Architecting for security

A case study

Claude Vigeant Ing.
President, OKIOK
Agenda

• Introduction
• Business context
• AMI and SmartGrid context
• The Question...
• Security Foundations
• Security Architecture
• Summary
• Questions
Introduction

• We will look at an enterprise security architecture currently being implemented by a major Canadian integrated utility that:
  
  – Defines controls along each of the three dimensions of people, processes and technology
  
  – Implements a scalable enterprise wide service fabric
  
  – Establishes a proactive stance for meeting the challenges related to AMI and smart grid deployments
  
  – Leverages the convergence between IT and domain specific "Operational Technologies"
• Hydro-Québec generates, transports and distributes electricity in the province of Québec (Canada)
• Its sole shareholder is the Québec government
• The company relies mainly on renewable generating options, in particular hydropower (worldwide biggest producer), and supports the development of wind energy through purchases from independent power producers
• It also conducts research in energy-related fields such as energy efficiency
• It is currently initiating several distribution automation projects as well as a large scale AMI project
AMI and smart grid context

- Small scale pilot projects completed
- Completing RFP phase for MDMS / Meters / Services
- 3.7M meter rollout
- Several T&D automation and efficiency projects

*Network will expand a hundredfold*
How can we attain and maintain an acceptable level of risk?
Enterprise Security Foundations

1. Effective Governance
2. Mature Processes
3. Forward-looking Architecture
Why a Security Architecture?

• To define a set of optimal and coherent solutions to security requirements

• To systematically apply security measures that
  – Are aligned to business context
  – Meet governance requirements
  – Meet acceptable risk target

• To ensure effectiveness of security program
Enterprise Security Architecture Model

People
- Protect before, during and after employment

Processes
- Build security in
- Control access
- Prevent and react

Technology
- Four IT domains
- Mission critical "Operational Technologies"

Metrics and indicators
- Track effectiveness of program

Security Architecture
- People:
  - Background Checks
  - Awareness and training
  - Staffing / Mandating
  - Onboarding / Offboarding
- Processes:
  - SSDLC
  - Access Management
  - Threat Management
  - Incident Management
  - Vulnerability Management
- Technology:
  - Information
  - Applications
  - Infrastructure
  - Perimeter and telecom
  - AMI / SCADAs
- Metrics
- Indicators
- Dashboards
Mapping Enterprise Security Architecture to SABSA

Enterprise Security Architecture

- Business objectives
- Policies and standards
- Legal and regulatory req.
- Risk management

Security Architecture

- People
  - Awareness and training
  - Background Checks
  - Staffing / Mandating
  - Onboarding / offboarding

- Processes
  - SSDLC
  - Access Management
  - Threat Management
  - Incident Management
  - Vulnerability Management

- Technology
  - Information
  - Applications
  - Infrastructure
  - Perimeter and telecom
  - AMI / SCADAs

- Metrics
- Indicators
- Dashboards

SABSA / Smart Grid Cyber Security Architecture Views

- Contextual Security Architecture
- Conceptual Security Architecture
- Logical Security Architecture
- Physical Security Architecture
- Component Security Architecture

Operational Security Architecture
# Mapping Enterprise Security Architecture to SABSA

<table>
<thead>
<tr>
<th>Contextual</th>
<th>Motivation (Why)</th>
<th>Process (How)</th>
<th>People (Who)</th>
<th>Location (Where)</th>
<th>Time (When)</th>
</tr>
</thead>
</table>

Business Context | Security Architecture | 5 Year Program | Operations
## Enterprise Security Architecture

### Logical Layer

<table>
<thead>
<tr>
<th>Domains</th>
<th>Security Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Services</strong></td>
<td><strong>Authentication</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Authorisation</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Confidentiality and Integrity</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Log Management</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Events Monitoring</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Backup</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Configuration control</strong></td>
</tr>
<tr>
<td></td>
<td><strong>IAM</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information</th>
<th>Authentication</th>
<th>Authorization</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Traceability</th>
<th>Monitoring</th>
<th>Availability and continuity</th>
<th>Compliance</th>
<th>Security Administration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perimeter and telecom.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AMI / SCADAs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Enterprise Security Services

- Authentication
- Authorization
- Confidentiality and Integrity
- Log management
- Real-time event monitoring (SIEM)
- Backup
- Configuration Control
- Security Mgmt. (ex. IAM)
Enterprise Authentication Service

Directories and Infrastructure

Enterprise Authentication Service

Corporate AD
Dev. AD
High Security Zones AD

Directories

Corporate AD
Dev. AD
High Security Zones AD

Assets

Perimeter
Intranet
Internet

Access Layer

Users

Employees
Employees
Customers
Employees
Enterprise Security Architecture
Logical Layer Details

Security Requirements

<table>
<thead>
<tr>
<th>RN 15.11.6</th>
<th>Contrôle de l'accès aux applications et aux informations</th>
</tr>
</thead>
<tbody>
<tr>
<td>RN 15.11.7</td>
<td>Informatique mobile et contrôle des accès en provenance d'un réseau externe</td>
</tr>
<tr>
<td>RN 15.11.5</td>
<td>Contrôle de l'accès aux systèmes d'exploitation</td>
</tr>
<tr>
<td>CIP 003-1-R5</td>
<td>Contrôle d'accès à l'information classée</td>
</tr>
</tbody>
</table>

Security Mechanisms

- **MEC 01**: Mot de passe
- **MEC 02**: Mot de passe unique (OTP)
- **MEC 05**: Jeton logiciel
- **MEC 06**: Jeton matériel
- **MEC 11**: Certificats X.509

Indicators

- **IND M12-03**: Gestion de la conformité (NERC CIP)

Design Patterns
Critical Processes
Secure Software Development Lifecycle

Building Security in...
(P+ Process)

- Opportunity analysis
- Preliminary analysis
- Architecture
- Design & development
- Implementation

- Meet governance requirements
- Align with Industry Best Practices

Training
- Core training

Requirements
- Define quality gates/bug bar
- Analyze security and privacy risk

Design
- Attack surface analysis
- Threat modeling

Implementation
- Specify tools
- Enforce banned functions
- Static analysis

Verification
- Dynamic/Fuzz testing
- Verify threat models/attack surface

Release
- Response plan
- Final security review
- Release archive

Response
- Response execution

Example: Microsoft Model

Also applies to procurement process...
- RFP Requirements
Critical Processes
Access Management

• **Formal access model**
  – Roles and rules (RBAC, ABAC)
  – Dynamic organisational representation
  – Access model governance

• **Access model used for**
  – Access provisionning / deprovisionning
  – Access control rule base
  – Security event monitoring

• **Focus on**
  – On boarding / off boarding
  – Periodic access re-certification
  – Background checks for critical resources
Summary

• **Security foundations**
  – Governance
  – Mature processes
  – Security Architecture

• **Security architecture**
  – People
  – Process
  – Technology

• **Scalable architecture**
  – Subset from SABSA / TOGAF / OSA models
  – 5 Domains
  – 9 Security requirements

• **Conceptual layer**
  – Guiding principles / Decisions
  – Critical Security processes
  – Enterprise Security Services

• **Logical Layer**
  – Regulatory requirements
  – Security mechanisms
  – Design patterns
  – Indicators

• **Interoperability**
  – Standards based services and mechanisms
  – Move security functions from applications / platforms to enterprise services
Questions? Thank you!

Claude Vigeant Eng.
President, OKIOK

cvigeant@okiok.com
www.okiok.com