Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

Nishit Narang
WILPD-CSIS
(nishit.narang@pilani.bits-pilani.ac.in)

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 2: Security Architectures + Security as a Process

Source Disclaimer: Content for many of the slides is from the course Textbook(s). Refer Course Handout for list of Textbooks.

Enterprise Security

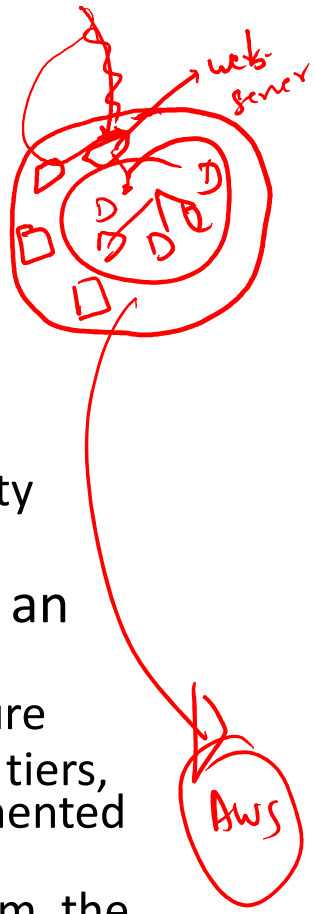
The Roadmap to Securing the Enterprise: Method and Approach

Security Architecture Models

- Generic Layered Model
  - Only connected layers communicate with each other
  - Example, the typical implementation of an Internet accessible web application positions the presentation and logic tiers within the DMZ infrastructure with the backend data located in the internal network
    - Micro-architectures (*refer* next slide)
- Complex Models
  - Source and destination zones, allowed protocols, special permitted communication channels per endpoint type
- Advanced Models
  - Based on **Data Risk***

***Data risk** is comprised of understanding what data needs protection including from whom and what, based on loss probability

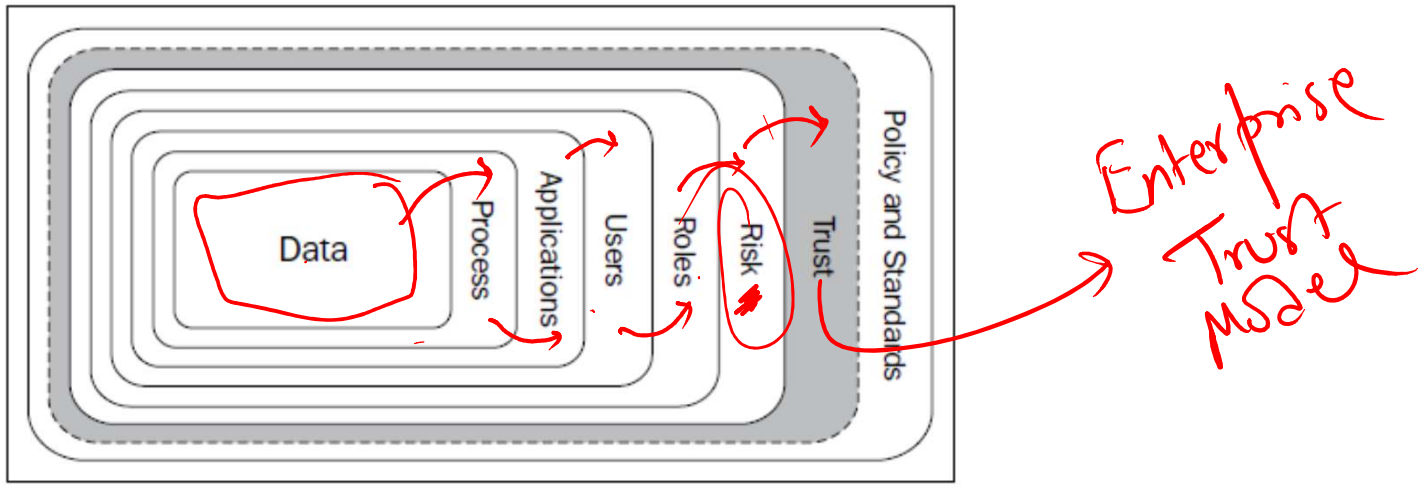
Micro Architectures



- A micro architecture is architecture within architecture
  - An example may be the logical three-tier DMZ architecture
    - Tier 1: Web or Presentation
    - Tier 2: Application or Logic
    - Tier 3: Database or Data
  - This type of architecture is more network-centric (aka network segments), but can play a part in the overall data-centric security architecture of an enterprise
- The method may be used in a cloud-based solution, where an enterprise desires to maintain the three-tier approach
  - Virtualization has had a unique effect on the security architecture
  - In order to enforce the presentation, application, and database tiers, there should essentially be three distinct physical systems segmented by a firewall
  - With the ability to host all three hosts on a single physical system, the lines of segmentation have been blurred
  - The segmentation happens at a lower physical hardware layer below the virtualized system's operating system, yet above the traditional physical network segmentation of switches, routers, and firewalls

Data-centric Security Architectures

- Data-centric security architectures emphasize enterprise data, where it is stored, how it is transmitted, and the details of any data interaction
- The focus of a security architecture is not the network segment or the system; it is the data, which is the purpose for the network, and the system
- ***Trust models*** need to be developed in such a way that they encompass all the interactions with the data they are designed to protect



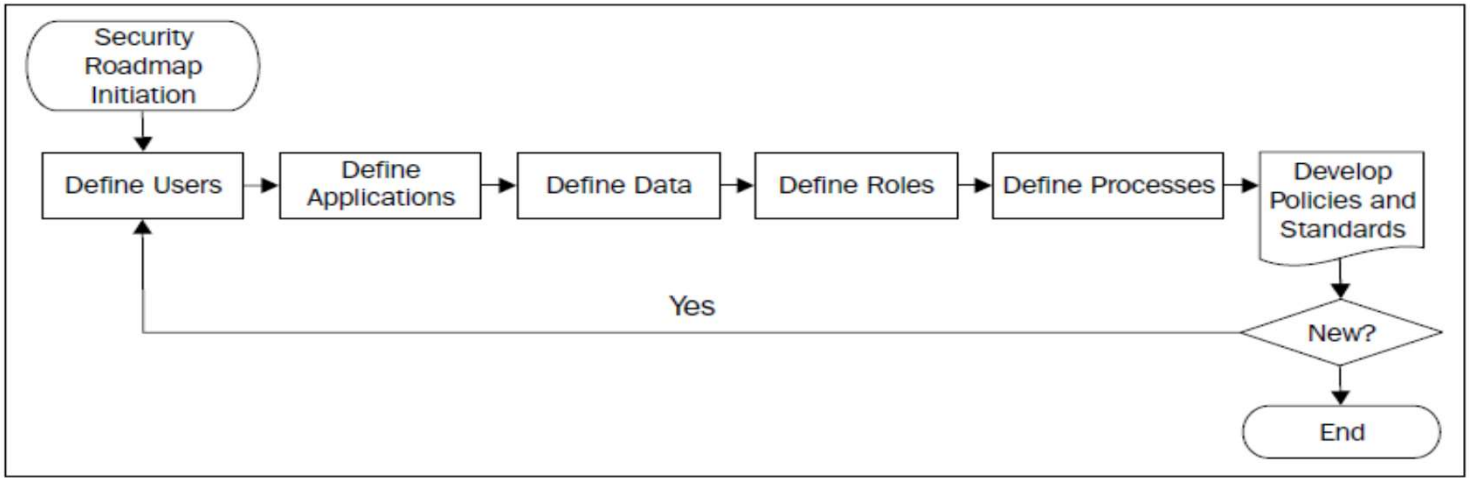
Determination of trust and how risk dictates trust and trust influences policies and standards

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Data Risk-centric Architectures

- ***Risk*** is a key factor of any security architecture
  - systems and applications exist because there is data to be generated, processed, transmitted, and stored
  - risk introduced in an enterprise is significantly data-driven
  - it does not mean that we only protect enterprise data; we still need to protect the network that makes data access possible
- What does data risk-centric mean?
  - from the perspective of the security architecture, we need to focus on the data with the most risk to the business (e.g. credit card data)
  - in other words, if the data is lost, stolen, or manipulated, it would cause adverse implications for the enterprise
- Trust models can be used as a method of placing certain user types in buckets, with these buckets further defined by a risk assessment

Architecture Roadmap: Overview



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

- Define Users within and those that interact with enterprise
- Define Applications and their purpose
- Define Data and associated needs (E.g. backup etc)
- Define roles and access rules
- Define Business Processes (business critical data and systems)
- Define policies for authorized access and standards for security
- Define existing Network Infrastructure (e.g. partner communication interfaces, website, VPN etc)
- Define Application Security Architecture to understand how security is integrated to applications through a formal SDLC. Applications are the preferred method for accessing enterprise data

Defining Data in a Trust Model

- An enterprise must understand what data exists, why the data exists, data sensitivity, and data criticality
  - This can all be assessed without thinking about the data location
- Data is the "what" portion of the data interaction
  - If it is determined that the data or "what" being accessed has little value or risk associated with it, then security mechanisms may be reduced or become non-existent.
- Typical locations of data can be determined by understanding business processes
  - In case they are not well defined, then an enterprise can begin by looking at databases and network shares for data at rest. This process should identify a majority of the enterprise data
  - Include end-point devices to look for local database instances and data stored in typical desktop processing applications. Laptops are one location that has been a significant cause of data breaches, because critical and high-risk data was stored on a laptop with no protection, and was stolen

Example: Data for Common Industries

Defining data types, value, and regulatory responsibilities per industry				
Industry	**Data type**	**Data purpose**	**Data value**	**Regulatory/legal responsibility**
Retail	Credit card numbers	Product sales	High	PCI
Healthcare	Patient information PII	Patient care and billing	High	HIPAA
Banking	Credit card numbers PII	Service Offerings	High	PCI, FTC, and SEC

If the enterprise is responsible for meeting the requirements of a regulatory body, it is imperative to fully understand the requirements and what is expected as proof of compliance. Requirements should then be integrated into the developed trust models and an effective security architecture.

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Defining Processes in a Trust Model

- Data to be protected needs to be identified
  - If the data is unknown, start with the current business processes; this should lead to the most critical data
  - This is the "why" of the data interaction
- Identify Risks in Business Processes
  - Once processes have been identified, opportunities should be taken to correct any process that introduces risks to the enterprise, as processes are primarily data-centric with direct data access and manipulation capabilities
  - Example: When scripts are used for automation in an enterprise environment, never store passwords in it

Defining Applications in a Trust Model

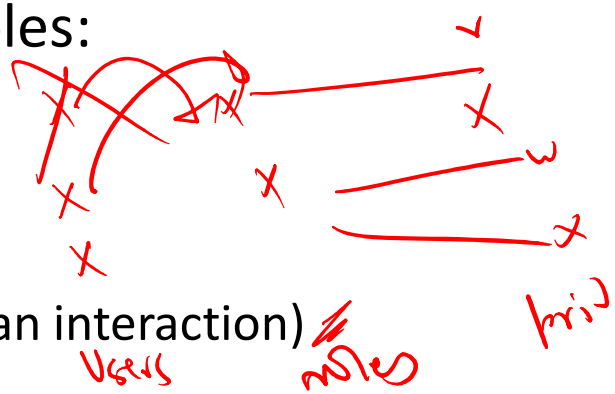
- After identification of the enterprise data and processes, we need to define the applications that transmit, process, or store the defined data
  - see the picture of "use and access"
  - Applications can be any application in the enterprise from e-mail clients to complex sales processing applications
- The methods in which the applications interact with the data become the factors defining users, roles, and ultimately the security mechanisms required
  - In some cases, applications and protocols can represent the same thing
  - Example: e-mail client applications running to access e-mails → POP3 and SMTP are the protocols leveraged to access the e-mails

Defining Users in a Trust Model

- User interacts with an application that has access to data
  - user may be a person, script, system, or another application
  - Not all users will require the same level of access
  - It is critical to identify as many users as possible and also the types of interactions with the enterprise data
  - Users can be discovered by thoroughly defining the processes in the enterprise
- There are high-level distinctions for users such as:
  - Internal (employee)
  - External (non-employee)
  - Business Partner
  - Contractor

Defining Roles in a Trust Model

- An important part of defining users is to identify the interactions that the users will have with the data including how the access will be facilitated—whether through an application, shell, script, or direct
  - This is where roles come into the picture and must be defined
- Example: Unix Administrator
  - what does the user need access to?
  - why is the access needed?
  - how is the access facilitated?
- Identified user roles based on information learned versus simply by departmental role. High-level roles:
  - Application User
  - Application Owner
  - System Owner
  - Data Owner
  - Automation scripts and applications (no-human interaction)



Defining Policies and Standards

- The last components that must be defined are:
  - the policies that will guide a secure access and use of the enterprise data, and
  - the standards that ensure a consistent application of policy
- Compliance bodies such as the PCI Council require the creation and implementation of a security policy, acceptable use policy, operational security policy, and so on
- Think of policies and standards as the law and enforcement of the security architecture

Enterprise Trust Models

- Once we have identified all the components that will help us define our trust models, they can be overlayed wherever necessary in the network—on systems, in the cloud, in applications, or anywhere applicable, as determined by the enterprise
- Depending on the trust that is given to each combination of data, process, application, and user, determination of the required security mechanisms can be defined
  - this is not a simple trust/no trust approach
  - degrees of trust depending not only on the user type, but also on the criticality of the data and associated risk
  - another way to think of this is to assign allowed trust levels depending on roles
  - any user type with a assigned trust level can access data according to the permissions associated with that assigned trust level

Example Case Study

Building an Enterprise Trust Model

Trust Model Building Blocks: Sample

Data	Process	Applications	Users	Roles	Policies and standards
Credit card numbers	Application for a new service	Web application	External, non-employee	Application user	Acceptable use Secure access
Credit card numbers	Fraud detection	Fraud software	Business partner	Application owner	Data protection standard
Credit card numbers	Storage	Database	Contractor	System owner	Data protection standard
Credit card numbers	Loyalty tracking	Business intelligence	Internal, employee	Data owner	Data protection standard
Credit card numbers	Order processing	Credit authorization and settlement	Automation	Automation	Data protection standard

Trust Model using a small scale, such as 1 to 3: 1 as *not trusted*, 2 as *median trusted*, and 3 as *trusted*

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Application User (External)

- Focus on the fact that the enterprise does not know the security posture of the end system
  - Example, an enterprise is neither responsible nor in a position to update the anti-virus signatures on the external system or make sure the end system is patched
  - the level of trust should be ***none*** with the highest level of monitoring and protection implemented

User type	External
Trust level	1: Not trusted
Allowed access	Tier 1 DMZ only, least privilege
Required security mechanisms	FW, IPS, and Web App Firewall

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Application Owner (Business Partner)

- Third party has access to a system on the internal network and the data it processes
  - there must be a level of trust
  - the enterprise more than likely signed a business contract to enable this relationship
  - with a contract in place, there are legal protections provided for the enterprise

User type	External
Trust level	2: Median trusted
Allowed Access	Tier 1 and 2, least privilege
Required security mechanisms	FW, IPS, Web App Firewall, and data loss prevention

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

System Owner (Contractor)

- Similar to a business partner, however, the contractor may seem more like an employee
  - they reside on-site and perform the job functions of a full-time staff member
  - the more access granted, the more security mechanisms must be in place to reduce the risk of elevated privileges

User type	External
Trust level	3: Trusted
Allowed access	Least privilege
Required security mechanisms	FW, IPS, Web App Firewall, and file integrity monitoring

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Data Owner (Internal)

- Has significant level of access to the enterprise data
  - As an internal employee, trust level is the ***most trusted***
  - With this access level, there is great responsibility not only for the data owner, but also for the enterprise
  - If the data is decided to have little value, then the security mechanisms can be reduced

User type	Internal
Trust Level	3: Trusted
Allowed access	Anywhere, least privilege
Required security mechanisms	FW, IPS, and Web App Firewall depending on the type of data that is being interacted with

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

Automation

- Unique, as no human interaction involved
  - many times the permissions are incorrectly configured and allow scripts the ability to launch interactive logons, and shell access equivalent to a standard user
  - also, if authentication is required the credentials are sometimes embedded in the script
  - these factors contribute to the trust level of the script and automation
  - scripts can be trusted, but not like an internal user

User Type	Automation
Trust level	2: Median trusted
Allowed access	Least privilege
Required security mechanisms	FW, IPS, Web App Firewall, file integrity monitoring, and data loss prevention depending on the data that is being interacted with

Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise