP, Agile, PRINCE2
All architectural frameworks manage complexity using multilayered views and each of the layers uses various models.

<table>
<thead>
<tr>
<th>All Architecture Frameworks and Models Follow a Multi Layered Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
</tr>
<tr>
<td>Security does not exist in a vacuum</td>
</tr>
<tr>
<td>Architecture View Cuts across all other views</td>
</tr>
<tr>
<td>Security is an emergent property.</td>
</tr>
<tr>
<td>Has: Functional aspects &amp; quality/ non-functional aspects</td>
</tr>
</tbody>
</table>

### DODAF EA Approach
- Operational View
- Technical View
- System view
- Other: Capably, Data, Information, Activity, Performance

### Zachman EA Approach
- Executive Perspective
- Business Management Perspective
- Architect Perspective
- Engineer Perspective
- Technician Perspective
- Enterprise Operations Perspective

### TOGAF
- Business
- Application
- Data
- Technology

### Others...

---

ISC2 Presentation - Sept 2014

Security Architecture & Design
## Introduction to SABSA – The Framework (Master matrix)

<table>
<thead>
<tr>
<th>Stakeholders:</th>
<th>ASSETS (What)</th>
<th>MOTIVATION (Why)</th>
<th>PROCESS (How)</th>
<th>PEOPLE (Who)</th>
<th>LOCATION (Where)</th>
<th>TIME (When)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Architects</strong></td>
<td>Taxonomy of Business Assets, including Goals &amp; Objectives</td>
<td>Opportunities &amp; Threats Inventory</td>
<td>Inventory of Operational Processes</td>
<td>Organisational Structure &amp; the Extended Enterprise</td>
<td>Inventory of Buildings, Sites, Territories, Jurisdictions, etc.</td>
<td>Time dependencies of business objectives</td>
</tr>
<tr>
<td><strong>逻辑</strong></td>
<td>Inventory of Information Assets</td>
<td>Domain Policies</td>
<td>Information Flows; Functional Transformations; Service Oriented Architecture</td>
<td>Entity &amp; Trust Framework</td>
<td>Domain Definitions; Inter-domain associations &amp; interactions</td>
<td>Start Times, Lifetimes &amp; Deadlines</td>
</tr>
<tr>
<td><strong>Components</strong></td>
<td>Data Dictionary &amp; Data Inventory</td>
<td>Risk Management Rules &amp; Procedures</td>
<td>Applications; Middleware; Systems; Security Mechanisms</td>
<td>User Interface to ICT Systems; Access Control Systems</td>
<td>Host Platforms, Layout &amp; Networks</td>
<td>Timing &amp; Sequencing of Processes and Sessions</td>
</tr>
<tr>
<td><strong>服务</strong></td>
<td>ICT Products, including Data Repositories and Processors</td>
<td>Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools</td>
<td>Tools and Protocols for Process Delivery</td>
<td>Identities; Job Descriptions; Roles; Functions; Actions &amp; Access Control Lists</td>
<td>Nodes, Addresses and other Locators</td>
<td>Time Schedules; Clocks, Timers &amp; Interrupts</td>
</tr>
</tbody>
</table>

© 1995 – 2009 SABSA Limited | info@sabsa.org
## Introduction to SABSA – Service Management Matrix

**SABSA SERVICE MANAGEMENT MATRIX (Aligned with ITIL v3)**

<table>
<thead>
<tr>
<th>Layer 6 of the Main SABSA Matrix:</th>
<th>ASSETS (What)</th>
<th>MOTIVATION (Why)</th>
<th>PROCESS (How)</th>
<th>PEOPLE (Who)</th>
<th>LOCATION (Where)</th>
<th>TIME (When)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Architecture:</td>
<td>Proxy Asset Development</td>
<td>Developing ORM Objectives</td>
<td>Service Delivery Management</td>
<td>Service Management Roles</td>
<td>Service Portfolio</td>
<td>Service Level Definition</td>
</tr>
<tr>
<td>Component Architecture:</td>
<td>Change Management; Software &amp; Data Integrity Protection</td>
<td>Operational Risk Data Collection</td>
<td>Operations Management</td>
<td>User Support</td>
<td>Service Resources Protection</td>
<td>Service Performance Data Collection</td>
</tr>
<tr>
<td></td>
<td>Product &amp; Tool Security &amp; Integrity; Product &amp; Tool Maintenance</td>
<td>ORMA Analysis; Monitoring and Reporting Tools &amp; Display Systems</td>
<td>Product &amp; Tool Selection and Procurement; Project Management</td>
<td>Security Management Tools</td>
<td>Products &amp; Tools for Managing Physical &amp; Logical Security of Installations</td>
<td>Service Analysis, Monitoring and Reporting Tools &amp; Display Systems</td>
</tr>
</tbody>
</table>

The row above is a repeat of Layer 6 of the main SABSA Matrix. The five rows below are an exploded overlay of how this Layer 6 relates to each of these other Layers.
# Introduction to SABSA – Bob’s Annotated Master Matrix

<table>
<thead>
<tr>
<th>Stage</th>
<th>Layer (Role View)</th>
<th>ASSETS (What)</th>
<th>MOTIVATION (Why)</th>
<th>PROCESS (How)</th>
<th>PEOPLE (Who)</th>
<th>LOCATION (Where)</th>
<th>TIME (When)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Taxonomy of Business Assets, Including Goals &amp; Objectives</td>
<td>Opportunities &amp; Threats Inventory</td>
<td>Inventory of Operational Processes</td>
<td>Organisational Structure &amp; the Extended Enterprise</td>
<td>Inventory of Buildings, Sites, Territories, Jurisdictions, etc.</td>
<td>Time dependencies of business objectives</td>
<td></td>
</tr>
<tr>
<td>LOGICAL ARCHITECTURE (Designer, Engineer)</td>
<td>Information Assets</td>
<td>Risk Management Policies</td>
<td>Process Maps &amp; Services</td>
<td>Entity &amp; Trust Framework</td>
<td>Domain Maps</td>
<td>Calendar &amp; Timetable</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inventory of Information Assets</td>
<td>Domain Policies</td>
<td>Information Flows; Functional Transformations; Service Oriented Architecture</td>
<td>Entity Schema; Trust Models; Privilege Profiles</td>
<td>Domain Definitions; Inter-domain associations &amp; interactions</td>
<td>Start Times, Lifetimes &amp; Deadlines</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data Dictionary &amp; Data Inventory</td>
<td>Risk Management Rules &amp; Procedures</td>
<td>Applications; Middleware; Systems; Security Mechanisms</td>
<td>User Interface to ICT Systems; Access Control Systems</td>
<td>Host Platforms, Layout &amp; Networks</td>
<td>Timing &amp; Sequencing of Processes and Sessions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ICT Products, including Data Repositories and Processors</td>
<td>Risk Analysis Tools; Risk Registers; Risk Monitoring and Reporting Tools</td>
<td>Tools and Protocols for Process Delivery</td>
<td>Identities; Job Descriptions; Roles; Functions; Actions &amp; Access Control Lists</td>
<td>Nodes, Addresses and other Locators</td>
<td>Time Schedules; Clocks, Timers &amp; Interrupts</td>
<td></td>
</tr>
</tbody>
</table>

## Standards
- **Why** column: Laws & Regs, 800-30, ITIL, ISO 27005, Basel II, COSO, OGC MoR
- **Color Legend**
  - Green - Assets
  - Red – Bus. Risk
  - Blue – Factors effecting risk
  - Yellow – Control objectives & targets
- **Op** risk process
- **White** - Controls

## Notes
- When column: Performance, CMMI, Bal. Scorecard, Financial measures (ROI...)
- All white/control cells: ISO 27002, 800-54, SOX, PCI-DSS, HIPAA, Cobit
Introduction to SABSA – The Suite of Framework Tools

The SABSA framework contains many more models and methods:

- The SABSA Master Architecture Matrix: SABSA Artifacts
- The SABSA Service Management Matrix: SABSA Processes
- Business Requirements Engineering Framework (e.g. Business Attributes Profiling)
- Lifecycle Model and Process
- Risk and Opportunity Model and Risk Management Process
- Multi-tiered control strategy model
- Policy Architecture Framework
- Governance Model and Process
- Security Domain Framework
- Security Services-Oriented Architecture Framework
- Maturity Profile
- Vitality Model
- Through-life Security Service Management & Performance Management Framework
Introduction to SABSA – Sampling of Framework Tools

Risk & Opportunity Model

Business Attributes Profile

Multi-Tiered Control Strategy Model
Security at the Logical Architecture Level - Purpose

• Purpose of this section:
  Describe logical security architecture & its value

• Relation of logical architecture to other aspects of enterprise architecture

• Not enough work is done at this level

• Material based on a presentation given at Oct 2013 COSAC Security Conference
Security at the Logical Architecture Level - Challenge

What is **Logical** architecture …

- What do you mean LOGICAL layer, of course our systems are logical!
- Are the servers built yet?
- Accounting needs a cost & bill of materials before you start!
- Have you started coding yet?
- Can we at least see a network diagram, you know, something tangible?
- Is this going to take very long?
- That’s not how our LDAP works!

For many in business, IT and security: don’t understand, question value, are frustrated

Perception problem – it’s not tangible
But LA is where we do **critical systems thinking**
Logical Security Architecture – Focus & Value

- LA is: Conceptual systems engineering approach to architecture
  - a.k.a. solution arch, high level arch
  - SABSA content guidance
    - Functional specifications - Component & Process maps
    - Security aspect data models/ERD - Security boundaries/domain models
    - Abstract Trust & Permissions models - Security policies
    - Map of security services vs. controls - Performance metrics

- Logical architecture process - critical systems thinking and decisions
  - Last place to declare, in depth, your technical vision and needs prior to being obsessed by vendor products & implementation issues
  - Think about fundamental design flaws (vs. bugs), attacks and mitigation (Example: does this data require authentication for access, and if so how good/ how much?)
  - Define security protection objectives in terms of services, assurance levels, qualities needed from business purpose perspective
  - Overlay and integrate with the rest of the (non-security) architecture
Logical Security Architecture – Where does it fit in ESA

- Logical security architecture
  - Is a design that is driven by the requirements of layer above (conceptual architecture)
  - Provides guidance to the next layer (physical architecture)
  - Traceability up and down

All these “cells” architectural elements are interrelated and must work together

Typical deliverables (from earlier slide)
Logical Security Architecture – Excerpts for IAM Service

- Building a portal. Logical architecture shows we need several related security services

1. Inventory: assets to be protected

2. Location: Define nested security domains

3. Identify Stakeholders and relations:
   - Company
   - Visitors
   - Vendor

4. Mapping of information flow

5. Allocate security attributes
   ID Security Services:
   - Login
   - Access Control
   - Authentication
   - Identity Management

Great Info Portal Company

IT infrastructure

Portal – System of Interest
- Assets held by System:
- Portal application (Domain Policy Authority)
- Visitor ID (Custodian)
- Visitor portal data (Custodian)

ID Security Services:
- Login
- Access Control
- Authentication
- Identity Management

Smartcard Vendor

Smarcard System
- Assets held by system:
  - Smartcard application (Domain Policy Authority)
  - ID data (Custodian)
  - Smartcard (Domain Policy Authority)

Website Visitors
- Assets held by person:
  - Smartcard (Custodian)
  - ID data (Domain policy authority)
  - Portal data (Domain policy authority)

#1 Register and get smartcard ID
#2 Request data access
#3 Validate ID
#4 Mapping of information flow
#5 Allocate security attributes

ISC2 Presentation - Sept 2014
Security Architecture & Design
• Design Patterns can provide Next level of detail

• Still at logical level, shows high level design of the service

• Shown here: Starting point for identity management and authentication services is selected from known patterns *

* Source: Security Pattern Patterns in Practice. Fernandez. 2013
Logical Security Architecture – Excerpts for IAM Service

- More detail from design patterns - example class diagram structure for pattern: IDENTITY PROVIDER*

Preserves technical dependency richness at detail level. But still independent of technology or product.

The logical layer is creates specifications and rationale for the physical layer.

* Source: Security Patterns in Practice. Fernandez. 2013
SABSA Logical Architecture - Design Pattern Synergy

• Typical Security Design Pattern Elements
  • Title
  • Thumbnail/intent (brief description of the problem it solves)
  • Situation example (of where this pattern may apply)
  • Context (fully define the context in which it is applicable)
  • Problem description
  • Solution description: text, structure (often UML component diagrams), dynamics (often UML sequence diagram)
  • Implementation guidance, considerations, instructions, cautions
  • Situation example – as resolved/fixed
  • Consequences (side effects)
  • Known uses
  • See also – identify related/complementary patterns, dependencies on other patterns

• SABSA Framework
  • Business attributes profile
  • Risk enablement/control objectives
  • Policy architecture
  • ICT Strategy
  • Basic logical architecture framework
  • Logical (and physical) service lists and definitions in SABSA textbook ch 11, 12
  • Horizontal and vertical integration among cells and layers

Arrows show: This one ———> That one

“Enhances”
Security at the Physical Architecture Level - Purpose

• Purpose of this section: Describe the nature of and distinct value of a physical security architecture

• Show how the physical architecture relates to other aspects of the enterprise security architecture

• Define vendor agnostic security technologies

• Material based on a presentation given at Oct 2013 COSAC Security Conference
Physical Security Architecture – Focus & Value

- Define how business information at the logical layer is mapped to data structures such as files and databases
- Mapping of physical security mechanisms to deliver logical security services
  - Define how the physical security mechanisms embedded within file systems and database systems can be applied to deliver security services required from the logical layer
  - Define rules, practices and procedures to provide the detailed implementation of security policies

SABSA provides guidance for P.A. architecture content, e.g.:

<table>
<thead>
<tr>
<th>Business Data Model</th>
<th>Security Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security rules, practices &amp; procedures</td>
<td>Users, Applications &amp; the UI for Security</td>
</tr>
<tr>
<td>Platforms and Networks Infrastructure (Layout)</td>
<td>Platforms and Networks Infrastructure (Capacity Plan and Resilience model)</td>
</tr>
</tbody>
</table>
SABSA Architecture Development

SABSA Fig 7-13: How Strategy and Concept/Design Process Fits Together
Physical Layer Development Principles

- Develop designs that meet requirements from the Logical Layer.
- Ensure the design supports the requirements of the Business.
- Ensure the design integrates and interoperates well with all layers of the SABSA Architecture.
- Does the design introduce unnecessary complexity for the business?
- Has the design been proven to perform as intended?
- Consider proven design patterns
Application of Design Patterns to ESA

- Design Patterns Are Helpful because:
  - represent field-tested solutions to common design problems
  - organize design intelligence into a standardized and easily “referencable” format
  - are generally repeatable by most IT professionals involved with design
  - can be used to ensure consistency in how systems are designed and built
  - can become the basis for design standards
  - are usually flexible and optional (and openly document the impacts of their application and even suggest alternative approaches)
  - can be used as educational aids by documenting specific aspects of system design (regardless of whether they are applied)
  - can sometimes be applied prior and subsequent to the implementation of a system
  - can be supported via the application of other design patterns that are part of the same collection
  - Erl, Thomas (2008-12-31). SOA Design Patterns
ESA Design Pattern Examples for the Physical Layer

- Two examples of Authentication mechanisms:
  - Brokered Authentication: X.509 PKI
  - Brokered Authentication: Security Token Service (STS)
**Problem:** The environment includes multiple organizational boundaries or autonomous security domains. The authentication broker must be able to issue security tokens that can be used across organizational boundaries.

**Solution:** Use brokered authentication with X.509 certificates issued by a certificate authority (CA) in a public key infrastructure (PKI) to verify the credentials presented by the requesting application.
Brokered Authentication: X.509 PKI

• Benefits:
  • Authentication can occur over well known Internet firewall-friendly ports through well-known protocols (for example, HTTP/HTTPS over port 80/443).
  • X.509 certificates can be used to authenticate clients and protect messages across organizational boundaries and security domains because the X.509 certificates are based on a broadly accepted standard. PKI using X.509 certificates has the capacity to establish a common basis of trust beyond the scope of individual organizations.
  • X.509 certificates can be distributed openly and used by anyone to encrypt messages to a client or to verify the digital signature of the client.
  • Digital signatures provide a means of supporting non-repudiation. This is because access to the private key is usually restricted to the owner of the key, which makes it easier to verify proof-of-ownership.
Brokered Authentication: X.509 PKI

- **Liabilities:**
  - Private keys need to be stored securely (such as on a smart card) and are therefore not as portable as passwords. An attacker could use a private key to impersonate the client. Therefore, you must make sure that the private key is not compromised.
  - Certificates by themselves are not well suited to provide role-based security, because role assignment tends to change relatively frequently and X.509 certificates typically have a long life time. However, you can supplement X.509 certificate authentication with a role store to provide more fine-grained authorization capabilities. One possible solution is to combine X.509 authentication with a Lightweight Directory Access Protocol (LDAP) directory or Active Directory with certificate mapping enabled.
**Problem:** Clients requiring authentication are implemented on a variety of platforms within the organization, and interoperability is required between those platforms. Using a standards based mechanism for authentication helps ensure interoperability between different platforms.

**Solution:** Use brokered authentication with a security token issued by a Security Token Service (STS). The STS is trusted by both the client and the Web service to provide interoperable security tokens.
Brokered Authentication: Security Token Service (STS)

• **Benefits:**
  • This pattern provides a flexible solution for exchanging one type of security token for another to accomplish a variety of goals in a Web service environment, such as authentication, authorization, and exchanging session keys.
  • The solution is not dependent on any one mechanism, such as the Kerberos protocol or X.509 to secure messages. This makes it easier to enable different authentication protocols to interoperate, by adding a level of abstraction on top of existing protocols.

• **Liabilities:**
  • The layer of abstraction provided by the STS means that the STS must use another underlying security protocol to provide functionality such as authentication and authorization. This can make the STS a more difficult solution to implement, particularly in cases where a custom solution is used.
Wrap Up - Key takeaways for Enterprise Security Architecture

- Framework to manage enterprise complexity
  - Integrate ESA into the rest of architecture
- Move from 100% Firefighting to Designed-in
  - Improve the strategic balance in how the security team works
- Business/Mission Perspective
  - Security Designed (traceably) to enable/sustain the Business/Mission
- Prioritized investments
  - Clearly identify high value assets and appropriate security protections
- Moving past compliance
  - Designed to meet Business security objectives, including compliance
- Address gaps in the NIST approach
  - Holistic Security for the enterprise connecting the Business/Mission with the technical implementation
More Discussion
Thank you

• References:
  • Main SABSA web site: http://www.sabsa.org/
  • SABSA courses and certifications: http://www.sabsa.org/training-schedule
  • Annual COSAC conference always includes the SABSA World Congress. This year runs from Sunday 28 September to Thursday 2 October in Naas, Ireland. http://www.cosac.net/

• Contact information:
  • Robert Trapp: Robert.Trapp@gmail.com
  • Perry Bryden: Perry.Bryden@gmail.com