

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

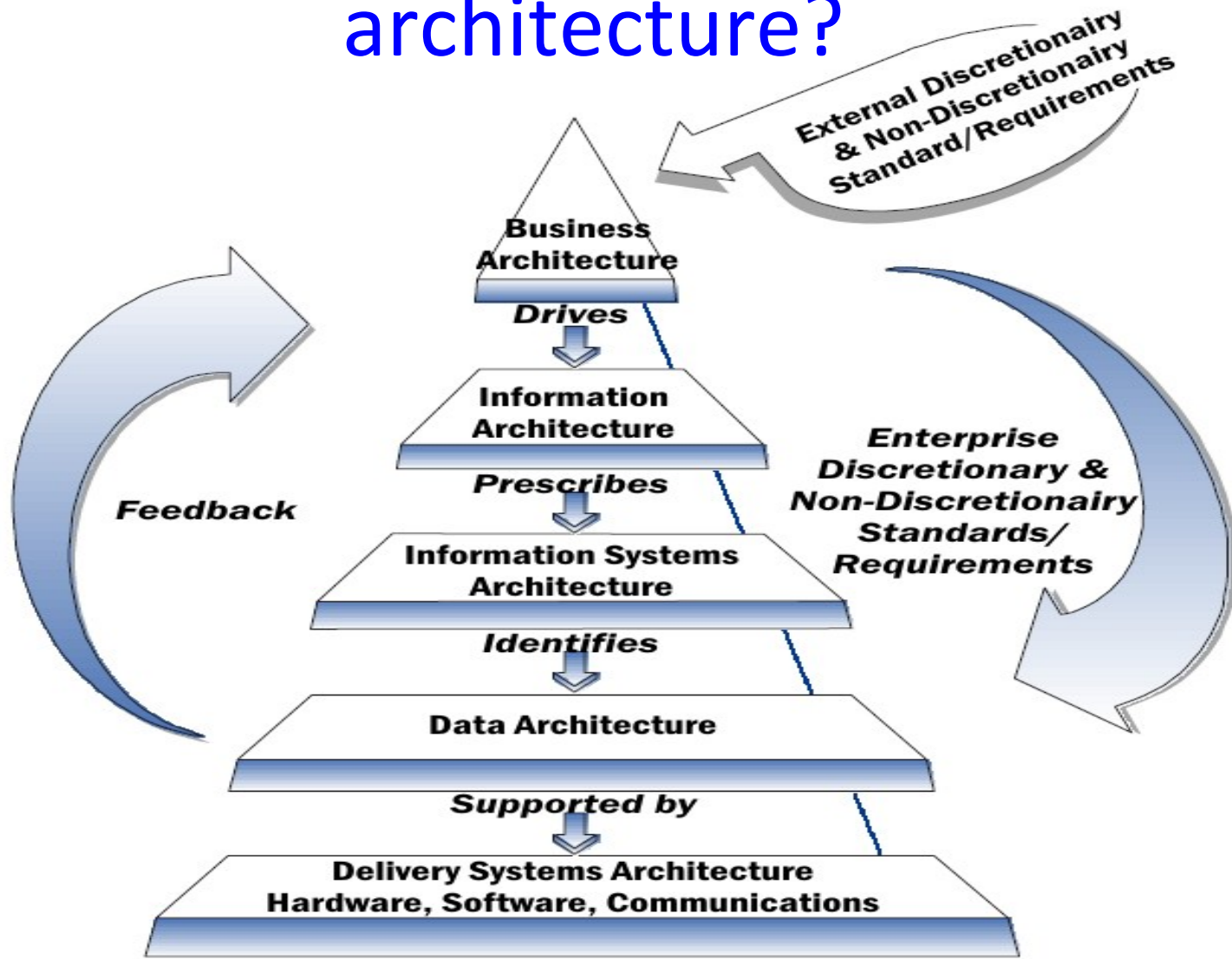
What do we mean by enterprise architecture?

- 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?



NIST

What do we mean by enterprise architecture?

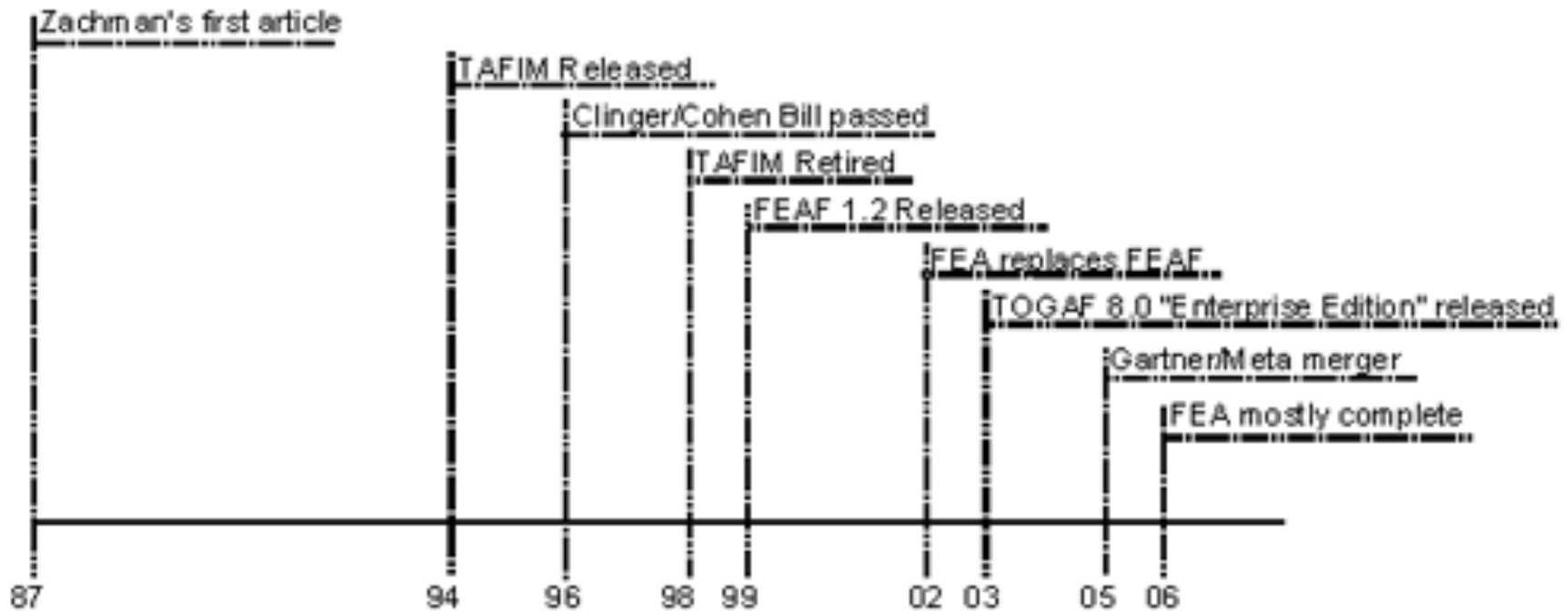
- Business perspective
- Application perspective
- Information perspective
- Technology perspective

Evolution of Enterprise Architecture

Why discuss this?

- Enterprise security parallels the evolution of enterprise architecture
- formal versus informal history

Formal History



- Microsoft

Informal History









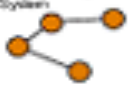



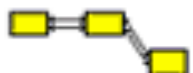

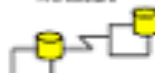















- Software vendors like Hogan Systems started building Enterprise systems for financial institutions in the mid-1980s
 - Security was at the application and database level
 - PC/terminal sessions identified specific system users by username and password
- Networks were still mostly private business communications 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 TM

	DATA <i>It'sr</i>	FUNCTION <i>It'sw</i>	NETWORK <i>It'sv</i>	PEOPLE <i>It'sy</i>	TIME <i>It'su</i>	MOTIVATION <i>It'sj</i>	
SCOPE (CONTEXTUAL)	List of Things Important to the Business 	List of Processes the Business Performs 	List of Locations in which the Business Operates 	List of Organizations Important to the Business 	List of Events/Cycles Significant to the Business 	List of Business Goals/Strategies 	SCOPE (CONTEXTUAL)
Planner	Ent/Tr = Class of Business Thing	Proc = Class of Business Process	Node = Major Business Location	People = Major Organization Unit	Time = Major Business Event/Cycle	End/Mean = Major Business Goal/Strategy	Planner
BUSINESS MODEL (CONCEPTUAL)	e.g. Semantic Model 	e.g. Business Process Model 	e.g. Business Logistics System 	e.g. Work Flow Model 	e.g. Master Schedule 	e.g. Business Plan 	BUSINESS MODEL (CONCEPTUAL)
Owner	Ent = Business Entity Reln = Business Relationship	Proc = Business Process IO = Business Resource	Node = Business Location Link = Business Linkage	People = Organization Unit Work = Work Product	Time = Business Event Cycle = Business Cycle	End = Business Objective Means = Business Strategy	Owner
SYSTEM MODEL (LOGICAL)	e.g. Logical Data Model 	e.g. Application Architecture 	e.g. Distributed System Architecture 	e.g. Human Interface Architecture 	e.g. Processing Structure 	e.g. Business Rule Model 	SYSTEM MODEL (LOGICAL)
Designer	Ent = Data Entity Reln = Data Relationship	Proc = Application Function IO = User Views	Node = I/O Function (Processor, Storage, etc.) Link = Line Characteristics	People = Role Work = Deliverable	Time = System Event Cycle = Processing Cycle	End = Struct and Assuring Means solution Assertion	Designer
TECHNOLOGY MODEL (PHYSICAL)	e.g. Physical Data Model 	e.g. System Design 	e.g. Technology Architecture 	e.g. Presentation Architecture 	e.g. Control Structure 	e.g. Rule Design 	TECHNOLOGY MODEL (PHYSICAL)
Builder	Ent = Segment/Table/etc. Reln = Pointer/key/etc.	Proc = Computer Function IO = Data Element/etc.	Node = Hardware/Systems Software Link = Line Specifications	People = User Work = Screen Format	Time = Execute Cycle = Component Cycle	End = Condition Means = Action	Builder
DETAILED REPRESENTATIONS (OUT-OF-CONTEXT)	e.g. Data Definition 	e.g. Program 	e.g. Network Architecture 	e.g. Security Architecture 	e.g. Timing Definition 	e.g. Rule Specification 	DETAILED REPRESENTATIONS (OUT-OF-CONTEXT)
Sub-Constructor	Ent = Field Reln = Address	Proc = Language Statement IO = Control Block	Node = Address Link = Protocol	People = Identity Work = Job	Time = Interrupt Cycle = Machine Cycle	End = Sub-condition Means = Step	Sub-Constructor
FUNCTIONING ENTERPRISE	e.g. DATA	e.g. FUNCTION	e.g. NETWORK	e.g. ORGANIZATION	e.g. SCHEDULE	e.g. STRATEGY	FUNCTIONING ENTERPRISE

© 1986 - 2005 John A. Zachman, Zachman International

See www.ZachmanInternational.com for 2005 Zachman Framework Standards

Security applied across the Zachman Framework

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

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 evolve 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 fully anticipate impact changing customer expectations
- Expensive to document and maintain
- Can become a mission in itself

Quiz