Enterprise Security Architecture
Concepts and Practice

Jim Whitmore
whitmore@us.ibm.com
Abstract

In the early 90’s IBM Global Services created a Security Consultancy to respond to the business opportunity for security services for IBM customers and in support of the IBM business.

In 1999 there was an initiative in IBM to establish the security discipline within the IT Architect profession, along with related design methods and practitioner support materials.

This presentation and discussion will offer a view of security architecture and security architecture methods.

Topic Flow:
• Roles
• Methods, Models and Modeling for Security
• Elements of Enterprise Security Architecture
Roles in solution development projects

Project Manager
A project manager is the person who leads and is accountable for the success of the project.

Consultant
A consultant is an agent of change, who advises and facilitates through: research, data collection, data analysis, preparation and presentation of recommendations, and project design.

Architect
The IT Architect designs solutions to client business problems through the reasoned application of information technology.

Specialist
IT Specialists develop proof of concepts, design, develop, build, test and implement systems. IT Specialists are the hands on professionals.

---

### Business representation of architecture
- Stakeholder view

### System representation of architecture
- Structural view
- User view
- Behavior view

### Physical representation of architecture
- Environment view
- Implementation view
- Operational view

---

Project timeline
consultant → architect → specialist
Security in IBM Global Professions

Security Architecture
Security Architecture involves the design of inter- and intra-enterprise security solutions to meet client business requirements in application and infrastructure areas.

Architects performing Security Architecture work must be capable of defining detailed technical requirements for security, and designing, documenting and assuring functional and operational architectures using appropriate security technology and process components, and validating that the solution meets the security requirements.
Methods, Models and Modeling
A design method requires a model and a systematic process with thoughtful constraints

Models are developed and applied in several ways:

1. an “example” is a model with no claims of correctness;
2. a “pattern” is a model that represents a clear and detailed archetype or prototype;
3. an “exemplar” is a faultless standard that is the source of comparison;
4. an “ideal” is the best possible exemplification, either real or conceptual.

Modeling is that part of the design process that creates a new form (an instance) from the initial form (a model).

It is common practice to iterate through the modeling process several times in order to consider all of the requirements, functions and constraints before achieving a balanced solution.

On a small scale, modeling can be a mental process for a single individual. Modeling expands dramatically when there are multiple designers and hundreds of diverse requirements that need to be reconciled.
## Modeling lifecycle

<table>
<thead>
<tr>
<th>Custom</th>
<th>Integrated sub-assemblies</th>
<th>Mass Customization</th>
<th>Plug-and-Play</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each instance of architecture is one of a kind.</td>
<td>Each overall architecture is one-of-a-kind, with recognizable elements.</td>
<td>Basic tools and seasoned reference materials that lead to consistent and repeatable instances of architecture.</td>
<td>Self-defining, self configuring technologies that can be integrated using intuitive tools.</td>
</tr>
</tbody>
</table>

- **Custom**
  - Few artifacts or reliable models

- **Integrated sub-assemblies**
  - Prototype models based upon artifacts

- **Mass Customization**
  - Archetype models
  - Vetted patterns

- **Plug-and-Play**
  - Embedded function

### Lifecycle timeline
- **Wireless networking**
- **Security**
- **Object oriented programming**
- **Wired networking**

**Lifecycle timeline**
Models for security
Depending upon your background, Information Technology Security may be expressed in various ways.

Information Assurance (IA)

Information Systems Security (INFOSEC)
Here is an alternate view that aligns knowledge and the responsibility to Application Development, Systems Operations and Network Operations organizations / departments.

- **Application and Data Security**
  - Authentication
  - Authorization
  - Access Control
  - Callable Security Services
- **System Security**
  - Performance
  - Availability
  - Configuration
  - Operations
- **Network Security**
  - Firewalls
  - Encryption
  - Virtual Private Networks
  - Intrusion Detection
However security is described, an effective Information Security strategy requires a broad understanding of the business landscape…
... and knowledge of how to apply a wide range of security-related technologies.

Authentication
Authorization
Access Control
Callable Security Services

Performance
Availability
Configuration
Operations

Application and Data Security

System Security

Network Security

Data Applications

Business Driven Integrated solutions Middleware

Services

Operating Systems

Biometrics

Hardware

Perimeters

Security Protocols

Anti-virus

Firewalls

Encryption

Virtual Private Networks

Intrusion Detection

This is not a model!
In support of IBM security practitioners, a conceptual model for Security functions has been developed from Common Criteria Security Functional Requirements.

**Common Criteria Functional Requirements classes**

- Security Audit (FAU)
- Communication (FCO)
- Cryptographic support (FCS)
- User data protection (FDP)
- Identification and authentication (FIA)
- Security management (FMT)
- Privacy (FPR)
- Protection of functions (FPT)
- Resource utilization (FRU)
- TOE access (FTA)
- Trusted path/channels (FTP)

**Security Subsystems**

- Credential Subsystem
- Access Control Subsystem
- Information Flow Control Subsystem
- Security Audit Subsystem
- Solution Integrity Subsystem

*Patent Pending # 20020157015*

*Method for Designing Secure Solutions, IBM Systems Journal, September 2001 (see References page)*
The model provides a bridge between multiple views of Information Systems Security and **Security Management** tasks of policy definition, enforcement and review.

---

**Security Subsystems**

- **Credential Subsystem**
- **Access Control Subsystem**
- **Information Flow Control Subsystem**
- **Security Audit Subsystem**
- **Solution Integrity Subsystem**
When combined with a thoughtful constraints, this Security system model can provide a starting point for design as well as a baseline for evaluating the completeness of a design.

### Output of the design process:
1. Stakeholder view
2. Structural view
3. User view
4. Behavior view
5. Environment view
6. Implementation view
7. Operational view

### Some thoughtful constraints:
1. All five subsystems exist in every design
2. All five subsystems are interdependent
3. The strength of security mechanisms and services helps determine trustworthiness of solution
4. The integration of security mechanisms and services with business processes helps determine trustworthiness of solution
5. Some security mechanisms and services may necessarily exist in "non-security" components
Modeling for security
Functional modeling vs. Pattern-based modeling

<table>
<thead>
<tr>
<th>Custom</th>
<th>Integrated sub-assemblies</th>
<th>Mass Customization</th>
<th>Plug-and-Play</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each instance of architecture is one of a kind.</td>
<td>Each overall architecture is one-of-a-kind, with recognizable elements.</td>
<td>Basic tools and seasoned reference materials that lead to consistent and repeatable instances of architecture.</td>
<td>Self-defining, self-configuring technologies that can be integrated.</td>
</tr>
</tbody>
</table>

- **Design Traceability via documentation**
- **Design by “best practice”?**
- **Design Traceability via certification**
- **Functional / Operational modeling**
- **Pattern-based modeling**

- Few artifacts or reliable models
- Prototype models based upon artifacts
- Archetype models
- Vetted patterns
- Embedded function

- **Wireless networking**
- **Security**
- **Object oriented programming**
- **Wired networking**

**Lifecycle timeline**
Functional / Operational Modeling for Security

Functional: Technology independent abstraction of security components

- Structural view
- User view
- Behavior view

Operational: Technology related mapping of security components

- Environment view
- Implementation view
- Operational view
Here is a sample e-Business architecture (see reference page)
Patterns-based modeling…
a starting point for architecture

<table>
<thead>
<tr>
<th>Examples</th>
<th>Business patterns</th>
<th>Composite patterns</th>
<th>Integration patterns</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Self service</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Collaboration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aggregation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Extended Enterprise</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>e-Commerce</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Portal</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Account Access</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Trading Exchange</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sell-side hub</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Buy-side hub</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Integration</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Application Integration</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web Presence</th>
<th>Y</th>
<th>Y</th>
<th>+/-</th>
<th>Y</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business-to-Consumer</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Business-to-Business</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

* [http://www.ibm.com/developerworks/patterns/]
## Patterns-based modeling for Security

<table>
<thead>
<tr>
<th>IBM Business Security Patterns**</th>
<th>Business patterns</th>
<th>Composite patterns</th>
<th>Integration patterns</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Presence</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Business-to-Consumer</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Business-to-Business</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Operational Security</td>
<td>Y</td>
<td>+/-</td>
<td>+/-</td>
</tr>
<tr>
<td>High Assurance</td>
<td>Y</td>
<td>+/-</td>
<td>+/-</td>
</tr>
</tbody>
</table>

- work in progress


Patterns-based Modeling...

Business representation

- Stakeholder view
- Business behavior view

System representation with security

- Structural view
- System behavior view
Patterns-based Modeling...

Business pattern: Self-service; Application pattern: Stand-Alone Single Channel
Security Application Services: Access Mgmt with Self-service Identity Mgmt

Runtime View

- User view
- Environment view
- Implementation view
- Operational view

(example)
Summary…

- Architecture has multiple views.
- A design method requires a model and a systematic process with thoughtful constraints.
- The effective practice of security architecture is dependent upon many aspects of the design process.
- More work needs to be done in the area of architecture representation and visualization.

<table>
<thead>
<tr>
<th>Business representation of architecture</th>
<th>System representation of architecture</th>
<th>Physical representation of architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>•Stakeholder view</td>
<td>•Structural view</td>
<td>•Environment view</td>
</tr>
<tr>
<td></td>
<td>•User view</td>
<td>•Implementation view</td>
</tr>
<tr>
<td></td>
<td>•Behavior view</td>
<td>•Operational view</td>
</tr>
</tbody>
</table>
## Selected Resource Links

<table>
<thead>
<tr>
<th>Resource</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Telecommunications Union</td>
<td><a href="http://www.itu.int/home/index.html">http://www.itu.int/home/index.html</a></td>
</tr>
<tr>
<td>International Organization for Standardisation</td>
<td><a href="http://www.iso.ch">http://www.iso.ch</a></td>
</tr>
<tr>
<td>Open Group (TOGAF)</td>
<td><a href="http://www.opengroup.org/togaf/start.htm">http://www.opengroup.org/togaf/start.htm</a></td>
</tr>
</tbody>
</table>