Approach to Information Security Architecture

Kaapro Kanto
Chief Architect, Security and Privacy
TeliaSonera
About TeliaSonera

• TeliaSonera provides network access and telecommunication services that help our customers communicate in an easy, efficient and environmentally friendly way. International strength combined with local excellence is what makes us truly unique – and provides a world class customer experience, all the way from the Nordic countries to Nepal.

• 190.6 million subscriptions

• ’Top 2’ global IP backbone directly connecting 345 million end-users. 80% of top content providers.

• Our network reaches 62 countries with 200 points of presence across Europe, North America and Asia

• 26 013 employees at year-end 2013
Kaapro Kanto
Certified Security Architect
SABSA, IAF, Togaf9, CISSP, CSSLP, CISA, CCSK

• TeliaSonera – Chief Architect, Security and Privacy
  – Leading Security Architects in technology domains and countries
  – Translating business strategy to technology and security strategy and programs
  – Enabling architects across to company to design and implement security and privacy

• KPMG – Head of Enterprise Architecture Business Line
  – Leading a team of Security and Enterprise architects in various assignments in government, media and finance sectors
  – Specialising in ICT transformations, corporate transactions and security architectures (design and audit).

• Capgemini – Security and Solution Architect
  – Chief Security Architect for outsourcing services and security manager for application services
  – Architecting banking, micro payment, global identity management and government eService solutions

• TeliaSonera
  – Senior Security Specialist in CSIRT/SOC
  – System Manager in Broadband Business Area
Information Security Architecture

Theory

Enterprise View

Operational View
The use of the term ‘security architecture’ is often applied within the information security community (eg by standards bodies, information security groups and vendors) for a variety of purposes, which include:

• describing the **security structure and components** of operating systems (eg Common Data Security Architecture (CDSA) and ISO7498-2)

• explaining the **security features** of applications and security protocols (eg Java Security Architecture and RFC 4301 (IPSec))

• highlighting the **security specifications** of business or IT infrastructure applications (eg Cisco SAFE Blueprint)

• promoting the **functionality and interoperability** of security products (eg Symantec SESA and Checkpoint NGX).
Security Architecture definition
Information Security Forums

Security architecture is a set of representations that describe the function, structure and interrelationship of the security components within an environment.

Provides the context in which the security architecture is applied. It can vary in type, structure, content and scale. Examples of environments include:

- software development (e.g. financial transaction systems, resource planning systems and manufacturing systems)
- IT infrastructure (e.g. WAN, LANs and isolated networks)
- major IT projects (e.g. deploying an enterprise resource planning (ERP) system or a customer relationship management (CRM) system)
- enterprise-wide systems (e.g. the combined architectures relating to networks, systems, applications and information within the organisation).

Referenced in the security architecture perform functions to protect the confidentiality, integrity and availability of information and information systems in an environment.

Security components can vary depending on the type of security architecture, but often include security controls (e.g. segregation of duties, security administration and physical protection), security services (e.g. authentication, access control and security event logging), and security products (e.g. firewalls, intrusion detection, anti-virus software and content filtering).
In practice, security architecture involves more than just producing a set of representations that relate to an environment. Security architecture can be supportive of, and influenced by various elements of the information security function, including:

- **security governance** (eg security strategy, security principles, security policy, security standards / procedures)
- **information risk analysis** (eg business impact assessments, threat and vulnerability assessments and control selection)
- **security operations** (eg asset management, information and security classification, and change management)
- information security-related **projects** (eg systems development, application security and systems configuration)
- other aspects of security (eg physical security and business continuity).
Security Architecture Process
Application Security Architecture

• Business Requirements
  – Business Model
  – Data Essentials
  – End-Users
  – Partners
  – Administrators
  – Regulations

• Application Requirements
  – Environment
  – Data Processing
  – Access
  – Application Monitoring
  – Application Design

• Infrastructure Requirements
  – Network
  – Systems
  – Infrastructure Monitoring
  – Virtualization and Externalization

• Security Program Requirements
  – Operations
  – Change Management
  – Software Development
  – Corporate

Diagram:
- Application
- Host
- Network
- Deployment and Infrastructure
- Security Frame
- Layer by Layer
  - Presentation
  - Business
  - Data
- Input Validation: Session Management
- Authentication: Cryptography
- Authorization: Parameter Manipulation
- Configuration Mgmt: Exception Management
- Sensitive Data: Auditing and Logging
Security in Software Architecture
Maturity Model view
Areas of Maturity Model

• **Governance** is centered on the processes and activities related to how an organization manages overall software development activities. More specifically, this includes concerns that cross-cut groups involved in development as well as business processes that are established at the organization level.

• **Construction** concerns the processes and activities related to how an organization defines goals and creates software within development projects. In general, this will include product management, requirements gathering, high-level architecture specification, detailed design, and implementation.

• **Verification** is focused on the processes and activities related to how an organization checks and tests artifacts produced throughout software development. This typically includes quality assurance work such as testing, but it can also include other review and evaluation activities.

• **Deployment** entails the processes and activities related to how an organization manages release of software that has been created. This can involve shipping products to end users, deploying products to internal or external hosts, and normal operations of software in the runtime environment.
The Threat Assessment (TA) Practice is centered on identification and understanding the project-level risks based on the functionality of the software being developed and characteristics of the runtime environment. From details about threats and likely attacks against each project, the organization as a whole operates more effectively through better decisions about prioritization of initiatives for security. Additionally, decisions for risk acceptance are more informed, therefore better aligned to the business.
ENTERPRISE ARCHITECTURE VIEW
Enterprise Architecture view

Enterprise Context
- Vision & Mission
- Strategy
- Drivers & Objectives
- Standards, Rules, Guidelines
- Business Models
- Principles
- Risks

Business Architecture
- Goals & Objectives
- Business Model
- Business Services
- Business Processes
- Business Roles

Information System Architecture
- Applications Landscape
- IS Components
- System Interactions
- Lifecycle

Information Architecture
- Information Objects
- Business Information Services
- Information Interaction
- Ownership, Usage, Classification

Technical Infrastructure
- Communication Services
- Computing Services
- Storage Services
- Management Services
- Generic Applications
Security & Privacy in Business Architecture

• Business Architecture sets the requirements for security and privacy.
  – Legal and Regulatory requirements and industry practices
  – Corporate Policies, Customer Promise
  – Trust and Control Frameworks, Security Principles

• Identification of key processes
  – Interaction with the customer
  – Roles in different parts of the process

• Business Impact Analysis
  – Business Continuity (Use vs Buy)
  – Confidentiality / Privacy (Buy vs End)

• Risk Analysis
  – Key risk areas and acceptable risk levels
**Information Aspect Area**

- What information do we collect, use, store?
- How do we classify that information and how does it affect the way we protect it?
- Who can access that information, why, when?
  - Customer?
  - Support Services?
  - Lawful Authorities?
- What is the Lifecycle of information?
  - Where do we use it?
  - How does it change?
  - When do we delete it?
- What is the value of information?
  - Increased Revenue
  - Better Services
  - Customer Trusts
Information Systems Aspect Area

- Business and Information views allow us to
  - Define what type of information systems are needed
  - Grouping based on drivers: cost, risk, …
  - Classification on Services
  - Information flows and lifecycle

- Common Services
  - Identity and Access Management
  - Perimeter Protection
  - Asset Management
  - Monitoring and Automation

- Rules, Practices, Guidelines
  - IT Security Policy & Requirements
Technology Infrastructure Aspect Area

• Technology Infrastructure creates the foundation for services
  – Networks, Servers, Storage, Middleware, etc.

• Security Standards, Rules and Guidelines
  – Network classification
  – Hardening guides
  – Logging & monitoring
  – Encryption services
  – Disaster recovery

• Service Levels
  – Bronze, Silver, Gold (Cost / Availability / Security)
OPERATIONAL APPROACH
Case: Coordinate and scale your resources

Security Governance

Architecture Governance

Governance, Risk and Compliance

Security Coordinators

IT

Security

Coordination of security related tasks during projects lifecycle
Reporting to stakeholders about compliance to policies and instructions

Security Design Review and Support

Security Validations and Operations

Project Team executing the implementation

DP0 → DP1 → DP2 → DP3 → DP4 → DP5 → DP6

Security Architects
Common security enablers
Standard solutions for security
Process and technology view

Security Operations Center
Security Audits for projects and services
Continuous compliance and reporting

Architecture Governance
Common Solutions
Cost efficiency and compliance
Longterm planning

Governance to track, involvement to enable
But aren’t incomplete architectures risky?

- Build in multiple iterations and scope only small improvements for them
  - If you run out of funding you still have done great improvements

- Requires spearheads who are able to market what you are doing and use incomplete work in big picture

- Focus on live knowledge: Document what is needed and spread the knowledge

- Make sure you have communicated strategy and report on measurable targets during the process

- Bare in mind your compliance requirements and work towards them through scoping and design
Collaboration brings Efficiency

• Architecture and Security communities
  – Collaboration between professionals to exchange knowledge
  – Collaboration between professions to deepen knowledge
  – 70 / 20 / 10 learning model

• People Capabilities
  – You learn by doing with your peers
  – You should also get some formal training
    – Certified x y z to support both security and technology
  – Make sure you can use externals when needed

• Reuse of solutions comes from people
## Pointers for organizations

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENABLEMENT</td>
<td><strong>Train and certify your professionals to support technology and security transformation.</strong> Architect with CISA or security validator with CCNA or MCP are strong assets teaching the organization.</td>
</tr>
<tr>
<td>LIVE KNOWLEDGE</td>
<td><strong>Share the knowledge between architects and security professionals in community work.</strong> Governance and documentation is important but focus is different.</td>
</tr>
<tr>
<td>COMPLIANCE</td>
<td><strong>Use compliance frameworks and audit against those but remember your fellow architect can perform your project audit</strong> and find new way to solve requirement.</td>
</tr>
<tr>
<td>COST</td>
<td><strong>Build a business case to small improvements even after you solved something.</strong> Each of those can work as your security enabler or architecture building block and those can decrease the overall cost.</td>
</tr>
<tr>
<td>CUSTOMER</td>
<td><strong>Ensure that customer expectations on security and privacy are met in all projects and services.</strong> Decrease complexity and create enablers for faster execution.</td>
</tr>
</tbody>
</table>
Thank you!

Kaapro Kanto

+358 40 30 25 709
kaapro.kanto@teliasonera.com