Security Architecture
- Week 8 -

Enterprise Architecture
Week 8

• Topics in-the-news
• Week 8 assignment:
  - RBAC vs ABAC
• Lecture: Enterprise Architecture
• Quiz
Enterprise Architecture

Enterprise architecture (EA) is a discipline for proactively and holistically leading enterprise responses to disruptive forces by identifying and analyzing the execution of change toward desired business vision and outcomes.

- Gartner
What do we mean by enterprise architecture?

- What do we mean by enterprise architecture
- Evolution of enterprise computing
- Architectural components
- Process Orientation
- Federal and NIST standards
- Advantages of Enterprise Architecture
- Limitation and vulnerabilities
What do we mean by enterprise architecture?

Microsoft's Michael Platt offers a view of enterprise architecture as containing four points-of-view called the business perspective, the application perspective, the information perspective, and the technology perspective.
What do we mean by enterprise architecture?

- Business Architecture
  - Drives
  - Information Architecture
    - Prescribes
      - Information Systems Architecture
        - Identifies
          - Data Architecture
            - Supported by
              - Delivery Systems Architecture
                - Hardware, Software, Communications

External Discretionary & Non-Discretionary Standards/Requirements
What do we mean by enterprise architecture?

• Business perspective
• Application perspective
• Information perspective
• Technology perspective
Evolution of Enterprise Architecture

Why discuss this?
- Enterprise security parallels the evolution of enterprise architecture
- formal versus informal history
Formal History

- Microsoft
Informal History

• Software vendors like Hogan Systems started building Enterprise systems for financial institutions in the mid-1980s
  – Security was at the application and database level
  – PC/terminal sessions identified specific system users by username and password

• Networks were still mostly private business communications systems. The internet existed but was mostly used by students, academics, government and for inter-company email
  – So, things were mostly locked down and local

• Increasing use of the internet (ISPs) during the 90s
  – Separate parts of company integrated with available broadband (fiber build out)
  – Manufacturing systems started integrated supply chain functions

• Risks of an interconnected world with an enterprise architecture that connects the entire supply chain
Implications for Security Architecture

• Evolved from a period of isolation
  - Isolated systems
  - Isolated networks
  - Private networks

• Adapting to complex connectivity context
  - Perimeter security orientation
  - Evolving application and “object” security
  - Move toward predictive analytics and advanced detection and response
Architectural Components

**Enterprise Architecture - A Framework**

<table>
<thead>
<tr>
<th>Scope (Contextual)</th>
<th>Data</th>
<th>Function</th>
<th>Network</th>
<th>People</th>
<th>Time</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planner</td>
<td>Entity = Class of Business Thing</td>
<td>List of Processes the Business Performs</td>
<td>List of Locations in which the Business Operates</td>
<td>People in the Organization</td>
<td>List of Events/Cycles Significant to the Business</td>
<td>List of Business Goals/Strategies</td>
</tr>
<tr>
<td>System Model (Logical)</td>
<td>e.g. Logical Data Model</td>
<td>e.g. Application Architecture</td>
<td>e.g. Distributed System Architecture</td>
<td>e.g. Business Rule Model</td>
<td>Ends = Structural Assumptions, Means = Solution Assumptions</td>
<td></td>
</tr>
<tr>
<td>Designer</td>
<td>Entity = Data Entity, Role = Data Relationship</td>
<td>Proc. = Application/Function, ID = User View</td>
<td>Node = IS Function, Classification, Source, etc.</td>
<td>Line = Line Characteristics</td>
<td>Time = System Event Cycle, Processing Cycle</td>
<td></td>
</tr>
<tr>
<td>Technology Model (Physical)</td>
<td>e.g. Physical Data Model</td>
<td>e.g. System Design</td>
<td>e.g. Interface Architecture</td>
<td>e.g. Business Rule Model</td>
<td>Ends = Condition Means, Action</td>
<td></td>
</tr>
<tr>
<td>Detailed Representations (Out-of-Context)</td>
<td>e.g. Data Definition</td>
<td>e.g. Program</td>
<td>e.g. Network Architecture</td>
<td>e.g. Business Rule Model</td>
<td>Ends = Sub-condition Means = Step</td>
<td></td>
</tr>
</tbody>
</table>


Greg Senko
## Security applied across the Zachman Framework

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>SECURITY COMPONENT(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Elemental Data control through database and application access control systems</td>
</tr>
<tr>
<td>Function</td>
<td>Application specific restrictions to tools and functions based on application level Access Control Language</td>
</tr>
<tr>
<td>System</td>
<td>System logon controls through ID/Password and two factor authentication processes</td>
</tr>
<tr>
<td>Technology</td>
<td>Device specific access controls – examples, WiFi encryption, MDM systems, identity security appliances</td>
</tr>
<tr>
<td>People</td>
<td>Identity Management Systems, Behavior-based access controls, predictive analytics</td>
</tr>
<tr>
<td>Time</td>
<td>Time-based data sensitivity classification, timed access permissions</td>
</tr>
</tbody>
</table>
Movement toward “Process Orientation”

- Inter-connected world allows for processes that expand beyond:
  - Company departments (accounts payable/sales)
  - Company operations (order management/production planning)
  - Supplier management (integrated supply chain/ JIT materials)
  - Dis-intermediated customer relationships (distributors versus direct client sales)

- What is the “perimeter?”
  - Vendor systems
  - Customer systems
  - Mobile devices
  - The internet
NIST and Other Standards

- Defense industry frameworks
  - DOD
  - Individual services
- Intelligence community frameworks
  - CIA
  - NSA
- Other Government frameworks
  - NIST
  - FEA
- Open-source frameworks
  - TOGAF
- Proprietary frameworks
  - IBM/Oracle reference architectures
Advantages of Enterprise Architecture

• Strategic perspective
• Opportunity for holistic approach
• Can evolves with advances in technologies
• Supported with well documented formal frameworks
• Well understood and tested approach
Limitations of Enterprise Architecture

• Legacy of perimeter security
• Slow to respond to rapid changes in technology
• Can never fuller anticipate impact changing customer expectations
• Expensive to document and maintain
• Can become a mission in itself
Quiz