



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



BITS Pilani

Pilani Campus



<SS ZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 1: Introduction

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

What we shall cover?

- Three sub-topics in Information and Computer Security (and their linkages)
 - Enterprise Security
 - IoT Security
 - Cloud Security
- How are the sub-topics in this course linked?



Textbooks:

T1	Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise . 1st ed. Birmingham: Packt Publishing Ltd., 2013.
T2	Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing , John Wiley & Sons, 2010
T3	Shancang Li Li Da Xu, Securing the Internet of Things , Syngress, 1st Edition, 2017



We will bankrupt ourselves in the vain search
for absolute security.



- Dwight D. Eisenhower, 34th President of the United States

“Security in principle is black and white, however, implementation and the real world is gray. When security personnel operate from a binary perspective on security principles it fosters a false perspective of an ideal enterprise security posture” → *Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise. 1st ed. Birmingham: Packt Publishing Ltd., 2013.* (Course Textbook)



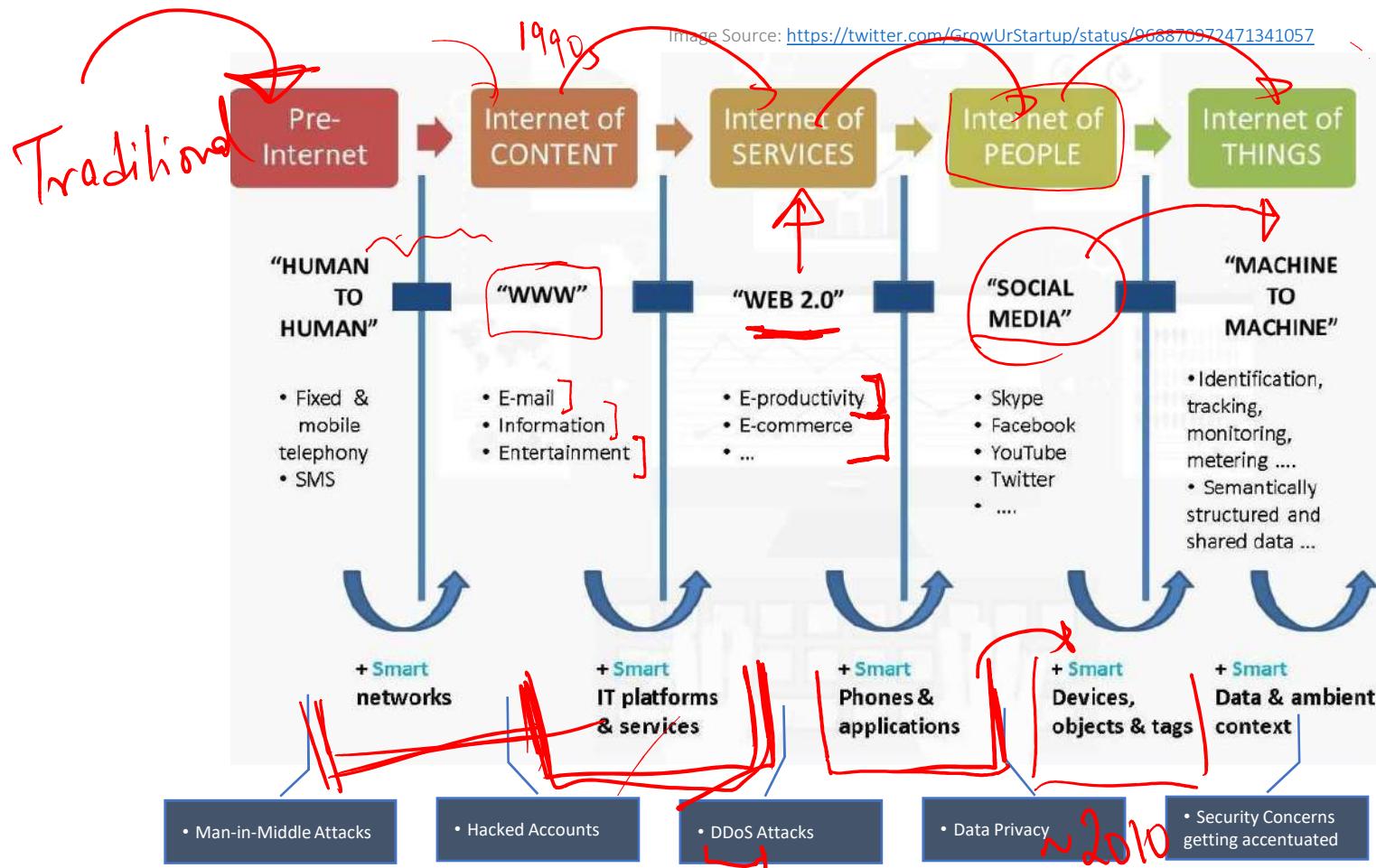
As the world is increasingly interconnected,
everyone shares the responsibility of securing
cyberspace.



- Newton Lee, Counterterrorism and Cybersecurity: Total Information Awareness



The Evolving Internet.... And the Evolving Security Concerns!



Enterprise Security

Overview, Evolution and Shortcomings



Enterprise Security: Introduction

- **Enterprise Security**

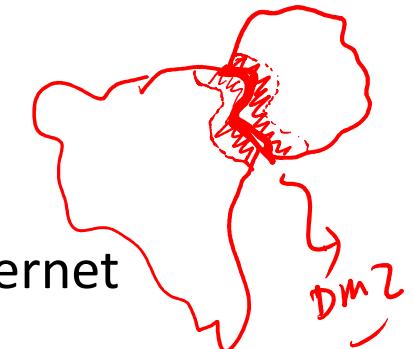
Securing the Enterprise

- What is the “Enterprise”?
 - Networks? Systems? Data? Humans?
- Traditional Enterprises vs Newer Enterprises
 - BYOD (Mobiles, Laptops, Tablets....)
 - Cloud Models
- What it means for Enterprise Security? **→ Focus on Data-centric Security**
 - A migration from a network-based concept to a data-centric focus as today's ever changing business landscape has invalidated the traditional security architectures

Enterprise Security Overview

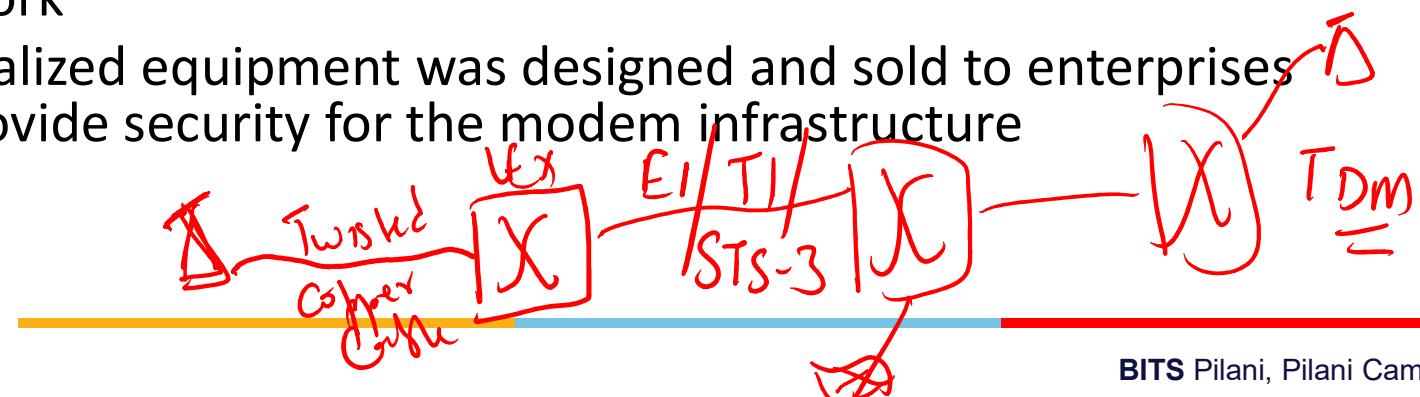
- History of Enterprise Security

- Older times → no concept of DMZ, as no public Internet existed
- Only form of Networking in the form of dial-up networking connections → not much security concerns as phone numbers had to be known
- Modems used to make outbound calls and accept inbound calls to primarily process batch jobs for large backend systems
- Security Challenge: ***war dialing*** became a method to identify modems in large banks of phone numbers for attackers to gain unauthorized access to the connected equipment or network
- Specialized equipment was designed and sold to enterprises to provide security for the modem infrastructure



ITU-T
SS7

ISER

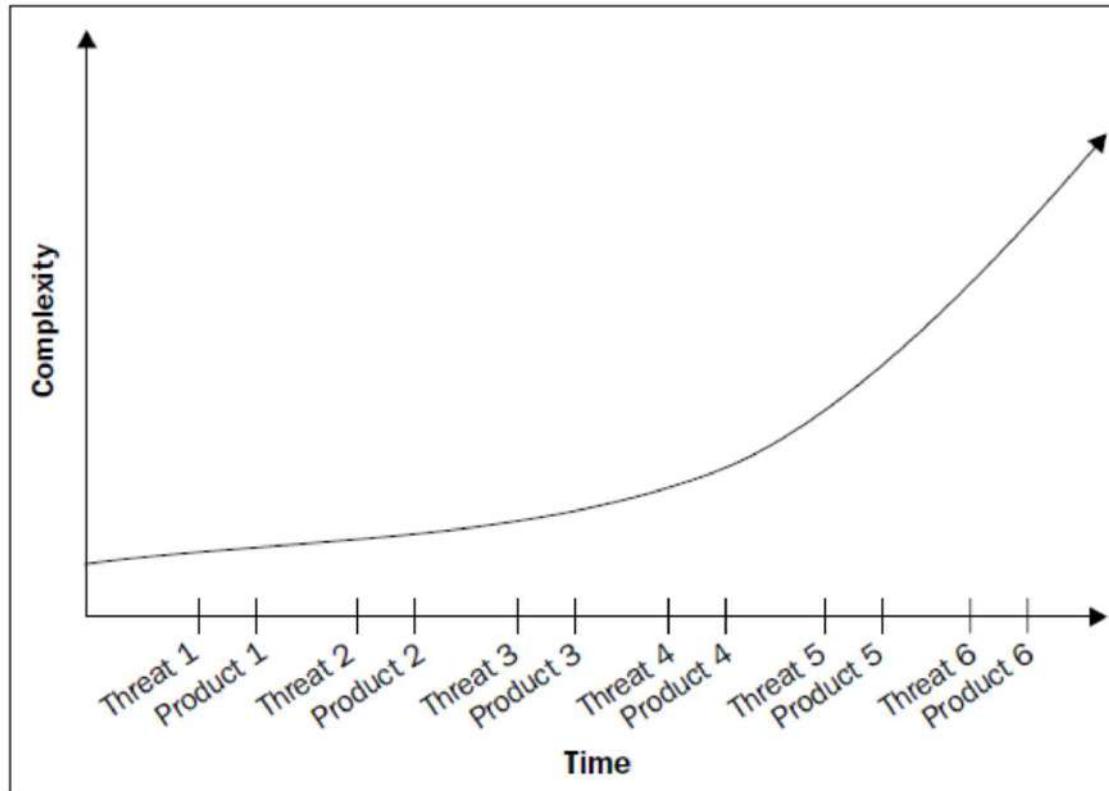




Enterprise Security Overview

- As networking technologies evolved:
 - enterprise assets became accessible on the Internet
 - weaknesses in the systems and network security were quickly identified by attackers
 - network equipment manufacturers started developing security products to defeat specific security threats as they were identified → ***“Band-aid Approach”***
 - pattern of reaction-based development of security tools continues, driven primarily by mitigating specific threats as they are identified
 - Anti-virus, firewalls, intrusion detection/prevention, and other security technologies are the direct result of an existing threat, and are *reactive*.
-

Enterprise Security Overview



Growing Complexity with each new threat



Band-Aid Approach

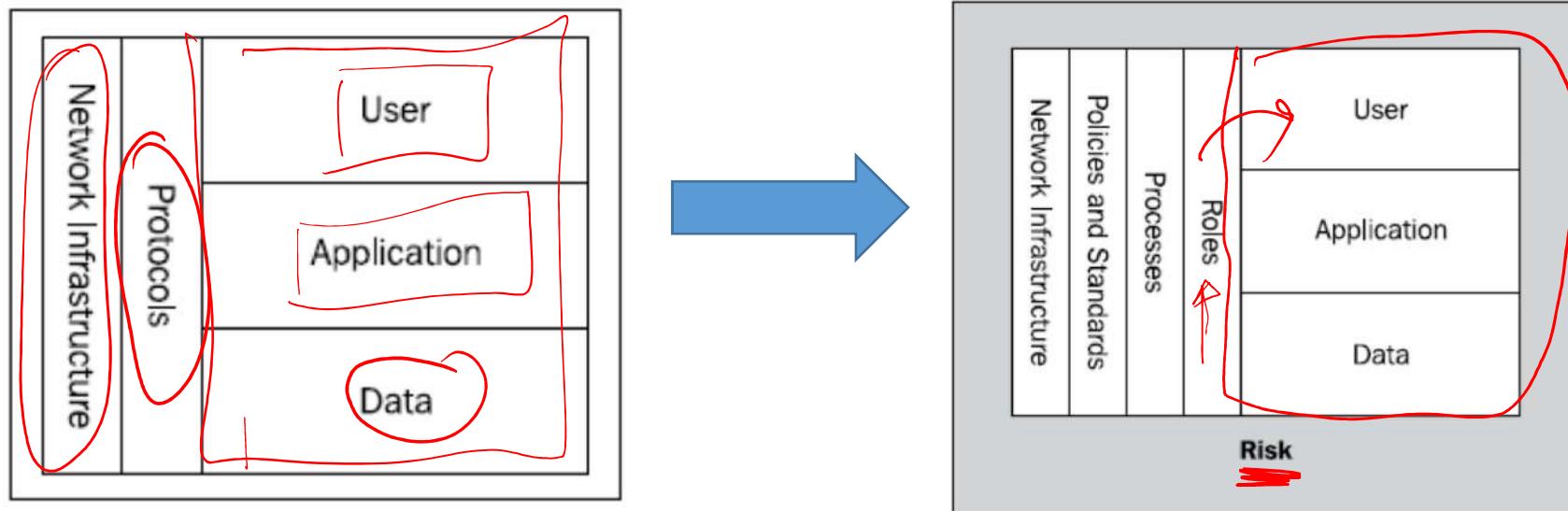
It has led to a relatively secure network perimeter instead of a functioning, extensible, enterprise-wide security architecture



Enterprise Security Overview

- Consequences:
 - Enterprise security → perimeter security by design and function
 - Until recently this made sense; though not true, it was thought that the known threat has always been external
 - It has led to bloated security budgets, crowded perimeter zones, and very little increase in security
 - We have purchased and implemented the latest next-generation firewall technology, intrusion prevention systems and a similar other myriad of security tools
 - We have increased the complexity, instead of effectiveness in mitigating threats holistically → ***the current Enterprise Security facade***

Enterprise Security Architecture



Older / earlier "security" architecture addresses user access to data in a very generic manner, focusing primarily on what protocols can be used at what tier of the network (VLAN etc)

The new security architecture addresses all facets of security and provides a realistic picture of the risk posed by any implementation.

It takes into account data, processes, applications, user roles, and users, in addition to the traditional network security mechanisms to provide end-to-end security from entry to the network to the data resident within the enterprise.



Enterprise Security Architecture

Pitfalls (1)

- The earlier security architectures do not meet the newer enterprise trends such as
 - **bring your own device (BYOD)** and
 - cloud migration and cloud computing
- It also does not address the internal network facet of information security
 - the older security architectures deemed internal assets, employees, contractors, and business partners as trusted



Enterprise Security Architecture

Pitfalls (2)

Example shortcomings of the earlier security architectures:

- It fails to secure internal assets from internal threats
- It remains static and inflexible; small deviations circumvent and undermine intended security
- All internal users are equal, no matter what device is used or if the user is a non-employee
- Security is weak for enterprise data; access is not effectively controlled at the user level



Dilemma in Enterprise Security

- Lack of senior management understanding of security issues
- But more importantly, **Budgetary constraints**
- Example:

The security team wants to spend \$150, 000 on a web application firewall; there is no data on current attacks against the enterprise, just the latest report on the Internet showing the trends in data breaches associated with web application security.

Another IT team needs to buy servers because the current servers are at capacity and without the purchase, several key IT initiatives will be impacted.

Where do you think the money will go?

- ✓ **Enterprise security is a risk-centered balancing act between business initiatives and security**



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



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



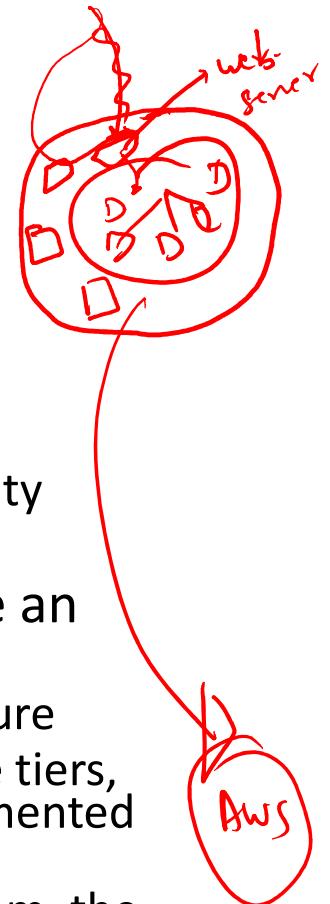
Security Architecture Models

- 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

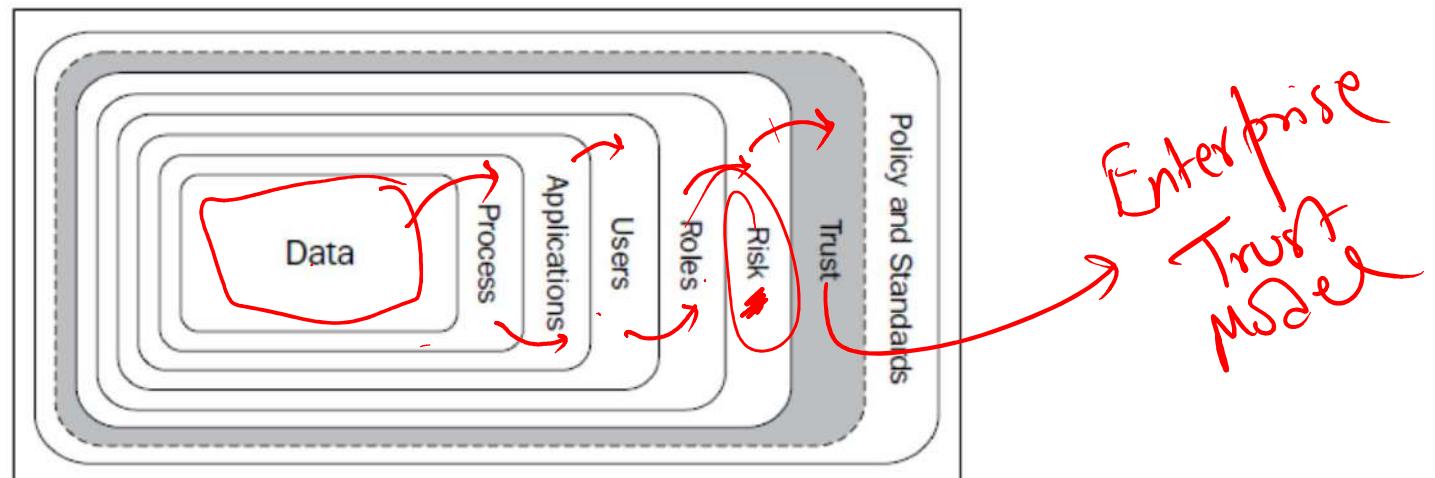
Micro Architectures

- 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

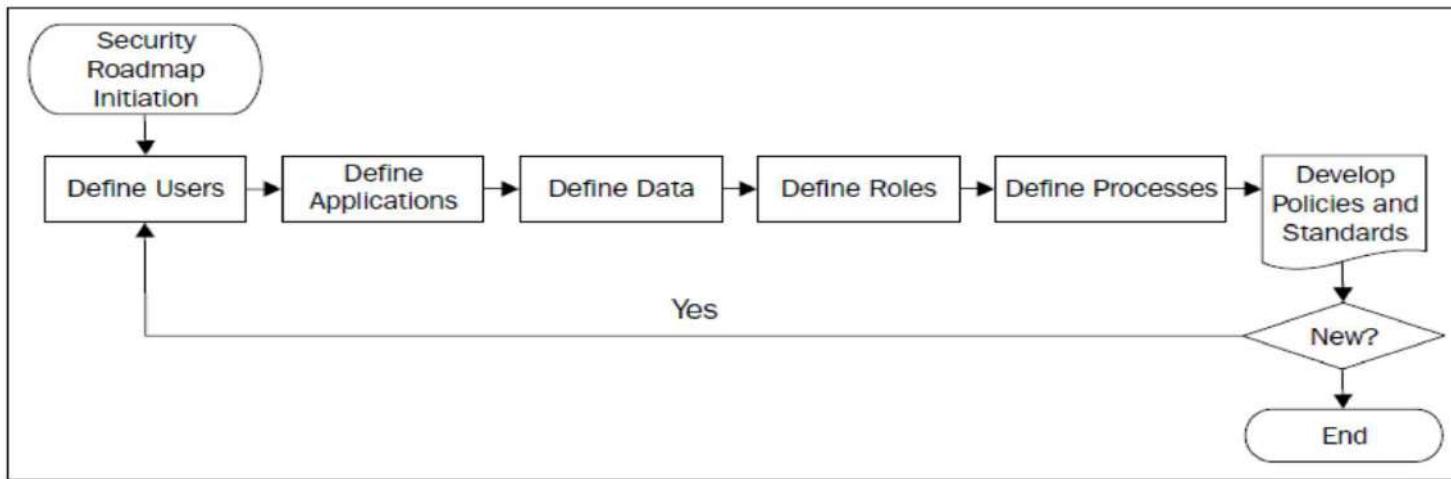
Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise



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



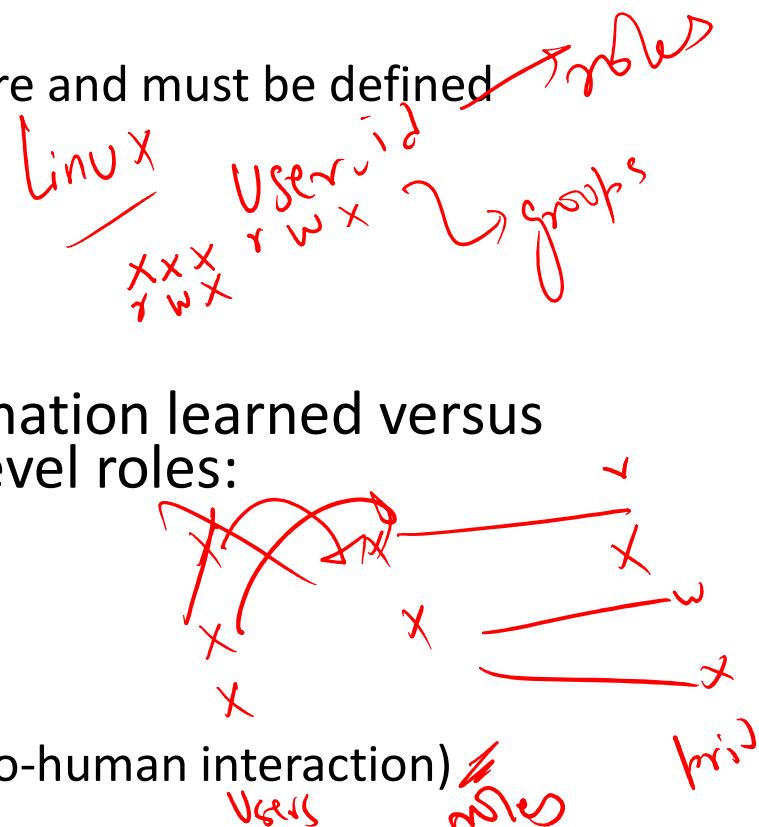
Defining Users in a Trust Model

- 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

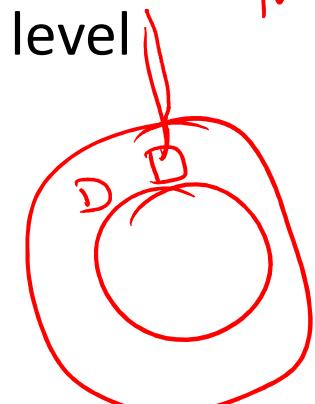
Trust Model using a small scale, such as 1 to 3: 1 as *not trusted*, 2 as *median trusted*, and 3 as *trusted*

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

r/w



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

RBAC

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



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 3: Enterprise Security

Security as a Process + Securing Enterprise **Network**

Enterprise = Network + Systems + Data + Humans + ...

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

Enterprise Security

Modern Initiatives and Impacts to Security Architectures

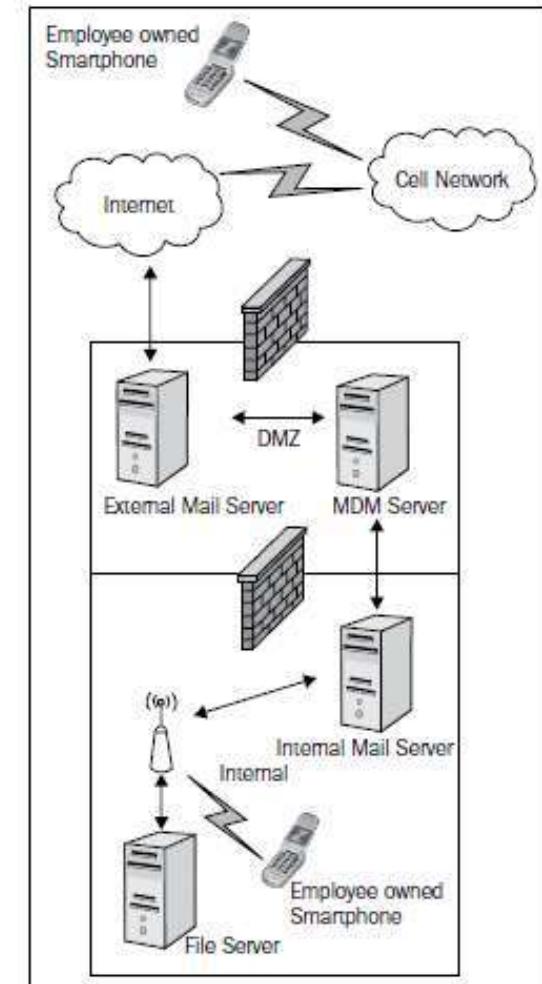


BYOD Initiatives

- Bring your own laptop, cell, and tablet are a few of the new initiatives
 - This model is being used by many enterprises to reduce their IT budgets
- Enterprise Security Architecture aspects:
 - how to properly secure the device(s)
 - secure the network it connects to, and
 - secure the data that these devices will have access and data they shall possibly store
- Data access typically occurs through systems owned by the enterprise
- In next couple of slides, we will look at two of the common BYOD initiatives and discuss considerations when applying trust models to attempt securing the data accessed, transmitted, and stored on these consumer end points

BYOD: Mobile Devices

- Most mobile devices are cellular smartphones or tablets
 - Key use case is employee access to emails, calendar etc
- Commonly implemented security measures include using a Mobile Device Management (MDM) solution
 - Generic platform - determining what exact data the device has access to will be up to the enterprise to decide
 - The enterprise will have to map the interaction to a defined trust model or develop one to meet this request



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



Exploring the
Future of Desktop Virtualization

BYOD: Personal Computers

- A more complicated initiative to secure, because maintaining a device by the enterprise that is not owned by the enterprise may cross some privacy and/or technical boundaries
 - However, there exist tremendous cost savings of allowing employees to bring their laptops to work to perform their jobs
- Some enterprises are leveraging virtualization in a "*trust no one*" model where the only way to access anything is through a virtual desktop environment
 - model is very secure, but comes at a cost to build a robust enough infrastructure to support it
- Other (generally smaller) organizations are allowing employees to bring their own PCs to access enterprise assets, with no virtualization and balancing access with risk
 - limit the access to all the data that has been assessed at a risk level of high and above, or to a level the enterprise's risk tolerance will allow

Security as a Process

Risk Analysis, Policies & Standards, Security Exceptions and
Review of Changes



Overview

- Security is a process that requires the integration of security into business processes to ensure enterprise risk is minimized to an acceptable level
- We will introduce the concept of using risk analysis to drive security decisions, and to shape policies and standards for consistent and measurable implementation of security



Risk Analysis

- **Risk analysis** is the process of assessing the components of risk; threats, impact, and probability as it relates to an asset, in our case enterprise data
 - A simple risk analysis output may be the decision to spend capital to protect an asset based on value of the asset and the scope of impact if the risk is not mitigated
- It is the method to properly implement security architecture for enterprise initiatives
 - Without this capability, the enterprise will either spend on the products with the best marketing, or not spend at all
 - In the next few slides, we take a closer look at the risk analysis components

Threat Assessment

- A **threat** is anything that can act negatively towards the enterprise assets
 - It may be a person, virus, malware, or a natural disaster
- Once a threat is defined, the attributes of threats must be identified and documented
 - The documentation of threats should include the type of threat, identified threat groupings, motivations if any, and methods of actions
- To gain understanding of pertinent threats for the enterprise, researching past events may be helpful
- Example:

Data	Threat	Motivation
Credit card numbers	Hacker	Theft, Cybercrime
Trade secrets	Competitor	Competitive advantage
Personally Identifiable Information (PII)	Disgruntled employee	Retaliation, Destruction
Company confidential documents	Accidental leak	None
Client list	Natural disaster	None

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



Impact Assessment

- **Impact** is the outcome of threats acting against the enterprise.
Examples:
 - a denial-of-service state where the agent, a hacker, uses a tool to starve the enterprise resources causing denial-of-service for legitimate users
 - the loss of customer credit cards resulting in online fraud, reputation loss, and countless dollars in cleanup and remediation efforts
- Types of Impacts: **Immediate** and **Residual**
 - Immediate impacts are rather easy to determine
 - Residual impacts are longer term and often known later
- Impact analysis needs to be thorough and complete. Example:

Data	Threat	Impact
Credit card numbers	Hacker	Critical
Trade secrets	Competitor	Medium
PII	Disgruntled employee	High
Company confidential documents	Accidental leak	Low
Client list	Natural disaster	Medium

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



Probability Assessment

- **Probability** is the likelihood of the Risk to mature
 - if threat actions may only occur once in three thousand years, investment in protecting against the threat may not be warranted
- Probability data is as difficult, if not more difficult, to find than threat data
- Probability and Impact are equally important to decide whether (or not) to handle a threat. It is the combination, normally, that matters
 - Example, in the game of Russian roulette, a semi-automatic pistol either has a bullet in the chamber or it does not. With a revolver and a quick spin of the cylinder, you now have a 1 in 6 chance on whether there is a bullet that will be fired when the firing pin strikes. How do you assess the Risk?

Data	Threat	Impact	Probability
Credit card numbers	Hacker	Critical	High
Trade secrets	Competitor	Medium	Low
PII	Disgruntled employee	High	Medium
Company confidential documents	Accidental leak	Low	Low
Client list	Natural disaster	Medium	High

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



Assessing Risk

- Now that we have identified threats to the data, rated the impact to the enterprise, and estimated the probability of the impact occurring, the next logical step is to calculate the risk of the scenarios
- There are two methods to analyze and present risk: **qualitative** and **quantitative**
 - The decision to use one over the other should be based on the maturity of the enterprise's risk office/ team
 - In general, a quantitative risk analysis will use descriptive labels like in any qualitative method
 - However, there is more financial and mathematical basis involved in a quantitative analysis



Qualitative Risk Analysis

- Qualitative risk analysis provides a perspective of risk in levels with labels such as Critical, High, Medium, and Low
 - The enterprise must still define what each level means in a general financial perspective
 - For instance, a Low risk level may equate to a monetary loss of \$1,000 to \$100,000
 - The dollar ranges associated with each risk level will vary by enterprise



Qualitative Risk Analysis

- Example Exercise:

Scenario: Hacker attacks website to steal credit card numbers located in backend database.

Threat: External hacker.

Threat capability: Novice to pro.

Threat capability logic: There are several script-kiddie level tools available to wage SQL injection attacks. SQL injection is also well documented and professional hackers can use advanced techniques in conjunction with the automated tools.

Vulnerability: 85 percent (how effective would the threat be with current mitigating mechanisms).

Estimated impact: High, Medium, Low (as indicated in the following table).

Risk	Estimated loss (\$)
High	> 1,000,000
Medium	500,000 to 900,000
Low	< 500,000

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



Quantitative Risk Analysis

- Quantitative risk analysis is an in-depth assessment of what the monetary loss would be to the enterprise if the identified risk were realized
 - In order to facilitate this analysis, the enterprise must have a good understanding of its processes to determine a relatively accurate dollar amount for items such as systems, data restoration services, and man-hour break down for recovery or remediation of an impacting event
 - Enterprises with a mature risk office will undertake this type of analysis to drive priority budget items or find areas to increase insurance, effectively transferring business risk
 - Ideally, the cost to mitigate would be less than the loss expectancy over a determined period of time. This is simple return on investment (ROI) calculation



Quantitative Risk Analysis

- A Few Definitions:
 - **Annual loss expectancy (ALE)**: The ALE is the calculation of what the financial loss would be to the enterprise if the threat event was to occur for a single year period
 - This is directly related to threat frequency
 - In a scenario, if this is once every three years, dividing the single lost expectancy by annual occurrence provides the ALE
 - **Cost of protection (COP)**: The COP is the capital expense associated with the purchase or implementation of a security mechanism to mitigate or reduce the risk scenario
 - An example would be a firewall that costs \$150,000. For a 3-year loss expectancy period, this is \$50,000 per each year of protection
 - If the cost of protection (over the same period) is lower than the loss, it is a good indication the investment is financially worthwhile



Quantitative Risk Analysis

- Example Exercise:

Scenario: Hacker attacks website to steal credit card numbers located in backend database.

Threat: External hacker.

Threat capability: Novice to pro.

Threat capability logic: There are several script-kiddie level tools available to wage SQL injection attacks. SQL injection is also well documented and professional hackers can use advanced techniques in conjunction with the automated tools.

Vulnerability: 85 percent (how effective would the threat be with current mitigating mechanisms).

Single loss expectation: \$250,000.

Threat frequency: 3 (how many times per year; this would be roughly once every three years).

ALE: \$83,000.

COP: \$150,000 (over 3 years). $\$83,000 \text{ (ALE)} - \$50,000 \text{ (COP)} = \$33,000 \text{ (cost benefit)}$

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



Security Policies and Standards

- Policy versus standard
 - Policy dictates what must be done, whereas Standard states how it gets done
 - A policy's intent is to address behaviors and state principles for IT interaction with the enterprise
 - Standards focus on configuration and implementation based on what is outlined in policy
- Example:
 - An employee cell phone policy may be created in response to the business request to use personal phones for business
 - However, with the ability to use a personal cell phone, there may be restrictions on using the "smart" features to access enterprise data, or a requirement to load a mobile device management application on the cell phone
 - The standard in this scenario may be a requirement of a certain smart phone operating system type and version level. This may be driven by management and security capabilities of the platform
- Role of Tools
 - Tools need to be implemented to measure compliance and provide enforcement of policies and standards



Security Policy Development

- Driven typically by an outside driver such as regulatory compliance, industry certification, or business driver
 - regulatory compliance, example, **Payment Card Industry Data Security Standard** or **PCI DSS**
- Typical set of security policies includes:
 - Information security policy
 - Acceptable use policy
 - Technology use policy
 - Remote access policy
 - Data classification policy
 - Data handling policy
 - Data retention policy
 - Data destruction policy



Information Security Policy

- General policy that addresses all the security-specific requirements that may or may not be addressed in other policies
 - outline of what is expected from employees to ensure technology implementations and use are on par with enterprise security posture
 - Example, use of only secure protocols, logging requirements of systems, requirement for regular risk analysis etc
 - policy in effect makes known that IT security exists
 - provides the basis for the security team to protect the enterprise data. This includes giving the right to monitor employee use of systems and data access and install software to do so
- What can be a starting point for a new organization?
 - SANS Security Policy Project has templates that can serve as a base or be used as is with little modification
 - <https://www.sans.org/information-security-policy/>



Acceptable Use Policy

- A ***code of conduct***, with consequences described for failure to comply!
 - may include items such as the network, employer provided equipment, website access, e-mail, and other use-based technologies
- Focus of this policy is to reduce not only security risk to the enterprise but legal liability too
 - example policy statement: “*employer-provided equipment must be used only for employer-sanctioned activities*”
 - What services are employees permitted to use?
 - What services can be abused and introduce risk?
 - What is the consequence for violating the policy?



Technology Use Policy

- May be developed separately from the acceptable use policy to call out specific technologies allowed and their approved use
 - Example, could be used to capture items such as BYOD initiatives or cloud initiatives
 - What is the technology?
 - How can it be used for better productivity?
 - What types of data can the technology access?
 - Who will be permitted to use the technology?
 - How will data and network access via the technology be managed?
 -



Remote Access Policy

- Defines what types of devices and who may connect to the enterprise network remotely
- Includes the appropriate authentication methods such as two-factor or simple username and password
- Some enterprises are very strict on employer-owned devices being the only method to use a VPN connection to the employer network



Data Classification Policy

- In a data-centric model for security architecture, data classification is an absolute
 - must know what data exists, where it resides, and how to protect it
 - data should be mapped to a classification model that outlines its sensitivity and high-level protection requirements
- Anytime new data is generated or old data discovered, it should go through the process of classification
 - Typically, data types will follow standard enterprise data labeling such as, confidential, restricted, and public
 - Based on the labeling, data protection scheme can be defined (e.g. Encryption, Restricted Access, or No Protection)



Data Handling Policy

- This policy is prescriptive on approved interactions with enterprise data
 - Interactions may be people, applications, or automation
 - A closely integrated policy would be the data classification policy
- Includes:
 - Acceptable storage for enterprise data
 - Enforcement of secure handling of appropriately classified data
 - Access and authorization procedures for sensitive data



Data Retention Policy

- A data retention policy simply states the length of time to retain data in the enterprise
 - The general rule is to only keep data as long as needed for data recovery and regulatory requirements
 - Maintaining data for long periods of time significantly increases the risk of data leakage
 - possible damage to the enterprise can be reduced by enforcing data retention limits
- This policy is tightly related to the data destruction policy



Data Destruction Policy

- A data destruction policy provides an enforceable and measurable method to ensure data is properly destroyed
 - Example: sanitize hard drives before trashing them
- Includes:
 - Requirement to securely wipe all functioning hard disks
 - Requirement to physically destroy non-working hard disks, tapes, and so on
 - If completed by third party, a formal process developed with verification
 - Labeling of systems with data that require destruction
 - Clear consequences for negligent data leakage



Enterprise Security Standards

- Wireless Network Security Standard
 - wireless networking extends the network outside of the physical bounds of the brick-and-mortar enterprise
 - The following are a few examples of wireless network security standards:
 - Implementation of WPA2-Enterprise
 - Two-factor authentication using certificates
- Enterprise Monitoring Standard
 - security monitoring of systems, networks, and users
 - necessary for both policy enforcement and as an implemented security mechanism
 - standard list of audit trail information



Enterprise Security Standards

- Enterprise Encryption Standard
 - Data encryption required for data in transit, storage, or being processed
 - The following are the areas to focus on to standardize encryption :
 - Whole disk encryption
 - Database encryption
 - File-level encryption
 - Secure transport encryption
 - Key management is probably the most involved and difficult task with encryption
- System Hardening Standard
 - reducing the attack surface of a system by
 - turning off unnecessary services,
 - patching the operating system and software, and
 - enabling attack mitigation features such as iptables for Linux and Windows Firewall for Windows
 - following are a few hardening guide sources:
 - NIST (<http://csrc.nist.gov/groups/SNS/checklists/>)
 - NSA (http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml)
 - Microsoft (<http://www.microsoft.com/en-us/download/details.aspx?id=16776>)



BITS Pilani

Pilani Campus



Securing the Enterprise Network



What we will cover?

- Notion of ***Defence-in-Depth***
 - Securing each tier of the enterprise network to mitigate attacks against assets at each tier
 - Introduce multiple technologies that can be implemented in the network
 - secure enterprise infrastructure, network services such as e-mail, DNS, file transfer, and web applications
 - Advancement in firewall technologies
 - provide more in-depth inspection and protection capabilities
 - Intrusion detection and prevention
 - protect against simple and the most advanced attacks across applications, systems, and network services
 - Security through network segmentation
-



Defence In Depth

- When developing an enterprise security strategy, a layered approach is the best method to ensure detection and mitigation of attacks at each tier of the network infrastructure
 - *“Defence in depth is a military strategy that seeks to delay rather than prevent the advance of an attacker, buying time and causing additional casualties by yielding space. Rather than defeating an attacker with a single, strong defensive line, defence in depth relies on the tendency of an attack to lose momentum over time or as it covers a larger area.”* Source: Wikipedia
- Although the enterprise network perimeter is changing, the basic network security mechanisms still have their purpose
 - the same types of security mechanisms need to persist, however, where they are implemented may change slightly depending upon the network architecture
- In general, we will not focus much on where the network perimeter is, but on what needs to be protected



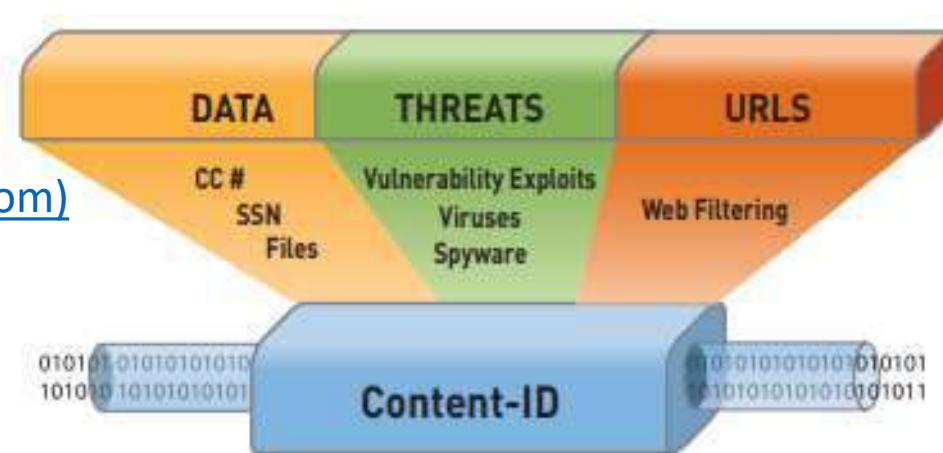
Next Generation Firewalls

- Standard firewalls simply check for the policy allowing the source IP, destination IP, and TCP/UDP port, without a further deep packet analysis
 - Next Generation Firewalls (NGFW) perform more deep packet analysis to mitigate malicious traffic masquerading as legitimate
 - Example: DNS traffic inspected by a standard firewall may look legitimate, but in reality, the DNS packets may be padded with data that is being ex-filtrated from the network
 - An NGFW can inspect traffic for data, threats, and web traffic

Content ID tech.pdf (paloaltonetworks.com)

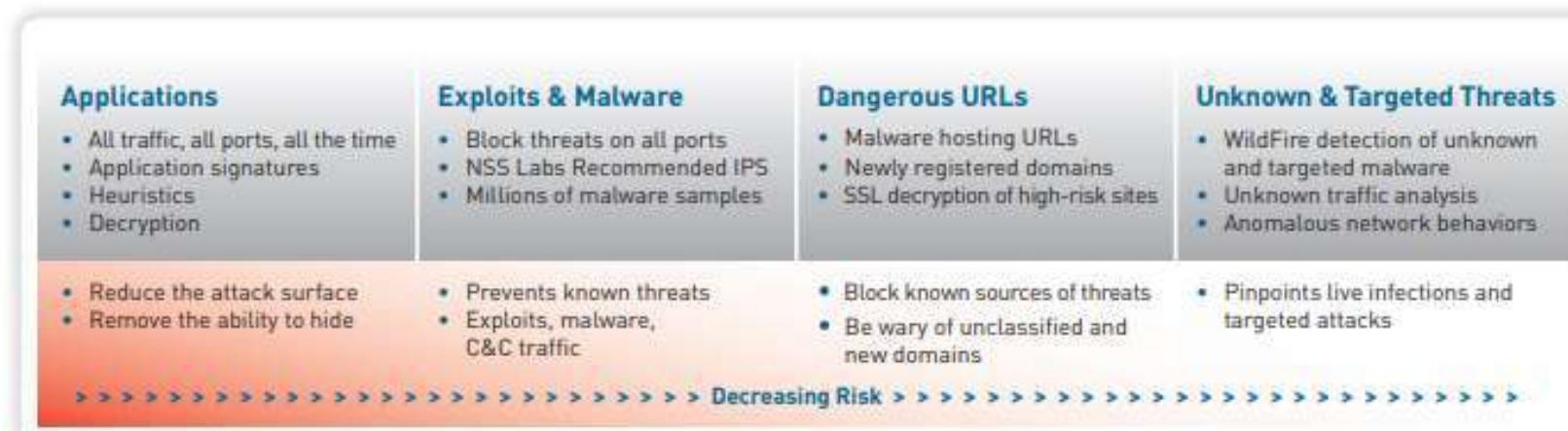


Palo Alto
Networks - ContentID





Case Study: Content-ID

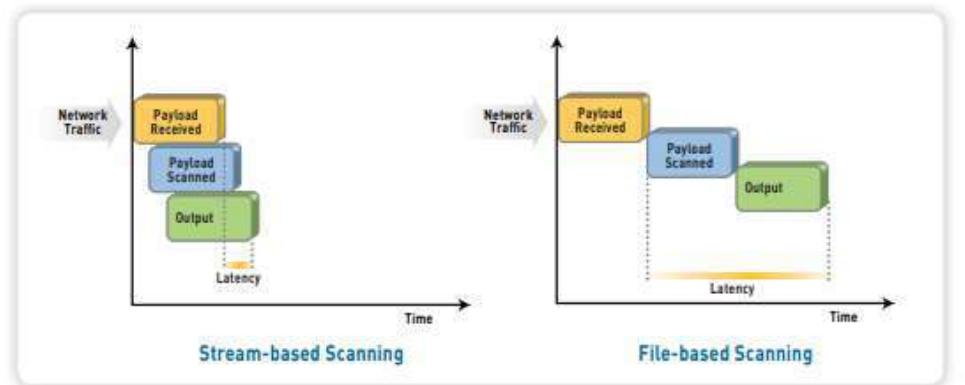


Source: PALO ALTO NETWORKS

- Single-pass architecture (SP3) integrates multiple threat prevention disciplines (IPS, anti-malware, URL filtering, etc) into a single stream-based engine with a uniform signature format
 - Allows traffic to be fully analyzed in a single pass without the incremental performance degradation seen in other multi-function gateways

The diagram illustrates the difference in processing time between Stream-based Scanning and File-based Scanning. Both diagrams show a vertical stack of three boxes: 'Payload Received' (yellow), 'Payload Scanned' (blue), and 'Output' (green). A horizontal arrow at the bottom indicates the progression of time from left to right.

 - Stream-based Scanning:** The boxes are stacked vertically. A small orange bar labeled 'Latency' is shown at the bottom, indicating the time delay between the end of scanning and the start of output.
 - File-based Scanning:** The boxes are also stacked vertically. In this model, the 'Payload Received' box is much larger than the others. A dashed vertical line separates the 'Payload Received' box from the 'Payload Scanned' and 'Output' boxes, which are grouped together. A longer orange bar labeled 'Latency' is shown at the bottom, indicating the total time delay from receiving the payload to producing the output.



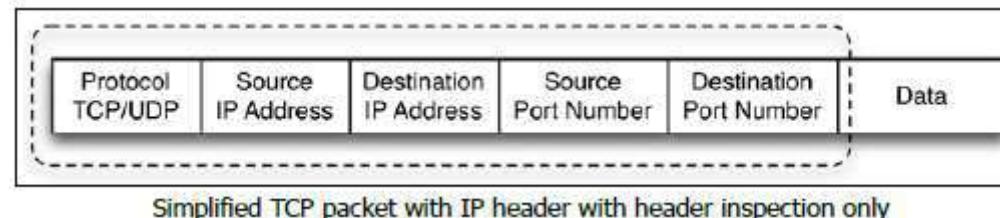


NGFW: Benefits and Challenges

- + Most significant benefit of the NGFW is **awareness** due to deep-packet inspection and analysis
 - + Reduced DMZ complexity - with next generation firewalls, new technologies become a part of the firewall tier, including intrusion prevention, user authorization, application awareness, and advanced malware mitigation
 - - This shift in firewall capabilities may add confusion to the role the appliance plays in the overall network protection
 - - In comparison to web application and database firewalls, while the next generation firewall provides some coverage across these areas today, the available platforms do not have the advanced capabilities of purposefully designed web application firewalls or database firewalls
 - NGFW is capable of basic detection and mitigation of common web application attacks, but lacks the more in-depth coverage provided by web application firewalls with database counterparts
 - Thus, implementing a NGFW in addition to web application and database firewalls provides the most comprehensive coverage for a network
-

NGFW: Application Awareness

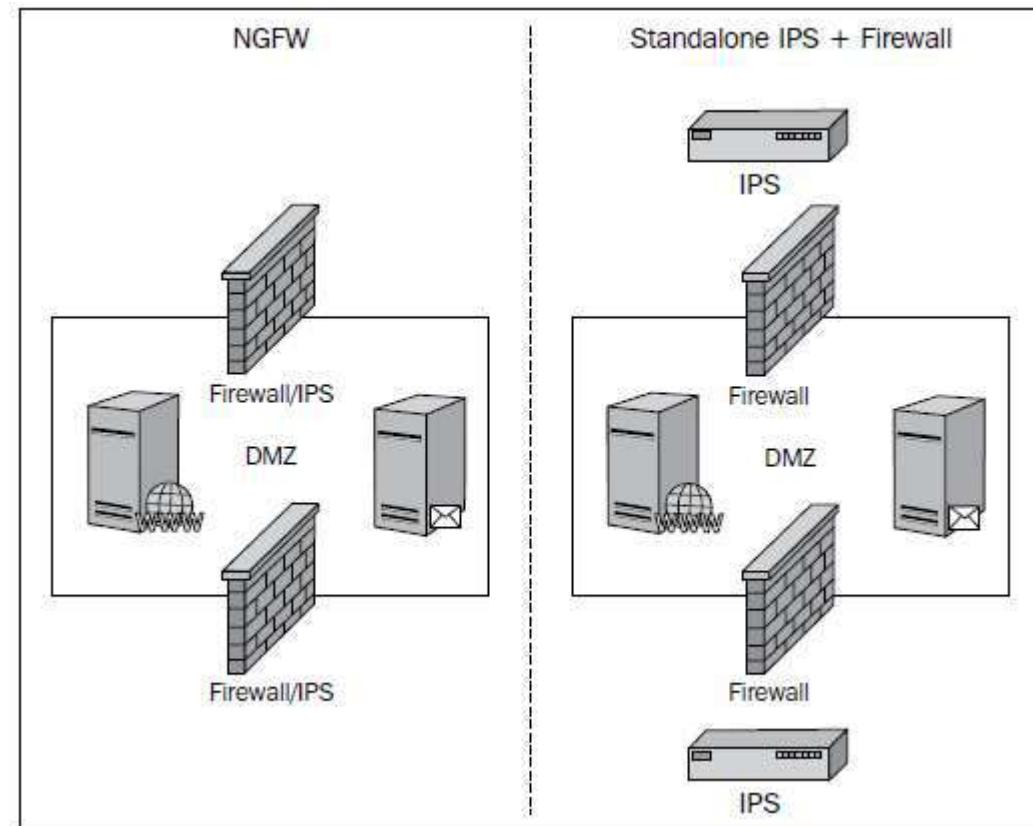
- Traditional firewalls only look at the source and destination IP addresses and the TCP or UDP port to make a decision to block or permit a packet



- NGFW is able to perform deep packet inspection to also decode and inspect the application data in network communication
 - Some firewall manufacturers, such as Palo Alto Networks, are able to identify over 3000 unique applications as traffic traverses the firewall
 - Offers ability to identify and take action on network traffic that violates security policy – e.g. torrent clients, anonymous proxy services, and tunneled connections back to a home, office, or other unapproved destinations

NGFW: Intrusion Prevention

- Intrusion prevention coverage is normally required for every connection to the enterprise network
 - With the average cost of an IPS being over \$40,000, this adds up quickly in addition to the support and maintenance costs
 - Simplifies management of IT security and the skillsets required to operationally support the solution
 - One less appliance in the DMZ - increases the performance



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



NGFW: Malware mitigation

- The newest addition to the features that NGFWs are offering is advanced malware protection in the form of botnet identification along with malware analysis in the cloud
 - Performed by a solution built into the firewall, where the malware is examined in the cloud, protection developed and mitigation implemented by the manufacturer
- While the next generation firewall implementation is less mature than the standalone solutions, leveraging the cloud and the vendor's entire customer base to provide samples will increase the effectiveness and value of the feature



IDS/IPS

- Intrusion detection and prevention technology has remained a mainstay at the network perimeter
 - While several firewall technologies are integrating intrusion prevention into their offerings, there has not been a complete shift to this implementation
- Intrusion detection is a method for detecting an attack but taking no action
 - this has been abandoned at the network perimeter when a breach is undesirable
 - it seems to still have a significant implementation in the internal network server segments to passively observe the behaviors of internal network users
 - has all the detection logic of intrusion prevention but without the ability to actively mitigate a threat
- Intrusion prevention is similar to intrusion detection, but has the capability to disrupt and mitigate malicious traffic by blocking and other methods
 - Many IPS devices have purposefully built denial of service mitigation technology
 - can be deployed at the network perimeter
 - should also be considered for implementation in the internal network to protect the most critical assets within the organization
- As the attacks have become advanced, there is debate on the overall advantage of the IDS/IPS
 - However, a defense in-depth strategy is best implemented by including IDS/IPS as an essential network protection mechanism



IDS/IPS: Detection Methods

- IDS/IPS devices use a combination of three methods to detect and mitigate attacks
 - behavior, anomaly, and signature
 - initial IDS/IPS systems were specialized in one method or another
 - Today, it is rare to find a detection method without the others
 - Also because attacks are not always as simple as protocol misuse or a known Trojan signature



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 4: Enterprise Security – Securing the Network & Systems

Enterprise = Network + Systems + Data + Humans + ...

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

Enterprise Security

Securing the Network (Contd.)



IDS/IPS

- Intrusion detection and prevention technology has remained a mainstay at the network perimeter
 - While several firewall technologies are integrating intrusion prevention into their offerings, there has not been a complete shift to this implementation
- Intrusion detection is a method for detecting an attack but taking no action
 - this has been abandoned at the network perimeter when a breach is undesirable
 - it seems to still have a significant implementation in the internal network server segments to passively observe the behaviors of internal network users
 - has all the detection logic of intrusion prevention but without the ability to actively mitigate a threat
- Intrusion prevention is similar to intrusion detection, but has the capability to disrupt and mitigate malicious traffic by blocking and other methods
 - Many IPS devices have purposefully built denial of service mitigation technology
 - can be deployed at the network perimeter
 - should also be considered for implementation in the internal network to protect the most critical assets within the organization
- As the attacks have become advanced, there is debate on the overall advantage of the IDS/IPS
 - However, a defense in-depth strategy is best implemented by including IDS/IPS as an essential network protection mechanism



IDS/IPS: Detection Methods

- IDS/IPS devices use a combination of three methods to detect and mitigate attacks
 - behavior, anomaly, and signature
 - initial IDS/IPS systems were specialized in one method or another
 - Today, it is rare to find a detection method without the others
 - Also because attacks are not always as simple as protocol misuse or a known Trojan signature



IDS/IPS: Behavior Analysis

- Behavioral analysis takes some intelligence from the platform to first gain an understanding of how the network "normally" operates
 - what systems communicate with other systems, how they communicate, and how much
- Any deviation from this baseline becomes an outlier and triggers the IDS/IPS based on this behavioral deviation
 - Example, if a system is compromised, the connection rates exceed what is common for the system
- The primary caveat with this approach is the mistake of baselining malicious traffic within standard network traffic as "normal"
 - This common and almost unavoidable mistake requires the other detection methods to bring real value



IDS/IPS: Anomaly Detection

- Malware writers often attempt to masquerade their application as a legitimate application
 - this method is commonly employed by chat clients, bit torrent, and other P2P applications
 - Such apps are typically not permitted, so developers have written the applications to look harmless
- Anomaly detection at the network perimeter can be extremely effective in analyzing inbound HTTP requests where the protocol is correct, but there has been some manipulation to the packet
- Nonetheless, understanding the RFC specifications for every protocol is a daunting task!!



IDS/IPS: Signature-based Detection

- A consistent method to detect known malicious attacks
- IDS/IPS looks for known patterns in the packets being inspected
- When a signature or pattern match is found, a predetermined action is taken
- Detects the most common, generic attacks
- Ineffective for the more sophisticated attacks
- Another annoyance with this method is the high rate of false positives

With a majority of attacks targeted at the network being Distributed Denial of Service (DDoS) and SQL injection (SQLi), signature-based IPS can be very effective in mitigating these attacks and continue to provide value at the network perimeter



APT Detection and Mitigation

- APT = **Advanced Persistent Threat**
- Are complicated and well disguised malware
 - use complicated zero-day vulnerabilities, multi-encoded malicious payloads, encryption, obfuscation, and clever masquerading techniques
- APT mitigation solutions work by providing a safe environment
 - usually virtualized instances or sandboxes of operating systems are employed, where malicious software can run and infect the operating system
 - The tool then analyzes everything the malicious software did, and decodes the payload to identify the threat and create a "signature" to mitigate further exploitation
 - Technology in this space is new and relatively less known
- Some tools are appliance-based. The decoding and analysis happens on the box. Other vendors provide the service in the cloud

Several manufacturers in the IDS/IPS and NGFW technology areas have made significant progress in providing APT detection and mitigation, both on the box and in the cloud

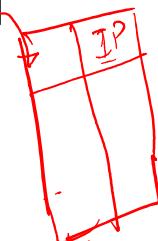


Securing Network Services (NS)

- Enterprises provide and leverage Internet services such as DNS, e-mail, and file transfer
 - The latest malware threats utilize these common services in order to redirect internal hosts to Internet destinations under the control of the malware writers
 - However, with correctly implemented architecture, this scenario would mostly be a mute point, and with additional security mechanisms, a rare occurrence
- In the next few slides, we will discuss the security implementations for DNS, Email, File Transfers and Websites



www.google
www.amazon



NS: DNS Service Security

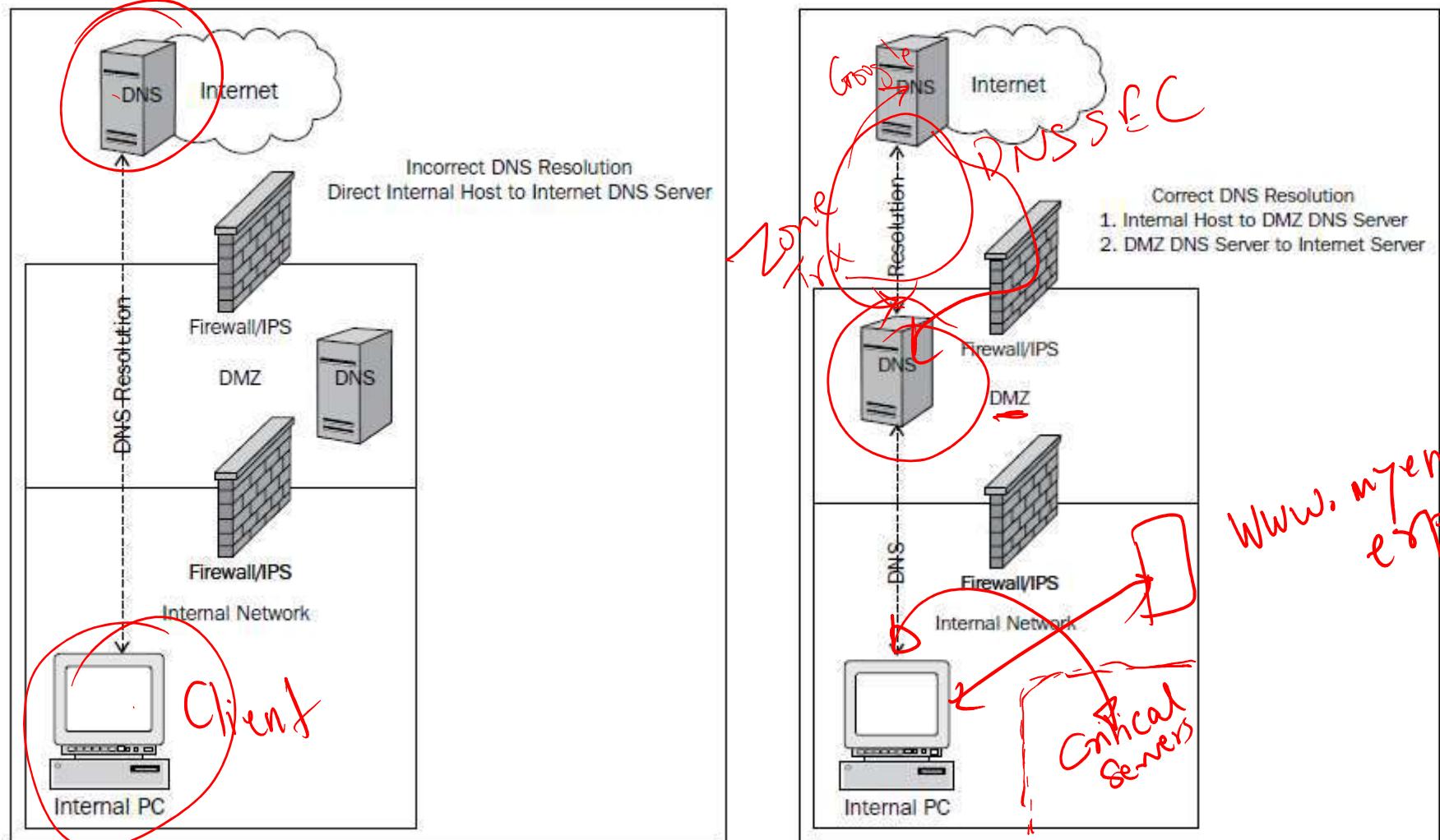
- DNS provides a mapping of an IP address to a fully qualified domain name
- A system can be directed anywhere on the Internet with DNS, so the authenticity of the source of this information is critical
- This is where **DNS Security Extensions (DNSSEC)** come into play
 - provide authenticity for DNS resolver data
 - DNS data cannot be forged and attacks like DNS poisoning, where erroneous DNS is injected into DNS and propagated, resulting in pointing hosts to the wrong system on the Internet is mitigated. This is a common method used by malware writers and in phishing attacks
- Another area of security in regards to DNS implementation are **DNS zone transfers**
 - mechanism used in DNS to provide other DNS servers with what domains the DNS server is responsible for and all the details available for each record in the zone



NS: DNS Resolution

- DNS resolution can make for easy exploitation if there is no control on where the mapping information is obtained
 - This has been the main method used by the Zeus botnet
 - Hosts are pointed to maliciously controlled Internet servers by manipulating DNS information
 - The method also relies on compromised or specifically built DNS servers on the Internet, allowing malware writers to make up their own, unique and sometimes inconspicuous domain names

NS: DNS Resolution (2)



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



NS: DNS Zone Transfer

- A DNS zone transfer should be limited to only trusted partners and limited to only zones that need to be transferred
 - An enterprise may have several domain names for various services they provide to business partners and employees that are not "known" by the general public
 - Example, office-specific records, a VPN URL, SIP address for VoIP, etc
 - While the fact remains that if the service is available on the Internet, it can be found, a simple zone transfer reduces the discovery process significantly
- There may be internal and external DNS implementations with records specific to the network areas they service
 - the internal DNS server may have records for all internal hosts and services, while a DNS server in the DMZ may only have records for DMZ services
 - it is critical to keep the records uncontaminated from other zones
 - Specifically, TXT may give too much information that can be used in a malicious manner against the enterprise



NS: DNSSEC

- Most prevalent DNS attack is **DNS poisoning**, where the DNS information on the Internet is poisoned with false information, allowing attackers to direct clients to whatever IP address they desire
- Security extensions have been added to the DNS protocol by the **Internet Engineering Task Force (IETF)** **DNS Security (DNSSEC)** specification
 - provides security for specific information components of the DNS protocol in an effort to provide authenticity to the DNS information
- The importance of DNSSEC is that it is intended to give the recipient DNS server confidence in the source of the DNS records or resolver data that it receives



NS: Email Service Security

- Email service is a critical business function
- With the increased growth and acceptance of cloud-based services, e-mail is amongst the first to be leveraged
- Some enterprises have already moved their e-mail implementation to the cloud
 - + Enables lower cost and *as-a-service* implementation
 - - enterprises have lower control over email security
- The next few slides will cover common e-mail threats and present methods to secure e-mail services



NS: Spam Filtering

- E-mail is one of the most popular methods to spread malware or lead users to malware hosted on the Internet
 - Most often, this is the single intent of unwanted e-mails in the form of SPAM
 - Receiving SPAM and becoming the source of SPAM while being used as a relay are two sides to the same coin
- Methods to protect the enterprise from SPAM include cloud-based and local SPAM filtering at the network layer and host-based solutions at the client
 - A combination of these methods can prove to be most effective

Userid & fgm

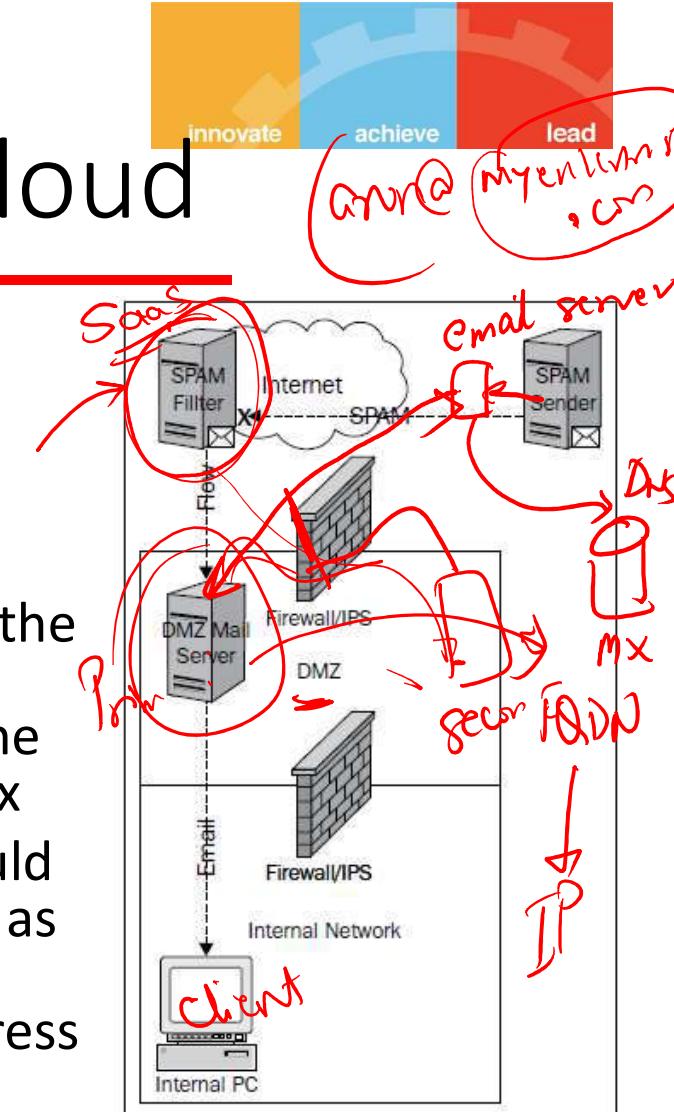
(aaron@nyentech.com)

NS: Spam Filtering @ Cloud

- Works by configuring the DNS **mail record (MX)*** to identify the service provider's e-mail servers
 - This configuration forces all e-mails destined to e-mail addresses owned by the enterprise through the SPAM solution filtering systems before forwarding to the final enterprise servers and user mailbox
 - Outbound mail from the enterprise would take the normal path to the destination as configured, to use DNS to find the destination domain email server IP address

FQDN
IP

mail.myenterprise.com



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

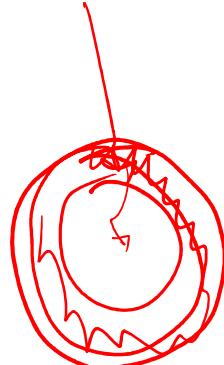
A *mail exchanger record (MX record)* specifies the *mail server responsible for accepting email messages on behalf of a domain name*. It is a *resource record in the Domain Name System (DNS)*. It is possible to configure several MX records, typically pointing to an array of mail servers for load balancing and redundancy. Source: Wikipedia



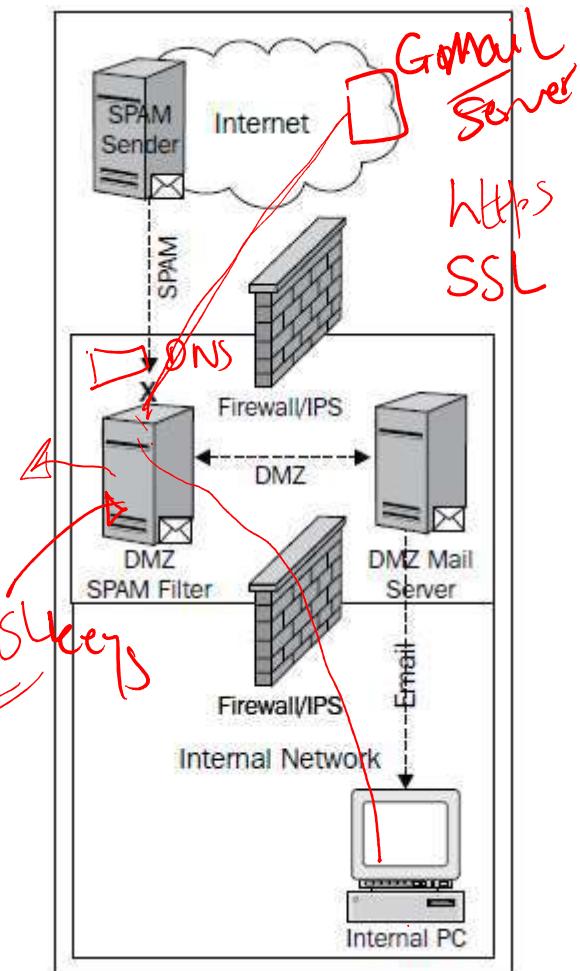
NS: Spam Filtering @ Cloud (2)

- Pros and Cons:
 - + Zero or limited administration of the solution
 - + Reduction in Spam traffic
 - + Reduction in malware and other threats
 - - Significant cost, depending on service fee structure
 - - lack of visibility and control of filters
 - - service failure => no email or unwanted delays
- Enterprise needs to do cost-benefit analysis before taking this option
 - Cost of service
 - Implicit cost (e.g. due to loss of service, or unwanted delays)
 - Benefits (savings due to reduction in spam emails or malware threats)

NS: Local Spam Filtering



- Only an option when the enterprise is not using a web-hosted/cloud-based email solution
 - With web-based e-mail hosting, the SSL connection exists from the user's browser or e-mail client to the hosted e-mail servers
 - SSL decryption could be possible, but the overhead and privacy implications should be weighed carefully
 - Decrypting SSL by presenting a false certificate in order to snoop breaks SSL theory and is considered a man-in-the-middle attack
- Several solutions exist to provide SPAM filtering and e-mail encryption in one appliance
 - may play a role in the enterprise data loss prevention and secure file transfer strategies, providing more than just SPAM filtering



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



NS: Local Spam Filtering (2)

- Pros and Cons:
 - + more control over configuration of filters
 - + vendor continuously updates the appliance to include new block list updates and signatures
 - + ability to also own the DNS infrastructure that tells other e-mail systems where to send e-mail
 - In the event of appliance failure, e-mails can be routed around the failure using DNS to maintain the e-mail service
 - - Technically, a debatable solution if web-based email solution is used
- Again, an enterprise must make an assessment for operational feasibility prior to making the decision to locally detect and mitigate SPAM

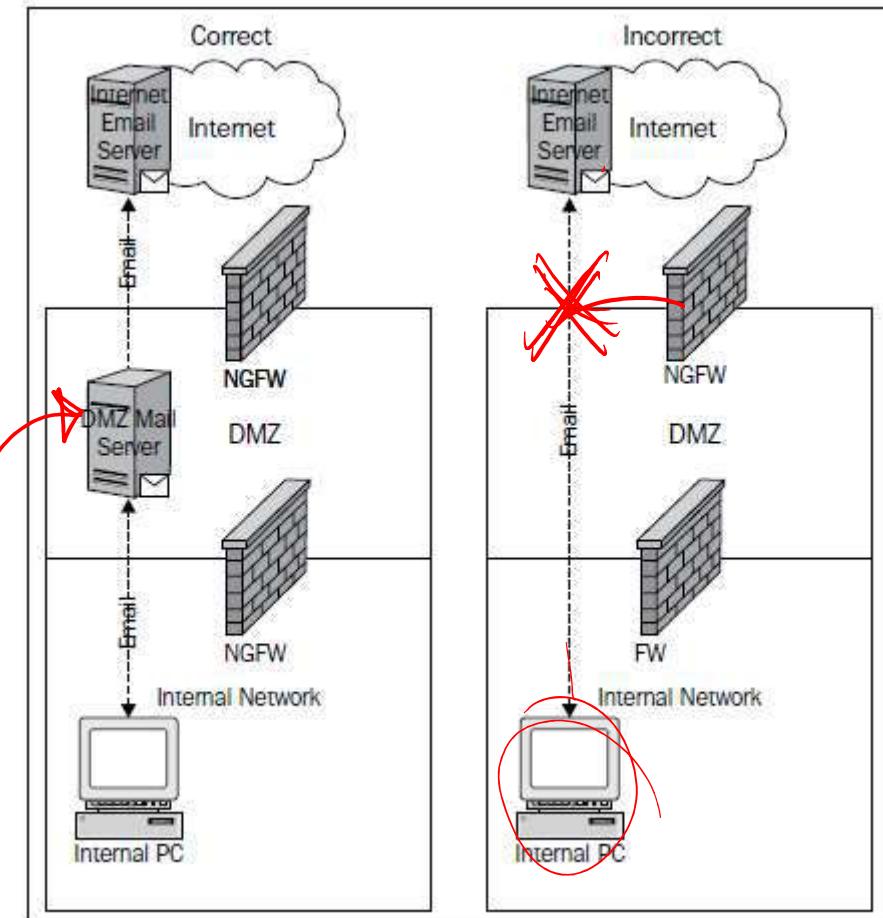


NS: Spam Relaying

- Misconfiguration of the enterprise mail servers may lead to exploitation in the form of using the servers as a SPAM relay
 - method uses the server's lack of sender authentication and capability to send e-mails from domains which it does not have authority to send e-mail
.gov.in Myenklister.com
- Unfortunately, this misconfiguration is common
 - Internet facing e-mail systems only authenticate for the internal mail relay
 - Internal servers for the requirement of non-human processes to send e-mails, such as the alerting mechanism on a security system
 - The internal server should still have restrictions on sending domains, to avoid the system being misused to send other spoofed e-mails

NS: Spam Relaying (2)

- Prevention:
 - Implement e-mail controls at the firewall to ensure that only the internal mail servers are able to directly send e-mails to the Internet
 - This method reduces the potential impact of end system malware, designed to send SPAM from inside the network
 - Some malware is specifically designed to blast e-mail SPAM from the infected system, thus getting the enterprise blocked by services such as [SPAMHAUS](#)



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



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:(nishit.narang@pilani.bits-pilani.ac.in))



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 4: Enterprise Security – Securing the Network & Systems

Enterprise = Network + Systems + Data + Humans + ...

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

Enterprise Security

Securing the Network (Contd.)



IDS/IPS

- Intrusion detection and prevention technology has remained a mainstay at the network perimeter
 - While several firewall technologies are integrating intrusion prevention into their offerings, there has not been a complete shift to this implementation
- Intrusion detection is a method for detecting an attack but taking no action
 - this has been abandoned at the network perimeter when a breach is undesirable
 - it seems to still have a significant implementation in the internal network server segments to passively observe the behaviors of internal network users
 - has all the detection logic of intrusion prevention but without the ability to actively mitigate a threat
- Intrusion prevention is similar to intrusion detection, but has the capability to disrupt and mitigate malicious traffic by blocking and other methods
 - Many IPS devices have purposefully built denial of service mitigation technology
 - can be deployed at the network perimeter
 - should also be considered for implementation in the internal network to protect the most critical assets within the organization
- As the attacks have become advanced, there is debate on the overall advantage of the IDS/IPS
 - However, a defense in-depth strategy is best implemented by including IDS/IPS as an essential network protection mechanism



IDS/IPS: Detection Methods

- IDS/IPS devices use a combination of three methods to detect and mitigate attacks
 - behavior, anomaly, and signature
 - initial IDS/IPS systems were specialized in one method or another
 - Today, it is rare to find a detection method without the others
 - Also because attacks are not always as simple as protocol misuse or a known Trojan signature



IDS/IPS: Behavior Analysis

- Behavioral analysis takes some intelligence from the platform to first gain an understanding of how the network "normally" operates
 - what systems communicate with other systems, how they communicate, and how much
- Any deviation from this baseline becomes an outlier and triggers the IDS/IPS based on this behavioral deviation
 - Example, if a system is compromised, the connection rates exceed what is common for the system
- The primary caveat with this approach is the mistake of baselining malicious traffic within standard network traffic as "normal"
 - This common and almost unavoidable mistake requires the other detection methods to bring real value



IDS/IPS: Anomaly Detection

- Malware writers often attempt to masquerade their application as a legitimate application
 - this method is commonly employed by chat clients, bit torrent, and other P2P applications
 - Such apps are typically not permitted, so developers have written the applications to look harmless
- Anomaly detection at the network perimeter can be extremely effective in analyzing inbound HTTP requests where the protocol is correct, but there has been some manipulation to the packet
- Nonetheless, understanding the RFC specifications for every protocol is a daunting task!!



IDS/IPS: Signature-based Detection

- A consistent method to detect known malicious attacks
- IDS/IPS looks for known patterns in the packets being inspected
- When a signature or pattern match is found, a predetermined action is taken
- Detects the most common, generic attacks
- Ineffective for the more sophisticated attacks
- Another annoyance with this method is the high rate of false positives

With a majority of attacks targeted at the network being Distributed Denial of Service (DDoS) and SQL injection (SQLi), signature-based IPS can be very effective in mitigating these attacks and continue to provide value at the network perimeter



APT Detection and Mitigation

- APT = **Advanced Persistent Threat**
- Are complicated and well disguised malware
 - use complicated zero-day vulnerabilities, multi-encoded malicious payloads, encryption, obfuscation, and clever masquerading techniques
- APT mitigation solutions work by providing a safe environment
 - usually virtualized instances or sandboxes of operating systems are employed, where malicious software can run and infect the operating system
 - The tool then analyzes everything the malicious software did, and decodes the payload to identify the threat and create a "signature" to mitigate further exploitation
 - Technology in this space is new and relatively less known
- Some tools are appliance-based. The decoding and analysis happens on the box. Other vendors provide the service in the cloud

Several manufacturers in the IDS/IPS and NGFW technology areas have made significant progress in providing APT detection and mitigation, both on the box and in the cloud



Securing Network Services (NS)

- Enterprises provide and leverage Internet services such as DNS, e-mail, and file transfer
 - The latest malware threats utilize these common services in order to redirect internal hosts to Internet destinations under the control of the malware writers
 - However, with correctly implemented architecture, this scenario would mostly be a mute point, and with additional security mechanisms, a rare occurrence
- In the next few slides, we will discuss the security implementations for DNS, Email, File Transfers and Websites



NS: DNS Service Security

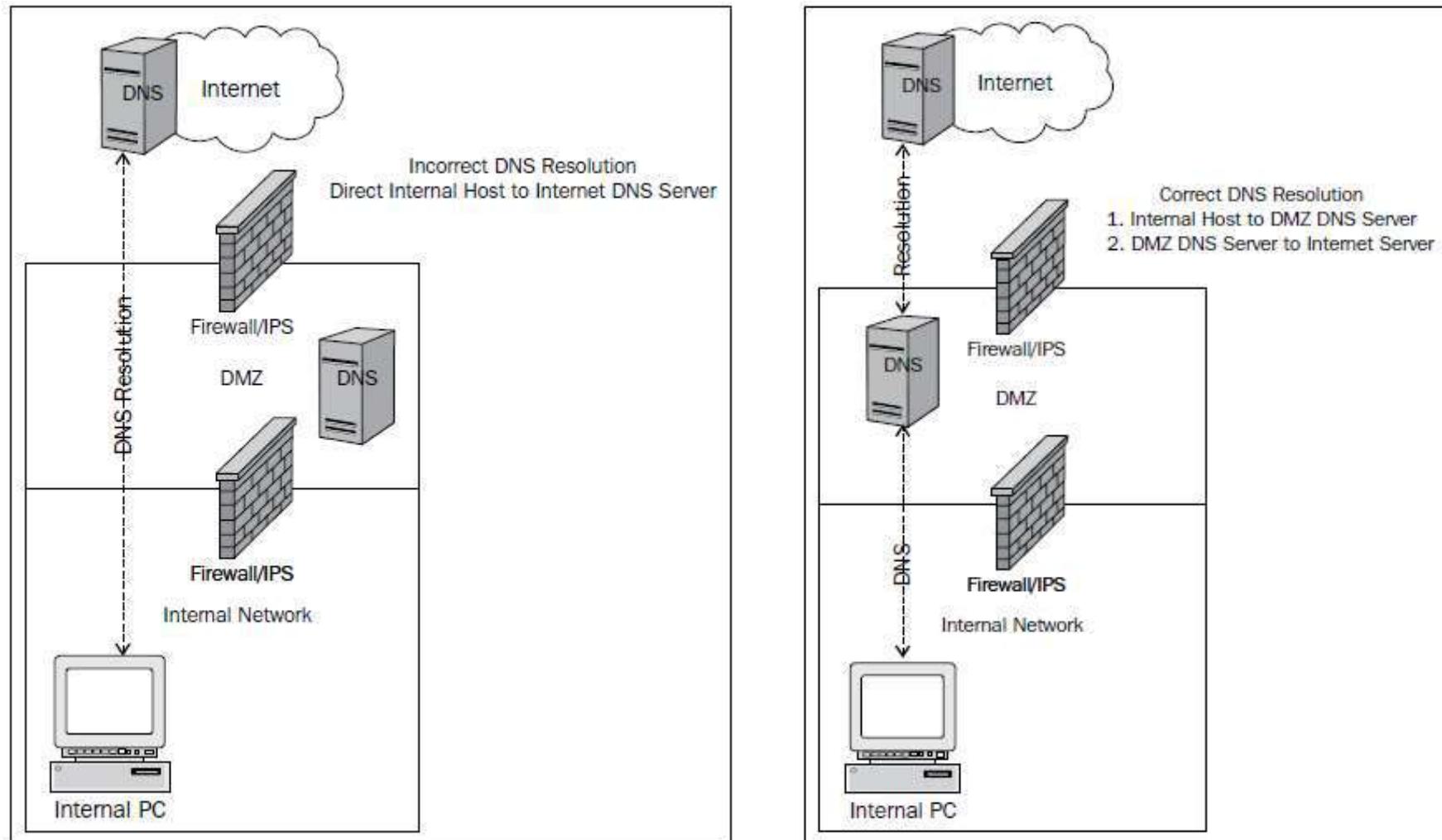
- DNS provides a mapping of an IP address to a fully qualified domain name
- A system can be directed anywhere on the Internet with DNS, so the authenticity of the source of this information is critical
- This is where **DNS Security Extensions (DNSSEC)** come into play
 - provide authenticity for DNS resolver data
 - DNS data cannot be forged and attacks like DNS poisoning, where erroneous DNS is injected into DNS and propagated, resulting in pointing hosts to the wrong system on the Internet is mitigated. This is a common method used by malware writers and in phishing attacks
- Another area of security in regards to DNS implementation are **DNS zone transfers**
 - mechanism used in DNS to provide other DNS servers with what domains the DNS server is responsible for and all the details available for each record in the zone



NS: DNS Resolution

- DNS resolution can make for easy exploitation if there is no control on where the mapping information is obtained
 - This has been the main method used by the Zeus botnet
 - Hosts are pointed to maliciously controlled Internet servers by manipulating DNS information
 - The method also relies on compromised or specifically built DNS servers on the Internet, allowing malware writers to make up their own, unique and sometimes inconspicuous domain names

NS: DNS Resolution (2)



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



NS: DNS Zone Transfer

- A DNS zone transfer should be limited to only trusted partners and limited to only zones that need to be transferred
 - An enterprise may have several domain names for various services they provide to business partners and employees that are not "known" by the general public
 - Example, office-specific records, a VPN URL, SIP address for VoIP, etc
 - While the fact remains that if the service is available on the Internet, it can be found, a simple zone transfer reduces the discovery process significantly
- There may be internal and external DNS implementations with records specific to the network areas they service
 - the internal DNS server may have records for all internal hosts and services, while a DNS server in the DMZ may only have records for DMZ services
 - it is critical to keep the records uncontaminated from other zones
 - Specifically, TXT may give too much information that can be used in a malicious manner against the enterprise



NS: DNSSEC

- Most prevalent DNS attack is **DNS poisoning**, where the DNS information on the Internet is poisoned with false information, allowing attackers to direct clients to whatever IP address they desire
- Security extensions have been added to the DNS protocol by the **Internet Engineering Task Force (IETF)** **DNS Security (DNSSEC)** specification
 - provides security for specific information components of the DNS protocol in an effort to provide authenticity to the DNS information
- The importance of DNSSEC is that it is intended to give the recipient DNS server confidence in the source of the DNS records or resolver data that it receives



NS: Email Service Security

- Email service is a critical business function
- With the increased growth and acceptance of cloud-based services, e-mail is amongst the first to be leveraged
- Some enterprises have already moved their e-mail implementation to the cloud
 - + Enables lower cost and *as-a-service* implementation
 - - enterprises have lower control over email security
- The next few slides will cover common e-mail threats and present methods to secure e-mail services

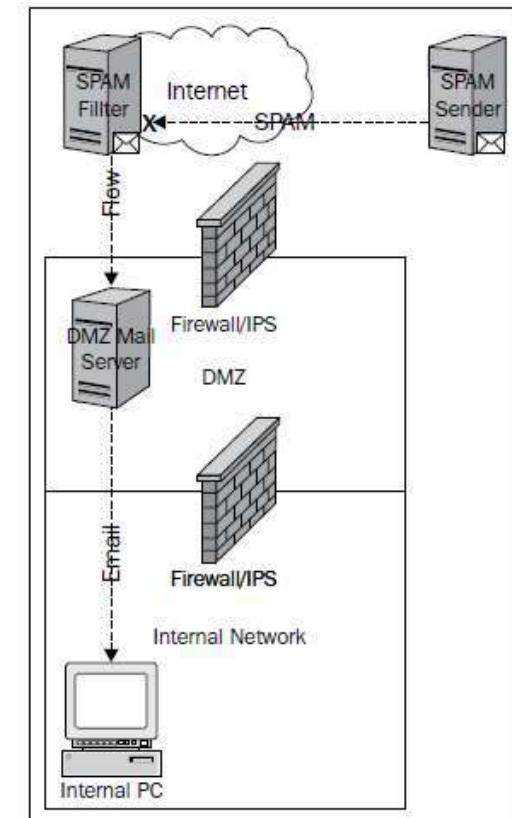


NS: Spam Filtering

- E-mail is one of the most popular methods to spread malware or lead users to malware hosted on the Internet
 - Most often, this is the single intent of unwanted e-mails in the form of SPAM
 - Receiving SPAM and becoming the source of SPAM while being used as a relay are two sides to the same coin
- Methods to protect the enterprise from SPAM include cloud-based and local SPAM filtering at the network layer and host-based solutions at the client
 - A combination of these methods can prove to be most effective

NS: Spam Filtering @ Cloud

- Works by configuring the **DNS mail record (MX)*** to identify the service provider's e-mail servers
 - This configuration forces all e-mails destined to e-mail addresses owned by the enterprise through the SPAM solution filtering systems before forwarding to the final enterprise servers and user mailbox
 - Outbound mail from the enterprise would take the normal path to the destination as configured, to use DNS to find the destination domain email server IP address



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

A mail exchanger record (MX record) specifies the mail server responsible for accepting email messages on behalf of a domain name. It is a resource record in the Domain Name System (DNS). It is possible to configure several MX records, typically pointing to an array of mail servers for load balancing and redundancy. Source: Wikipedia

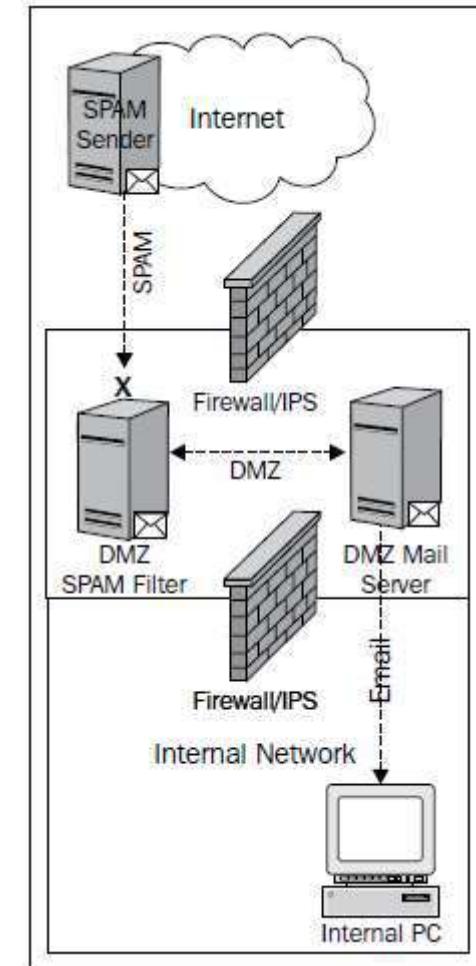


NS: Spam Filtering @ Cloud (2)

- Pros and Cons:
 - + Zero or limited administration of the solution
 - + Reduction in Spam traffic
 - + Reduction in malware and other threats
 - - Significant cost, depending on service fee structure
 - - lack of visibility and control of filters
 - - service failure => no email or unwanted delays
- Enterprise needs to do cost-benefit analysis before taking this option
 - Cost of service
 - Implicit cost (e.g. due to loss of service, or unwanted delays)
 - Benefits (savings due to reduction in spam emails or malware threats)

NS: Local Spam Filtering

- Only an option when the enterprise is not using a web-hosted/cloud-based email solution
 - With web-based e-mail hosting, the SSL connection exists from the user's browser or e-mail client to the hosted e-mail servers
 - SSL decryption could be possible, but the overhead and privacy implications should be weighed carefully
 - Decrypting SSL by presenting a false certificate in order to snoop breaks SSL theory and is considered a *man-in-the-middle* attack
- Several solutions exist to provide SPAM filtering and e-mail encryption in one appliance
 - may play a role in the enterprise data loss prevention and secure file transfer strategies, providing more than just SPAM filtering



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



NS: Local Spam Filtering (2)

- Pros and Cons:
 - + more control over configuration of filters
 - + vendor continuously updates the appliance to include new block list updates and signatures
 - + ability to also own the DNS infrastructure that tells other e-mail systems where to send e-mail
 - In the event of appliance failure, e-mails can be routed around the failure using DNS to maintain the e-mail service
 - - Technically, a debatable solution if web-based email solution is used
- Again, an enterprise must make an assessment for operational feasibility prior to making the decision to locally detect and mitigate SPAM

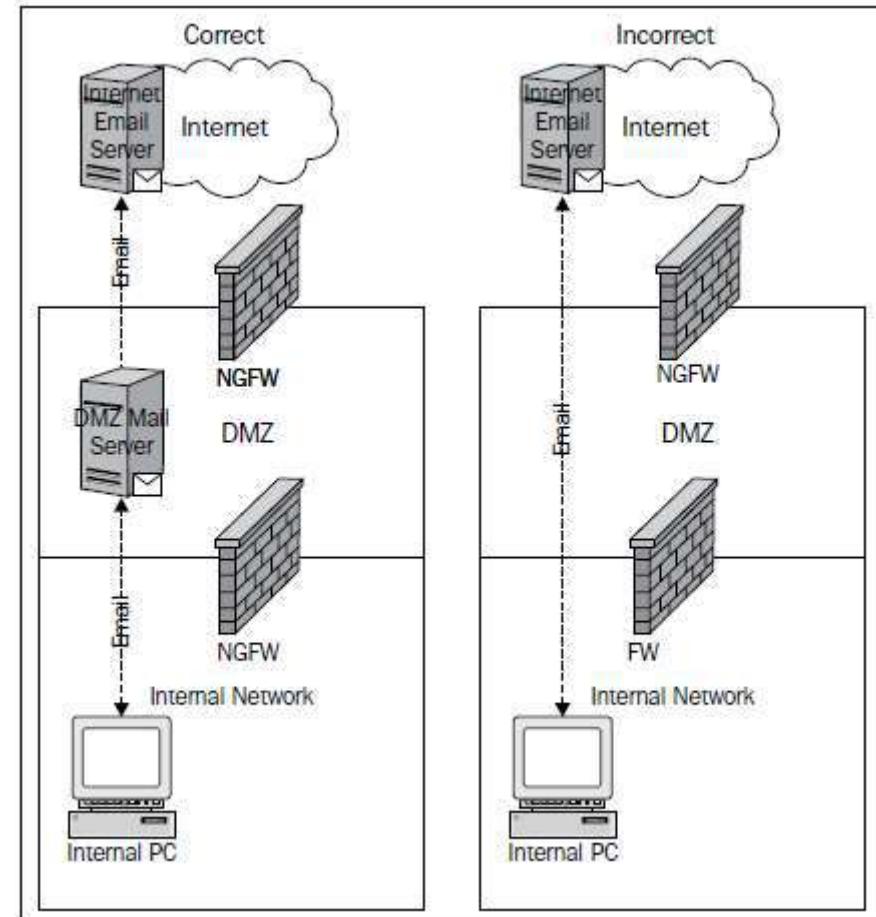


NS: Spam Relaying

- Misconfiguration of the enterprise mail servers may lead to exploitation in the form of using the servers as a SPAM relay
 - method uses the server's lack of sender authentication and capability to send e-mails from domains which it does not have authority to send e-mail
- Unfortunately, this misconfiguration is common
 - Internet facing e-mail systems only authenticate for the internal mail relay
 - Internal servers for the requirement of non-human processes to send e-mails, such as the alerting mechanism on a security system
 - The internal server should still have restrictions on sending domains, to avoid the system being misused to send other spoofed e-mails

NS: Spam Relaying (2)

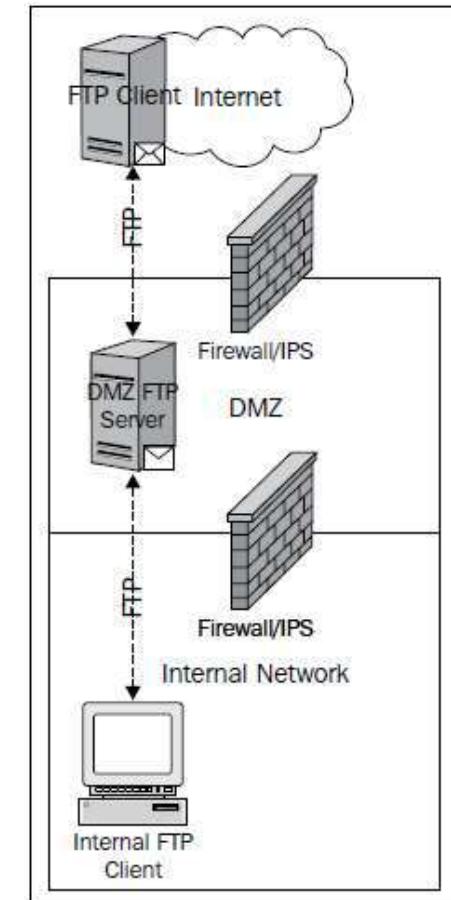
- Prevention:
 - Implement e-mail controls at the firewall to ensure that only the internal mail servers are able to directly send e-mails to the Internet
 - This method reduces the potential impact of end system malware, designed to send SPAM from inside the network
 - Some malware is specifically designed to blast e-mail SPAM from the infected system, thus getting the enterprise blocked by services such as SPAMHAUS



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

NS: File Transfer Service

- Many times is a necessity to facilitate business operations
 - protocols and methods that are viable options include FTP, SFTP, FTPS, SSH, and SSL; many more proprietary options available too
 - migration to secure protocols has been driven primarily by security standards: PCI DSS, ISO 27001, and NIST
- It is not possible to allow uncontrolled encrypted file transfer from a user's desktop to any Internet destination
 - it would circumvent most network-based security controls
- A method to ensure secure communication and the ability to control what is transferred and to whom is to implement an intermediary transfer host
 - Solution should also require authentication to be used and the user list audited regularly, for both voluntarily and involuntarily terminated employees



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

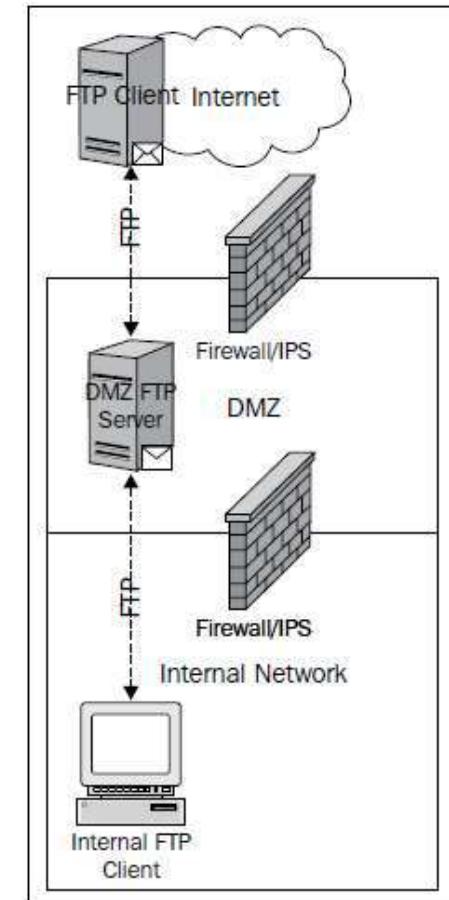


NS: Secure File Transfer

- Not all enterprises that have implemented secure protocols use a secure file transfer
 - Choice by design, such as credit card authorizers, where the risk is accepted due to the overhead and complexity of managing secure communications for a high number of clients
- It can be challenging to implement a secure transfer solution, especially if not using an SSL implementation where encryption can be managed by certificates
 - In instances where SSH or SFTP is used, this can be more complicated to provide authentication and encryption

NS: File Transfer Service

- Many times is a necessity to facilitate business operations
 - protocols and methods that are viable options include FTP, SFTP, FTPS, SSH, and SSL; many more proprietary options available too
 - migration to secure protocols has been driven primarily by security standards: PCI DSS, ISO 27001, and NIST
- It is not possible to allow uncontrolled encrypted file transfer from a user's desktop to any Internet destination
 - it would circumvent most network-based security controls
- A method to ensure secure communication and the ability to control what is transferred and to whom is to implement an intermediary transfer host
 - Solution should also require authentication to be used and the user list audited regularly, for both voluntarily and involuntarily terminated employees



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



NS: Secure File Transfer

- Not all enterprises that have implemented secure protocols use a secure file transfer
 - Choice by design, such as credit card authorizers, where the risk is accepted due to the overhead and complexity of managing secure communications for a high number of clients
- It can be challenging to implement a secure transfer solution, especially if not using an SSL implementation where encryption can be managed by certificates
 - In instances where SSH or SFTP is used, this can be more complicated to provide authentication and encryption

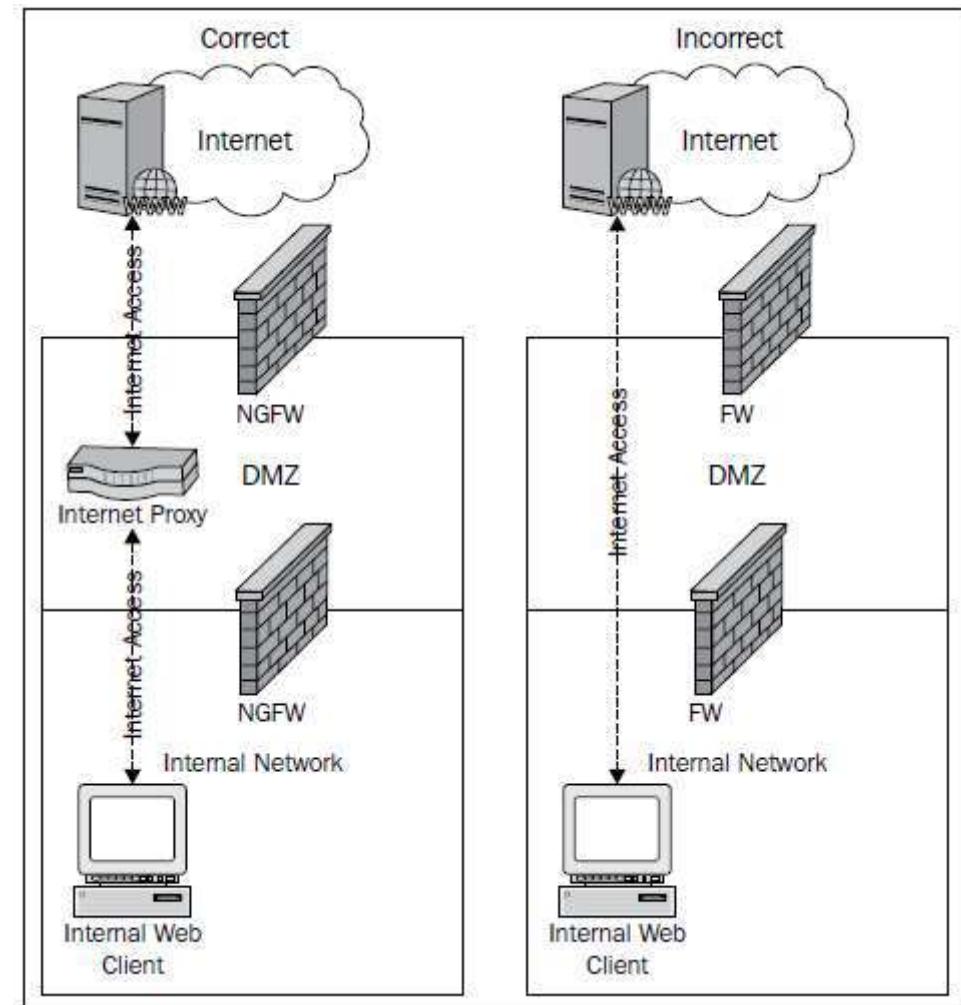


NS: User Authentication

- For SSH, SFTP, and other such protocols, there are two methods of authentication, namely user credentials and keys
 - 1) Enterprise configures either locally or using directory services, such as Windows Active Directory for users that can access the service
 - Security implications involved:
 - For local accounts, the fact that they are locally stored on the server may leave them vulnerable to compromise
 - The system administrator will also have to manually manage user credentials on each and every system configured
 - For systems that rely on a central user directory, the implementation must be thought out to ensure that any compromise of the system does not lead to a compromise of the internal user directory
 - 2) Authentication via **Simple Public Key Infrastructure (SPKI)**
 - private-public key combination can be used for authenticating systems, applications, and users

NS: Securing Internet Access Service

- Internal user access to the Internet is probably deemed a more critical service than even e-mails
- To provide some level of security and monitoring, the use of Internet proxy technology is required
- There are standalone proxy solutions and the aforementioned NGFWs have this feature, which allows for URL filtering based on category and known malicious destinations



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



NS: Securing Websites

- Internet accessible websites are the most targeted asset on the Internet due to common web application security issues, such as SQL injection
- There are several approaches to securing websites, but it is truly a layered security approach requiring:
 - Secure Coding
 - Firewalls
 - IPS



NS: Websites: Secure Coding

- Utilizing a **secure software development lifecycle (S-SDLC)** is the best method to ensure that secure coding practices are being followed
 - framework for how the coding process is to be completed with testing and validation of the code
 - process is iterative for each new instance of code or modified portions of code
 - Several open source and commercial products available for testing not only via web scanning, but source code analysis as well
 - Vulnerabilities identified should be documented and tracked through remediation within a centralized vulnerability or defect management solution
 - Secure coding must be the focal point of the security strategy for securing web applications
-



NS: Websites: NGFW

- NGFW can be leveraged to protect Internet-facing enterprise websites and applications
 - Threats within seemingly benign connection attempts to the web servers can be detected and mitigated with the application aware firewall
 - The benefit of using a next generation firewall is that access can be provisioned by applications, such as web browsing, and is not restricted by TCP port
 - NGFW can also be used for inspecting and mitigating all illegitimate traffic, such as denial of service attacks, before they reach the web servers



NS: Websites: IPS and Web-Application Firewalls

- IPS
 - Intrusion prevention may also be implemented at the network perimeter to mitigate known attack patterns for web applications
 - IPS can provide excellent denial of service protection and block exploit callbacks
- Web-application Firewalls:
 - designed to specifically mitigate attacks against web applications through pattern and behavioral analysis
 - SQL injection, cross-site scripting, command injection, and misconfigurations
 - advanced web application firewalls use another component at the database tier of the web applications. Benefits include:
 - Ability to determine if a detected threat warrants further investigation; i.e. whether the threat was able to interact with the database or not (how safe is the data!!)
 - attacks that do get past the first layer of the web application firewall can be mitigated at the database tier of the network architecture
 - enforce security controls for database access initiated not only by the web application but also by database administrators

A commercial product leader in this space is **Imperva** (<http://www.imperva.com>). Their solutions provide comprehensive web attack mitigation and database security through database access and activity management capabilities

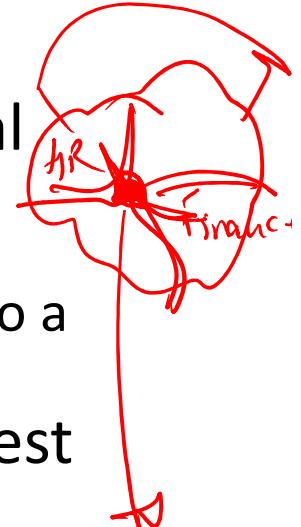


Network Segmentation

- Even with the most sophisticated security mechanisms, without network segmentation, their value will be greatly undermined
- Internal segmentation is often overlooked, but is extremely important to prevent spread of malware throughout the enterprise
 - advanced threats are introduced through infected consultant systems, unauthorized introduction of personal devices and business-critical applications

Network Segmentation Strategy

- Before any network segmentation can occur, critical data, processes, applications, and systems must be identified
 - helps determine the complexities of moving the assets to a network segment separated by a firewall
- Network segmentation using a firewall is the simplest network-based security control
- Alongside, highly recommended security monitoring tools, such as **Security Information and Event Management (SIEM)** and **File Integrity Monitoring (FIM)** should be implemented to ensure that in the event of an attack, there is monitoring for early detection and timely incident response
- In some cases, leveraging data loss prevention tools may be ideal to protect against data leakage



Enterprise Security

Securing the Systems



What we will cover?

- Organization processes and methods to secure enterprise computer systems
 - we will focus on server systems that are used within the enterprise to conduct business functions
- Processes and methods covered:
 - System Classification
 - File integrity monitoring (FIM)
 - Application Whitelisting
 - Host-based intrusion prevention system (HIPS)
 - Host Firewalls
 - System Protection using Anti-virus
 - User account management

Enterprise = N|w + Sys + Data + humans --



System Classification (SC)

- When securing Enterprise Network, Network Segmentation plays a key role:
 - Helps placing systems of high value and criticality in segmented areas of the network
- To identify these systems, it is necessary to understand the important business processes and applications
 - as with any classification model, there should be tiers based on criticality
 - tiers of classification should have a criteria for each level to ensure security and availability requirements are met
 - tier classification may also include service-level agreement information, expected recovery times, and the priority of security incidents involving the systems
- System labels applied will serve as an input to the overall security architecture
 - Labels shall be referenced in other business processes such as change management, user account management, protection tool selection, monitoring, and incident response



Example: System Classification

- A system classification model may look like the following table:

Level	Classification	Process(es)/Function(s)	Requirement
1	Critical	Transaction processing, Deposit functions	Network redundancy, File integrity monitoring, User monitoring, Encryption
2	High	Payroll processing	Network redundancy, User monitoring
3	Medium	Customer e-mail promotion functions	Network redundancy
4	Low	Corporate communication processes	N/A

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

- Individual systems will not be identified in the table, only processes or functions
- Labeling of the systems should happen in an asset management tool or a **configuration management database (CMDB)** if using the ITIL framework

** The enterprise may also decide to create a classification for systems that have regulatory compliance requirements for specific controls to be implemented*



SC: System Management

- An important part of securing systems
 - Includes process of inventory management, system labeling indicating system classification, defining system owners, and required security control mechanisms
 - Plays a significant role in implementing system patching requirements and change management process
- Once systems have been properly classified, asset inventory labels must reflect the classification
 - ensures the correct controls are in place and that policies and standards are enforced

Without asset inventory there is no record of what systems exist, what data is located on the systems, and the risk introduced by the improper securing or loss of the systems!!



SC: System Management (2)

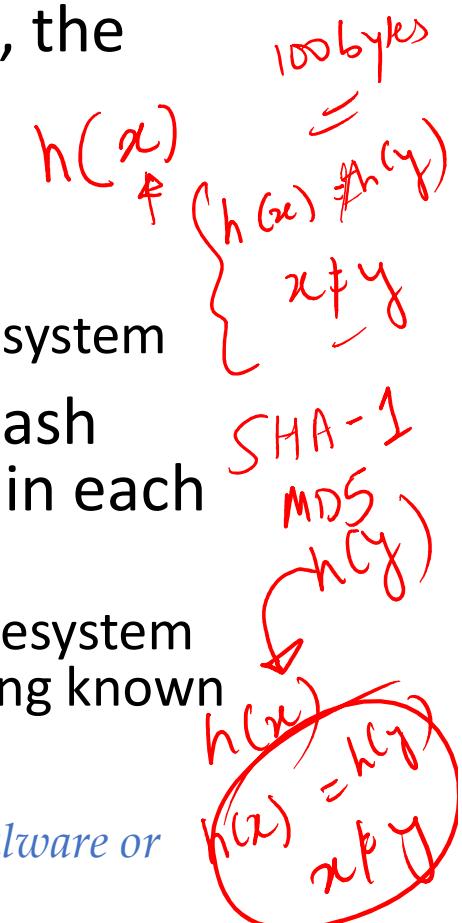
- System patching may be based on
 - A) criticality of the system,
 - B) the severity of the vulnerability, or
 - C) impact of an unpatched software package
- System classification plays a significant role in the patching cycle of systems and must be integrated in the patch and vulnerability management processes
 - When systems remain unpatched and vulnerabilities continue to exist, the window is also extended for malicious actors to exploit

With other weaknesses in the network such as lack of segmentation, systems may be at greater risk when a strict patching cycle is not implemented!!

File Integrity Monitoring (FIM)

- One of the methods used to detect changes to a known filesystem's files, and in the case of Windows, the registry
- when a system has malicious activity, either:
 - changes are made to existing files or
 - harmful files are placed in critical areas of the filesystem
- To detect these changes, FIM tools create a hash database of the known good versions of files in each filesystem location
 - tool can then periodically or real-time scan the filesystem looking for any changes to the installation including known files and directories

A caveat to using this type of tool is the accidental addition of malware or unapproved configuration added to the system baseline hash





FIM Operation Modes

- **Real-time FIM:**

- all add, delete, and modification actions are detected in real time allowing for almost immediate ability to review and remediate
- but the constant running of the tool may be taxing to a system that is loaded with several agents for various purposes

- **Manual mode FIM:**

- least taxing on the system because the scans only run when the console initiates the scan either adhoc or on a schedule
- IT knows when the system may have higher memory and processor utilization and it ideally will not affect business operations
- A caveat to this solution is that changes can go undetected for longer periods of time depending on how often scans are run on schedule



Application Whitelisting

- A method to control what applications have permission to run on a system
 - if malicious software is installed on the system, it will not be able to execute
- This model is closer to the trust model discussed in *Lecture 2, Security Architectures*
 - Only trusted applications are allowed to execute
- Tool can also prevent unapproved application install
 - If the application is not preapproved, the installation can be blocked
 - If the installation is successful, the tool can block the application from running

This tool could possibly replace an anti-virus solution and complement other advanced tools in the network such as advanced persistent threat tools and NGFW to provide a layered mitigation implementation!!



HIPS

- **Host-based intrusion prevention system (HIPS)** is very similar in concept to network intrusion prevention (discussed earlier)
 - Network-based IPS is a bigger challenge since it is implemented on the network wire, where the applications across various systems can be huge or unknown
 - HIPS leverages being installed on the system it is protecting => it has additional awareness of running applications and services
- Host-based intrusion detection uses the same types of detection methods as the network-based counterpart
 - primary method is signature-based detection as this is the easiest method to implement on a host without taxing the operating system with true behavioral analysis
 - However, it should be noted that a combination of methods should be employed for comprehensive protection



Host Firewall

- Host firewall can be a great method to filter traffic to and from the system
- Firewall should be considered as another layer of defense from intrusion attempts against applications, services, and the host itself
 - solution is similar to application whitelisting in regards to the requirement of knowing what applications are running and how they must communicate
 - Some applications open random ports or have extremely large ranges of ports. Some host firewalls are able to allow dynamic port use, thus alleviating the need to go through the exercise of analyzing the application



Anti-virus

- Anti-virus is considered as a necessary security mechanism for the low-hanging fruit -- **predictable malware**
 - most of it is old, easy to detect, and still dangerous
- Anti-virus primarily use two methods to detect malware:
 - **Signature:** This method looks for known patterns of malware
 - **Heuristics:** In this method the behavior of potential malware is analyzed for malicious actions
- Typically, anti-virus solutions will install an agent on the endpoint, run scans continuously, and any new file introduced is scanned immediately
 - this method of protecting a system can be taxing

Anti-virus are reactive → can only work after the virus is discovered and understood!!



User Account Management (UAM)

- Accounts on a system are some level of access that may be the door in for malicious activity
 - it is easier to use a known account to access a system versus finding another method to exploit the system
 - review of system accounts should be in accordance to the system classification and other security policies
- User Roles and Permissions
 - Need for properly defining system users and roles to perform required tasks
 - Both for server systems and end-user systems (e.g. elevated privileges to install software applications on desktop/laptop)



UAM (2)

- User Account Auditing
 - To detect rogue accounts on systems, the enterprise should perform user account auditing across all systems on a regular basis
 - Accounts should be disabled or deleted at the time of termination as part of a formal process
- Policy Enforcement
 - how the enterprise expects employees to use assets and consequences to actions contrary to policy statements
 - Enforcement may come in the form of an implemented tool, but it may also come from the monitoring of user activity on systems



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:(nishit.narang@pilani.bits-pilani.ac.in))



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 5: Enterprise Security – Securing Enterprise Data

Enterprise = Network + Systems + Data + Humans + ...

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



What we shall cover?

- Developing and enforcing a data classification model is a foundational component to securing enterprise data
- This lecture will focus on the steps required to develop functional data classification and how to protect high-value data in the enterprise
- We shall cover:
 - Data identification and classification ✓
 - Data loss prevention methods and techniques ✓
 - Data protection methods and techniques such as ✓ encryption, hashing, and access controls

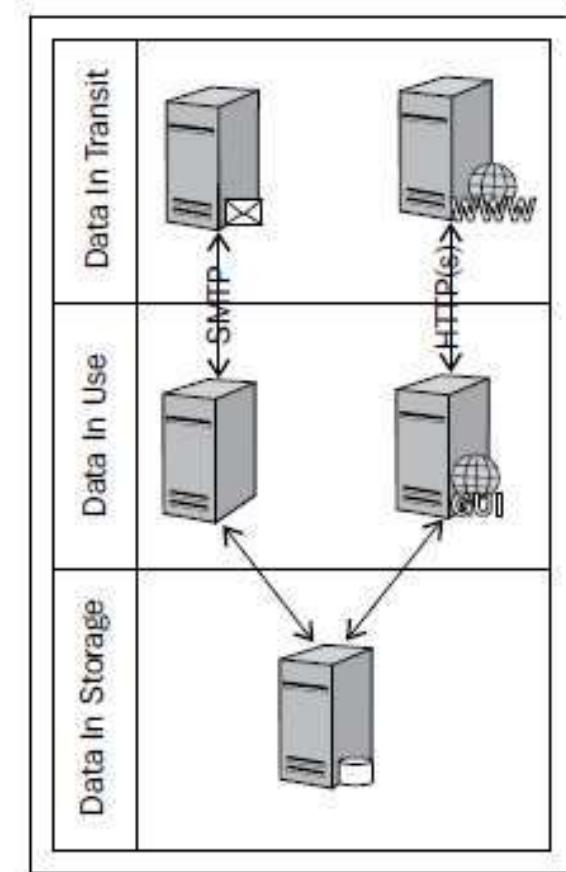


Data Classification Process

- Involves two steps: identification and classification of enterprise data
 - specific handling methods defined for interacting with the classified data
 - data owners are assigned, enterprise criticality is scored
 - supporting processes are developed to ensure confidentiality, availability, and integrity
- Classification is done based on:
 - importance and
 - impact potential (i.e. impact of enterprise data compromise or loss)

Step 1: Data Identification

- What we have already said about this in past lectures?
 - There are many data types that exist in order for the business to operationally function
 - Example: Employee human resources data, Company private data (business plans, acquisition strategies, brands, and so on), Company confidential data, Company public data (product releases, press releases) etc
 - Data can be located in multiple places both internal and external to the enterprise network, including in employer-owned and employee-owned assets
 - Example: Network shares, Document repositories, File transfer systems, Business partner and third-party systems, Employer and employee laptops/desktops etc
 - Data can be at rest, in use or in transit
 - Each will have a unique set of challenges to provide the protection dictated by the classification model



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



Step 2: Data Classification Assignment

- The act of assigning a label to identified data types that indicate required protection mechanisms
 - driven by business risk and data value
- Example Data Classification:

	Restricted confidential (Level 1)	Confidential (Level 2)	Public (Level 3)
Data type	<p>Customer:</p> <ul style="list-style-type: none">• CC#• PII <p>Employee:</p> <ul style="list-style-type: none">• SSN#• PII <p>Company:</p> <ul style="list-style-type: none">• Merger Plans• New product	<p>Customer:</p> <ul style="list-style-type: none">• PII <p>Employee:</p> <ul style="list-style-type: none">• PII <p>Company:</p> <ul style="list-style-type: none">• Internal documents	<ul style="list-style-type: none">• Anything not in the previous sections.• Items considered to be available in the public domain.
Data protection	Data encryption, hashing, or tokenization	Restricted access permissions	None

PII = Personally identifiable information
CC = Credit Card
SSN = Social Security Number

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



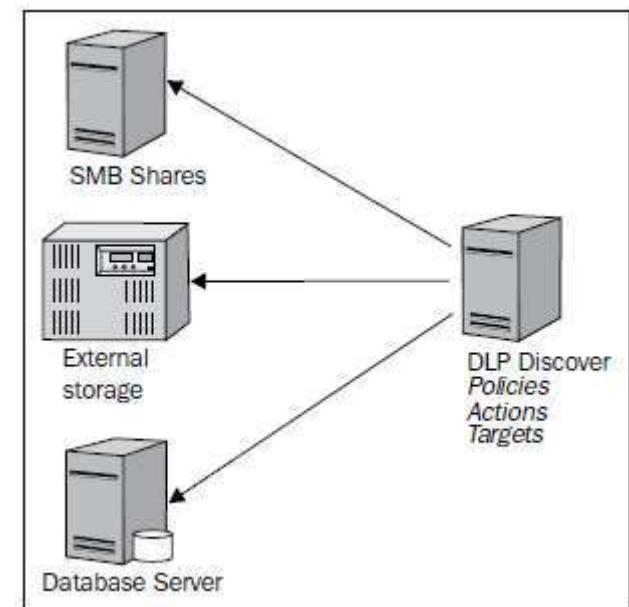
Data Loss Prevention

- **Data Loss Prevention (DLP)** is a tool that can enforce protection of data that has been classified
- The primary purpose of DLP is to protect against the unauthorized exfiltration of enterprise data
- In general, DLP solutions can:
 - Help find data in various locations within the enterprise
 - enforce encryption, in some cases
 - block insecure transmission, and
 - block unauthorized copying and storing of data, based upon data classification
- In next slides, we will cover the implementation of DLP for the common data locations in the enterprise

NEED FOR DLP: *No network monitoring device will detect if, for example, thousands of medical records are saved to a local machine and moved to a USB storage device, but Endpoint DLP can detect and prevent this action!!*

DLP: Data in Storage

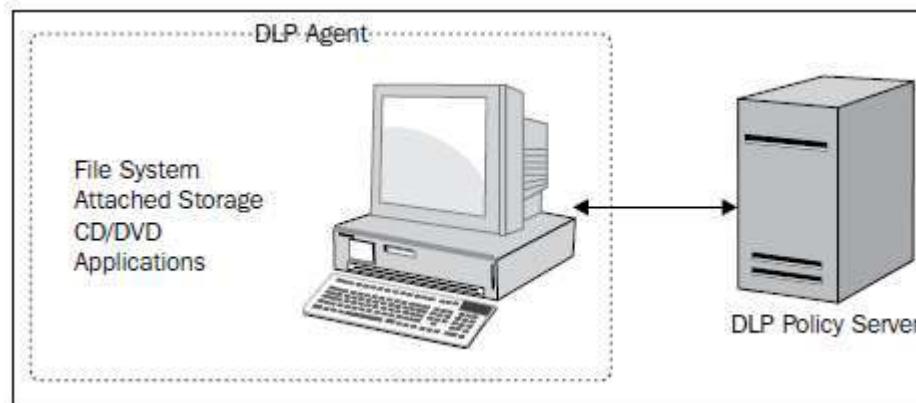
- Data can be stored in network shares, databases, document repositories, online storage, and portable storage devices
- Most DLP solutions have the ability to scan data stores and also provide an agent that can be deployed on end systems to monitor and prevent unauthorized actions for classified enterprise data
- Using DLP, a discovery scan can be initiated to identify data in locations
- Also, it can be used in an ongoing scheduled scan to continuously monitor the data stores for data that should or should not reside in the data location



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

DLP: Data in Use

- Data in use is data that is actively processed within an application, process, memory or other location, temporarily for the duration of a function or transaction
 - i.e. enterprise data not stored long term, only long enough to perform a function or transaction
 - there is an application or function involved to read, add, remove, and modify data
- Data in use is the unique facet of DLP that is a little more complex than dealing with data in storage or data in transit
 - Data in use can be monitored by an agent installed on the end system to permit only certain uses of the data and deny actions such as storing the data locally or sending the data via e-mail or other communication method
 - implementation on employee-owned devices introduces privacy issues because any personal transactions such as online banking, medical record lookup, and so on may be detected and details of the transaction stored in the DLP database for review → **must be carefully evaluated when considering a BYOD deployment!!**

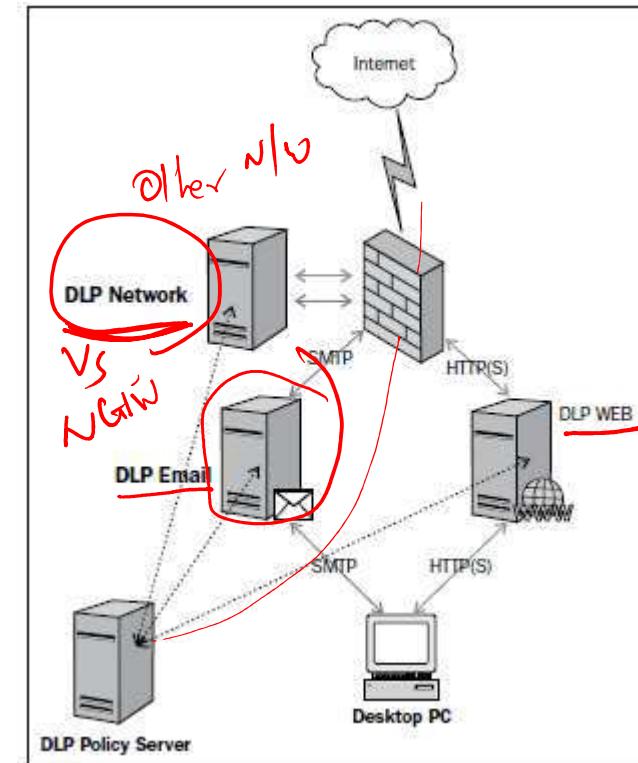


Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

DLP: Data in Transit

- Data in transit is data that is being moved from one system to another, either locally or remotely, such as file transfer systems, e-mail, and web applications
 - focus of DLP for data in transit is specifically data leaving the enterprise through egress connections
 - Yet, it is recommended that all data including credentials be transmitted only using secure methods, even within the internal enterprise network
- Many enterprise communication applications may be invisible to network-based security solutions
 - Example, use of instant messaging to send files or data
- Various DLP solutions have accounted for this fact and provide solutions capable of intercepting and decrypting communications to look for classified data

Careful choice needed from enterprise security admin if the next generation firewall (NGFW) can be better used or a DLP!!



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



Implementation of DLP

- The challenge with the DLP toolset is deciding what methods to employ, in what phases, and how to digest the output from the tool
 - => *challenge exists in operationalizing the solution and delivering value on the investment!!*
- The best method to implementing any solution in the enterprise is to first understand the problem to be solved, and then determine the course of action
- The following slides cover the DLP solutions, approaches to successfully implementing them, overcoming challenges, and getting value from a DLP implementation



CSIRT

DLP Network

- simplest solution to implement in an enterprise environment
- also the quickest method to determine what data is leaving the network in an insecure manner
- Implementation Considerations:
 - Volume of traffic to be inspected
 - Server size requirements to run DLP function (*else, overflooding can lead to data being lost!!*)
 - Protocols to be inspected (to limit inspection volume)
 - Person or team to whom findings are to be reported



DLP Email and Web

- Email and Internet access are the most commonly used enterprise services
- DLP (Email and Web) goes beyond the basic network portion of DLP
 - Focus more on loss of enterprise confidential data via emails or web
- Implementation Considerations:
 - Placement of DLP (e.g. along-side existing Internet proxy servers and e-mail forwarders)
 - changes to the use of e-mail and web within the enterprise (e.g. encrypted emails)



DLP Discover

- Is a tool that can scan network shares, document repositories, databases, and other data at rest
- Requires an account with permissions to be configured, to allow the scans to open the data stores and inspect for policy matches
- Implementation Considerations:
 - advisable to run scans during off hours as the solution may increase the I/O on the system being scanned and impact performance
 - permission errors impede the success of the scan; testing by initiating a limited scan can help identify simple issues that will otherwise derail the scan
 - If there are file auditing controls in place, the DLP solution may trigger alerts based on file access operations → such false positive alerts should be possible to identify and ignore



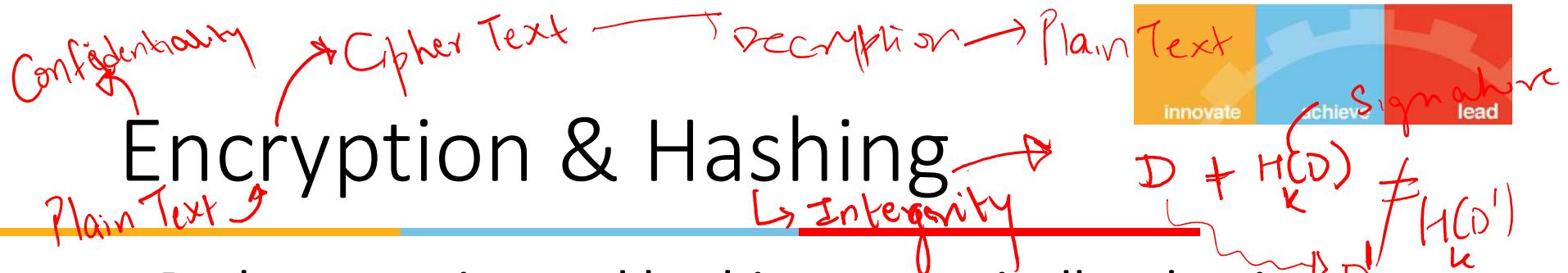
DLP Endpoint

- DLP Endpoint is an agent-based technology that must be installed on every end point
 - closest to the end user where the human interaction is the highest and, in theory, where the greatest risk is introduced to enterprise data
- In a typical enterprise, there will be more end point systems than any other hardware combined
 - => requires a significant implementation of agents that have to be installed, managed, and the output operationalized for meaningful and actionable reporting
- Implementation Considerations:
 - Use of enterprise common software management tools to install agents remotely on end point systems
 - Verification of agent for a variety of platforms (OS etc)
 - incidents may be exponentially higher than from other DLP solutions
 - Employee personal data and operations privacy issue!!



Data Protection Methods

- Earlier slides discussed Data Loss Prevention methods and techniques
- Next few slides will discuss methods for Data Protection, using different methods
 - Encryption and Hashing
 - Tokenization
 - Data Masking
 - Authorization



- Both encryption and hashing are typically what is thought of when data protection is discussed whether in storage, transit, or in use by applications
 - Mostly for data in storage or in transit
- Encryption is the method of mathematically generating a cipher text version of clear text data to render it unrecognizable
 - There are two general types of encryption – symmetric and asymmetric
 - data encrypted using a symmetric key can also be decrypted with the same key $Pk\}$
 - Asymmetric encryption is different than symmetric methods because the master key (private key) is never shared; data encrypted is done so using the server's public key
- Hashing is simpler, but only supports data integrity
 $E(D) + H(D)$



Encryption: Data at rest

- encryption can happen at the location of storage, prior to storage, or during the process of storing
 - ensure the business processes and applications can support the method used
- Another aspect to encrypting data at rest is online versus offline encryption
 - online encryption is in effect while data is accessible
 - offline is when data is not directly accessible such as on backup tapes, turned off systems, etc
 - An example of offline encryption is a whole disk encryption, once the operating system is booted and the volume is decrypted for use. Post boot, data is no longer encrypted and can be accessed in an unauthorized manner



Data @ Rest Encryption

- Data stored in databases can be encrypted via two methods
- first method utilizes the built-in encryption capabilities of the database itself to protect the stored data
 - beneficial when attempting to make encryption invisible to the applications and processes accessing the data
 - Caveat: If not configured properly, the system administrators can circumvent the database encryption
- Second method uses encrypting at the application and process layer
 - All data is encrypted before it is stored in the database



Application Encryption

- the encryption of the data occurs in the application not the database
- data arrives as already encrypted in the database
- all applications and processes using this data need a method to decrypt and encrypt the data → typically a shared private key
- Benefits:
 - Database performance gains for not using encryption at the database tier
 - The data is always encrypted in the databases (no DB admin or SYS admin visibility)
 - Data encryption is implemented end to end



Selective Database Encryption

- refers to encrypting only portions of the database; typically selected columns that contain sensitive data
- Benefits
 - often employed to reduce the overall load on the database server for encryption
 - also to make it easier for the DB admins to ensure the data inserted into the database is correct
- Caveat
 - DB admin has full control over the database encryption, if the individual decides to see the data in an unauthorized method, by changing configuration
 - However, monitoring and detection of the unauthorized change can be the only real protection from this unauthorized access
- Alternate to selective DB encryption is the Complete DB encryption
 - The method implemented must make sense from data protection and risk analysis perspectives, due to its overhead costs



File Share Encryption

- As with databases, many operating systems offer native encryption
- There are technologies available that will encrypt data as it is being written to the file system
- Similar options exist:
 - Encryption within the application
 - Encryption outside the application
 - Require other methods for enforcing least privilege and ensuring only the necessary processes, applications, and users have permissions to access data



Data in Use Encryption

- Not many use cases
- An example could be fraud investigators leveraging stored credit card and transaction information for an investigation
 - In this scenario, access to the data is necessary but should not be visible to prying eyes on the network
- Requires commercial software offering secure communication and views that can be created to ensure that only the fields needed are viewable



Data in Transit Encryption

- Performed via use of secure transport methods to transfer data
 - E.g. SSL, SFTP, FTP-S, and SSH, in addition to proprietary solutions
 - If the transport cannot be secured, then the data itself must be encrypted



Tokenization

- **Tokenization** is a method that assigns a value to a segment of data, so that the initial sensitive data value no longer exists
 - use in applications and storage in the database
 - processes, systems, and applications are able to process the token value as they would process the sensitive data
 - however, this method ensures that the token has no real value to anyone or anything outside of the process
- A database is used to map the original data to the token value
- A common use for tokenization is in the retail industry for the replacement of credit card data within the network and assets
 - allows retailers to escape the prescriptive security controls required (i.e. reduce PCI DSS scope)
 - is an option gaining momentum
- There is no real standard for tokens but one method to consider is format preserving to reduce complexity in rewriting applications for new formats



Data Masking

- This method is commonly used in processes where there is human interaction
 - example would be looking at your stored credit card information at an online retailer
 - Typically, your credit number will be masked (series of asterisks) except for the last four digits
- A similar method can be achieved in database views and specialized encryption solutions to enforce the least privilege and access only on a *need-to-know* basis
- Pros-and-Cons:
 - + relative ease of implementation
 - - Masking as used on a database implementation is simply a view presented with the original data intact and viewable by database administrators
 - - While the solution does provide some protection, it is not at the same level as tokenization, encryption, or hashing



Authorization

- Granting permissions based on who or what the authorized is
 - An important part of the enterprise data protection and security program
 - each of the previous approaches on data security relies on proper authorization to underlying operating systems, applications, and the data
- This facet of data security highlights the defense in depth mantra of information security
 - Regardless of the technologies implemented for encryption, tokenization, and masking, a developed process for authorization including access provisioning, account removal, level of access, and auditing will not only ensure that the data remains secure, but provides a defensible data security strategy that can aide in reducing risk and cost associated with external auditing engagements



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 7: IoT Security – An Overview

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



What we shall cover?

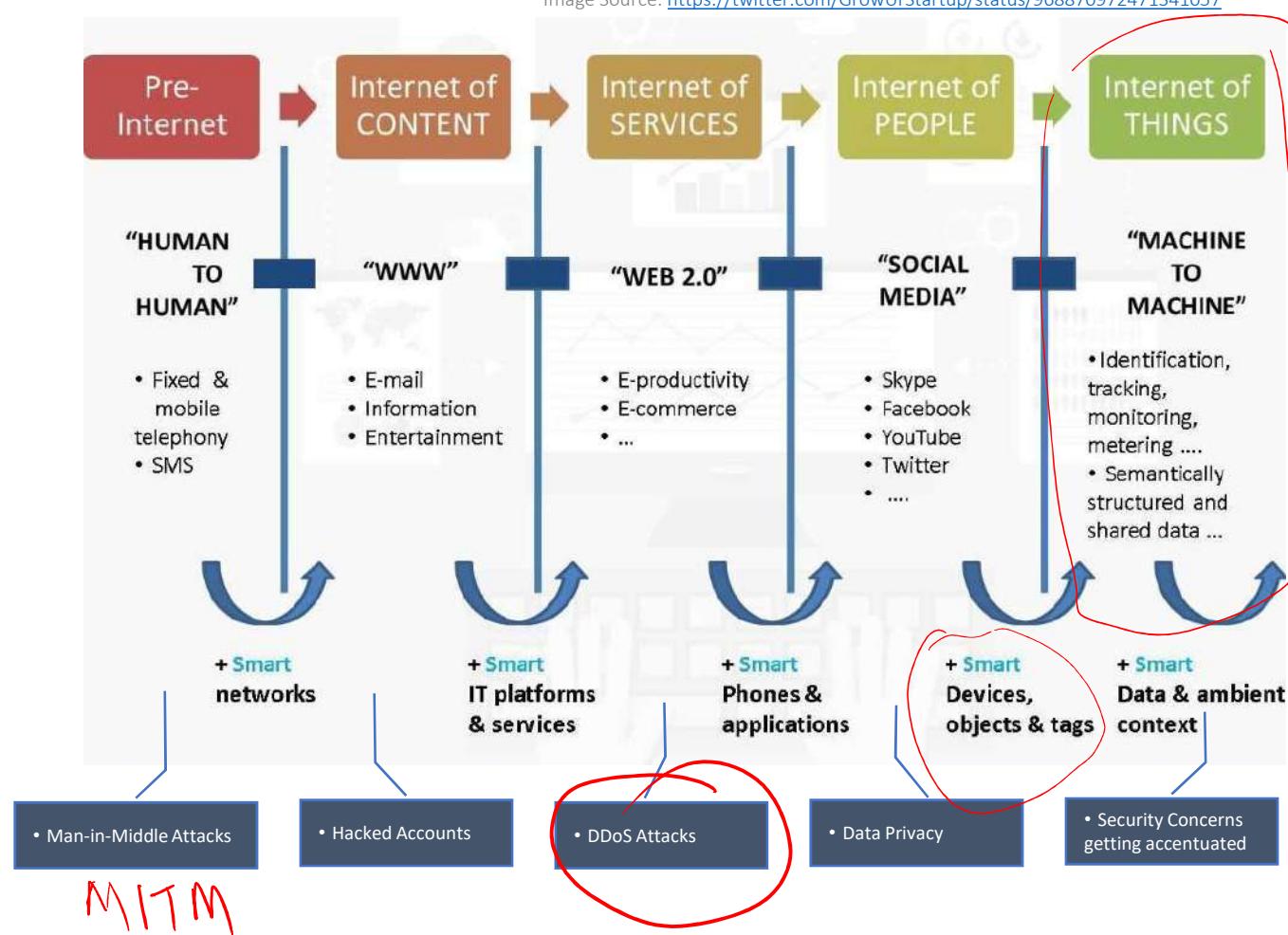
- 01 Context: IoT and its Verticals
 - 02 Need for IoT Security
 - 03 The Changing IoT Landscape and What it means for IoT Security
 - 04 Security Practices for the IoT World
-

RECAP:



The Evolving Internet.... And the Evolving Security Concerns!

Image Source: <https://twitter.com/GrowUrStartup/status/968870972471341057>

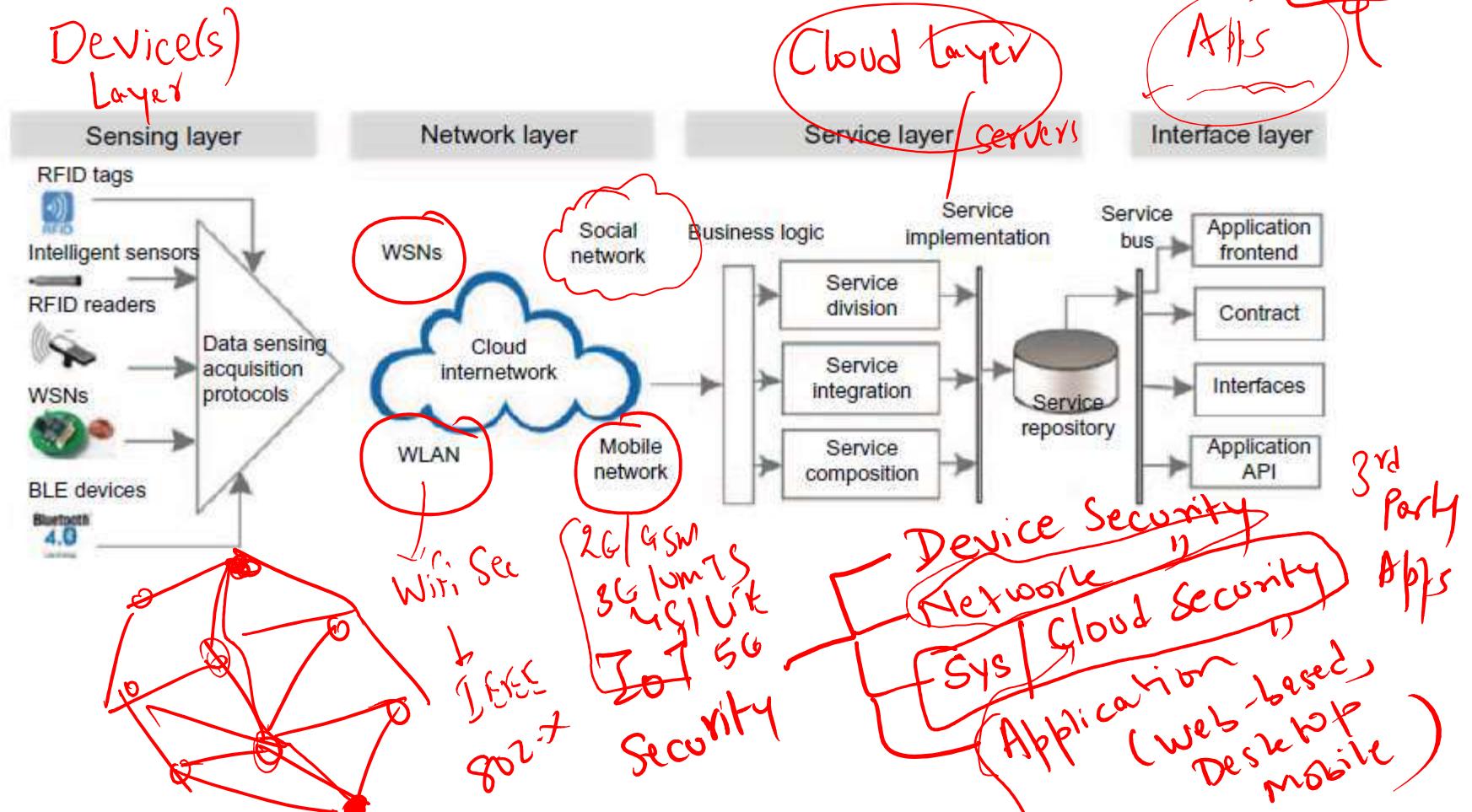




IoT is Everywhere



IoT Layers: A Security Perspective



Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017



The Stuxnet Attack!

IOT

Industry 4.0

- Discovered in 2010
- Targeted Attack (Microsoft Windows OS → Siemens Step 7 software)
- Compromised Iranian PLCs, causing fast spinning centrifuges to tear themselves apart
- Ruined almost one-fifth of Iran's Nuclear Centrifuges
- Overall, infected 200,000 computers, 1000 machines



Siemens Simatic S7-300 PLC CPU with three I/O modules attached

Affected Country	Share of infected computers
Iran	58.85%
Indonesia	18.22%
India	8.31%
Azerbaijan	2.57%
United States	1.56%
Pakistan	1.28%
Other countries	9.2%

PLCs
11008pm



URL | fQDNK → IP Addy
172.16.8.5



How Safe Are IoT Devices?

- **The 2016 Dyn DNS Service DDoS Attack**
- Orchestrated via IoT devices like printers, IP cameras, home gateways etc
- Tens of millions of remotely controlled IoT devices used in attack
- IoT devices were infected by the Mirai malware
- With an estimated load of 1.2 terabits per second, the attack is, according to experts, the largest DDoS on record

Source: <http://downdetector.com/status/level3>



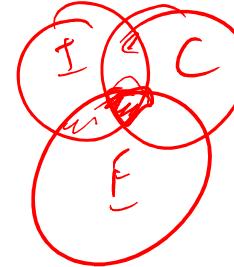
Map of areas most affected by attack,
16:45 UTC, 21 October 2016.

Affected services [edit]

Services affected by the attack included:

- Airbnb^[11]
- Amazon.com^[8]
- Ancestry.com^{[12][13]}
- The A. V. Club^[14]
- BBC^[13]
- The Boston Globe^[11]
- Box^[16]
- Business Insider^[13]
- CNN^[13]
- Comcast^[16]
- CrunchBase^[13]
- DirecTV^[13]
- The Elder Scrolls Online^{[13][17]}
- Electronic Arts^[16]
- Etsy^{[11][18]}
- FiveThirtyEight^[13]
- Fox News^[19]
- The Guardian^[19]
- GitHub^{[11][16]}
- Grubhub^[20]
- HBO^[13]
- Heroku^[21]
- HostGator^[13]
- iHeartRadio^{[12][22]}
- Imgur^[23]
- Indiegogo^[12]
- Mashable^[24]
- National Hockey League^[13]
- Netflix^{[13][19]}
- The New York Times^{[11][16]}
- Overstock.com^[13]
- PayPal^[18]
- Pinterest^{[16][18]}
- Pixar^[13]
- PlayStation Network^[16]
- Qualtrics^[12]
- Quora^[13]
- Reddit^{[12][16][18]}
- Roblox^[25]
- Ruby Lane^[13]
- RuneScape^[12]
- SaneBox^[21]
- Seamless^[23]
- Second Life^[26]
- Shopify^[11]
- Slack^[23]
- SoundCloud^{[11][18]}
- Squarespace^[13]
- Spotify^{[12][16][18]}
- Starbucks^{[12][22]}
- Storify^[15]
- Swedish Civil Contingencies Agency^[27]
- Swedish Government^[27]
- Tumblr^{[12][16]}
- Twilio^{[12][13]}
- Twitter^{[11][12][16][18]}
- Verizon Communications^[16]
- Visa^[28]
- Vox Media^[29]
- Walgreens^[13]
- The Wall Street Journal^[19]
- Wikia^[12]
- Wired^[15]
- Wix.com^[30]
- WWE Network^[31]
- Xbox Live^[32]
- Yammer^[23]
- Yelp^[13]
- Zillow^[13]

Source: [Wikipedia](https://en.wikipedia.org/w/index.php?title=2016_Dyn_DNS_Service_DDoS_Attack&oldid=750000000)



How Safe Are IoT Devices?

**IoT Goes Nuclear:
Creating a ZigBee Chain Reaction**
Eyal Ronen^(✉), Colin O'Flynn[†], Adi Shamir* and Achi-Or Weingarten*
^{*}Weizmann Institute of Science, Rehovot, Israel
{eyal.ronen,adi.shamir}@weizmann.ac.il
[†]Dalhousie University, Halifax, Canada
coflynn@dal.ca

Abstract—Within the next few years, billions of IoT devices will densely populate our cities. In this paper we describe a new type of threat in which adjacent IoT devices will infect each other with a worm that will rapidly spread over large areas, provided that the density of compatible IoT devices exceeds a certain critical mass. In particular, we developed and verified such an infection using the popular Philips Hue smart lamps as a platform. The worm spreads by jumping directly from one lamp to its neighbors, using only their built-in ZigBee wireless connectivity and their physical proximity. The attack can start by plugging in a single infected bulb anywhere in the city, and then catastrophically spread everywhere within minutes. It enables the attacker to turn all the city lights on or off, to permanently brick them, or to exploit them in a massive DDOS attack. To demonstrate the risks involved, we use results from percolation theory to estimate the critical mass of installed devices for a typical city such as Paris whose area is about 105 square kilometers: The chain reaction will fizz if there are fewer than about 15,000 randomly located smart lamps in the whole city, but will spread everywhere when the number exceeds this critical mass (which had almost certainly been surpassed already).

To make such an attack possible, we had to find a way to remotely yank already installed lamps from their current networks, and to perform over-the-air firmware updates. We overcame the first problem by discovering and exploiting a

the next five years more than fifty billion "things" will be connected to the internet. Most of them will be cheaply made sensors and actuators which are likely to be very insecure. The potential dangers of the proliferation of vulnerable IoT devices had just been demonstrated by the massive distributed denial of service (DDoS) attack on the Dyn DNS company, which exploited well known attack vectors such as default passwords and the outdated TELNET service to take control of millions of web cameras made by a single Chinese manufacturer [1].

In this paper we describe a much more worrying situation: We show that without giving it much thought, we are going to populate our homes, offices, and neighborhoods with a dense network of billions of tiny transmitters and receivers that have ad-hoc networking capabilities. These IoT devices can directly talk to each other, creating a new unintended communication medium that completely bypasses the traditional forms of communication such as telephony and the internet. What we demonstrate in this paper is that even IoT devices made by big companies with deep knowledge of security, which are protected by industry-standard cryptographic techniques, can be misused by hackers to create a new kind of attack: By using this new communication medium to spread infectious malware from one IoT device to all its physically adjacent neighbors, hackers can rapidly cause city-wide disruptions which are very difficult to stop and to investigate.

E. Ronen, A. Shamir, A. Weingarten and C. O'Flynn, "*IoT Goes Nuclear: Creating a ZigBee Chain Reaction*," **2017 IEEE Symposium on Security and Privacy (SP)**, San Jose, CA, 2017, pp. 195-212.
doi: 10.1109/SP.2017.14

In the same period as the Dyn Attack,
researchers uncovered a flaw in the radio
protocol Zigbee.

- Demonstrated using an aerial drone to target a set of smart Philips light bulbs in an office tower
- Infected the bulbs with a virus that let the attackers to turn the lights on and off flashing an "SOS" message in Morse code
- This malware was also able to spread like a pathogen among the devices neighbors.



How Safe Are IoT Devices?

SUNDAY TIMES OF INDIA, NEW DELHI / GURGAON
AUGUST 4, 2019

THE ECONOMIC TIMES

day

Hackers can track you through your smartband



This randomised address can be decoded with something researchers call a 'rainbow table.'

in.pc当地.com

This randomised address can be decoded with something researchers call a 'rainbow table.'

10

- Findings from a group of researchers in Boston University
- Location Tracking by exploiting a Bluetooth Vulnerability
- Pose issues related to
 - Personal Security
 - Stalking
 - Abuse

- Findings from Microsoft Threat Intelligence Center in April 2019
- Discovered a targeted attack against IoT devices—a VOIP phone, a printer and a video decoder
- Attack hit multiple locations, using the devices as soft access points into wider corporate networks

<https://www.forbes.com/sites/zakdoffman/2019/08/05/microsoft-warns-russian-hackers-can-breach-companies-through-millions-of-simple-iot-devices/amp/>

17,129 views | Aug 5, 2019, 3:42 pm

Microsoft Warns Russian Hackers Can Breach Secure Networks Through Simple IoT Devices

Zak Doffman contributor

Cybersecurity

I write about security and surveillance.



TASS VIA GETTY IMAGES

Just ahead of Black Hat 2019, Microsoft has reported that in April its Threat Intelligence Center discovered a targeted attack against IoT devices—a VOIP phone, a printer and a video decoder. The attack hit multiple locations, using the devices as soft access points into wider corporate networks. Two of the three devices still carried factory security settings, the software on the third hadn't been updated.



How Safe Are IoT Devices?

August 13, 2019 Times of India

India sees most IoT attacks in Apr-Jun

Sindhu.Hariharan
@timesgroup.com

Chennai: India has emerged as the 'most vulnerable' to cyberattacks due to the deployment of Internet of Things (IoT) systems. On February 28 this year, the day of heightened tensions between India and Pakistan, the country found itself as the most-targeted nation as it experienced a large spurt in attacks, according to a recent study by cybersecurity firm Subex. The country also saw a 22% jump in total number of attacks in the IoT segment during the quarter ended June, the report said. Globally, cyberattacks increased by 13% during the same period.

The Bengaluru-based Sub-

BIG TARGET

Total number of cyberattacks from IoT deployments registered 22% growth compared to the previous quarter



► Critical infrastructure projects are at high risk of malware attacks
► India among the most-attacked nations in the world for the second consecutive quarter

► A strong 'geopolitical influence' noted in some of the attacks on critical infrastructure
► Mumbai, Delhi NCR and Bengaluru among the most attacked cities
► Czech Republic, Poland, Slovenia are top countries of origin for cyberattacks on India

ex captured details of attacks from its "honeypot" network (a decoy computer system for trapping hackers) that covers over 4,000 IoT devices. During the June quarter, Subex researchers recorded 33,450 high-gra-

de attacks, 500 of which were of "very high sophistication".

As many as 15,000 new samples of malware were discovered this quarter and, in a sign of increased sophistication of threats, 17% of the

samples collected were modular malware—an advanced attack on a system that acts in different stages.

Subex MD and CEO Vinod Kumar said there are also strong geopolitical influences seen in some of the attacks on critical infrastructure with patterns of IP-spoofing with an intent to hide the geography of origin. Even as IoT in India moves from proof of concept to full-scale deployments rapidly, the country's deep expertise and preparedness level hasn't kept pace, he added. IoT systems related to smart cities, financial services, and transportation sectors were the top targets for hackers, accounting for over 51% of all cyberattacks registered.



Recent, back home....



Tuesday, March 02, 2021

March 02, 2021

Chinese ops target India's energy infra

HT Correspondents

letters@hindustantimes.com

NEW DELHI/MUMBAI: Chinese-government-linked attackers possibly gained access to computer networks part of India's power infrastructure, a US-based cybersecurity firm has said, citing technical clues that federal power sector officials' statements said had been on their radar, fueling speculation that a blackout in Mumbai last year may have been the result of sabotage.

First reported by the New York Times on Monday, security consultancy Recorded Future said the attackers (which it calls RedCell) targeted at least "70 distinct power sector organizations" with a malware known as ShadowPad.

Hours after the disclosure,

A SECURITY CONSULTANCY SAID ATTACKERS TARGETED AT LEAST '70 DISTINCT POWER SECTOR ORGANISATIONS' WITH A MALWARE

month of November 2020," said a statement by the Union power ministry, which added that "there is no impact on any of the functionalities carried out by POSOCO (Power System Operation Corporation Limited) due to the referred threat," the ministry said.

"No data breach/ data loss has been detected due to these incidents."

The statement appeared to suggest that the attacks were not behind the October 12, 2020 power outage in Mumbai that had lasted up to 12 hours in some parts of India's financial capital, bringing the city's local trains to a halt and forcing the airport to switch to back-up supply.

Recorded Future's InSikt Group, the cyber threat intelligence



- Chinese attackers gained access to computer networks in India's power infrastructure
- Speculation that last year Mumbai power outage may be a result of this sabotage
- Malware known as ShadowPad
- Targeted at least 10 district power sector organizations



Why IoT Security?

- Rapid Growth of IoT Devices and Solutions
- TTM pressures leading to security compromises
- Robust Security and Data Privacy are key for Businesses to survive
- Data / Information Loss can lead to far reaching consequences

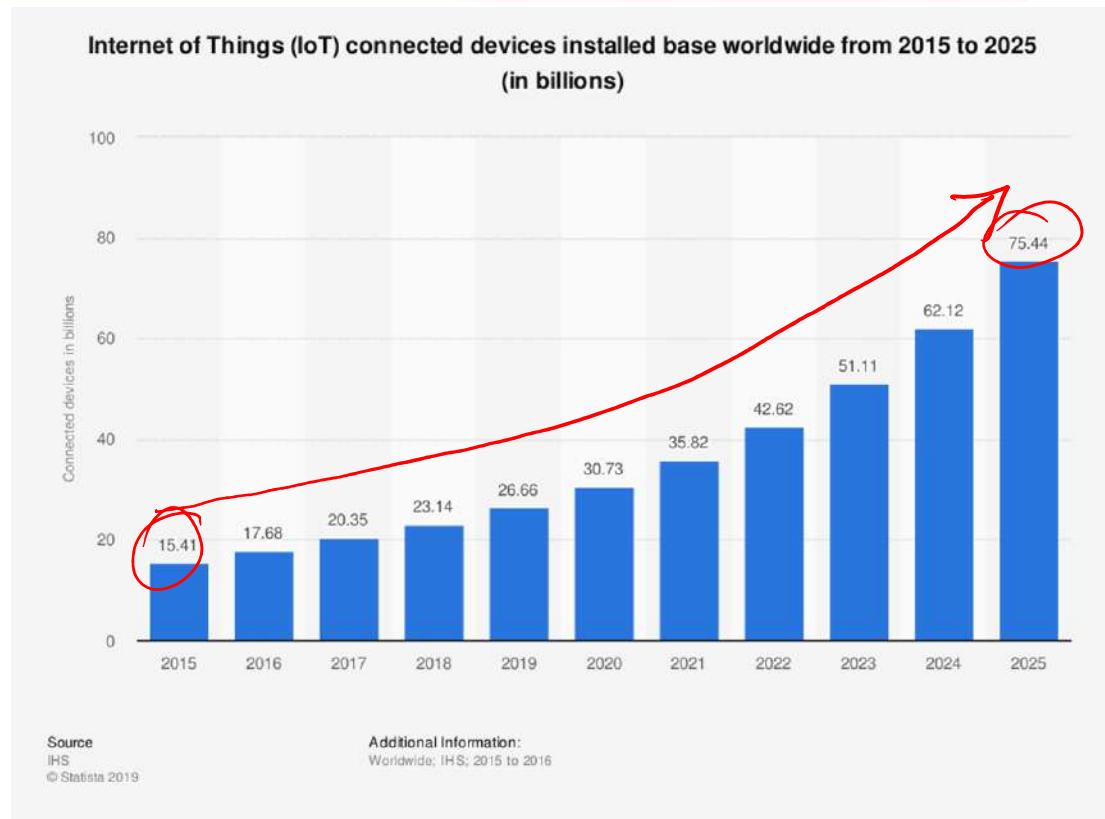
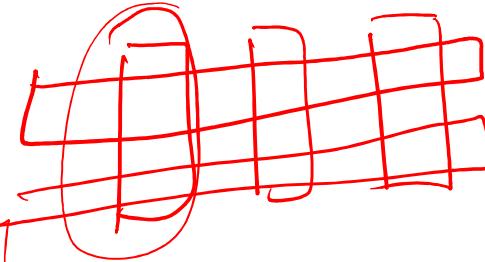


Image Source: <https://www.slideshare.net/akabhay/internet-of-things-the-battle-for-your-home-commute-and-life>



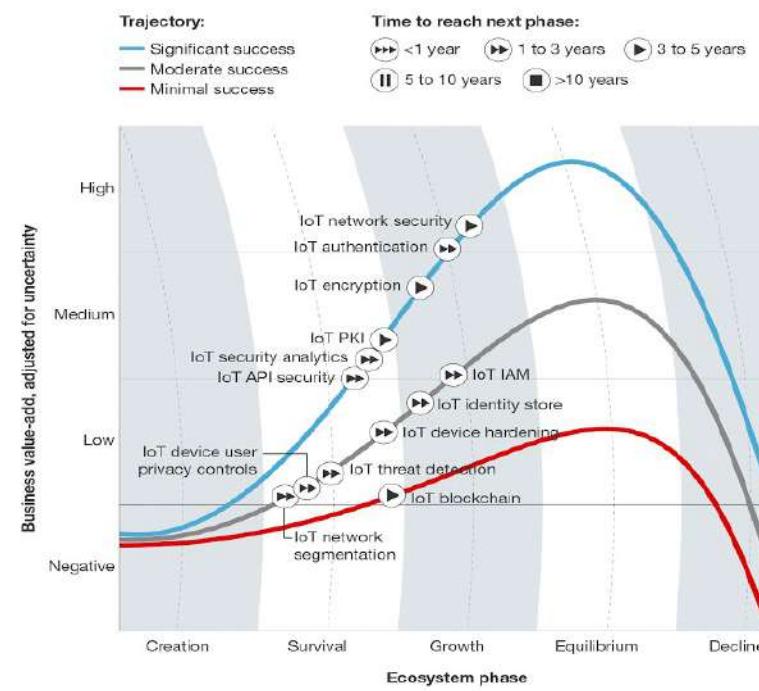
IoT Security: Involved Domains

- Device Security
 - Securing the IoT Device
 - Challenges: Limited System Resources
- Network Security
 - Security the network connecting IoT Devices to Backend Systems
 - Challenges: Wider range of devices + communication protocols + standards
- Cloud/ Back-end Systems Security
 - Securing the backend Applications from attacks
 - Firewalls, Security Gateways, IDS/IPS
- Mutual Authentication
 - Device(s) ↔ User(s)
 - Passwords, PINs, Multi-factor, Digital Certificates
- Encryption
 - Data Integrity for data at rest and in transit
 - Strong Key Management Processes

lower Computational ability
Storage

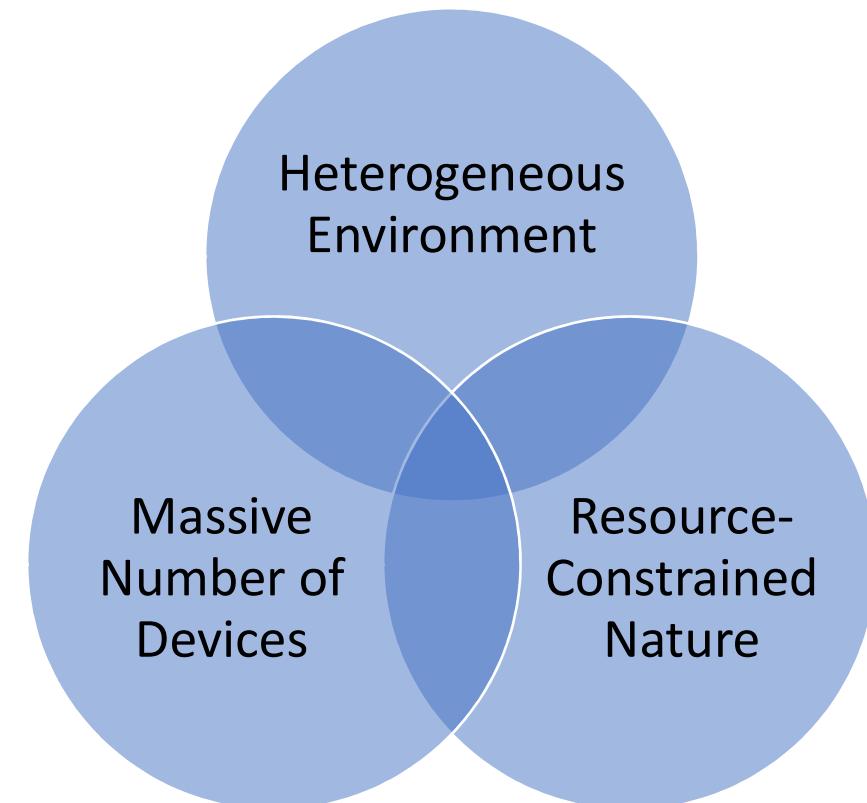
Cloud security

FORRESTER RESEARCH
TechRadar™: Internet Of Things Security, Q1 '17
TechRadar™: Internet Of Things Security, Q1 2017





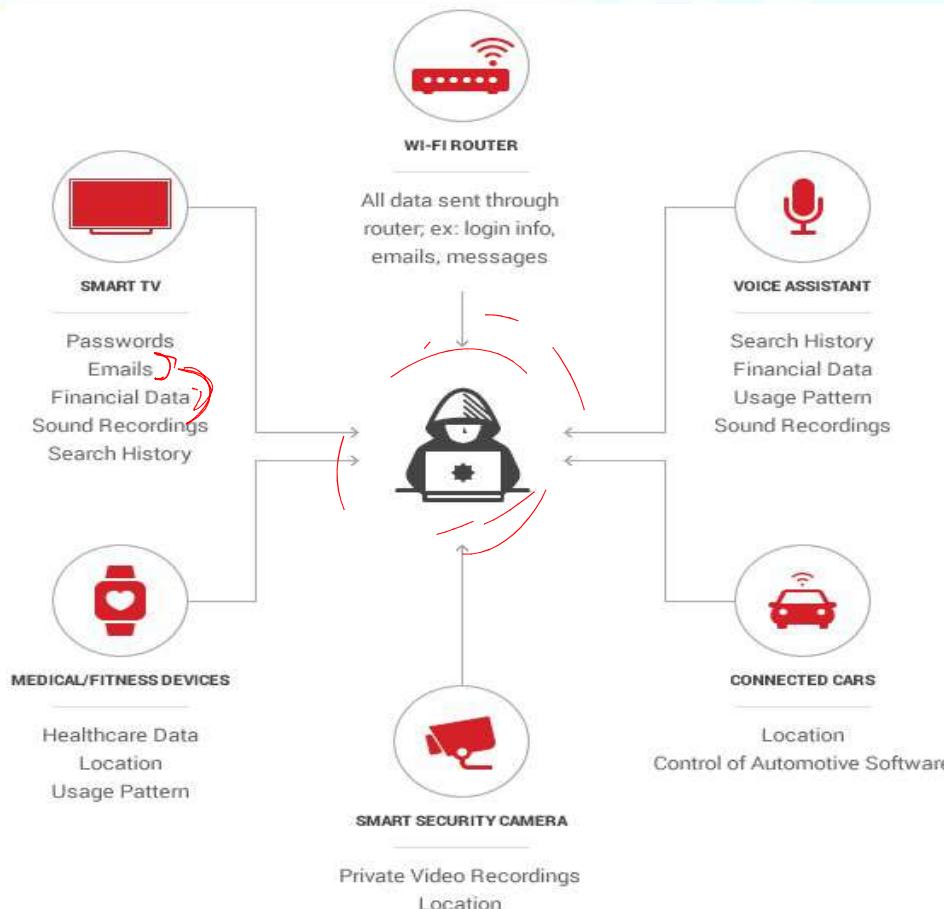
IoT Device Security : Key Focus Area in IoT Security



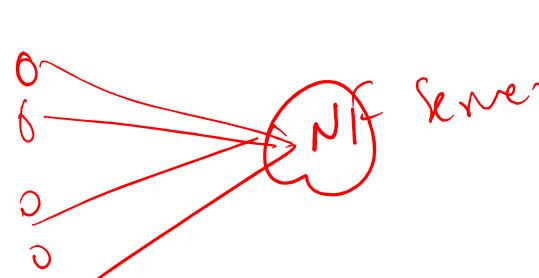


Data Privacy Issues with IoT Devices

Information a malicious hacker can obtain from an IoT device



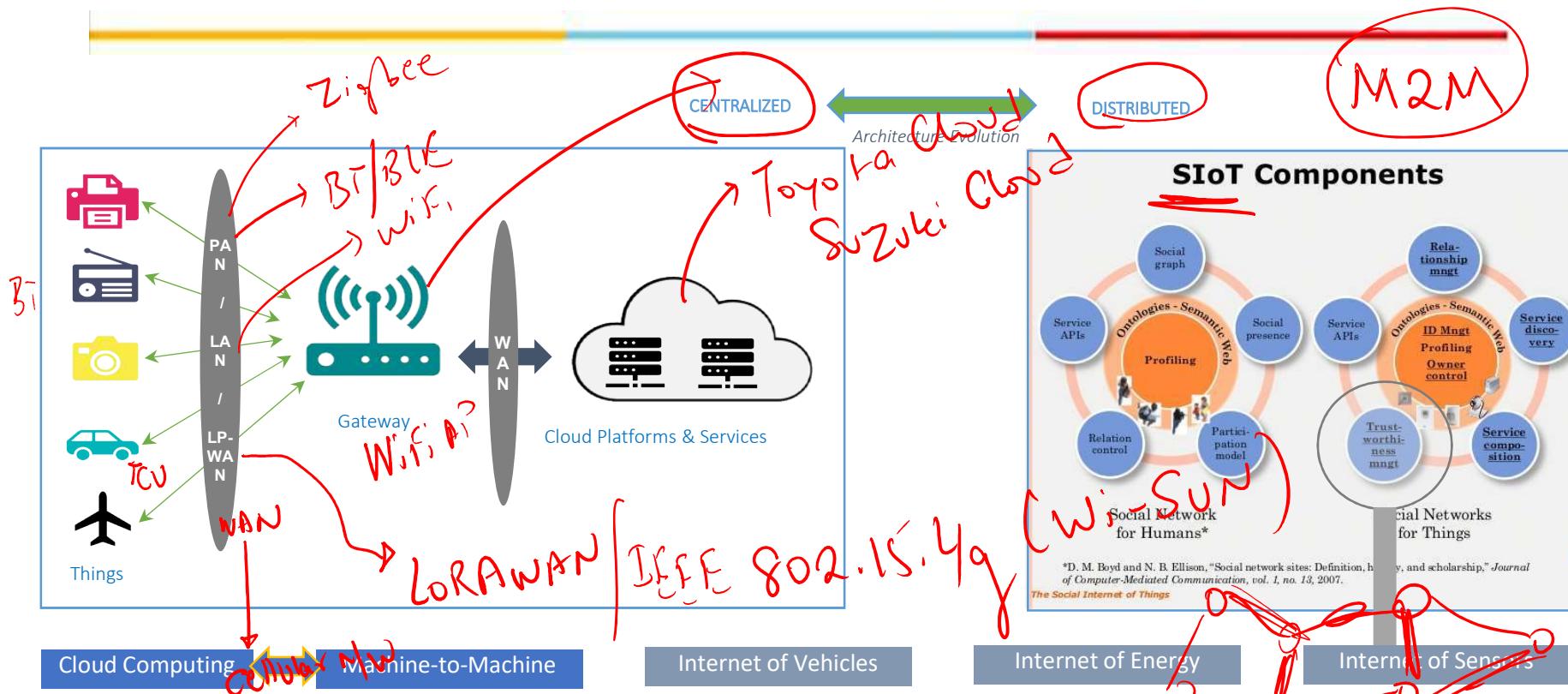
Source: HEIMDAL



SCADA

P2P

IoT Architectures – The Evolving Landscape!



- “The way to **secure the Internet of Things** is to allow the self-organizing migration of services away from a central cloud alone and into local infrastructure ecosystems where they can act independently” - <https://www.scmagazineuk.com/doriot-project-secure-internet-things/article/1590701>

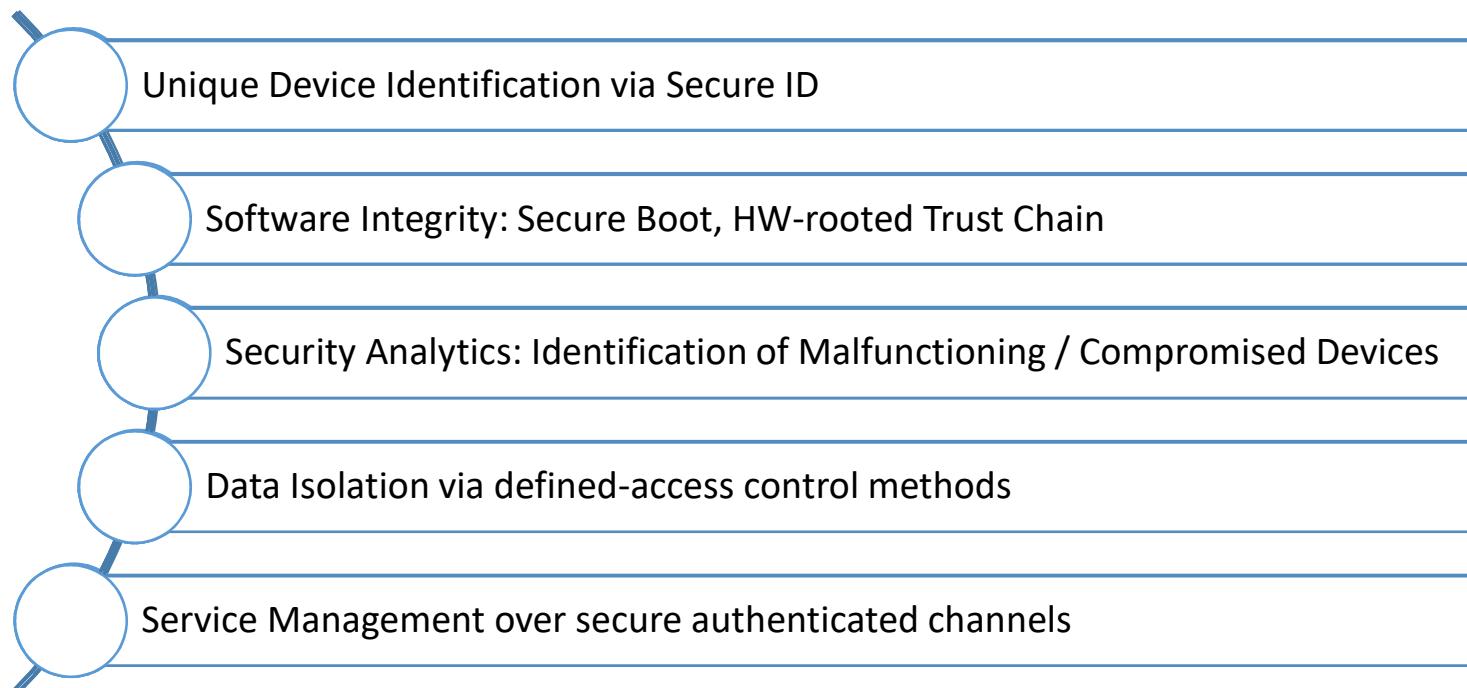
Vulnerabilities with IoT Devices

Security Threats	Description
Unauthorized access	Due to physically capture or logic attacked, the sensitive information at the end-nodes is captured by the attacker
Availability	The end-node stops to work since physically captured or attacked logically
Spoofing attack	With malware node, the attacker successfully masquerades as IoT end-device, end-node, or end-gateway by falsifying data
Selfish threat	Some IoT end-nodes stop working to save resources or bandwidth to cause the failure of network
Malicious code	Virus, Trojan, and junk message that can cause software failure
DoS	An attempt to make a IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path

Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017



IoT Device Security



Case Study: AWS IoT and AWS IoT Device Defender



Vulnerabilities with IoT Networks

Security Threats	Description
Data breach	Information released of secure information to an untrusted environment
Public key and private key	It comprises of keys in networks
Malicious code	Virus, Trojan, and junk message that can cause software failure
DoS	An attempt to make an IoT end-node resource unavailable to its users
Transmission threats	Threats in transmission, such as interrupting, blocking, data manipulation, forgery, etc.
Routing attack	Attacks on a routing path

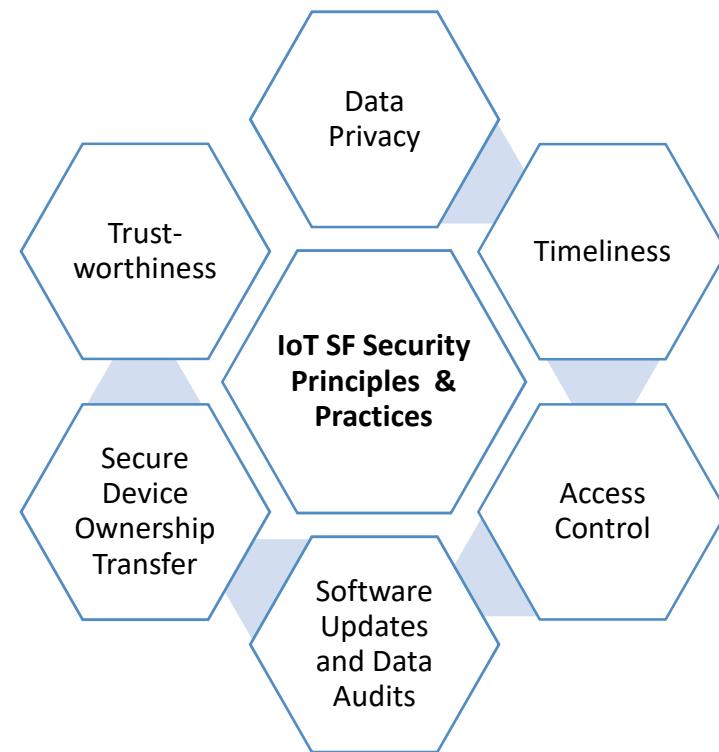
Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017



Guidelines for Secure System Engineering

- Forrester Research: “*There is no single, magic security bullet that can easily fix all IoT security issues*”
- IoT Security Foundation
 - Establishing Principles for Internet of Things Security
 - » Does the data need to be private?
 - » Does the data need to be trusted?
 - » Is the safe and/or timely arrival of data important?
 - » Is it necessary to restrict access to or control of the device?
 - » Is it necessary to update the software on the device?
 - » Will ownership of the device need to be managed or transferred in a secure manner?
 - » Does the data need to be audited?
 - Do not re-invent the wheel – rely on reusing existing cyber security principles and practices

“the underlying principles that inform good security practices are well established and quite stable” – IoT SF





BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:(nishit.narang@pilani.bits-pilani.ac.in))



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

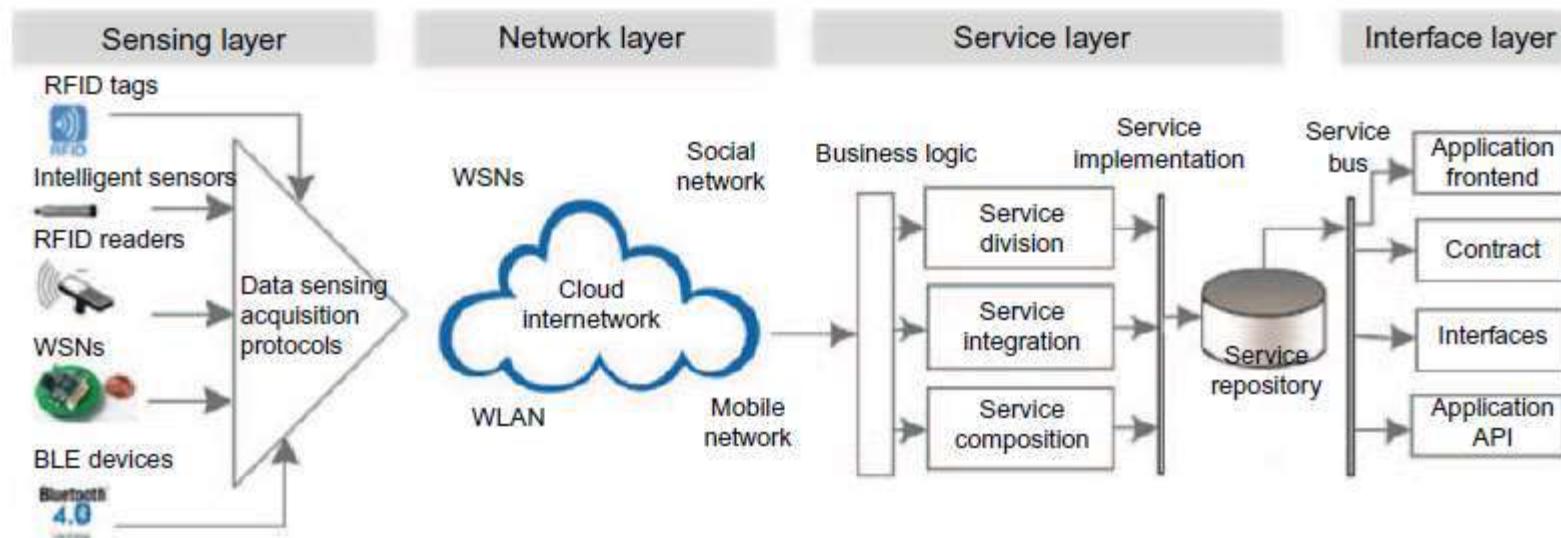
Lecture: IoT Security

Requirements, Reference Guidelines, Vulnerabilities, Security Framework Features and Implementation Methods

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



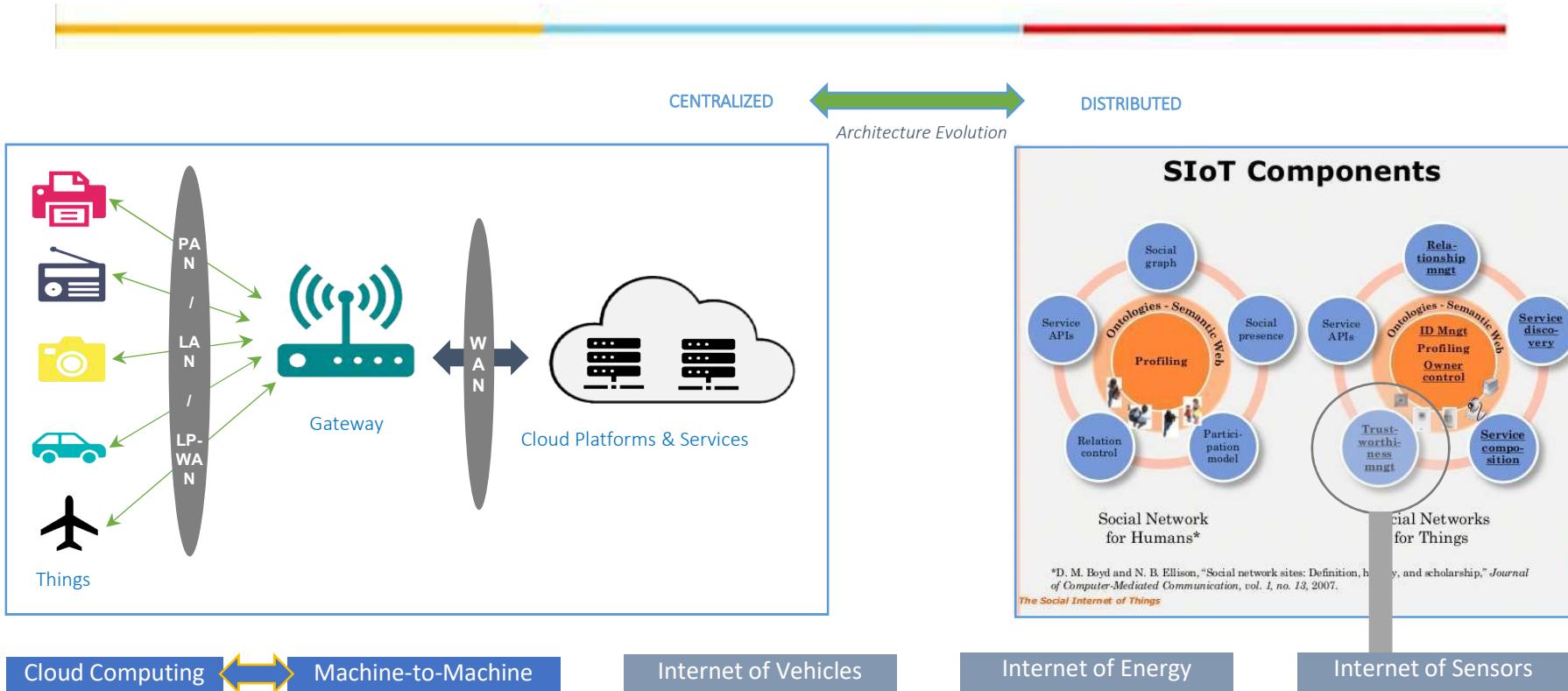
RECAP: IoT Layers: A Security Perspective



Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017



RECAP: IoT Architectures – The Evolving Landscape!



- “The way to **secure the Internet of Things** is to allow the self-organizing migration of services away from a central cloud alone and into local infrastructure ecosystems where they can act independently” - <https://www.scmagazineuk.com/doriot-project-secure-internet-things/article/1590701>



RECAP: IoT Security: Involved Domains

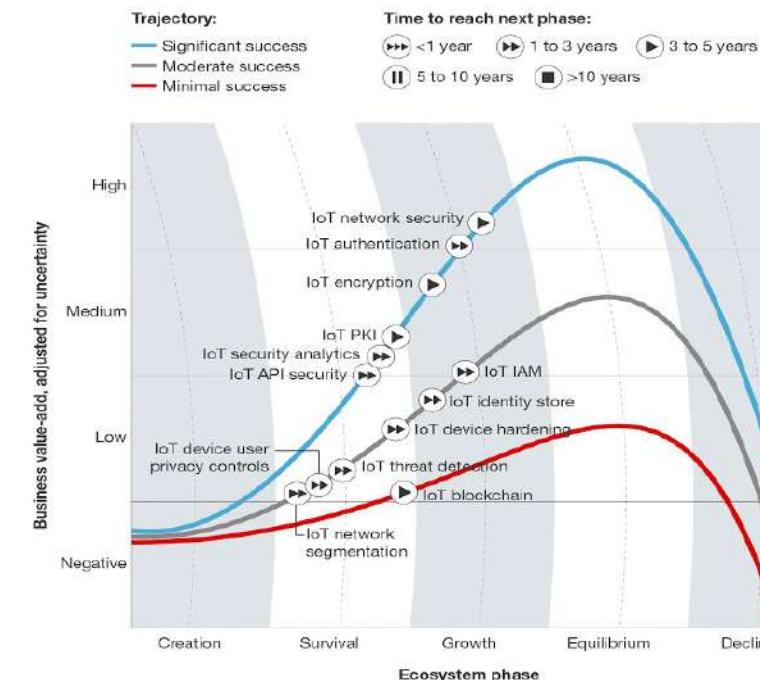
"Cyber security is also a moveable feast - what is deemed secure today may not be tomorrow" – IoTSF

- Device Security (aka Sensing Layer)
 - Securing the IoT Device
 - **Challenges:** Limited System Resources
- Network Security (aka Network Layer)
 - Security the network connecting IoT Devices to Backend Systems
 - **Challenges:** Wider range of devices + communication protocols + standards
- Cloud/ Back-end Systems Security (aka Service and Interface Layer)
 - Securing the backend Applications from attacks
 - Firewalls, Security Gateways, IDS/IPS
- Mutual Authentication (Across Layers)
 - Device(s) ↔ User(s)
 - Passwords, PINs, Multi-factor, Digital Certificates
- Encryption (Across Layers)
 - Data Integrity for data at rest and in transit
 - Strong Key Management Processes

FORRESTER® RESEARCH

TechRadar™: Internet Of Things Security, Q1 '17

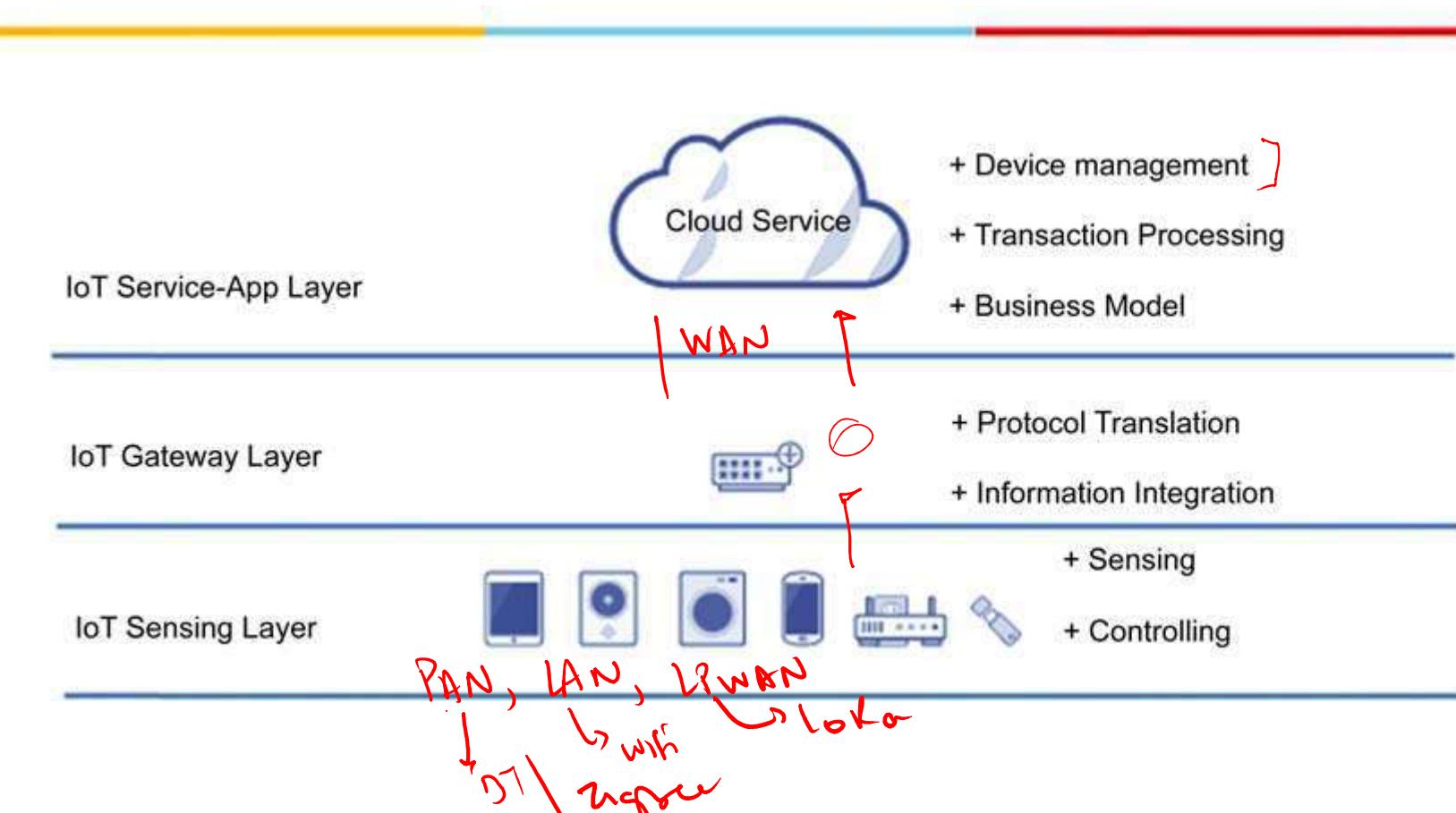
TechRadar™: Internet Of Things Security, Q1 2017



IoT Security Requirements



Example of a Simple IoT System / Solution

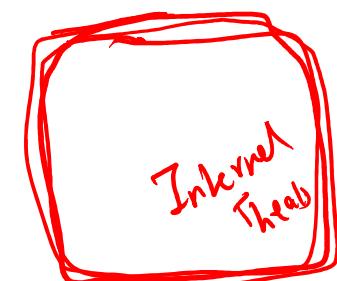


Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017



Security Requirements for IoT Systems

- IoT introduces large quantities of new devices that will be deployed
- Each connected device could be a potential doorway into the IoT infrastructure or personal data → **Data Security** happens to be the biggest challenge even in IoT Systems → Data-centric Security Approaches
- Security Requirements for IoT systems are handled via a combination of:
 - Sensing Layer Security
 - Network Layer Security
 - Service (& Interface) Layer Security



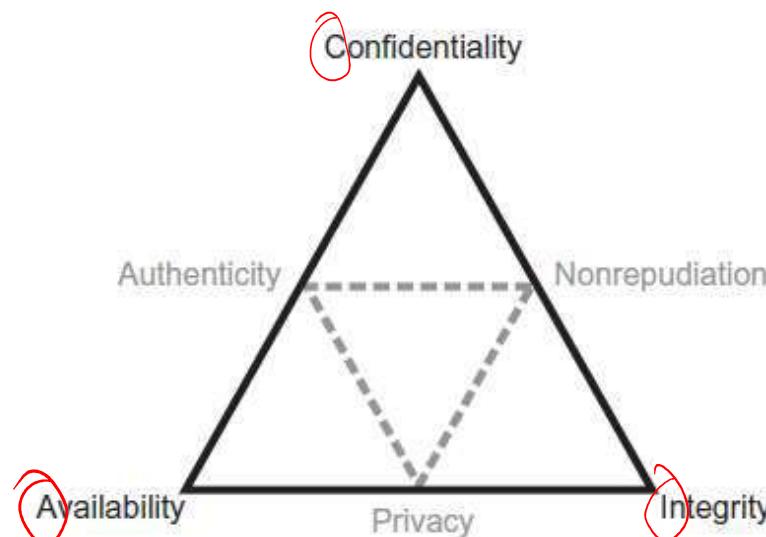


CIA-Triad



IoT Data Security

- For IoT Data Security, the main security requirements are addressed from six aspects, as shown in the figure



- Confidentiality**—data is secured to authorized parties
- Integrity**—data is trusted
- Availability**—data is accessible when and where needed
- Nonrepudiation**—service provides a trusted audit trail
- Authenticity**—components can prove their identity
- Privacy**—service does not automatically see customer data

Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017



Sensing Layer Security

- This layer of the framework is characterized as the intersection of people, places, and things
 - These things can be simple devices like connected thermometers and light bulbs, or complex devices such as medical instruments and manufacturing equipment
 - For security in IoT to be fully realized, it must be designed and built into the devices themselves. This means that IoT devices must be able to
 - prove their identity to maintain authenticity
 - sign and encrypt their data to maintain integrity, and
 - limit locally stored data to protect privacy
 - The security model for devices must be strict enough to prevent unauthorized use, but flexible enough to support secure, ad hoc interactions with people and other devices on a temporary basis
 - Physical security is another important aspect for devices
 - This creates the need to design tamper resistance into devices so that it is difficult to extract sensitive information like personal data, cryptographic keys, or credentials
 - Lastly, devices must support software updates to patch vulnerabilities and exploits
-



Network Layer Security

- This layer of the IoT framework represents the connectivity and messaging between things and cloud services
- Communications in the IoT are usually over a combination of private and public networks, so securing the traffic is obviously important.
- This is probably the most understood area of IoT security, with technology like TLS/SSL encryption ideally suited to solve the problem.
- The primary difficulty arises when you consider the challenges of cryptography on devices with constrained resources. E.g. 8-bit microcontrollers with limited RAM. For example:
 - an Arduino Uno takes up to 3 min to encrypt a test payload when using RSA 1024 bit keys
 - however an elliptical curve digital signature algorithm with a comparable RSA key length can encrypt the same payload in 0.3 s.
 - This indicates that device manufacturers cannot use resource constraints as an excuse to avoid security in their products
- Another security consideration for the network layer is that many IoT devices communicate over protocols other than WiFi
 - This means the IoT gateway is responsible for maintaining confidentiality, integrity, and availability while translating between different wireless protocols, from Z-Wave or ZigBee to WiFi for example.



Service Layer Security

- This layer of the framework represents the IoT management system and is responsible for onboarding devices and users, applying policies and rules, and orchestrating automation across devices
- Access control measures to manage user and device identity and the actions they are authorized to take is critical at this layer
- To achieve nonrepudiation, it is also important to maintain an audit trail of changes made by each user and device so that it is impossible to refute actions taken in the system
- Big Data Challenges:
 - providing clear data use notification so that customers have visibility and fine-grained control of the data sent to the cloud service
 - keeping customer data stored in the cloud service segregated and/or encrypted with customer-provided keys, and
 - when analyzing data in aggregate across customers, the data should be anonymized

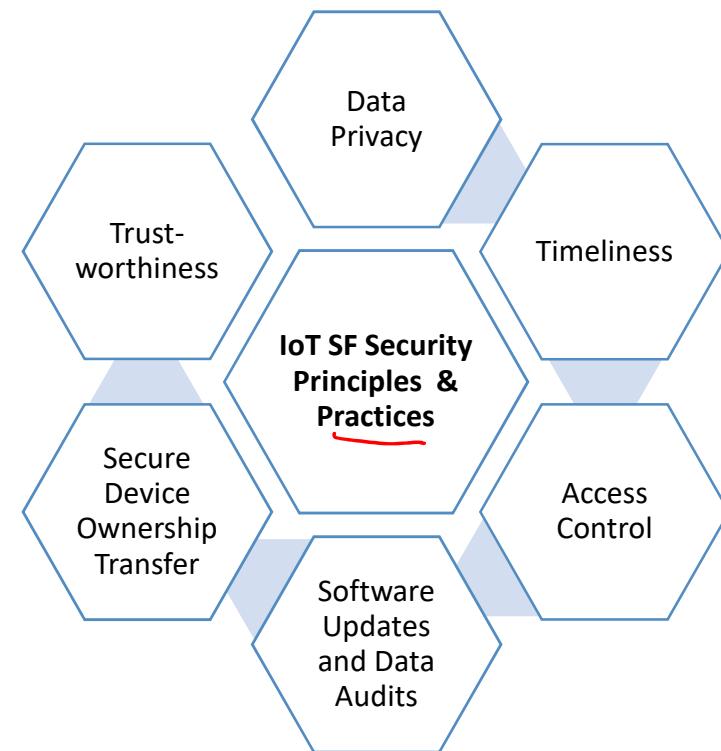
IoT Security: Reference Guidelines



Guidelines for Secure System Engineering

- Forrester Research: “*There is no single, magic security bullet that can easily fix all IoT security issues*”
- IoT Security Foundation
 - Establishing Principles for Internet of Things Security
 - » Does the data need to be private?
 - » Does the data need to be trusted?
 - » Is the safe and/or timely arrival of data important?
 - » Is it necessary to restrict access to or control of the device?
 - » Is it necessary to update the software on the device?
 - » Will ownership of the device need to be managed or transferred in a secure manner?
 - » Does the data need to be audited? }
- Do not re-invent the wheel – rely on reusing existing cyber security principles and practices

“the underlying principles that inform good security practices are well established and quite stable” – IoT SF





NIST GUIDANCE ON INTERNET OF THINGS

- NISTIR 8259: Foundational Cybersecurity Activities for IoT Device Manufacturers
 - Intended for a wide range of IoT devices, but only those that are newly developed
 - It is not meant to be a retroactive *band-aid* for devices already out on the market!
- The guidance provides six clear steps that manufacturers should follow, which are further separated into two phases:
 - **Pre-Market:** before the device is sold
 - **Post-Market:** after the device is sold
- Because over half of the recommendations are specifically for a manufacturer to perform before releasing their product, NISTIR 8259 cannot be applied to IoT devices already on the market
 - Four pre-market activities (1–4) and two post-market activities (5–6) for IoT manufacturers to address cybersecurity in IoT devices
 - Activity 1: Identify expected customers and define expected use cases.
 - Activity 2: Research customer cybersecurity goals.
 - Activity 3: Determine how to address customers' goals.
 - Activity 4: Plan for adequate Support of customers' goals.
 - Activity 5: Define approaches for communication to customers.
 - Activity 6: Decide what & how to communicate to customers.

Use
Ref 2

]

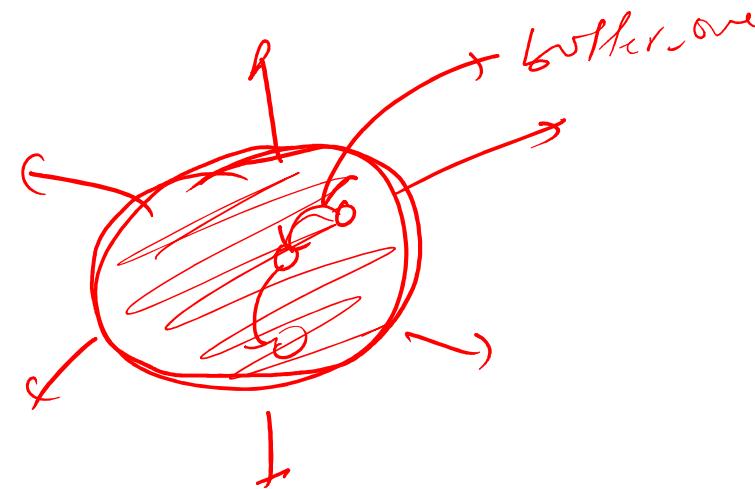
Source(s): <https://risk3sixty.com/2020/08/17/securing-iot-devices-with-nistir-8259/>
<https://www.mwe.com/insights/nist-guidance-on-internet-of-things/>



NISTIR 8259A

- NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline provides six capabilities, cross-referenced with applicable industry and federal standards, as a default for minimally securable IoT devices.
 - Device identification: The IoT device can be uniquely identified logically and physically.
 - Device configuration: The configuration of the IoT device's software can be changed, and such changes can be performed by authorized entities only.
 - Data protection: The IoT device can protect the data it stores and transmits from unauthorized access and modification.
 - Logical access to interfaces: The IoT device can restrict logical access to its local and network interfaces, and the protocols and services used by those interfaces, to authorized entities only.
 - Software update: The IoT device's software can be updated by authorized entities only using a secure and configurable mechanism.
 - Cybersecurity state awareness: The IoT device can report on its cybersecurity state and make that information accessible to authorized entities only.

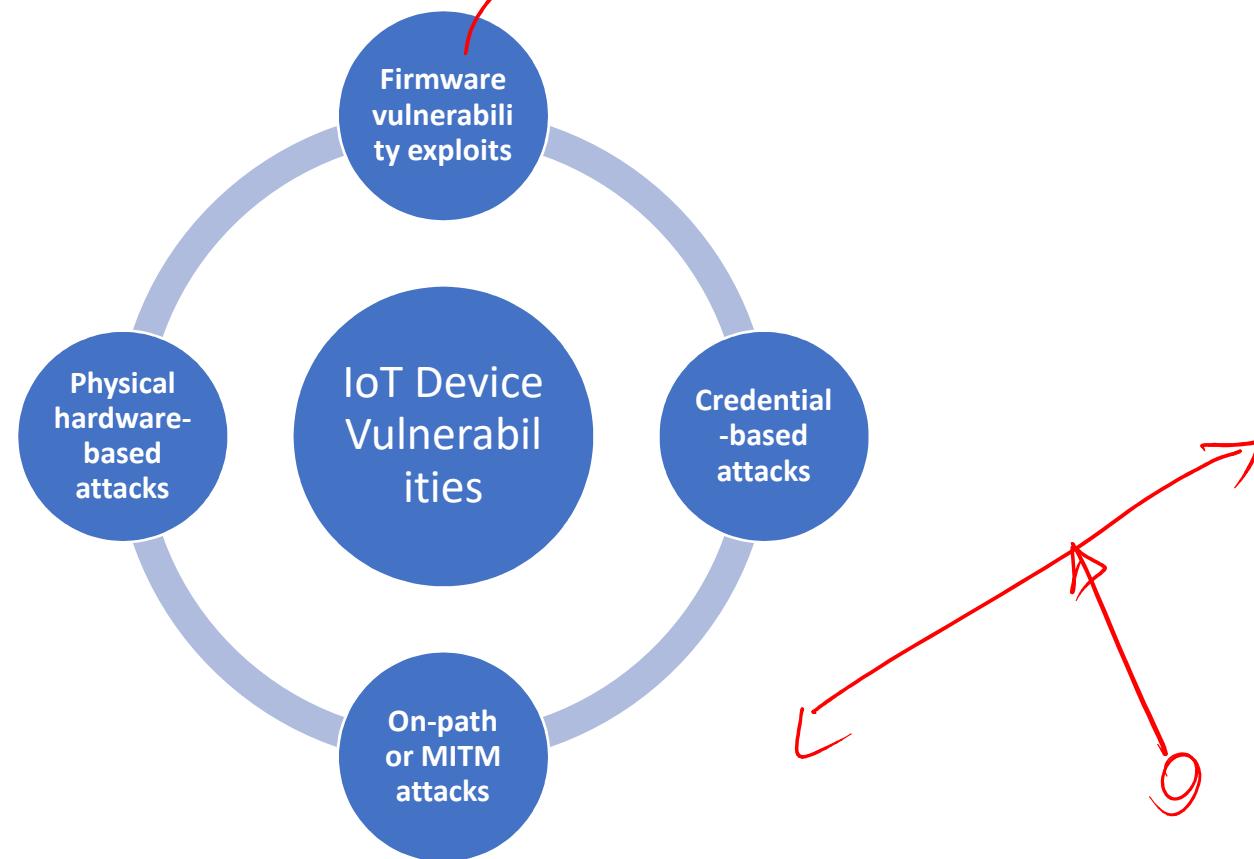
Source(s): <https://www.mwe.com/insights/nist-guidance-on-internet-of-things/>



IoT Security: Current Vulnerabilities



IoT Device Vulnerabilities





IoT Device Vulnerabilities (2)

- Firmware vulnerability exploits
 - For the majority of IoT devices, the firmware is essentially the operating system or the software underneath the OS
 - Most IoT firmware does not have as many security protections in place
 - Often the vulnerabilities in the firmware cannot be patched
- Credential-based attacks
 - IoT devices come with default administrator usernames and passwords
 - Well-known, or simple to guess, and often, not very secure
 - In some cases, these credentials cannot be reset
 - Often, IoT device attacks occur simply because an attacker guesses the right credentials

Source: <https://www.cloudflare.com/en-in/learning/security/glossary/iot-security/>

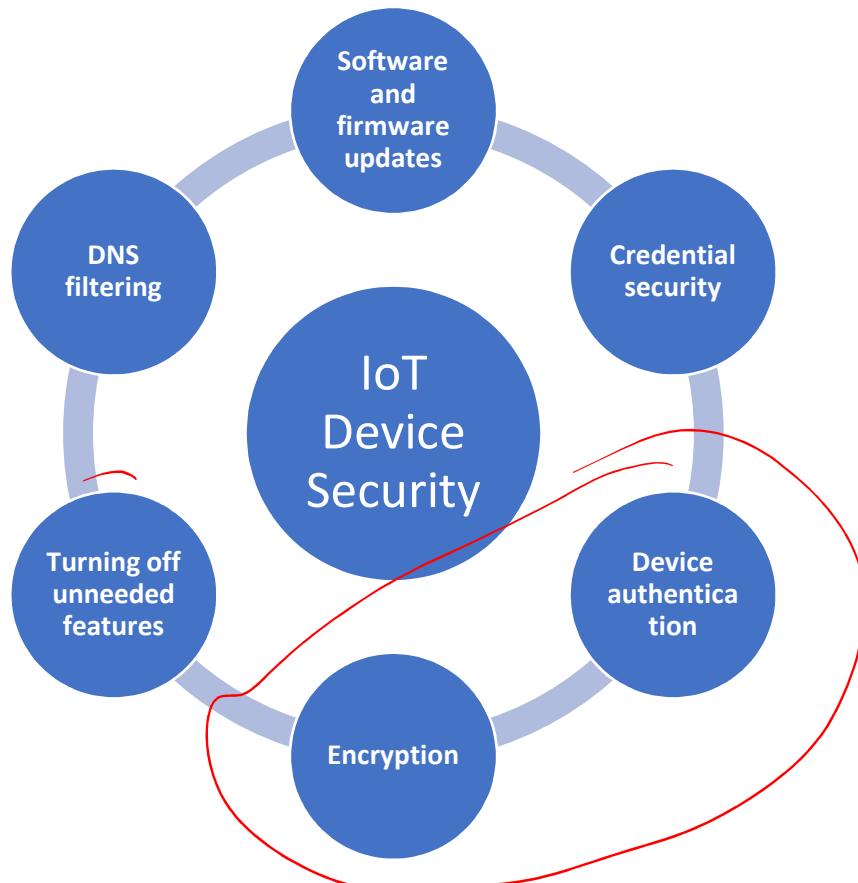


IoT Device Vulnerabilities (3)

- On-path attacks (or Man-in-the-Middle attacks)
 - IoT devices are particularly vulnerable to such attacks because many of them do not encrypt their communications by default
 - On-path attackers position themselves between two parties that trust each other and intercept communications between the two
 - MITM attacks can also happen by Impersonation, where a malicious node sets up two sessions (with device and server), impersonating and relaying messages between them
- Physical hardware-based attacks
 - Many IoT devices, like IoT security cameras, stoplights, and fire alarms, are placed in more or less permanent positions
 - An attacker having physical access to an IoT device's hardware can steal its data or take over the device
 - They could do this by accessing programmatic interfaces left on the circuit board, such as JTAG and RS232 serial connectors
 - Some microcontrollers may have disabled these interfaces, but could still allow direct reads from the attached memory chips if the attacker solders on new connection pins
 - This approach would affect only one device at a time, but a physical attack could have a larger effect if the attacker gains information that enables them to compromise additional devices on the network



Common Measures to overcome Device Vulnerabilities





Device Security (1)

- Software and firmware updates:
 - IoT devices need to be updated for vulnerability patch or software update
- Credential security:
 - IoT device admin credentials should be updated if possible.
 - It is best to avoid reusing credentials across multiple devices and applications — each device should have a unique password
- Device authentication:
 - IoT devices connect to each other, to servers, and to various other networked devices. Every connected device needs to be authenticated to ensure they do not accept inputs or requests from unauthorized parties
- Encryption:
 - Prevents on-path attacks.
 - Encryption must be combined with authentication to prevent MITM attacks. Otherwise, the attacker could set up separate encrypted connections between one IoT device and another, and neither would be aware that their communications are being intercepted.



Device Security (2)

- Turning off unneeded features:
 - Most IoT devices come with multiple features, some of which may go unused by the owner
 - Even when features are not used, they may keep additional ports open on the device
 - The more ports an Internet-connected device leaves open, the greater the attack surface — often attackers simply ping different ports on a device, looking for an opening
 - Turning off unnecessary device features will close these extra ports.
- DNS filtering:
 - DNS filtering is the process of using the Domain Name System to block malicious websites
 - Adding DNS filtering as a security measure to a network with IoT devices prevents those devices from reaching out to places on the Internet they should not (i.e. an attacker's domain)

IoT Security Framework



IoT Security Framework

At the heart of the IoT Security Framework are the following key functions:

- Authentication ✓
- Authorization ✓
- Access Control ✓
- *(Apart from the obvious function – Encryption!)* ✓

We discuss these functions in the following slides.



Authentication

- At the heart of the framework is the authentication layer, used to provide and verify the identity information of an IoT entity
- When connected IoT/ M2M devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device
- The way to store and present identity information may be substantially different for the IoT devices (as against human credentials, like username/password, etc)
 - Device identifiers include RFID, shared secret, X.509 certificates, the MAC address of the endpoint, or some type of immutable hardware based root of trust
 - Establishing identity through X.509 certificates provides a strong authentication system. However, in the IoT domain, many devices may not have enough memory to store a certificate or may not even have the required CPU power to execute the cryptographic operations of validating the X.509 certificates
 - There exists opportunities for further research in defining smaller footprint credential types and less compute-intensive cryptographic constructs and authentication protocols (*aka Lightweight Cryptography*)



Authorization

- The second layer of this framework is authorization that controls a device's access (to network services, back-end services, data etc)
 - This layer builds upon the core authentication layer by leveraging the identity information of an entity
 - With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information
- Trust relationships can sometimes also be formed in absence of Authorization techniques, and is necessary in some conditions
 - E.g in the absence of a common Authentication and Authorization framework
 - Or, for latency sensitive applications, e.g. those built using the distributed M2M or SiOT architectures



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)

IoT Security Framework (Contd.)



Recap: IoT Security Framework

At the heart of the IoT Security Framework are the following key functions:

- Authentication
- Authorization
- Access Control
- *(Apart from the obvious function – Encryption!)*

We discuss these functions in the following slides.



Recap: Authentication

- At the heart of the framework is the authentication layer, used to provide and verify the identity information of an IoT entity
- When connected IoT/ M2M devices (e.g., embedded sensors and actuators or endpoints) need access to the IoT infrastructure, the trust relationship is initiated based on the identity of the device
- The way to store and present identity information may be substantially different for the IoT devices (as against human credentials, like username/password, etc)
 - Device identifiers include RFID, shared secret, X.509 certificates, the MAC address of the endpoint, or some type of immutable hardware based root of trust
 - Establishing identity through X.509 certificates provides a strong authentication system. However, in the IoT domain, many devices may not have enough memory to store a certificate or may not even have the required CPU power to execute the cryptographic operations of validating the X.509 certificates
 - There exists opportunities for further research in defining smaller footprint credential types and less compute-intensive cryptographic constructs and authentication protocols (*aka Lightweight Cryptography*)



Recap: Authorization

- The second layer of this framework is authorization that controls a device's access (to network services, back-end services, data etc)
 - This layer builds upon the core authentication layer by leveraging the identity information of an entity
 - With authentication and authorization components, a trust relationship is established between IoT devices to exchange appropriate information
- Trust relationships can sometimes also be formed in absence of Authorization techniques, and is necessary in some conditions
 - E.g in the absence of a common Authentication and Authorization framework
 - Or, for latency sensitive applications, e.g. those built using the distributed M2M or SIoT architectures



Access Control Types

- Role Based Access Control (or RBAC):
 - Most existing authorization frameworks for computer networks and online services are role based
 - First, the identity of the user is established and then his or her access privileges are determined from the user's role within an organization
 - That applies to most of existing network authorization systems and protocols (RADIUS, LDAP, IPSec, Kerberos, SSH)
 - Rule Based Access Control:
 - An administrator may define rules that govern access to a resource
 - Rules may be based on conditions, such as time of day and location
 - Can work in conjunction with RBAC
-

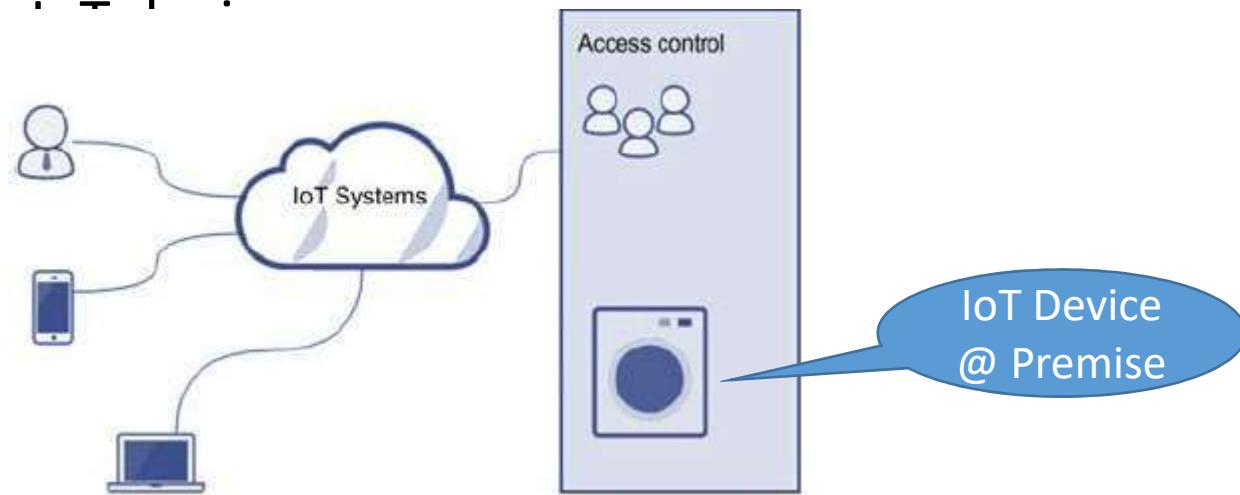


Access Control Types (2)

- Attribute Based Access Control (or ABAC):
 - Attributes (e.g. age, location, etc) are used to allow access
 - Users or devices need to prove their attributes
 - In ABAC, it is not mandatory to verify the identity of the user to establish his or her access privileges, just that the user/device possesses the attributes is sufficient
 - Discretionary access control (or DAC):
 - Owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource
 - Not a good method, since these methods are not centralized and hard to scale
-

ACL-based Systems

- ACL = Access Control List
- A table that can tell the IoT system all access rights each user/ application has to particular IoT end node
 - Most common privileges include the ability to access or control a . . .



Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017

Device

Cloud

~~*Network*~~

~~*Network*~~

Server

Client



Challenge with ACL-based Systems

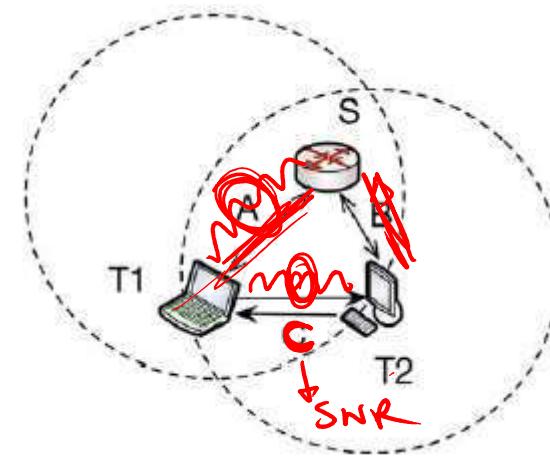
- In many architectures, IoT devices operate as “servers”, with clients connecting to them to fetch collected data
- Server IP and port information is public knowledge => no security
- Minimum security is typically implemented using <username, password> → an embodiment of IoT ACL-based device systems
 - Approach is not scalable as ~~more users join or are revoked~~
 - Complexity of managing the ACL at the device can become a bottle-neck
- A more scalable approach for IoT is to use “capabilities” for enabling “**capability-based access**”
 - A capability is essentially a cryptographic key, that gives access to some ability (e.g. to communicate with the device)

IoT Security: Implementation Methods

Lightweight Cryptography



- Recently, the lightweight cryptography for IoT has attracted lots of research effort
 - The traditional cryptography is designed at the application layer without regard to the limitations of IoT Devices, making it difficult to directly apply the existing cryptography primitives to IoT
- Recently, the idea of designing lower layer security schemes, such as physical layer crypto and lightweight crypto supports the resources (computation, RAM, energy supply, etc.) limited to IoT devices
- The idea of physical layer security scheme and lightweight cryptography over resource-limited IoT devices first appeared in the works of Wyner (1975) and Korner (2002)
 - They investigated a channel model using the “wiretap channel,” in which a transceiver attempts to communicate reliably and securely with a legitimate receiver over a noisy channel, while its messages are being eavesdropped by a passive adversary through another noisy channel



Source: Shancang Li Li Da Xu, Securing the Internet of Things, Syngress, 1st Edition, 2017

Lightweight Cryptography: Some Background

C = B log₂(1/H_{min})
bps



- **Definition:** Information-theoretic Security
 - “A cryptosystem is considered to have information-theoretic security (also called **unconditional security**) if the system is secure against adversaries with unlimited computing resources and time. In contrast, a system which depends on the computational cost of cryptanalysis to be secure (and thus can be broken by an attack with unlimited computation) is called computationally, or conditionally, secure.”
- The concept of information-theoretic secure communication was introduced in 1949 by American mathematician ~~Claude Shannon~~ Claude Shannon, one of the founders of classical information theory
 - In Shannon’s wiretap model, he assumed both the main and eavesdropper’s channels to be noiseless
 - Shannon’s results discouraged further research in information theoretic secrecy
- Wyner revisited this problem with relaxed assumptions, mainly:
 - The noiseless communication assumption of Shannon was relaxed by assuming a possibly noisy main channel and an eavesdropper channel that is a noisy version of the signal received at the legitimate receiver
 - Wyner’s results showed that positive secure rates of communication are achievable, under certain conditions of noise or interference in the channels

Searched Wikipedia



Lightweight Cryptography: Some Background (2)

- Wyner's work is highly applicable to Wireless Channels (most often used for IoT communications)
 - Wireless channels have natural impairments (e.g. attenuation in signal strength) that make the received signal different from the one originally transmitted
 - Secure communication without the need to share a secret key, or what is now called as the **key-less security approach** suggested a new paradigm of secure communication protocols
 - That is, exploiting properties of the wireless medium (noise or interference or jamming) to satisfy the secrecy constraints
- The key-less security approach can be used in wireless networks to securely exchange the shared-secret key between two communicating nodes, which can be used for all subsequent communications
 - Simpler alternative to secure key exchange protocols like the Diffie-Hellman Key Exchange (which is based on Mathematical Principles of Elliptic Curve Cryptography)



Lightweight Cryptographic Algorithms

- Lightweight cryptography is a ~~cryptographic~~ algorithm or protocol tailored for implementation in constrained environments including RFID tags, sensors, contactless smart cards, healthcare devices, and so on.
- Due to IoT push, Lightweight cryptography has gained momentum:
 - The properties of lightweight cryptography have already been discussed in ISO/IEC 29192 in ISO/IEC JTC 1/SC 27
 - ISO/IEC 29192 is a new ~~standardization~~ project of lightweight cryptography, and the project is in process of standardization
 - NIST received 57 submissions to be considered for standardization. After the initial review of the submissions, 56 were selected as Round 1 Candidates
 - Due to the large number of submissions and the short timeline of the NIST lightweight cryptography standardization process, some of the candidates were eliminated from consideration early in the first evaluation phase in order to focus analysis on the more promising ones
 - Out of 56 Round 1 candidates, 32 were selected to go for Round 2 evaluation
 - On March 29, 2021, NIST announced ten finalists as ASCON, Elephant, GIFT-COFB, Grain128-AEAD, ISAP, Photon-Beetle, Romulus, ~~Sparkle~~, TinyJambu, and Xoodyak
 - The final round of the standardization process was expected to last approximately 12 months. NIST will host a workshop near the end of the evaluation period



Transport Encryption

- SSL/TLS, DTLS (Chapter 4)
- The transport encryption is done using secure transport protocols such as TLS and SSL
 - Both the TLS and SSL are cryptographic protocols that provide communications security over a network
 - TLS uses TCP and therefore does not encounter packet reordering and packet loss issues
- Datagram Transport Layer Security (DTLS):
 - DTLS is developed based on TLS by providing equivalent security services, such as confidentiality, authentication, and integrity protection
 - In DTLS, a handshake mechanism is designed to deal with the packet loss, reordering, and retransmission
 - DTLS provides three types of authentication:
 - non-authentication, server authentication, and server and client authentication



mutual TLS (mTLS)

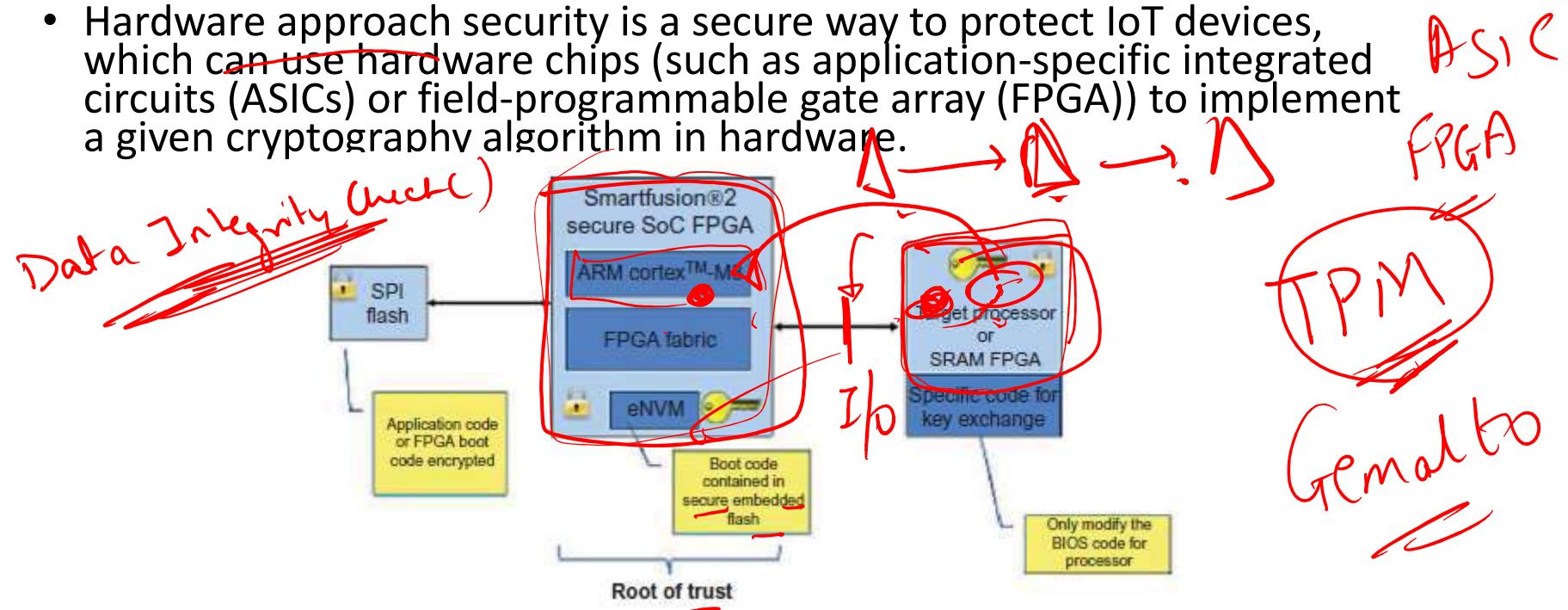
Mutual Auth



- Mutual Transport Layer Security (mTLS) is a type of mutual authentication, which is when both sides of a network connection authenticate each other.
 - TLS is a protocol for verifying the server in a client-server connection;
 - mTLS verifies both connected devices, instead of just one.
- mTLS is important for IoT security because it ensures only legitimate devices and servers can send commands or request data.
 - It also encrypts all communications over the network so that attackers cannot intercept them.
- mTLS requires issuing ~~TLS certificates~~ to all authenticated devices and servers.
 - A TLS certificate contains the device's public key and information about who issued the certificate.
 - Showing a TLS certificate to initiate a network connection can be compared to a person showing their ID card to prove their identity.

Hardware Security Solutions

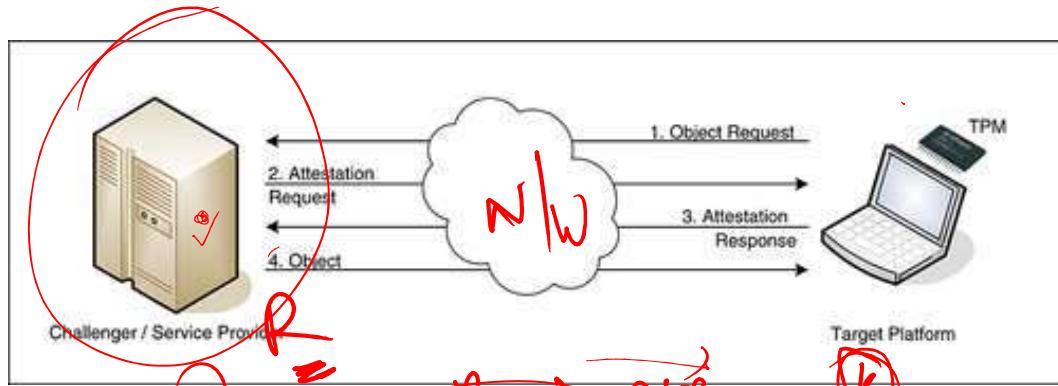
- Hardware approach security is a secure way to protect IoT devices, which can use hardware chips (such as application-specific integrated circuits (ASICs) or field-programmable gate array (FPGA)) to implement a given cryptography algorithm in hardware.



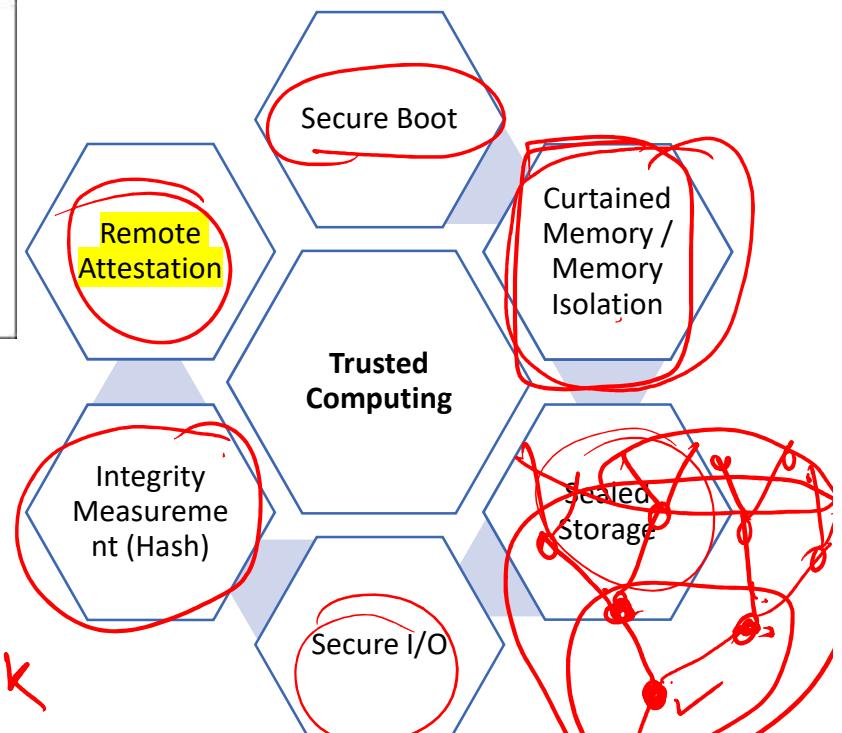
Secure boot: It is a process involving cryptography that allows an electronic device to start executing authenticated and trusted software to operate. It is the foundation of trust but the nodes still need protection from various run-time threats.



Device Attestation Techniques



- Attestation techniques
- HW-based Solution (TPM)
 - SW-based Solution (e.g. PIONEER, 2005)
 - Hybrid Solution (e.g. SMART - Secure & Minimal Architecture for Remote Trust)
 - Swarm Attestation (e.g. SEDA, SANA...)





Security Analytics

- This method can be used for detection of compromised devices
- A security analytics infrastructure can significantly reduce vulnerabilities and security issues related to the Internet of Things
 - This requires collecting, compiling, and analyzing data from multiple IoT sources, combining it with threat intelligence, and sending it to the security operations center (SOC)
 - Applies AI/ML practices to IoT Security
- Extra Reading:
 - An analytics framework to detect compromised IoT devices using mobility behavior: DOI: 10.1109/ICTC.2013.6675302

Use of Raw Public Keys (RPKs)

- In resource-constrained IoT devices, such as intelligent sensors or RFID tag, the certificate chains or even single certificate may be too big to process
- Recently, IETF recommended the use of RPKs instead of certificates for TLS and DTLS
 - IETF RFC 7250 [*Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*]
- Traditionally, TLS client and server public keys are obtained in PKIX containers **in-band** as part of the TLS handshake procedure and are validated using trust anchors based on a [PKIX] certification authority (CA)
 - TLS is, however, also commonly used with self-signed certificates in smaller deployments where the self-signed certificates are distributed to all involved protocol endpoints out-of-band.
 - This practice does, however, still require the overhead of the certificate generation even though none of the information found in the certificate is actually used



Use of Raw Public Keys (RPKs) [2]

- Alternative methods are available that allow a TLS client/server to obtain the TLS server/client public key:
 - The TLS client can obtain the TLS server public key from a DNSSEC-secured resource record using DNS-Based Authentication of Named Entities (DANE) [RFC6698]
 - The TLS client or server public key is obtained from a [PKIX] certificate chain from a Lightweight Directory Access Protocol [LDAP] server or web page.
 - The TLS client and server public key is provisioned into the operating system firmware image and updated via software updates.
 - With raw public keys, only a subset of the information found in typical certificates is utilized: namely, the *SubjectPublicKeyInfo* structure of a PKIX certificate that carries the parameters necessary to describe the public key
 - Public-Key Information of a certificate carries the public key values and the algorithm identifier of the cryptographic algorithm used to generate it. Other parameters found in PKIX certificates are omitted
 - This results in the raw public key being fairly small in comparison to the original certificate, and the code to process the keys can be simpler
 - Only a minimalistic ASN.1 parser is needed; code for certificate path validation and other PKIX-related processing is not required
 - The RPK requires the out-of-band validation of the public key
 - The mechanism defined in the RFC only provides authentication when an out-of-band mechanism is also used to bind the public key to the entity presenting the key
-



BITS Pilani

Pilani Campus

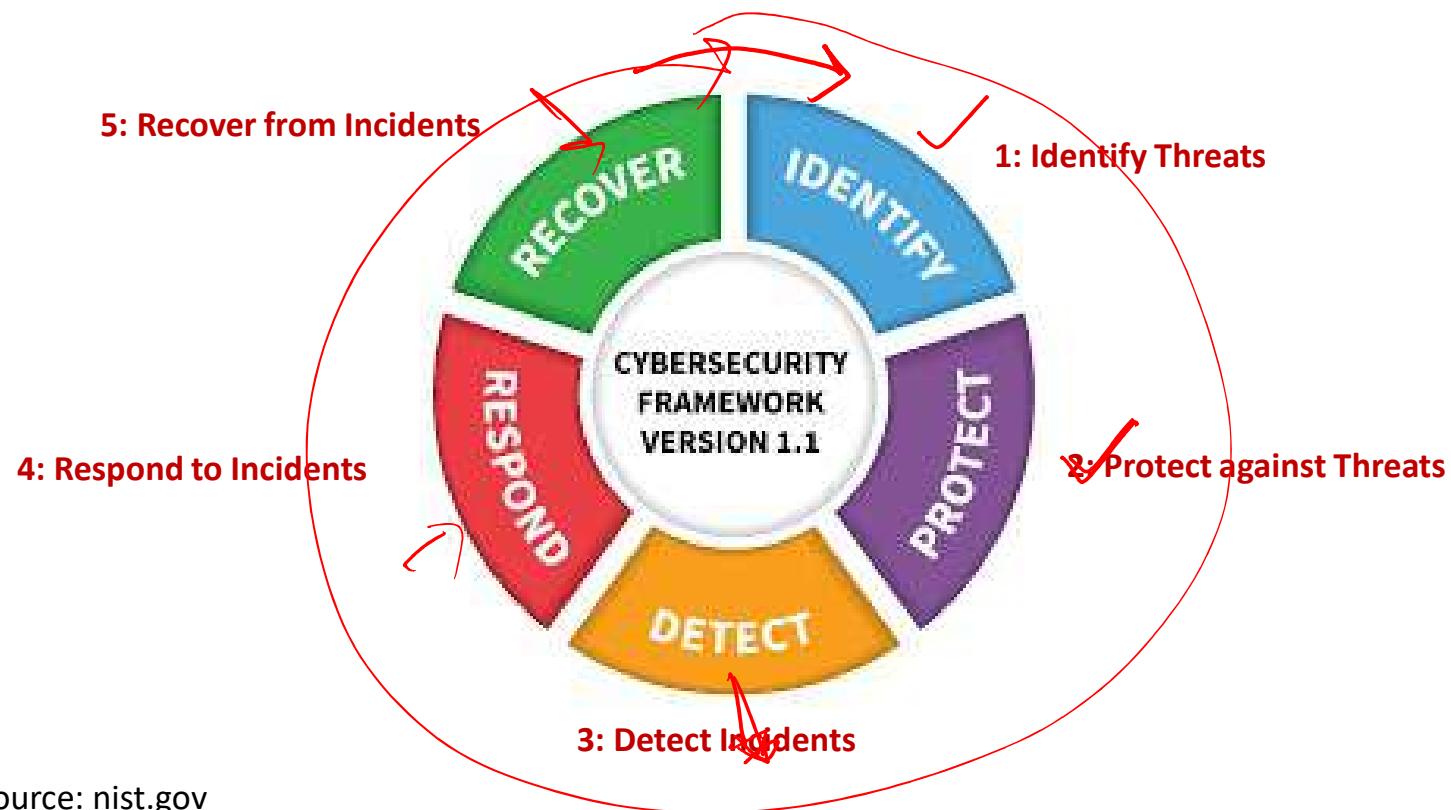


IoT Security

Sub-Topic: IoT Forensics



Cybersecurity: NIST Framework



Source: nist.gov



What is Cyber Forensics....

- “.... is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.”

Source: What is Computer Forensics (Cyber Forensics)?
<https://searchsecurity.techtarget.com> ›



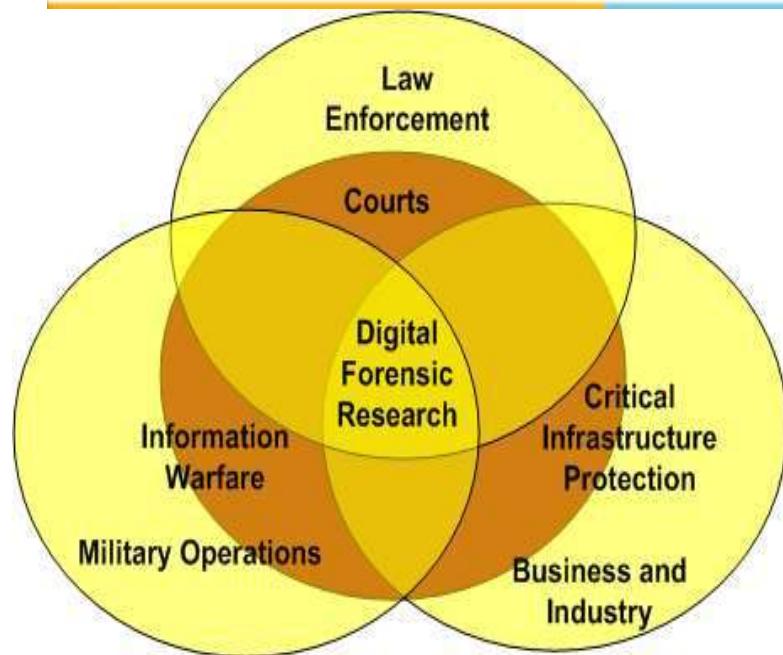
Definition: Digital Forensic Science (DFS)

“The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.”

Source: (2001). Digital Forensic Research Workshop (DFRWS)



Digital Forensic Science



[Source: Cyber Forensics by Eric Katz](#)

Table 1 - Suitability Guidelines for Digital Forensic Research

Area	Primary Objective	Secondary Objective	Environment
Law Enforcement	Prosecution		After the fact
Military IW Operations	Continuity of Operations	Prosecution	Real Time
Business & Industry	Availability of Service	Prosecution	Real Time

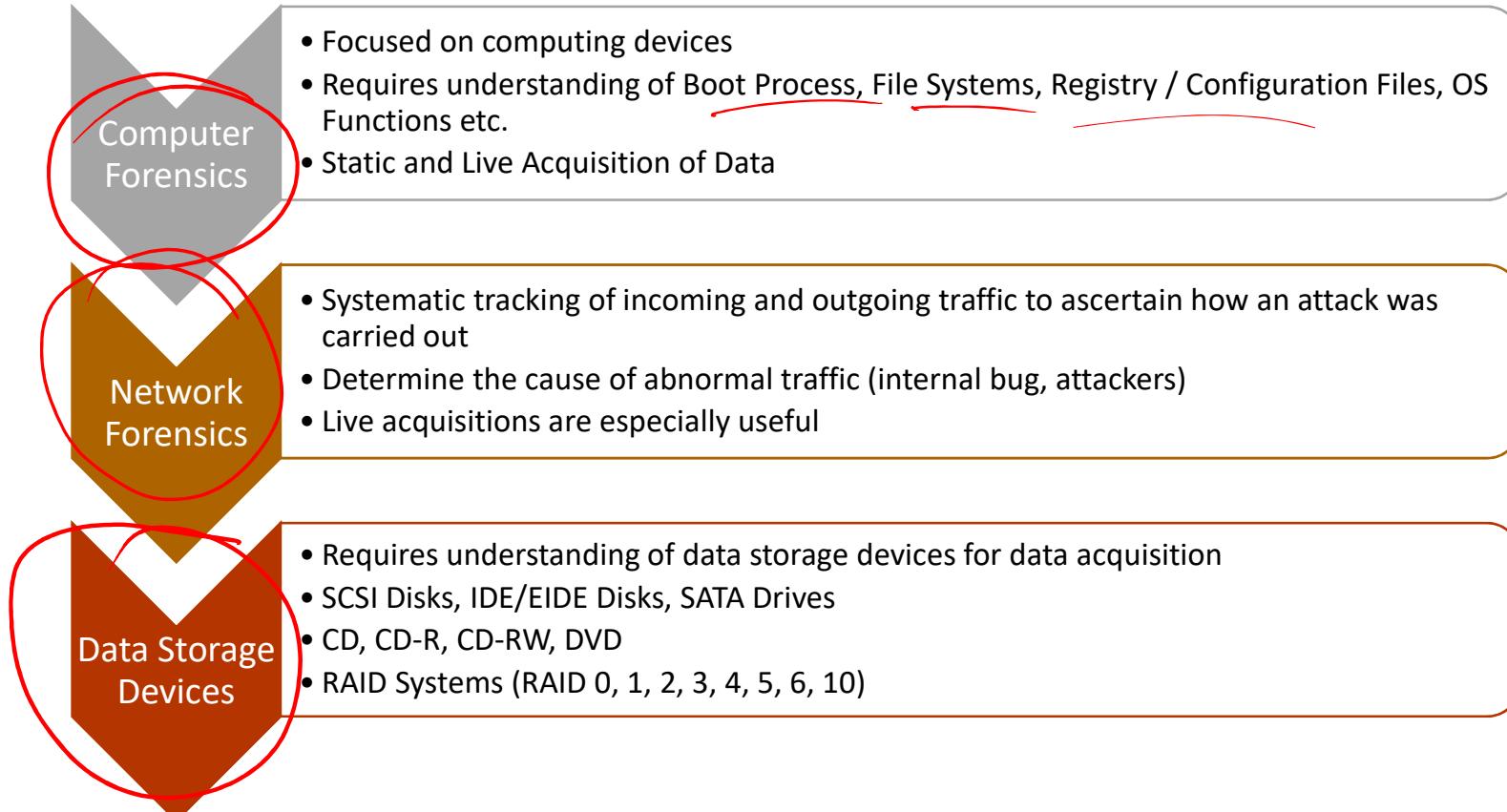


Digital Forensics Process





History of Cyber Forensics

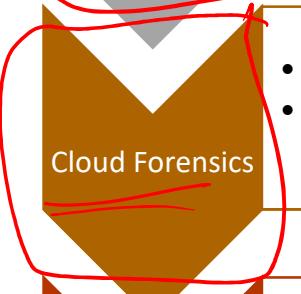




Evolution of Cyber Forensics



- A wealth of information on cell phones/ Smart Phones
- Crimes targeting Mobile Devices
- Requires understanding of Mobile Device Organization, OS, File System and Storage system



- Combines cloud computing with digital forensics
- Requires investigators to work with multiple computing assets, such as virtual and physical servers, networks, storage devices, applications, and much more



- IoT is a combination of many technology zones: Device, Network and Cloud
- IoT Forensics thus covers: Cloud forensics, Network forensics and Device forensics.
- Evidence could be from home appliances, cars, tags readers, sensor nodes, medical implants in humans or animals, or other IoT devices

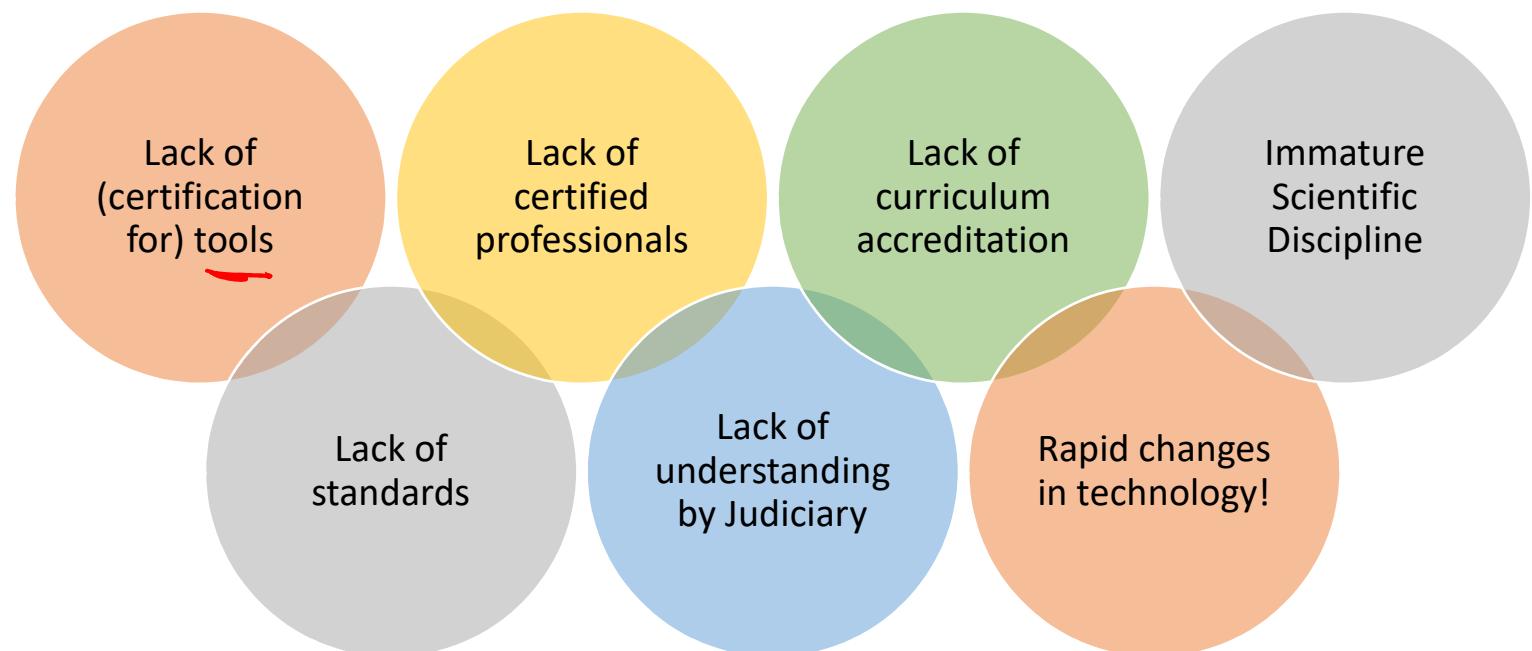


Introduction to IoT Forensics

- Growth in IoT raises challenges for the digital investigator when IoT devices involve in criminal scenes
- Current research in the literature focuses on security and privacy for IoT environments rather than methods or techniques of forensic acquisition and analysis for IoT devices
- Cybercrimes with the power of IoT technology can cross the virtual space to threaten human life and the increasing number of these crimes is one of the main reasons why we need IoT forensics
- IoT digital evidence is a rich and often unexplored source of information
- From the forensic perspective, each IoT device will provide important artifacts that could help in the investigation process



IoT Forensics: Issues





Devices Identification: A Complex Task with IoT!



[Source: Cyber Forensics by Eric Katz](#)



Traditional Forensics Vs IoT Forensics

There are several aspects of differences and similarity between traditional and IoT forensics

- In terms of evidence sources, traditional evidence could be computers, mobile devices, servers or gateways. In IoT forensics, the evidence could be home appliances, cars, tags readers, sensor nodes, medical implants in humans or animals, or other IoT devices.
- In terms of Jurisdiction and Ownership, there are no differences, it could be individuals, groups, companies, governments, etc.
- In terms of evidences data types, IoT data type could be any possible format, it could be a proprietary format for a particular vendor. However, in traditional forensics, data types are mostly electronic documents or standard file formats.
- In terms of networks, the network boundaries are not as clear as the traditional networks, increasing in the blurry boundary lines.



IoT Forensics

- IoT technology is a combination of many technology zones: IoT zone, Network zone and Cloud zone.
- These zones can be the source of IoT Digital Evidences
- Evidence can be collected from a smart IoT device or a sensor, from an internal network such as a firewall or a router, or from outside networks such as Cloud or an application.
- Based on these zones, IoT Forensics covers three aspects in term of forensics: Cloud forensics, network forensics and device level forensics.
 - Most of IoT devices have the ability to (directly or indirectly) connect through applications to share their resources in the Cloud, with all valuable data that is stored in the Cloud → Cloud Forensics.
 - Different kinds of networks that IoT devices use to send and receive data. It could be home networks, industrial networks, LANs, MANs and WANs. For instance, if an incident occurs in IoT devices, all logs from network devices through which the traffic flows could be potential evidence
 - Device Level Forensics include all potential digital evidence that can be collected from IoT devices like graphics, audio, video. Videos and graphics from CCTV camera or audios from Amazon Echo, can be great examples of digital evidences in the device level forensics.



Challenges in IoT Forensics

- **Data Location:**
 - Most of the IoT data is spread in different locations, which are out of the user control. This data could be in the Cloud, in third party's location, in mobile phone or other devices.
 - To identify the location of evidence is considered as one of the biggest challenges an investigator can face in order to collect the evidence.
 - In addition, IoT data might be located in different countries and be mixed with other users information, which means different countries regulations are involved
- **Lifespan limitation of Digital Media Storage:**
 - Because of limited storage in IoT devices, the lifespan of data in IoT devices is short and data can be easily overwritten, resulting in the possibility of evidence being lost
 - Therefore, one of the challenges is the period of survival of the evidence in IoT devices before it is overwritten.
 - Transferring the data to a local Hub or to the Cloud could be an easy solution to solve this challenge. However, it presents challenges related to securing the chain of evidence and to prove the evidence has not been changed or modified
- **Lack of Individual Identity:**
 - Even though the investigators find an evidence in the Cloud that prove a particular IoT device in crime scene is the cause of the crime, it does not mean this evidence could lead to identification of the criminal



Challenges in IoT Forensics (Contd.)

- Lack of Security:
 - Evidence in IoT devices could be changed or deleted because of lack of security, which could make these evidence not solid enough to be accepted in a court of law
- Variety of Device Types:
 - In identification phase of forensics, the digital investigator needs to identify and acquire the evidence from a digital crime scene.
 - Usually, evidence source is types of a computing system such as computer and/or a mobile phone.
 - However, in IoT, the source of evidence could be objects like a smart refrigerator or smart coffee maker
 - The device could be turned-off because it could have run out of battery, which makes its chances to be found difficult, especially if the IoT devices is very small, in hidden places or looks like a traditional device.
 - Carrying the device to the lab and finding a space could be another challenge that investigators face
 - Extracting evidence from these devices is considered another challenge as most of the manufacturers adopt different platforms, operating systems and hardware.
- Lifecycle Changes in Data Formats:
 - The format of the data that is generated by IoT devices is not identical to what is saved in the Cloud.
 - Data processing using analytic and translation functions in different places is likely before being stored in the Cloud. Hence, in order to be accepted in a court of law, the data form should be returned to its original format before performing analysis



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



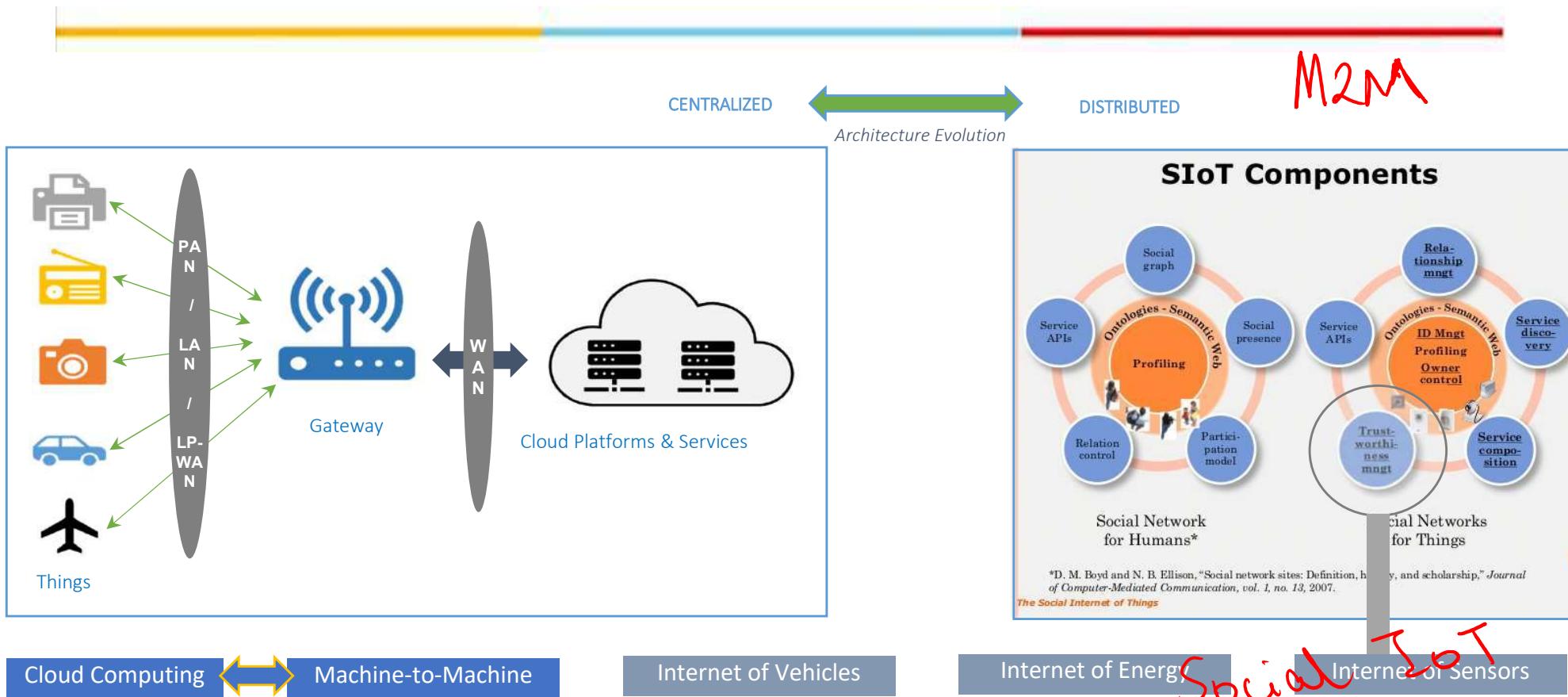
<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 10: IoT Security

Social IoT and Trust Management



RECAP: IoT Architectures – The Evolving Landscape!

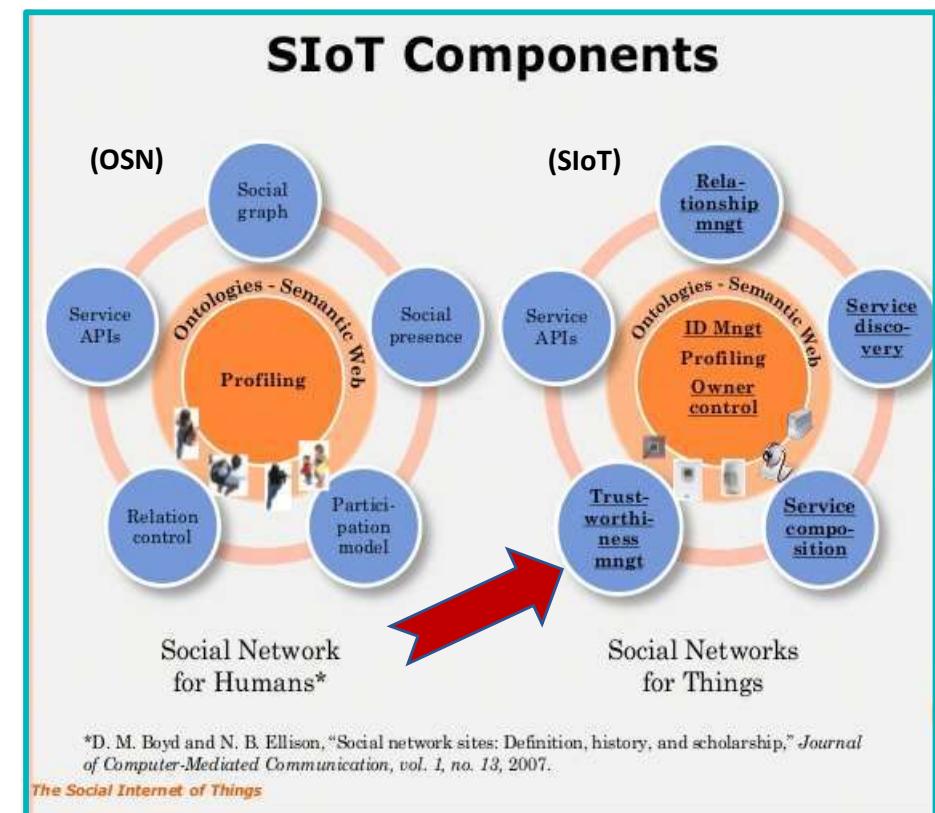


- “The way to **secure the Internet of Things** is to allow the self-organizing migration of services away from a central cloud alone and into local infrastructure ecosystems where they can act independently” - <https://www.scmagazineuk.com/doriot-project-secure-internet-things/article/1590701>



What is Social IoT?

- Social IoT (SIoT)
 - An SIoT Network is to IoT Devices what a Social Network (SN) is to Humans
 - Enables collaborative computing as against centralized / stand-alone computing
- Human Social Networks
 - Physical-world collaborative networks (e.g. @workplace, @community,)
 - Online Social Networks (OSNs), like Facebook, Twitter, ...





Big Picture: *Trust* in Online Social Networks (OSNs)



Alice

Can Alice Trust Bob?

Target → Bob
Topic → Service offered by Bob

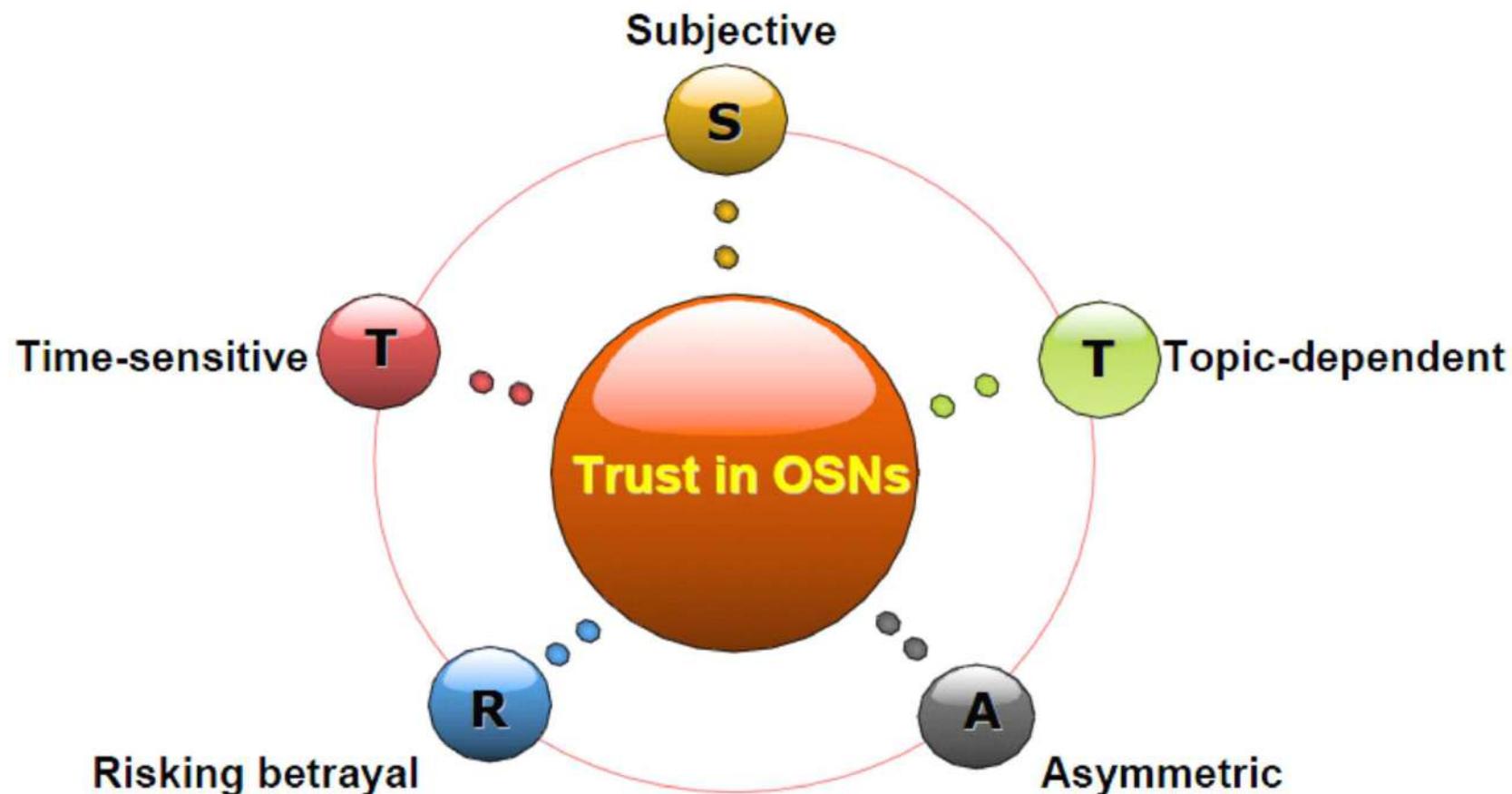


Bob





Properties of Trust: START Properties

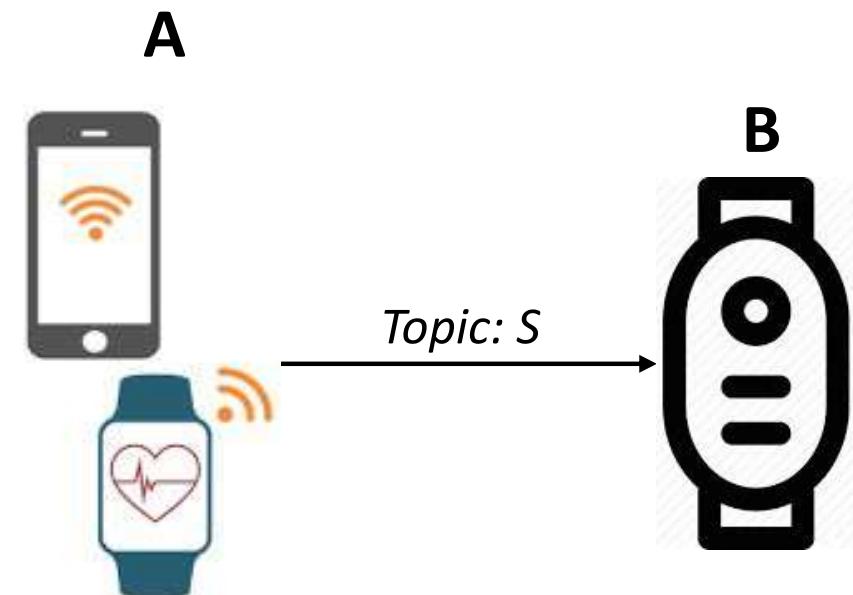


Source: Jiang Wenjun, Hunan University
(Presented in WTC workshop in CSU, 2015)



Trust in Social IoT Service Networks

- Similarities to OSN Problem:
 - Same Question → *how can a node trust another node in a social network?*
 - Similar properties → *START properties of Trust*
- Challenges:
 - Heterogeneous network
 - Multi-vendor
 - Multi-device types
 - Resource considerations
 - Storage
 - Compute
 - Variety of Attacks
 - on-off attack, ballot stuffing attack, bad-mouthing attack, sybil attacks



Can device 'A' Trust device 'B' for Service 'S'?



Big Picture: Relevance of *Trust* in any Social or Service Network?

Trust is the basis of all interactions

Heuristics

Influence is a tool that triggers **Trust**

Recommendation is a method for propagation of **Influence**

For many SIoT systems, a reasonable estimate of the tie-strength, based on some (semi-) static network properties may be a sufficiently accurate measure of Trust.

In OSNs:

- Interaction-based Methods for Tie-strength Measurement
 - “**Trust** is the basis of all Interactions”
 - More interactions => higher Trust
- **Advantages:** Higher-accuracy; Dynamic updation
- **Disadvantages:** High-volume traffic analysis; Impacted by changes in interaction patterns

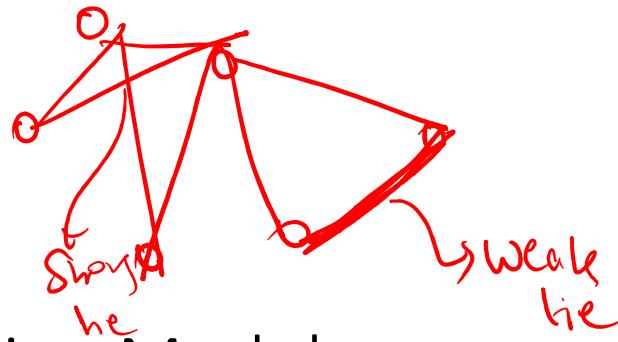
In Service Networks:

- Recommendation-based Methods for Service Provider Ranking
 - “**Recommendation** is a method for propagation of **Influence**.”; “**Influence** is a tool that triggers **Trust**”
 - Higher rating/ better reviews => higher ranking of Service Provider
- **Advantages:** Higher-accuracy
- **Disadvantages:** Generates higher traffic volume; requires higher processing



Existing Approaches to SIoT Trust Management

- The topic of trust modelling, trust mining and tie strength measurement in online social networks (OSNs) is a vast and well-researched area
- Similarly, service-based networks have their trust models, including models for e-commerce platforms and P2P service networks
- In the last decade, IoT networks have seen similar research in trust modelling
- In general, SIoT trust models have immensely borrowed ideas from online social network (OSN) trust models due to the social nature of the nodes in either kind of networks



A Classification of Existing Models

Elghomary et al.* classify trust models into one of the three types:

Graph-based models

- Use (semi-)static graph structure (or network tie information) to deduce trustworthiness

Dynamic interaction-based models

- Use inter-node interactions to estimate the strength of each social tie

Hybrid models

- Try to balance the benefits and shortcomings of more than one method for trust management

Narang et al. ** propose the following alternate classification method:

Ratings-based models

- Trust evaluation using a system of ratings. Ratings given to individual transactions lead to node-level ratings

Opinion-based models

- Use a combination of *direct opinion* (i.e. self-opinion) and *indirect opinions* (i.e. opinions of other nodes) to calculate the overall trustworthiness

Cross-Integrated models

- Trust relationships gathered from one kind of social or service network and applied to other systems

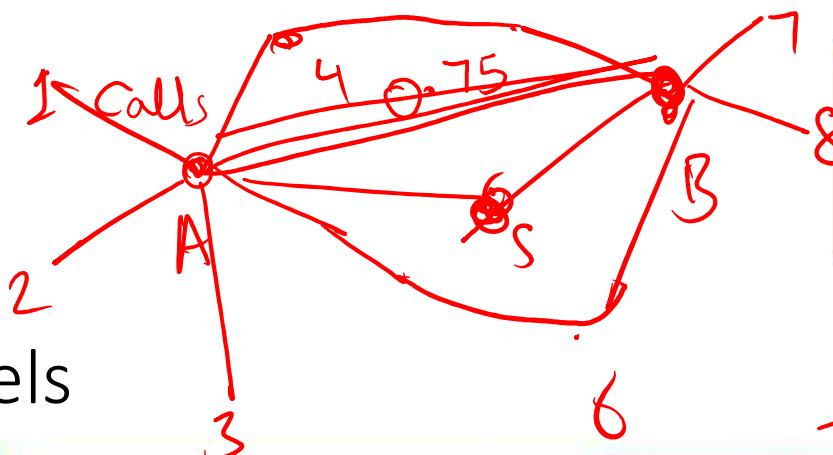
[*] K. Elghomary, D. Bouzidi, and N. Daoudi, "A Comparative Analysis of OSN and IoT Trust Models for a trust model adapted to MOOCs platforms," in *Proceedings of the 2nd International Conference on Networking, Information Systems & Security*, New York, NY, USA, Mar. 2019, pp. 1–8. doi: 10/gjkw2k.

** "A hybrid trust management framework for a multi-service social IoT network", Elsevier Computer Communications Vol 171 (2021), Pages 61-79 (DOI: <https://doi.org/10.1016/j.comcom.2021.02.015>)



$$0 \rightarrow 1$$

Graph-based Models

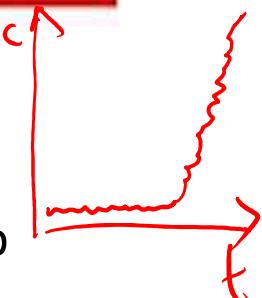


$$\frac{A \cap B}{A \cup B} = \frac{\alpha \beta}{8}$$

- Work by American Sociologist Mark Granovetter
 - *The Strength of Weak Ties* (1973)
 - ✓ Described how the degree of overlap between two individual's friendship network varies directly with the strength of their social tie
 - ✓ Described the strength of the Weak Ties in connecting disparate network components
- Work by Onella et al. extending the work by Granovetter
 - Studied structure and tie strengths in mobile communication networks
 - CDRs from mobile communication networks were used to quantify the measure of interaction between humans, which was used as a measure of tie strength between the people involved in the calls
 - Showed a direct correlation between neighbourhood overlap and tie strengths



Granovetter
(1973)



Onella (2007)

$$V \propto D^{\alpha}$$



Interaction-based Models

- X. Li, H. Fang, Q. Yang, and J. Zhang, “Who is Your Best Friend? Ranking Social Network Friends According to Trust Relationship,” in *Proceedings of the 26th Conference on User Modeling, Adaptation and Personalization*, New York, NY, USA, Jul. 2018, pp. 301–309. doi: 10/gfrfds.
 - In OSNs e.g. Facebook, the relationship between users is binary, i.e., either friend (trust) or stranger (distrust)
 - However, in real-world life, people always have different trust relationships with others (e.g., best friend, acquaintance, frenemy)
 - For various applications such as social recommendation and semantic web, it is more worthwhile to know the trust strength between users
 - In this work, a unique dataset obtained from a Facebook is studied to map trust values with users' online interactions, and thus build personalized trust models



Ratings-based Models

- Frequently used with E-commerce Service Networks
- E-commerce systems have introduced trust management mechanisms that offer valuable information to customers
 - depict the trust level of sellers for forthcoming transactions
- Sample Read:
 - Y. Wang and K.-J. Lin, “Reputation-Oriented Trustworthy Computing in E-Commerce Environments,” *IEEE Internet Comput.*, vol. 12, no. 4, pp. 55–59, Jul. 2008, doi: 10/cbqb3d.



Opinion-based Models

- Use of opinions instead of ratings
- Opinions are consolidated-views based on past transactions
- Direct and Indirect Opinions
- Sample Read:
 - E. Kokoris-Kogias, O. Voutyras, and T. Varvarigou, "TRM-SIoT: A scalable hybrid trust & reputation model for the social Internet of Things," in *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)*, Berlin, Germany, Sep. 2016, pp. 1–9. doi: 10.1109/ETFA.2016.7733612.

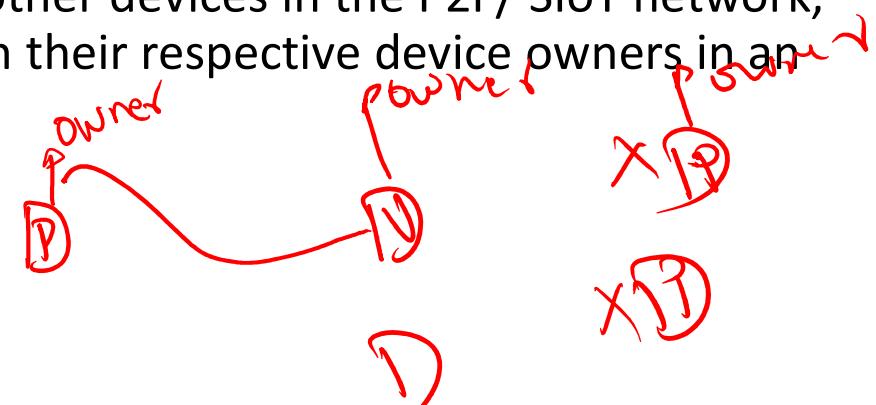
Parameter/Feature/Function	TRM-SIoT
Trust Model Categorization	Opinion-based model
Information Sources for Trust Model	SIoT device opinions
Direct Opinion Computation Method	Weighted average of past service transactions, based on QoS and criticality of transaction.
Service Provider Prioritization Method	Weighted average of indirect opinions from few credible nodes. The weights for weighted average being the Trust of a node on the recommender node.
Indirect Opinion Distribution Method	Nodes continuously poll indirect opinions from neighbourhood nodes.
Frequency of Indirect Opinion Distribution	Once when creating a new social tie with a node, but not updated regularly.
Malicious node identification for Indirect Opinions	Use of statistical methods (mean and standard deviation) to identify nodes whose opinions fall outside the opinion range of few credible nodes.
Centralized/Distributed Computation	Distributed only, since each node has its own set of credible nodes that keeps changing. This results in node-specific provider assessments.

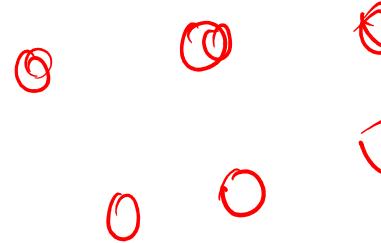


Cross-Integrated Models

- P. Deshpande, P. A. Kodeswaran, N. Banerjee, A. A. Nanavati, D. Chhabra, and S. Kapoor, “M4M: A model for enabling social network based sharing in the Internet of Things,” in *2015 7th International Conference on Communication Systems and Networks (COMSNETS)*, Jan. 2015, pp. 1–8. doi: [10.1109/COMSNETS.2015.7098685](https://doi.org/10.1109/COMSNETS.2015.7098685).

- Propose using information about device owner ties from online social networks (like Facebook, Twitter, etc.) to identify trustworthy links between M2M or SIoT devices.
- An IoT device can offer its services to other devices in the P2P/ SIoT network, provided an association exists between their respective device owners in an online social network





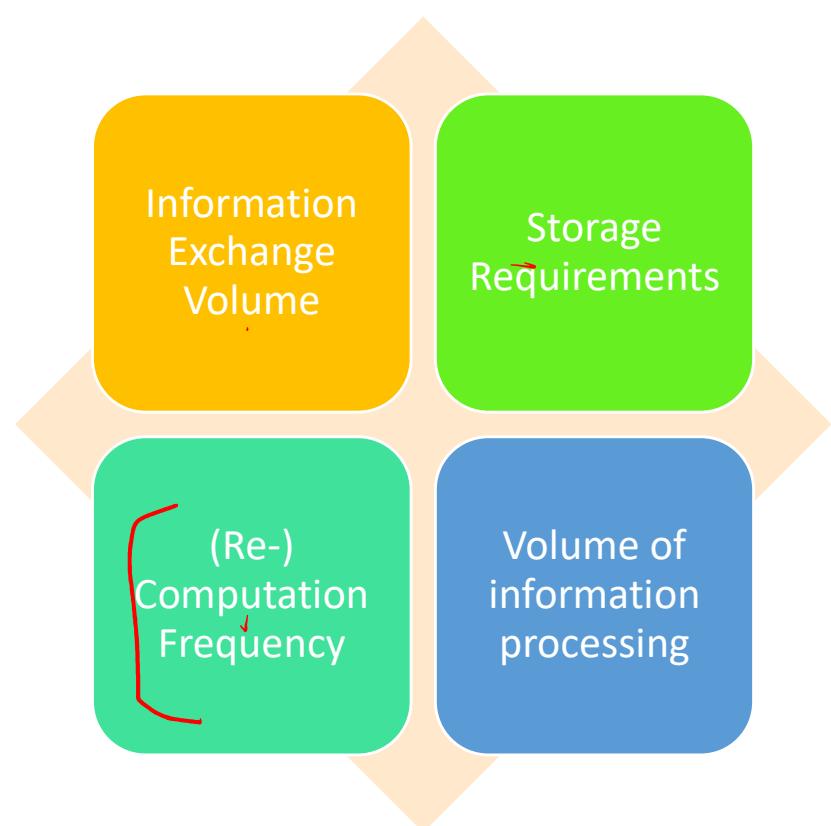
Relationship-based Model

- Atzori, L., Iera, A., Morabito, G., Nitti, M., 2012. The social internet of things (SIoT) when social networks meet the internet of things: concept, architecture and network characterization. *Comput. Networks* 56 (16), 3594–3608.
 - same idea as behind the approaches involving the use of swarm intelligence and swarm robotics
 - groups of objects, which will cooperate in order to reach the overall interest of providing services to users
 - Relies upon basic kinds of relationships such as the parental object relationship (POR), which is established among objects belonging to the same production batch, or the ownership object relationship (OOR), which is based on heterogeneous objects belonging to the same user (e.g., mobile phones, game consoles, etc.).
 - Other relationships defined include: Co-location Object Relationship and Co-work Object Relationship
 - Mathematical quantification of trustworthiness based on relationship weights



Relevance of Existing Techniques for SIoT

Following parameters are important to understand relevance of existing models for SIoT networks:



1. The amount of information dissemination required over the SIoT network
2. The volume of storage needed at IoT devices
3. The frequency of computations performed at each IoT device and
4. The amount of information processing required for each computational leg or run of the trust model



Limitations of Existing Techniques

Ratings-based Models

- Distribution of rating of every service transaction in the network leads to a high-volume information broadcast
- High consequent storage requirement in the system
- Frequent re-assessment of Trust due to frequent changes in distributed ratings

Opinion-based Models

- Frequent re-assessment of *Trust* due to frequent changes in both the direct and indirect opinions
- Too many configurable parameters - computation of opinions requires a considerable tuning of parameters to get the correct effect

Cross-Integrated Models

- Limited or no role for IoT nodes in making trust-decisions and creating social ties
- Lack of co-relation across the two systems
- Data Privacy challenges in using OSN data



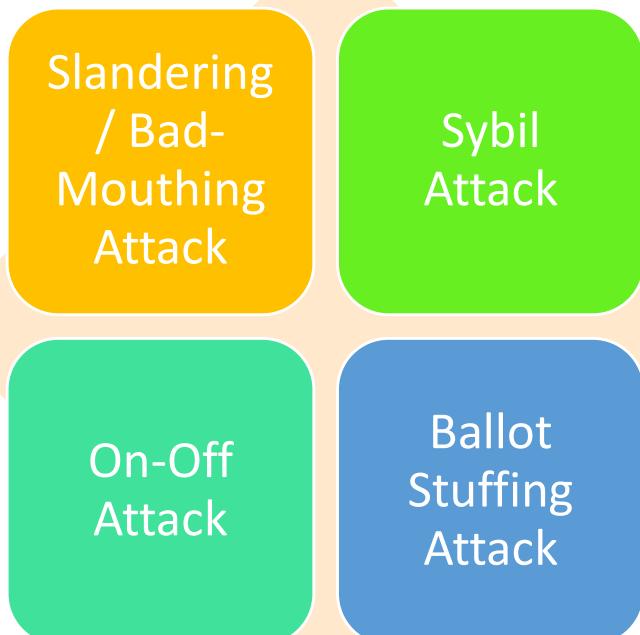
New Trust Models for SIoT

- Is an area of active research!
- Trust models that can be fit across heterogeneous devices, multi-service networks are required
- Trust models are themselves insecure and can be under a variety of attacks from malicious nodes in the network → need to address those issues.



Attack Scenarios for SIoT Trust Models

At the least, following attack scenarios must be considered in designing SIoT Trust Models



1. A **slander** (or bad-mouthing) attack can be launched by a malicious user by sharing a low rating (or opinion) of the node under attack
2. In a **Sybil attack**, a single malicious node makes multiple different identities of itself to trigger a more meaningful attack
3. In an **On-Off attack**, a malicious node behaves opportunistically by switching between trustworthy and untrustworthy behaviour
4. In a **ballot stuffing attack**, a colluding group of nodes promote a single node (or service-provider device), thereby unfairly increasing the node's ratings



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 11: Cloud Security

An Overview to Cloud Computing

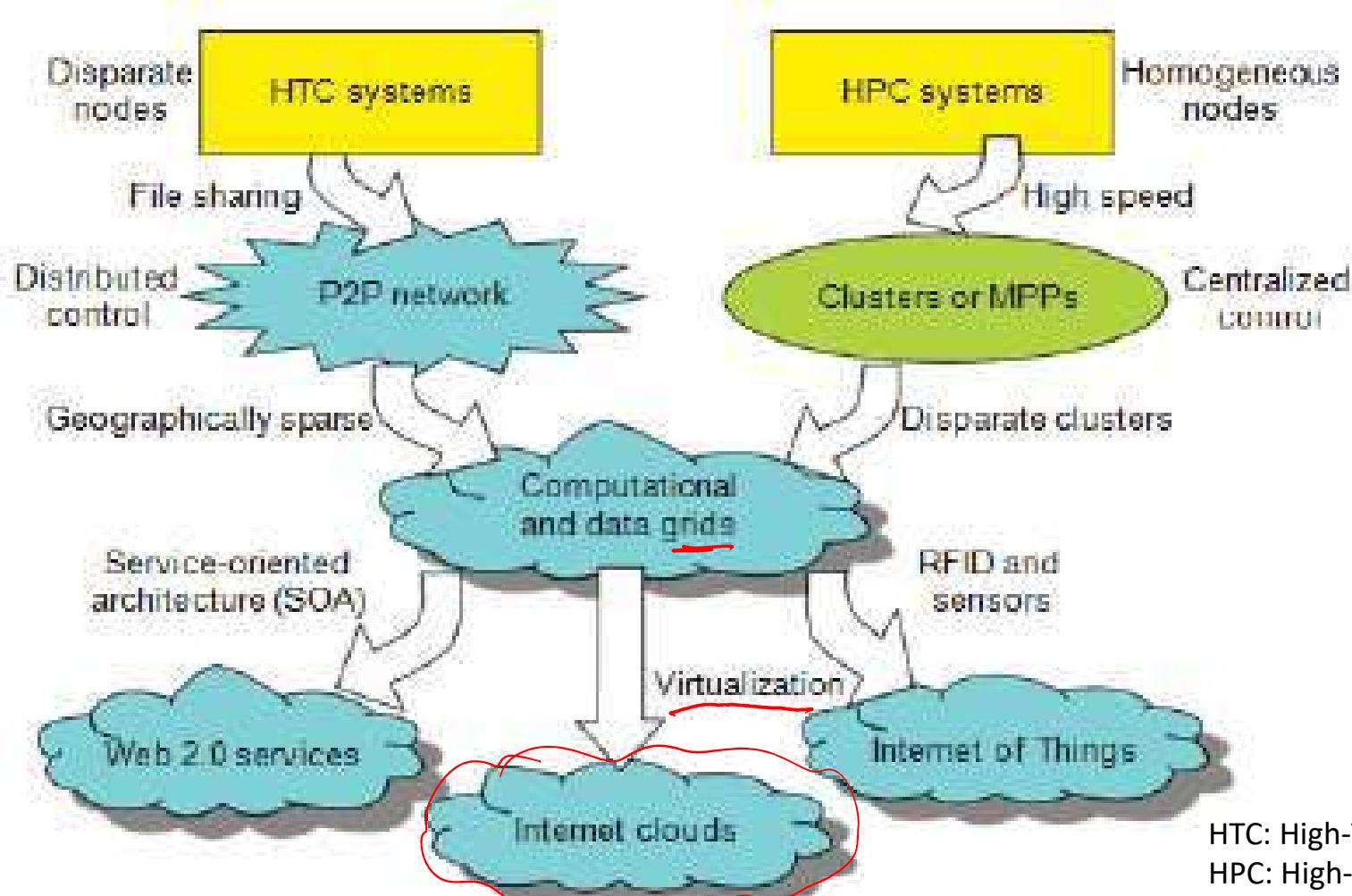
Source Disclaimer: Content for some of the slides is from the course Textbook(s). Refer Course Handout for list of Textbooks.



Definition

- What is Cloud Computing?
 - NIST Special Publication 800-145 (“The NIST Definition of Cloud Computing”) offers the following definition of the term “Cloud Computing”:
 - *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*
 - The NIST publication describes the cloud model as something that is composed of five essential characteristics, three service models, and four deployment models

Evolution of Cloud Computing



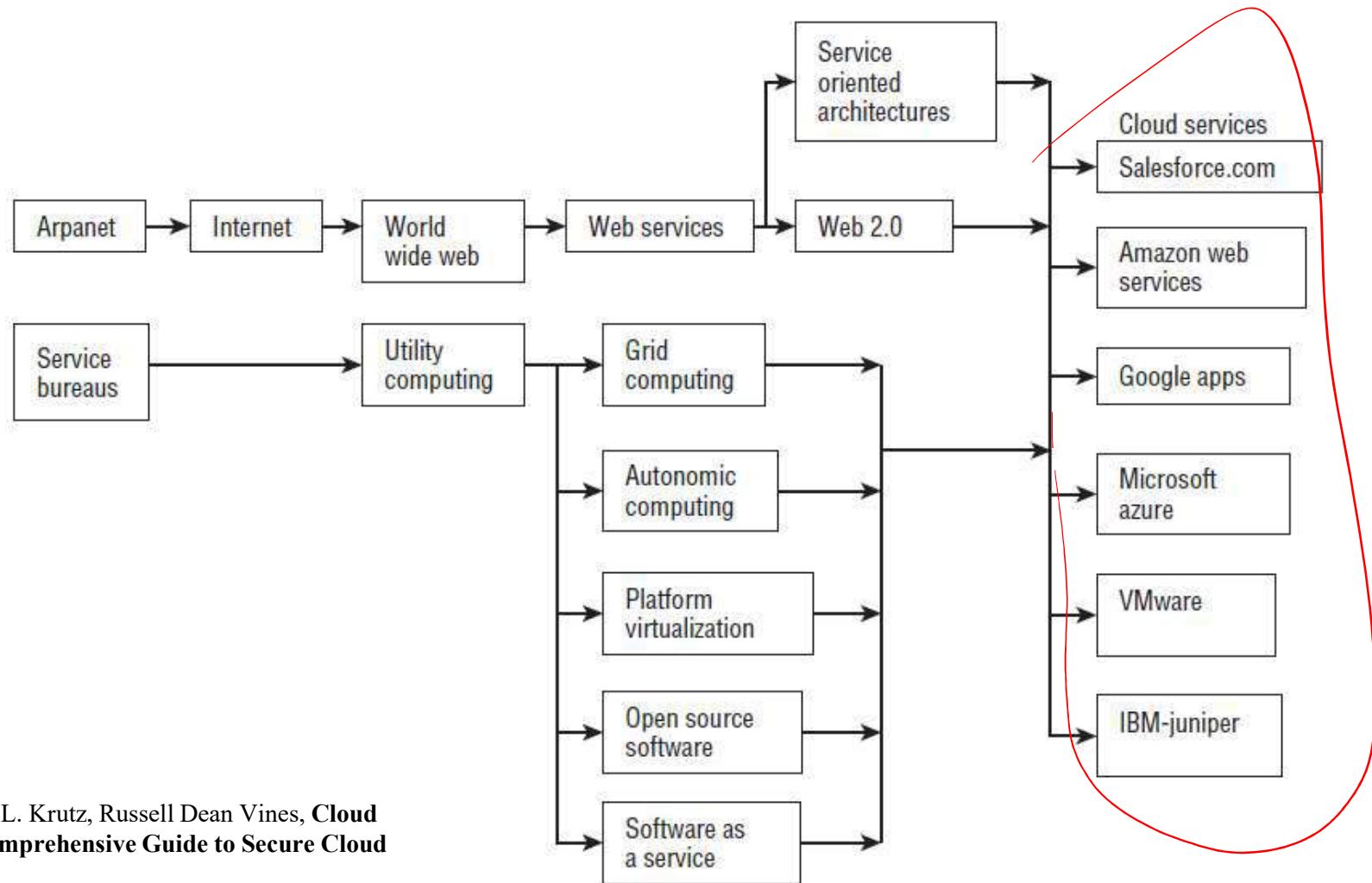
Abbv:

HTC: High-Throughput Computing
HPC: High-Performance Computing

Source: Lecture Notes on Cloud Computing, Institute of Aeronautical Engineering, Hyderabad



Another Evolution View



Source: Ronald L. Krutz, Russell Dean Vines, **Cloud Security: A Comprehensive Guide to Secure Cloud Computing**



NIST: 5 Essential Characteristics

Source: NIST Special Publication 800-145

On-demand self-service.

- A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access.

- Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling.

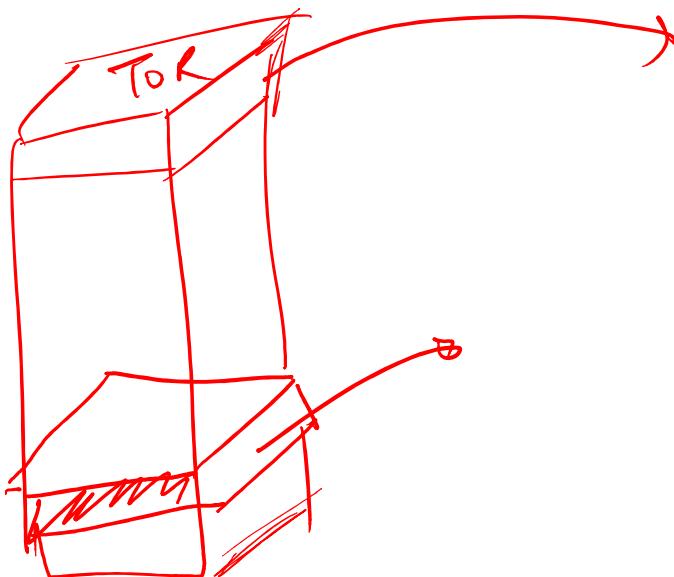
- The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.
- There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter).
- Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity.

- Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand.
- To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service.

- Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).
- Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.



DCN
=



Data Center– Design Goals

- Data center is a pool of resources (compute, storage, network) interconnected using a communication network (Data Center Network or DCN)
- Is a critical piece in the migration towards cloud computing and support of IoT applications

Concurrency

- Connected Devices
- High Ingress traffic

Scale

- Application Architecture designed for Scale out
- Infrastructure AutoScaling

Availability

- Geo redundant infrastructure

Monitoring

- Infrastructure and Application Monitoring and Metering
- Managed Support Services

API Management

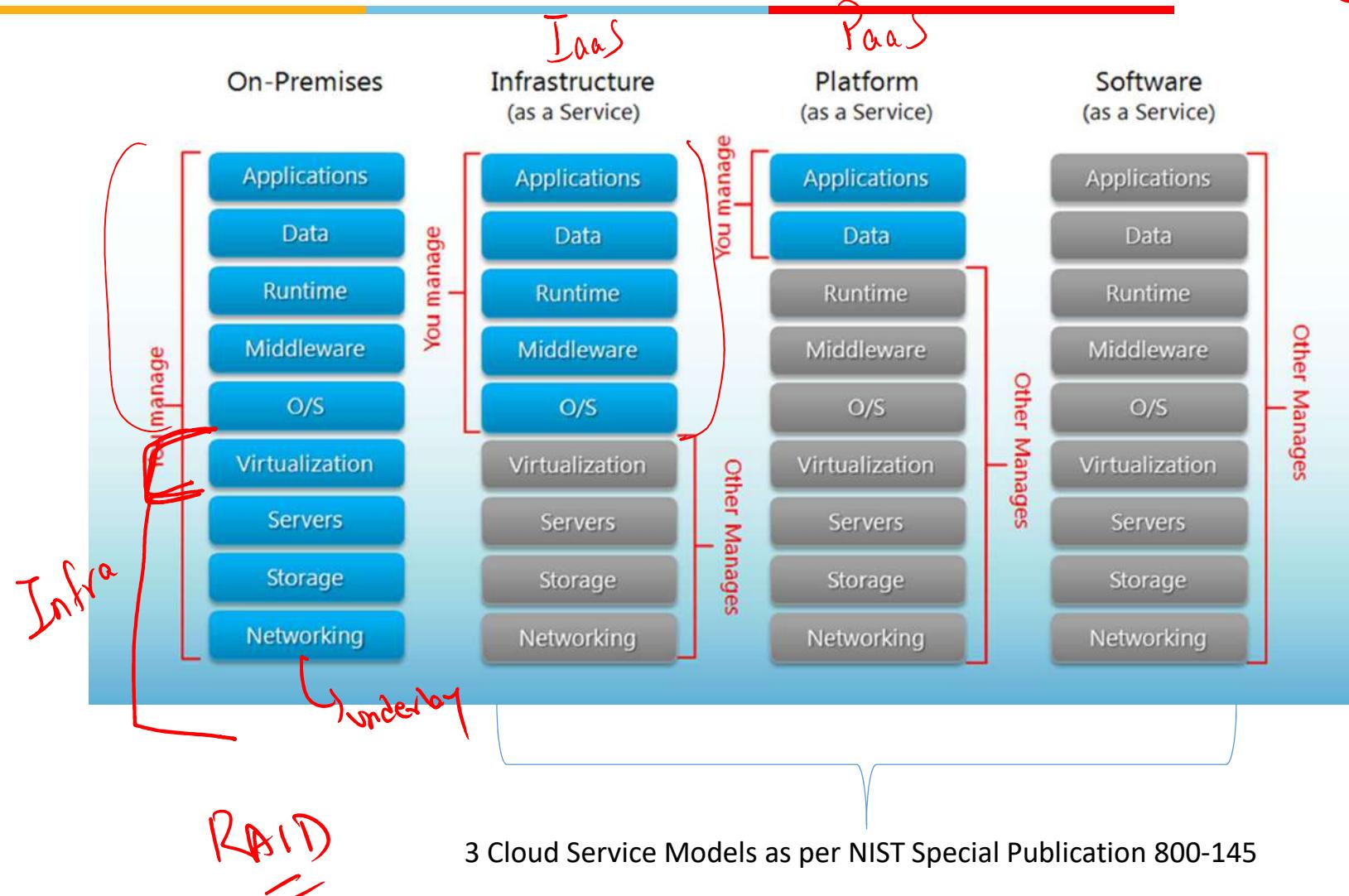
- Service Metering
- Security, Access Control and Governance

Integration

- Connectivity with transaction systems

Data Center: Service Models!

CSR





NIST: 4 Deployment Models

Source: NIST Special Publication 800-145

Private cloud.

- The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units).
- It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud.

- The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations).
- It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud.

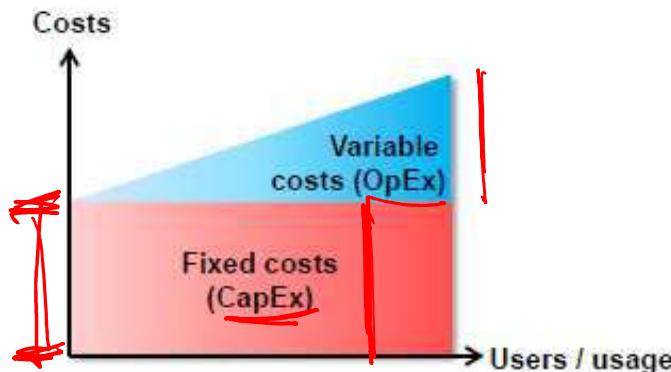
- The cloud infrastructure is provisioned for open use by the general public.
- It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them.
- It exists on the premises of the cloud provider.

Hybrid cloud.

- The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

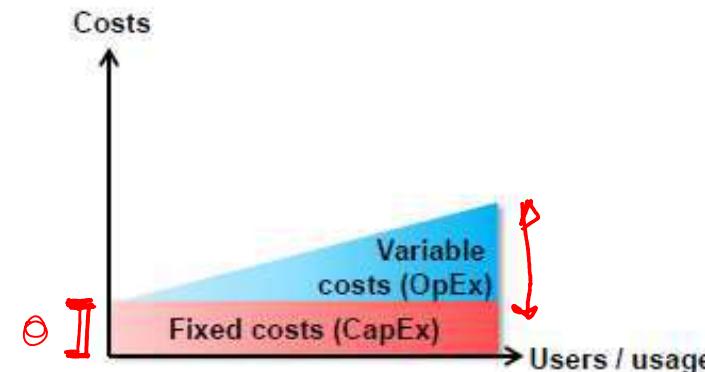
Rationale for Cloud Computing

Traditional IT:



Data centers, servers etc. require a large up-front investment (CapEx). The infrastructure must be dimensioned to accommodate a certain peak load. Variable costs incur on top of CapEx (run-time licenses for users etc.).

Cloud computing:



Fixed costs are transferred to the cloud provider and thus largely reduced for the customer (customer infrastructure reduced to network, workstations). Variable costs vary according to usage demand. The variable costs are reduced since the cloud provider exploits economy of scale.

Source: Peter R. Egli (indigoo.com)

Landscape for Cloud Computing

Cloud Service Providers (CSP):

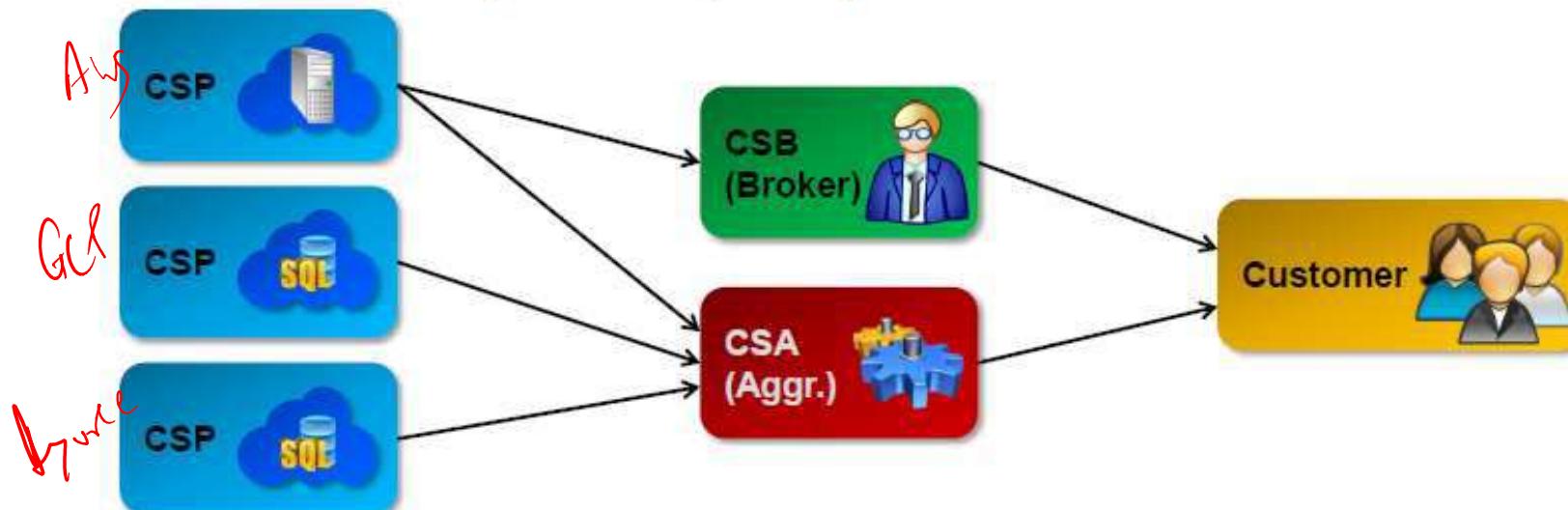
CSPs offer IaaS, PaaS and SaaS services as private, hybrid or public clouds.

Cloud Service Brokers (CSB):

CSBs resell and sometimes integrate CSP cloud services. CSBs focus on consultancy services, (help customers choose the right cloud solution, provide best practices for cloud deployment).

Cloud Service Aggregators (CSA):

CSAs integrate cloud services into value-added services, e.g. bundling storage services from different CSPs into a high-availability offering.



Source: Peter R. Egli (indigoo.com)

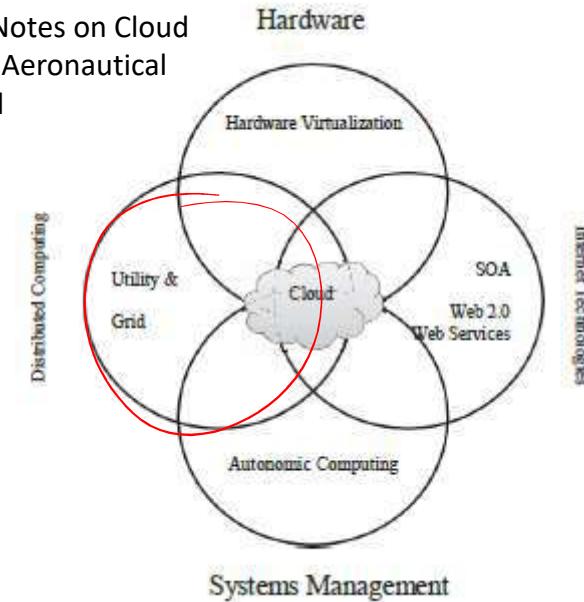


Enabling Technologies

Uses 2 key technologies....

- SDN
 - Software Defined Networking
- NFV
 - Network Function Virtualization

Image Source: Lecture Notes on Cloud Computing, Institute of Aeronautical Engineering, Hyderabad



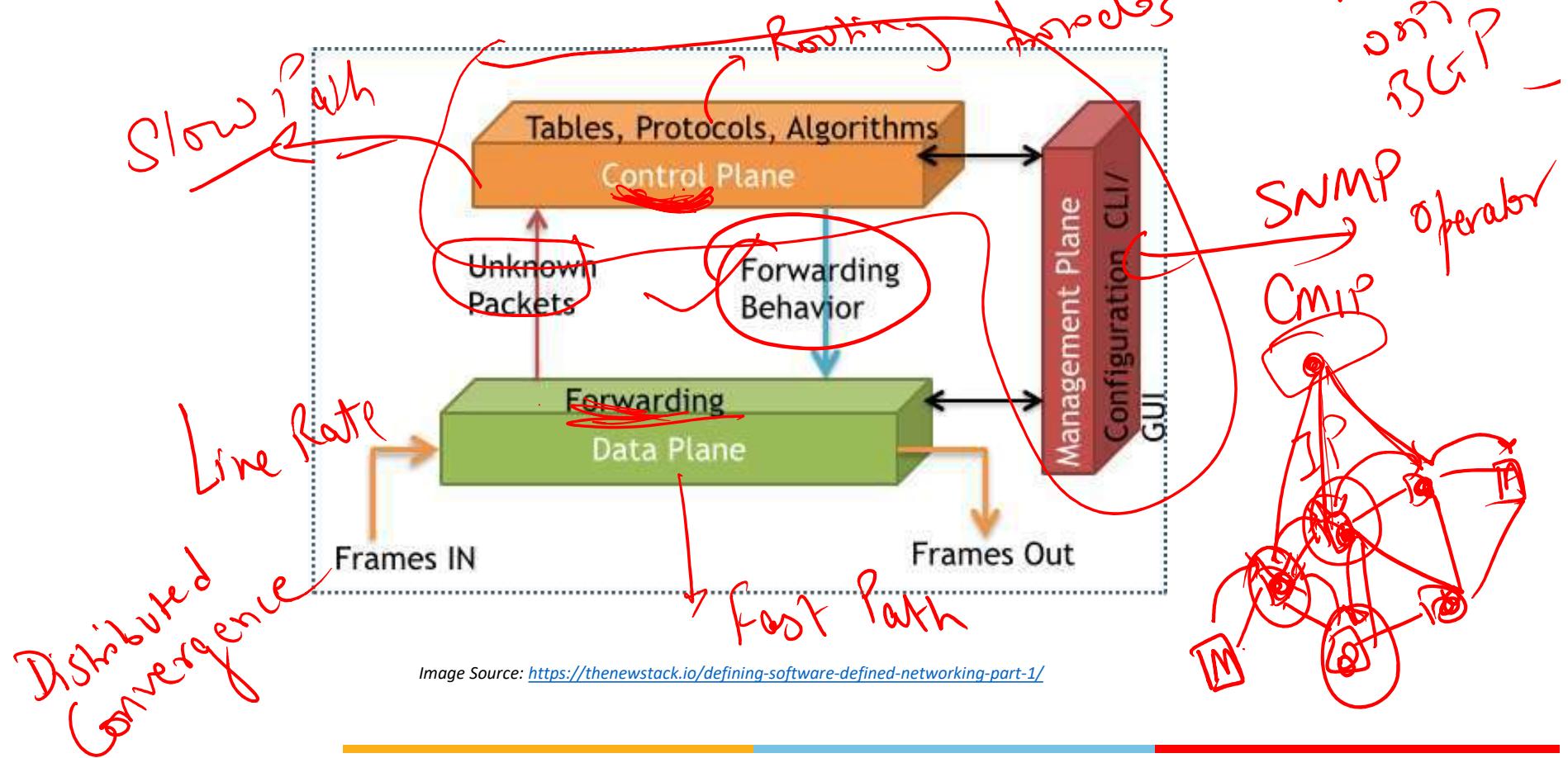
.....Alongside many other supporting technologies:

- Broadband Network Access
 - Diminishing the distinction between LAN and WAN bandwidth
- Distributed Computing
 - Including Middleware supporting interoperability for cloud-based distributed applications
- Grid Technology
 - Large number of connected physical servers for demand-based computing

Software Defined Networking (SDN): Background



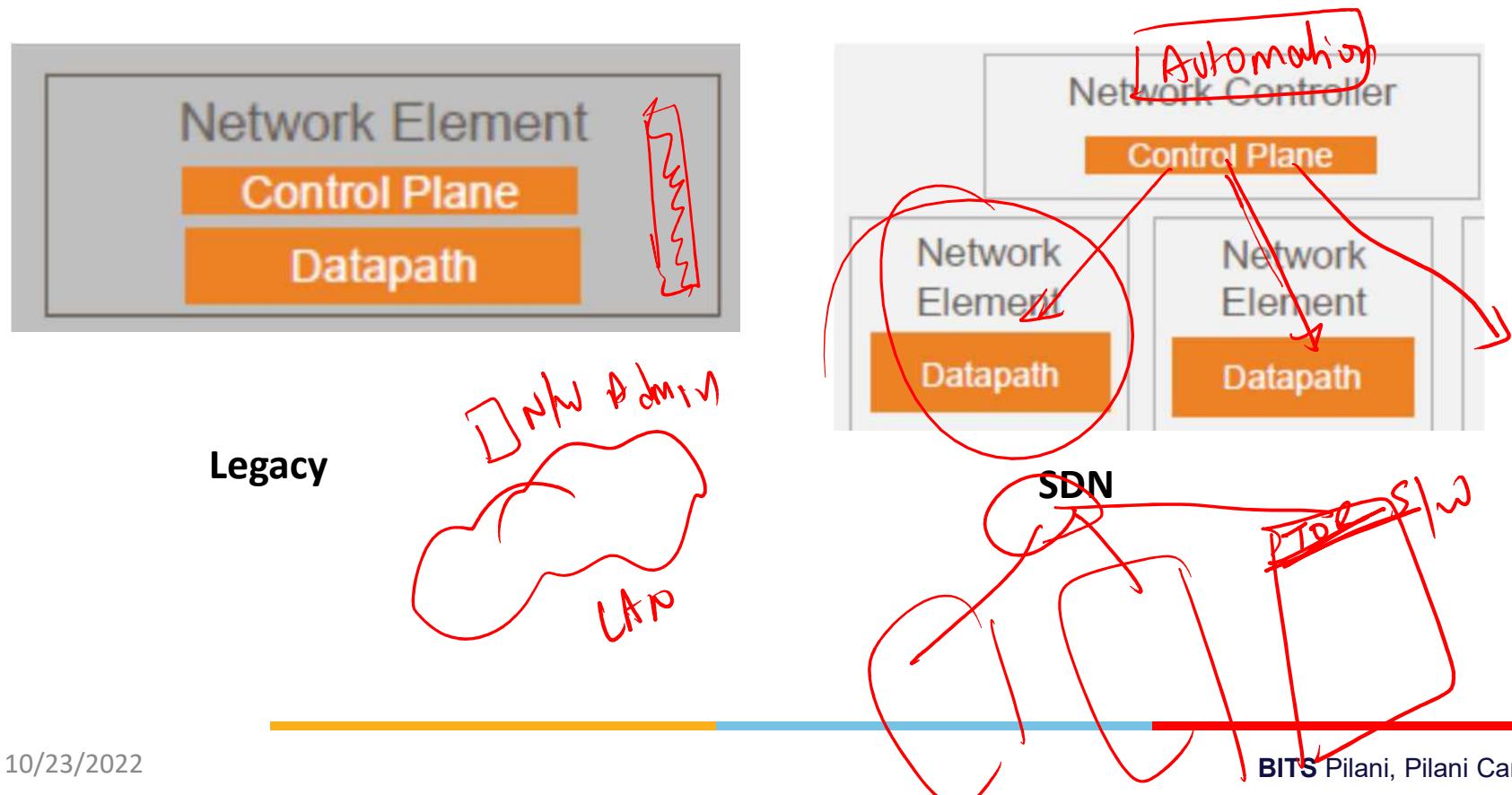
- Three Plane Architecture of Network Elements



Software Defined Networking (SDN): Main Concepts



- Separation of Control Plane from Data Plane



Software Defined Networking (SDN): Key Benefits

- ✓ • Software-driven control / Programmability
- Simplified Network Equipment available as COTS
- Standardized management of Network Equipment → interoperability
- Cost Reduction, especially for large infrastructure setups as in Data Centers
 - Example: 1K switches required for a networking configuration
 - Without SDN:
 - Cost of Switch = \$5K
 - Total Cost = \$5M
 - With SDN:
 - Cost of SDN Controller (manages 100 switches) = \$80K
 - Cost of COTS switch = \$1K
 - Total Cost = $(\$80K * 10) + (\$1K * 1000) = \$1.8M$

SDN Architecture / Layers

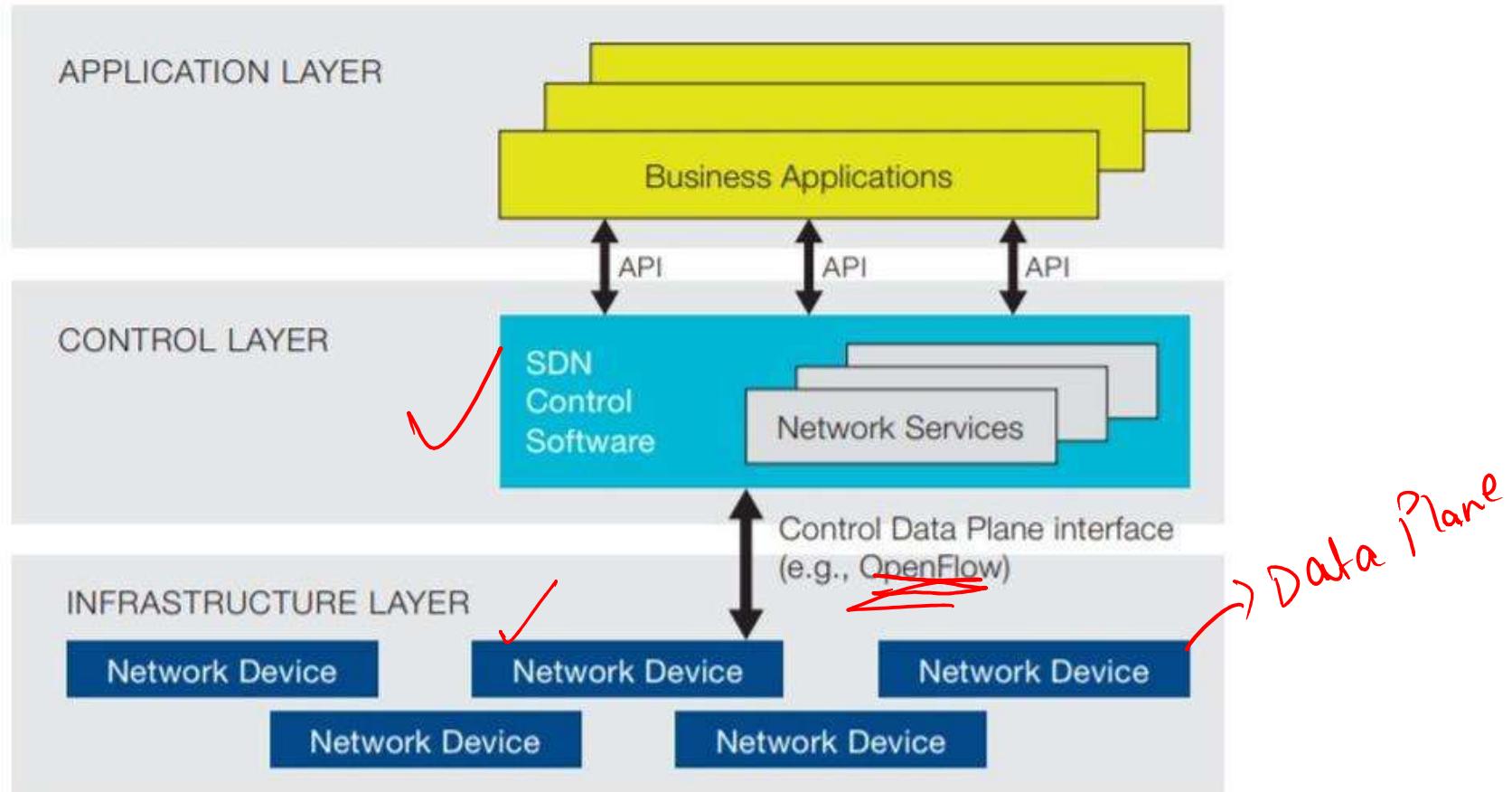
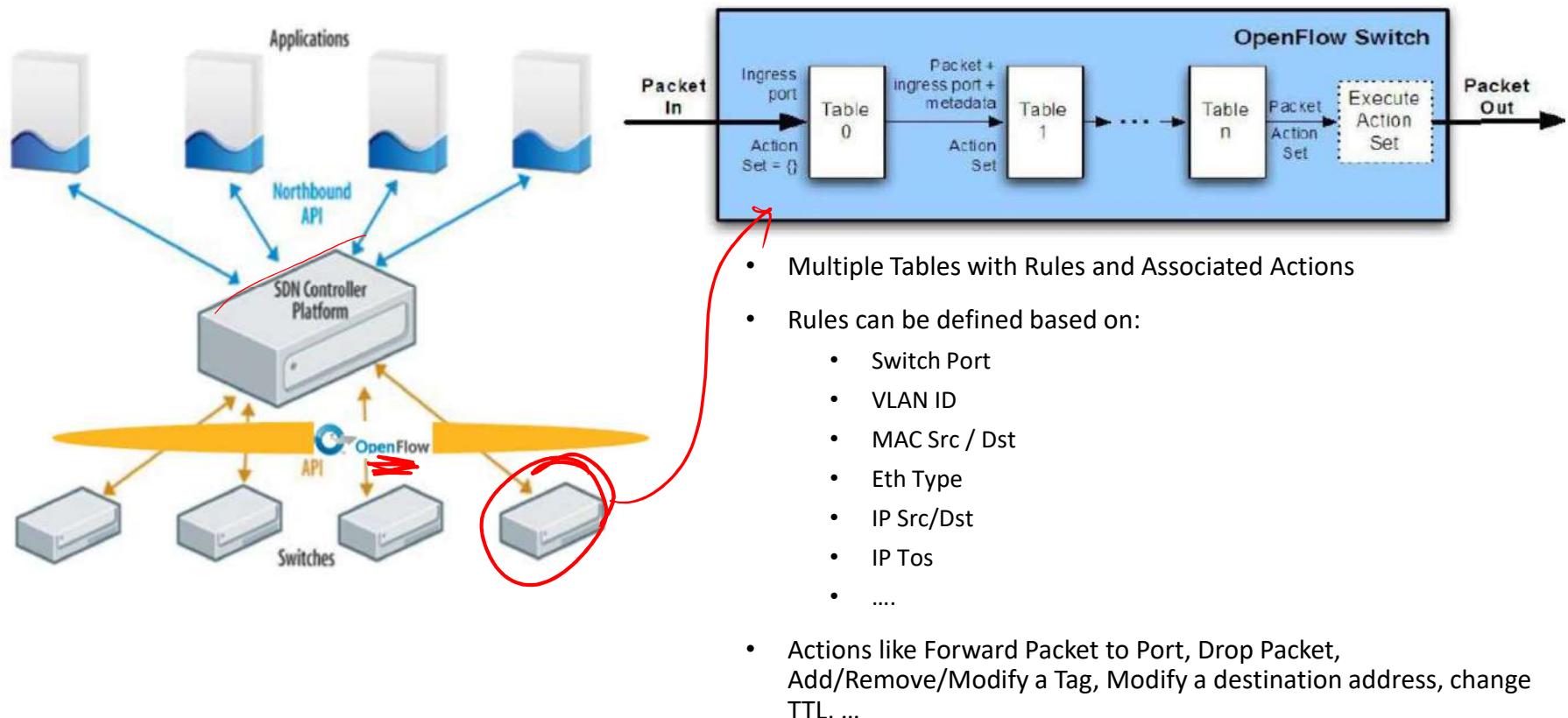


Image Source: Open Networking Foundation

OpenFlow Protocol



Open Flow: Provisioning Approaches for Flows



Flow Provisioning

- Reactive Provisioning
 - React to an incoming packet that results in a miss
 - Data Plane Driven Approach
- Proactive Provisioning
 - Pre-configure all flows that could hit the switch
 - Configuration Driven Approach

Flow Removal

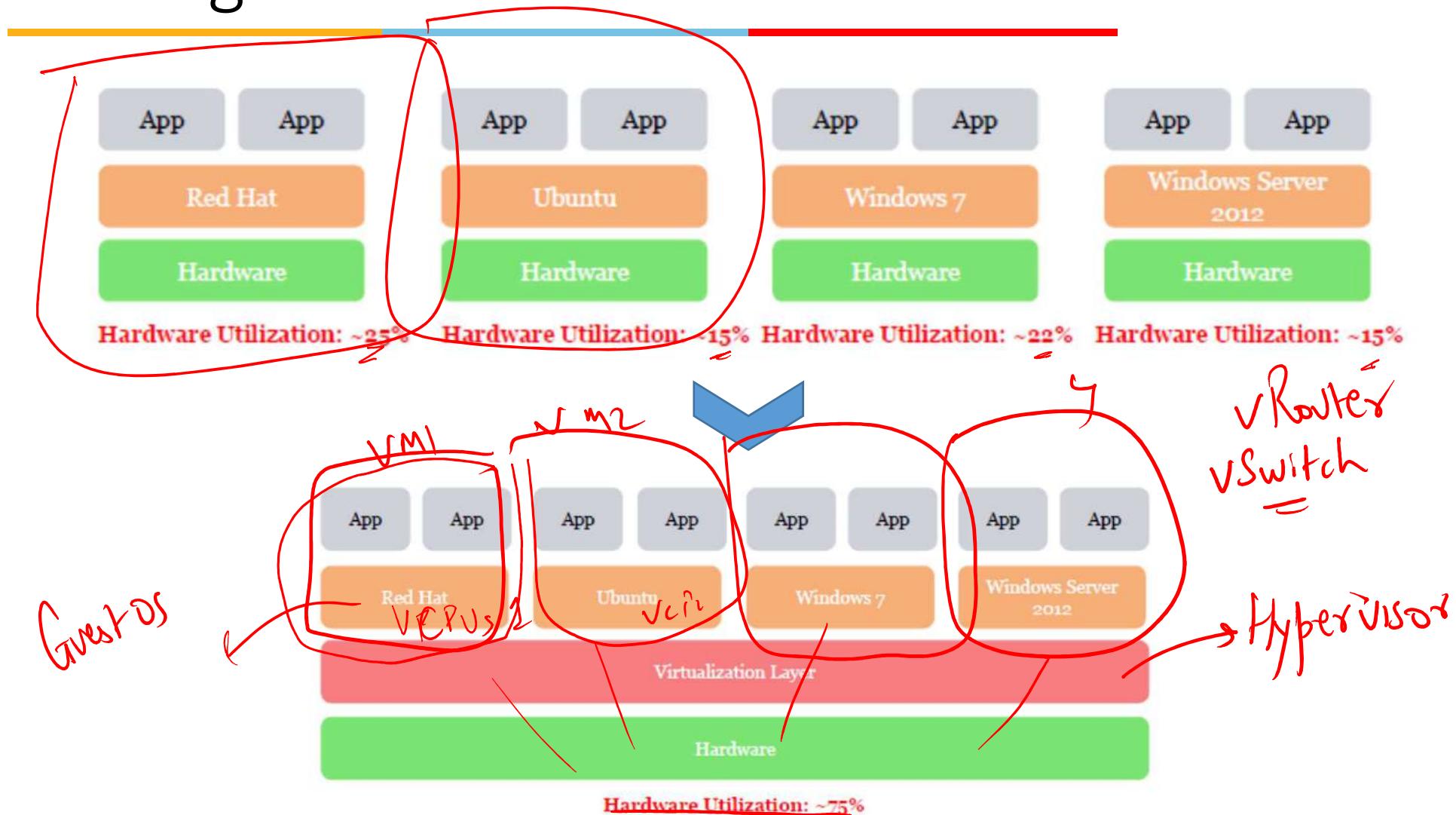
- Idle Timeout
- Explicit removal from Controller



SDN Application Examples

- Route Optimization
 - Steer traffic based on network conditions, e.g. congestion
- Load Balancing
 - Steer traffic onto alternate routes
- Dynamic Bandwidth Allocation
 - Allocation based on QoS
- Network Monitoring
 - Debugging, Lawful Interception etc

Network Function Virtualization: Background





NFV: Enabling Solution Component

- Hypervisor
 - A technology that allows sharing of hardware resources of a single machine by multiple guest Operating Systems (OS)
 - Results in multiple Virtual Machines (VMs) on same physical machine

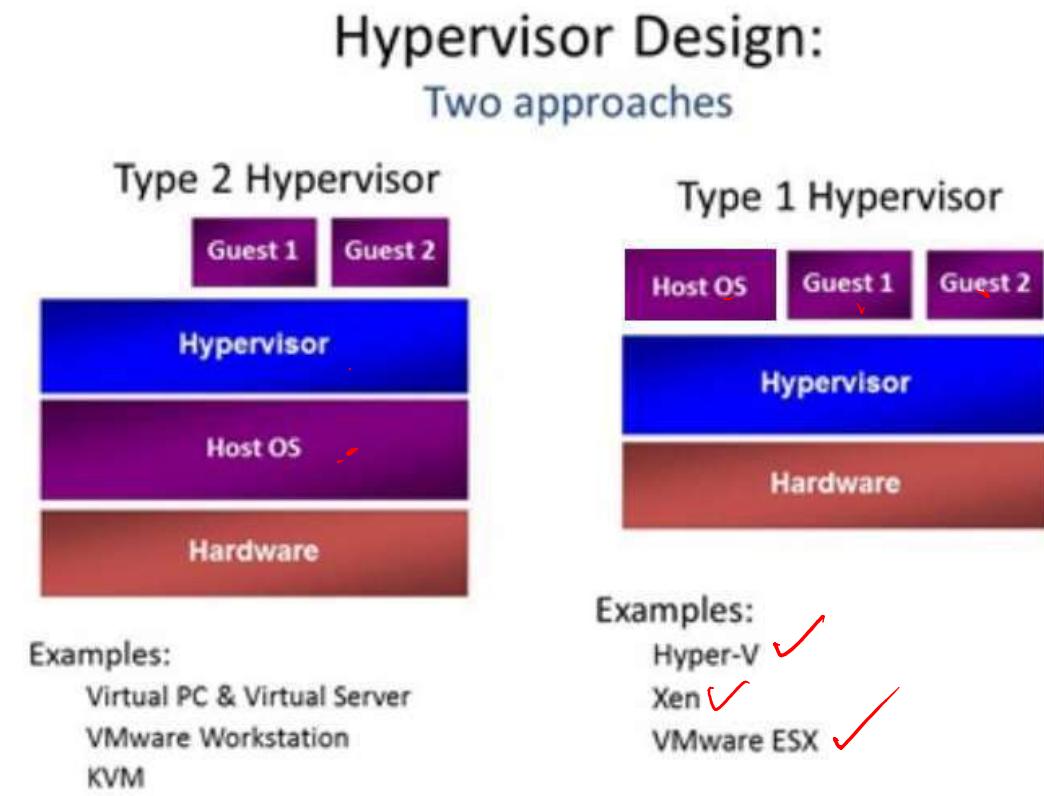


Image Source: <https://www.tenforums.com/virtualization/119469-hypervisor-type-1-type-2-a.html>

NFV Architecture

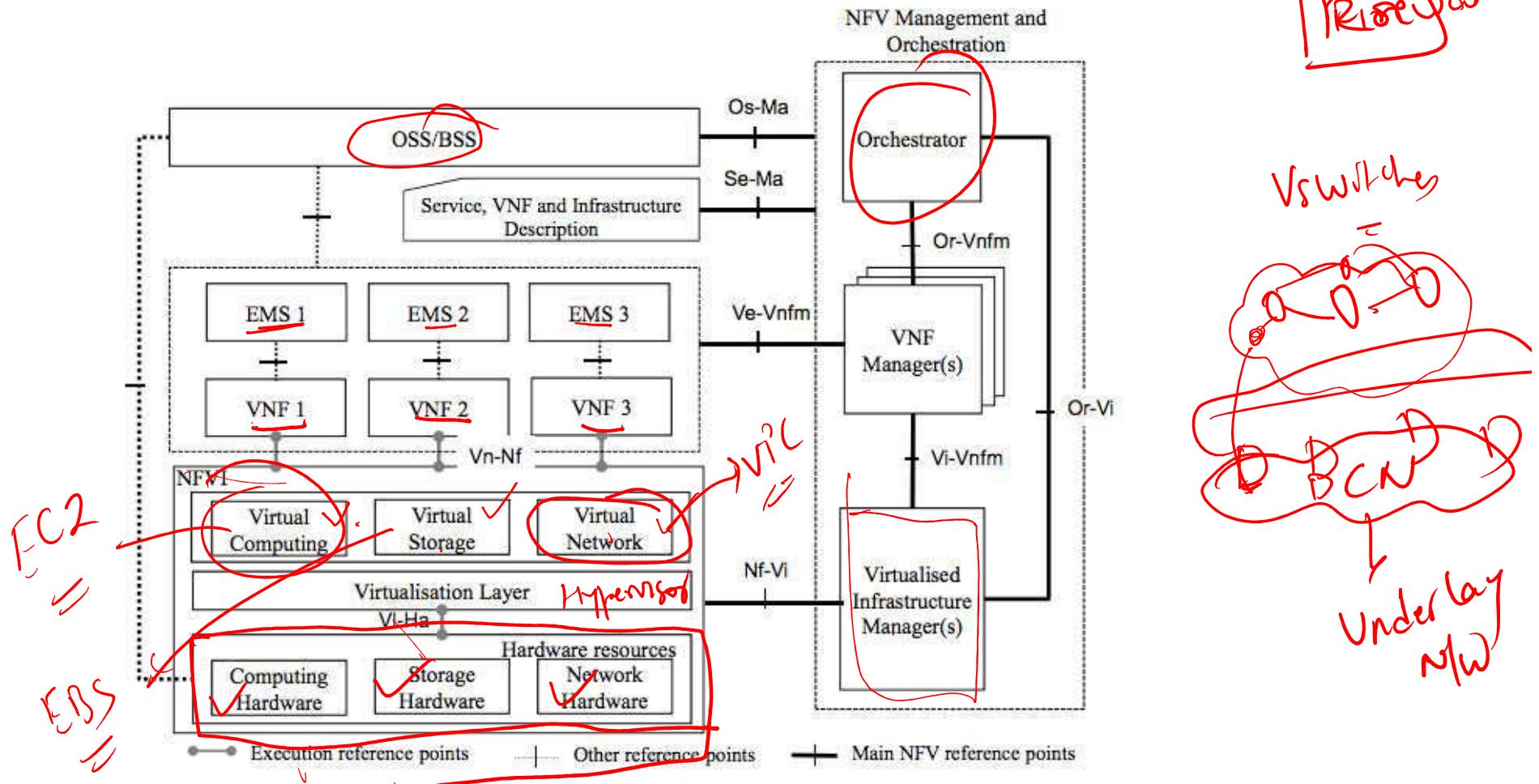


Image Source: SDxCentral



NFV Service Chaining

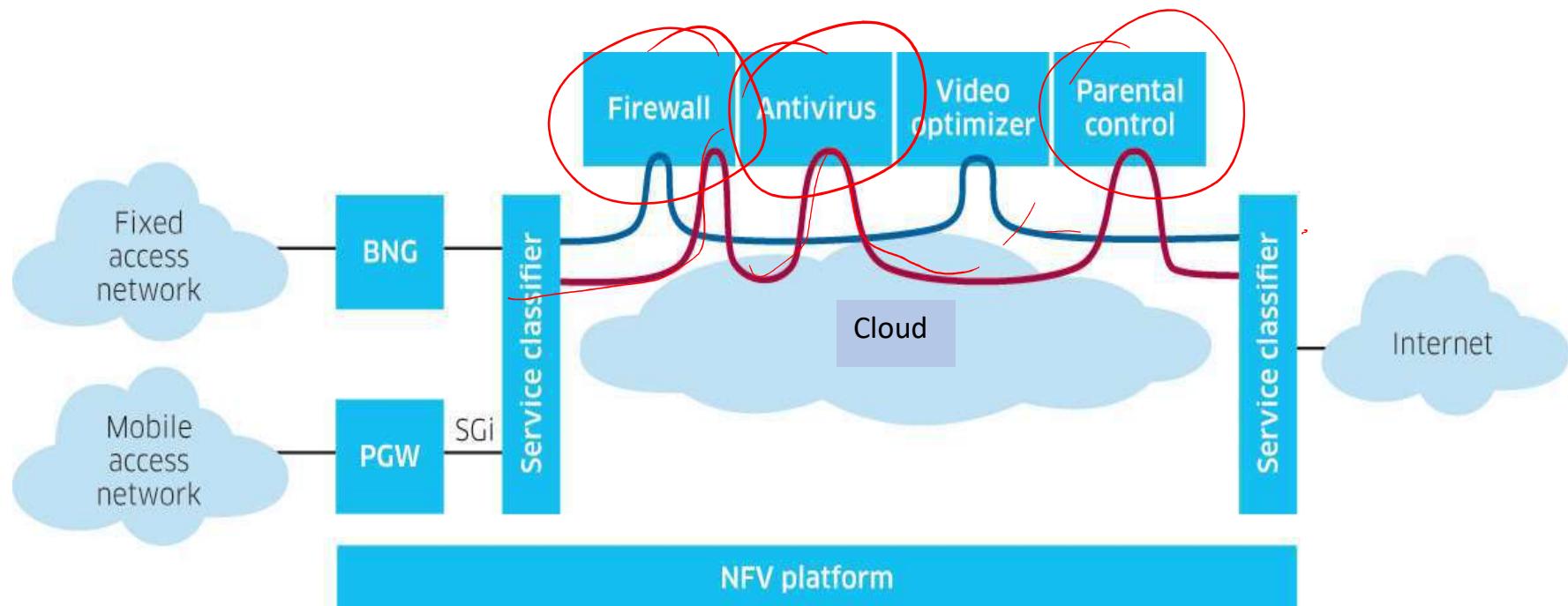


Image Source: SDxCentral



SDN/NFV in the Data Center



- NFV Data Center
 - Used by service providers to host communications and networking services
 - Services can be loaded as cloud-based software on commercial off-the-shelf (COTS) server hardware
 - Applications are hosted in data center so they could be accessed via cloud
- SDN can work in tandem with NFV
 - Traffic Steering in an NFV Data Center

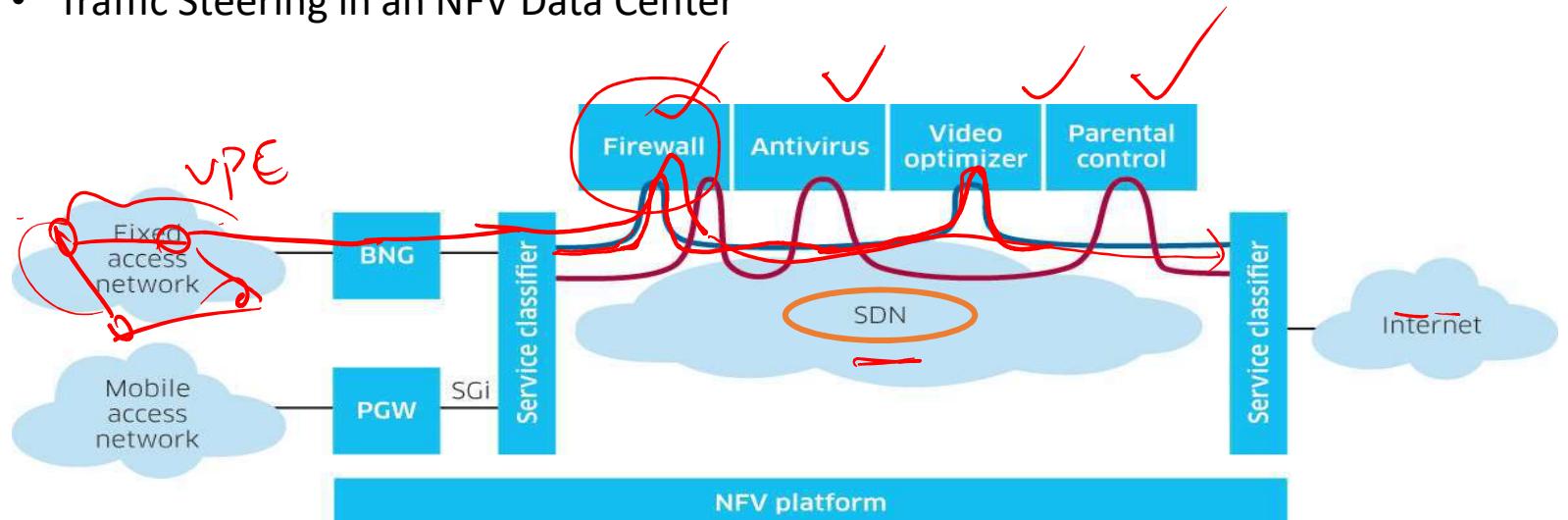
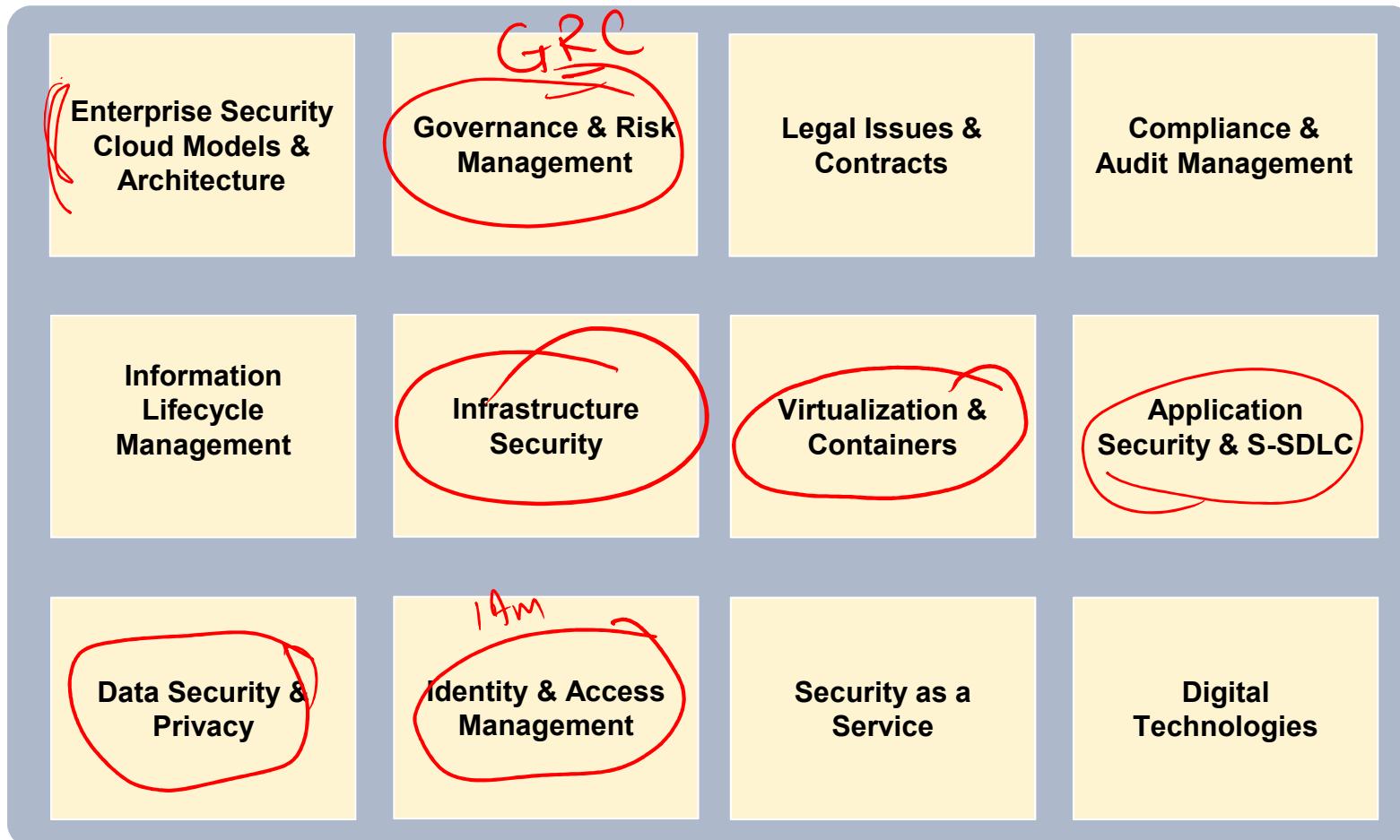


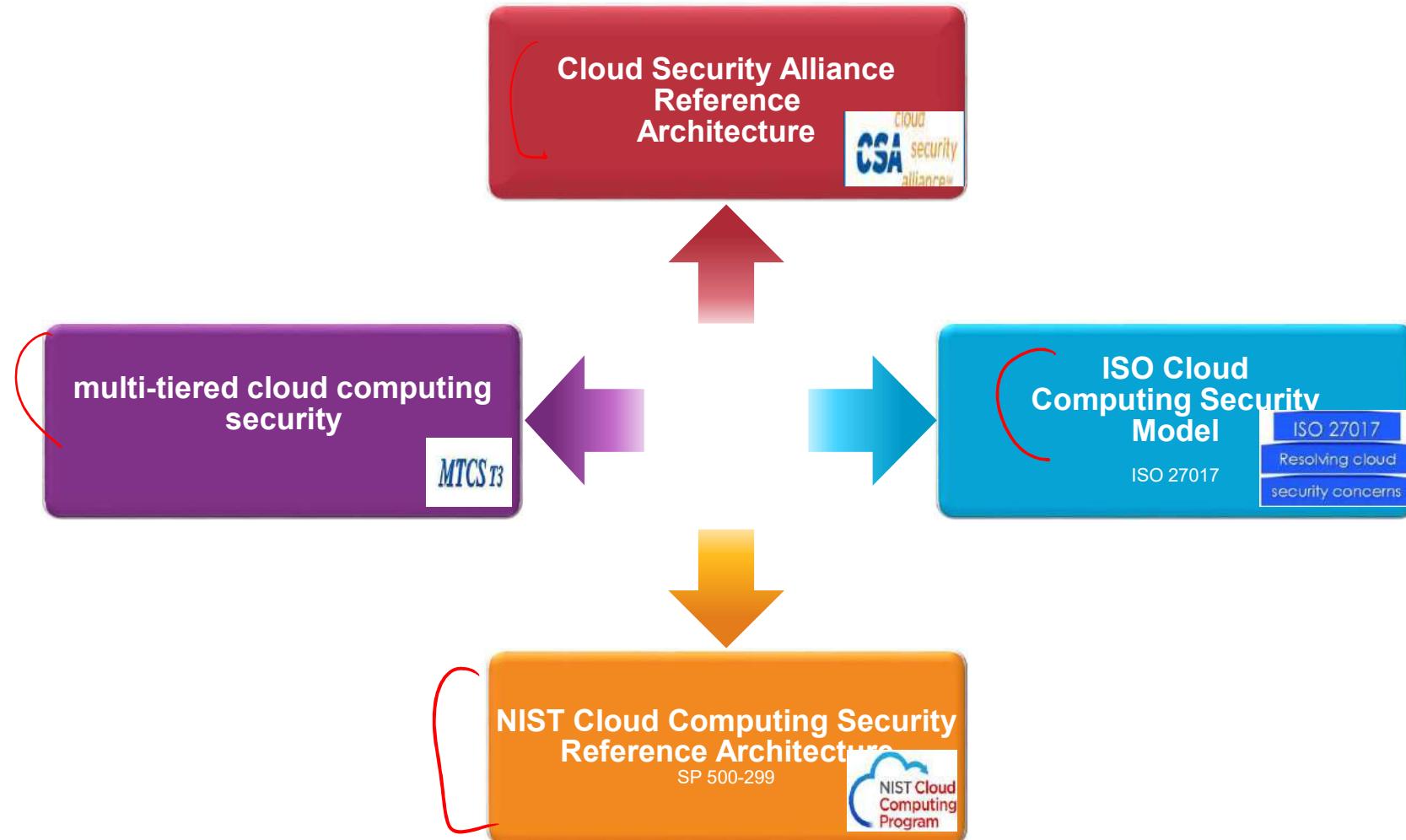
Image Source: SDxCentral



Security Topics for Cloud Computing



Cloud Security Reference Architectures & Standards





BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 11: Cloud Security

Cloud Security Fundamentals

Source Disclaimer: Content for some of the slides is from the course Textbook:

Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley & Sons, 2010

Some of the other slides are taken from Microsoft Educator Learn Material (Microsoft Azure Security Technologies)

Overview

- Why Cloud Security?
 - Security is a principal concern when entrusting an organization's critical information to geographically dispersed cloud platforms not under the direct control of that organization
 - Designing security into cloud software during the software development life cycle can greatly reduce the cloud attack surface → Secure SDLC / DevSecOps
- Case Study:
 - On-premise application sever moved to cloud environment.
 - How will the various roles of Web Admin, System Admin etc continue to work in a secure fashion?





Secure Software Lifecycle

Refer “*Security Guidance for Critical Areas of Focus in Cloud Computing*” by the Cloud Security Alliance

- Emphasizes the importance of secure software life cycle in their listing of 15 cloud security domains. Example:
 - Domain 6, Information Lifecycle Management
 - *“Understand cloud provider policies and processes for data retention and destruction and how they compare with internal organizational policy. Be aware that data retention assurance may be easier for the cloud provider to demonstrate, but data destruction may be very difficult. Perform regular backup and recovery tests to assure that logical segregation and controls are effective.”*
 - Domain 11, Application Security
 - *“IaaS, PaaS and SaaS create differing trust boundaries for the software development lifecycle, which must be accounted for during the development, testing and production deployment of applications.”*
 - Domain 14, Storage
 - *“Understand cloud provider storage retirement processes. Data destruction is extremely difficult in a multi-tenant environment and the cloud provider should be utilizing strong storage encryption that renders data unreadable when storage is recycled, disposed of, or accessed by any means outside of authorized applications.”*
 - Irrespective of whoever develops the software, the process requires a strong commitment to a formal, secure software development life cycle, including design, testing, secure deployment, patch management, and disposal → Secure SDLC, DevSecOps etc
-



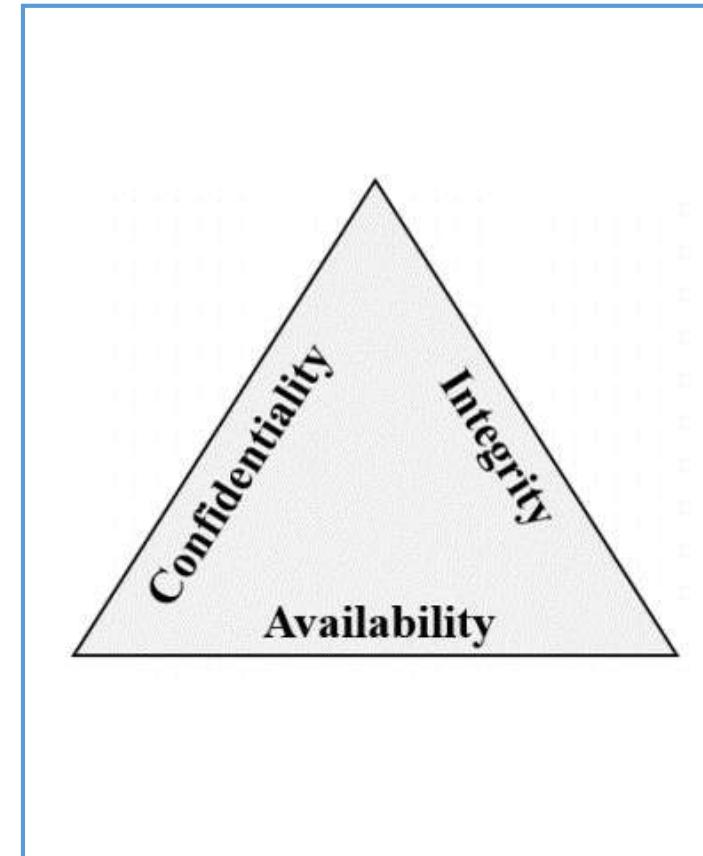
Cloud Information Security Objectives

- Data and Analysis Center for Software (DACS) requires that software must exhibit the following three properties to be considered secure:
 - **Dependability** — Software that executes predictably and operates correctly under a variety of conditions, including when under attack or running on a malicious host
 - **Trustworthiness** — Software that contains a minimum number of vulnerabilities or no vulnerabilities or weaknesses that could sabotage the software's dependability. It must also be resistant to malicious logic
 - **Survivability (Resilience)** — Software that is resistant to or tolerant of attacks and has the ability to recover as quickly as possible with as little harm as possible
- Seven complementary principles that support information assurance are:
 - Confidentiality, Integrity, Availability (CIA Triad), and
 - Authentication, Authorization, Auditing, and Accountability (AAAA)
- These 7 principles are summarized in the following slides.

Confidentiality, Integrity, Availability (CIA)

CIA - A way to think about security trade-offs.

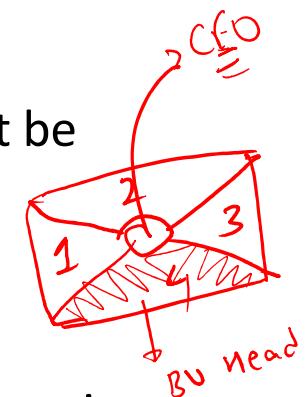
- **Confidentiality** refers to the need to keep confidential sensitive data such as customer information, passwords, or financial data.
- **Integrity** refers to keeping data or messages correct.
- **Availability** refers to making data available to those who need it.



Confidentiality in Cloud Systems

- Confidentiality in cloud systems is related to the areas of intellectual property rights, covert channels, traffic analysis, encryption, and inference:

- Intellectual property (IP) includes inventions, designs, and artistic, musical, and literary works
- Covert channels: A covert channel is an unauthorized and unintended communication path that enables the exchange of information. Covert channels can be accomplished through inappropriate use of storage mechanisms, as example
- Encryption involves scrambling messages so that they cannot be read by an unauthorized entity, even if they are intercepted
- Traffic analysis is a form of confidentiality breach that can be accomplished by analyzing the volume, rate, source, and destination of message traffic, even if it is encrypted
- Inference is usually associated with database security. Inference is the ability of an entity to use and correlate information protected at one level of security to uncover information that is protected at a higher security level

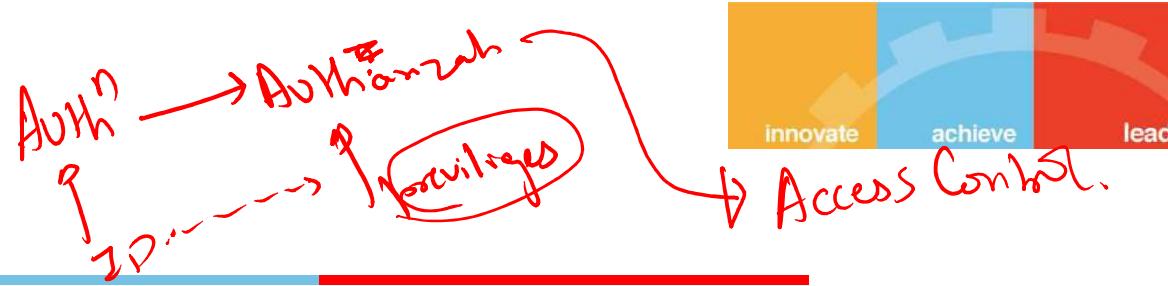


Integrity and Availability in Cloud Systems

- Integrity requires that the following three principles are met:
 - Modifications are not made to data by unauthorized personnel or processes.
 - Unauthorized modifications are not made to data by authorized personnel or processes.
 - The data is internally and externally consistent, i.e. the internal information is consistent both among all sub-entities and with the real/external-world
- Availability ensures the reliable and timely access to cloud data or cloud computing resources by the appropriate personnel. Availability guarantees that
 - the systems are functioning properly when needed.
 - In addition, this concept guarantees that the security services of the cloud system are in working order.
 - A denial-of-service attack is an example of a threat against availability.

The reverse of confidentiality, integrity, and availability is disclosure, alteration, and destruction (DAD)!!

AAAAA



~~IAM~~

- *Authentication* is the testing or reconciliation of evidence of a user's identity. It establishes the user's identity and ensures that users are who they claim to be.
- *Authorization* refers to rights and privileges granted to an individual or process that enable access to computer resources and information assets.
- Auditing: To maintain operational assurance, organizations use two basic methods: system audits and monitoring. These methods can be employed by the cloud customer, the cloud provider, or both, depending on asset architecture and deployment
 - A *system audit* is a one-time or periodic event to evaluate security.
 - *Monitoring* refers to an ongoing activity that examines either the system or the users, such as intrusion detection
 - An *audit trail or log* is a set of records that collectively provide documentary evidence of different cloud operations
- *Accountability* is the ability to determine the actions and behaviors of a single individual within a cloud system
 - Accountability is related to the concept of *nonrepudiation*, wherein an individual cannot successfully deny the performance of an action
 - Audit trails and logs support accountability



Cloud Security Design Principles

- A 1974 paper (***that is still relevant today!***) addresses the protection of information stored in a computer system by focusing on hardware and software issues that are necessary to support information protection
 - “The Protection of Information in Computer Systems” by Saltzer and Schroeder
 - <https://www.cs.virginia.edu/~evans/cs551/saltzer/>
 - The paper presented the following 11 security design principles
 - ✓ • Least privilege
 - Separation of duties
 - ✓ • Defense in depth
 - Fail safe
 - Economy of mechanism
 - Complete mediation
 - Open design
 - Least common mechanism
 - Psychological acceptability
 - ✓ • Weakest link
 - Leveraging existing components
 - The following slides summarize these design principles
-



Principle 1: Least Privilege

- The principle of *least privilege* maintains that an individual, process, or other type of entity should be given the minimum privileges and resources for the minimum period of time required to complete a task.
- This approach reduces the opportunity for unauthorized access to sensitive information.



Principle 2: Separation of Duties

- *Separation of duties* requires that completion of a specified sensitive activity or access to sensitive objects is dependent on the satisfaction of a **plurality** of conditions. For example:
 - an authorization that requires signatures of more than one individual, or
 - the arming of a weapons system that requires two individuals with different keys
- Thus, separation of duties forces collusion among entities in order to compromise the system.



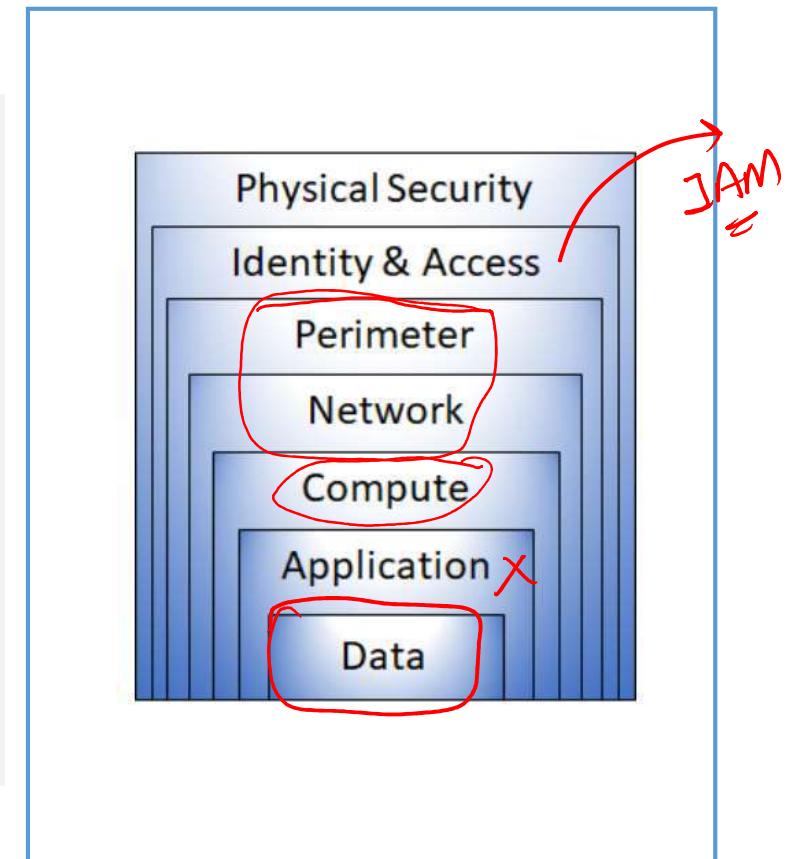
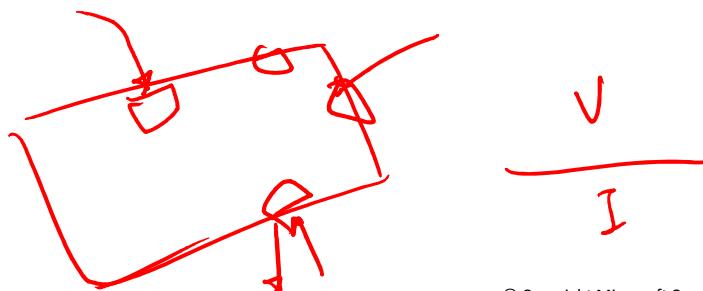
Principle 3: Defense in Depth

- *Defense in depth* is the application of multiple layers of protection wherein a subsequent layer will provide protection if a previous layer is breached
- The Information Assurance Technical Framework Forum (IATFF), an organization sponsored by the National Security Agency (NSA), has produced a document titled the “Information Assurance Technical Framework” (IATF) that provides excellent guidance on the concepts of defense in depth
 - **Defense in multiple places** — Information protection mechanisms placed in a number of locations to protect against internal and external threats
 - **Layered defenses** — A plurality of information protection and detection mechanisms employed so that an adversary or threat must negotiate a series of barriers to gain access to critical information
 - **Security robustness** — An estimate of the robustness of information assurance elements based on the value of the information system component to be protected and the anticipated threats
 - **Deploy KMI/PKI** — Use of robust key management infrastructures (KMI) and public key infrastructures (PKI)
 - **Deploy intrusion detection systems** — Application of intrusion detection mechanisms to detect intrusions, evaluate information, examine results, and, if necessary, take action

Defense in depth: Cloud Context

Defense in depth uses a layered approach to security:

- **Physical** security such as limiting access to a datacenter to only authorized personnel.
- **Identity and access** security controlling access to infrastructure and change control.
- **Perimeter** security including distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- **Network** security can limit communication between resources using segmentation and access controls.
- The **compute** layer can secure access to virtual machines either on-premises or in the cloud by closing certain ports.
- **Application** layer security ensures that applications are secure and free of security vulnerabilities.
- **Data** layer security controls access to business and customer data, and encryption to protect data.





Principle 4: Fail Safe

- *Fail safe* means that if a cloud system fails it should fail to a state in which the security of the system and its data are not compromised.
 - One implementation of this philosophy would be to make a system default to a state in which a user or process is denied access to the system.
 - A complementary rule would be to ensure that when the system recovers, it should recover to a secure state and not permit unauthorized access to sensitive information.
 - In the situation where system recovery is not done automatically, the failed system should permit access only by the system administrator and not by other users, until security controls are reestablished.



Principle 5: Economy of Mechanism

- *Economy of mechanism* promotes simple and comprehensible design and implementation of protection mechanisms, so that unintended access paths do not exist or can be readily identified and eliminated
 - The principle states that Security mechanisms should be as simple and small as possible
 - If the design and implementation are simple and small, fewer possibilities exist for errors
 - The checking and testing process is less complicated so that fewer components need to be tested



Principle 6: Complete Mediation

- *In complete mediation*, every request by a subject to access an object in a computer system must undergo a valid and effective authorization procedure
- This mediation must not be suspended or become capable of being bypassed, even when the information system is being initialized, undergoing shutdown, being restarted, or is in maintenance mode



Principle 7: Open Design

- There has always been an ongoing discussion about the merits and strengths of security designs that are kept secret versus designs that are open to scrutiny and evaluation by the community at large.
 - A good example is an encryption system
- For most purposes, an open-access cloud system design that has been evaluated and tested by a myriad of experts provides a more secure authentication method than one that has not been widely assessed



Principle 8: Least Common Mechanism

- This principle states that in systems with multiple users, the mechanisms allowing resources shared by more than one user should be minimized as much as possible.
 - This principle may also be restrictive because it limits the sharing of resources
 - Shared access paths can be sources of unauthorized information exchange and can provide unintentional data transfers (also known as *covert channels*)
 - Example: If there is a need to access a file by more than one user, then these users should use separate channels to access the resource, as this helps to prevent from unforeseen consequences that could cause security problems
- Thus, the *least common mechanism* promotes the least possible sharing of common security mechanisms
 - Only a minimum number of protection mechanisms should be common to multiple users



Principle 9: Psychological Acceptability

- *Psychological acceptability* refers to the ease of use and intuitiveness of the user interface that controls and interacts with the cloud access control mechanisms
 - The principle states that a security mechanism should not make the resource more complicated to access if the security mechanisms were not present
 - In other words, the principle recognizes the human element in computer security
 - If security-related software or computer systems are too complicated to configure, maintain, or operate, the user will not employ the necessary security mechanisms

Trivia: When we enter a wrong password, the system normally only tells us that the user id or password was incorrect. It does not tell us that only the password was wrong as this gives the attacker information!!



Principle 10: Weakest Link

- A chain is only as strong as its weakest link
- In context of cloud-systems, the security of a cloud system is only as good as its weakest component
- Thus, it is important to identify the weakest mechanisms in the security chain and layers of defense, and improve them so that risks to the system are mitigated to an acceptable level

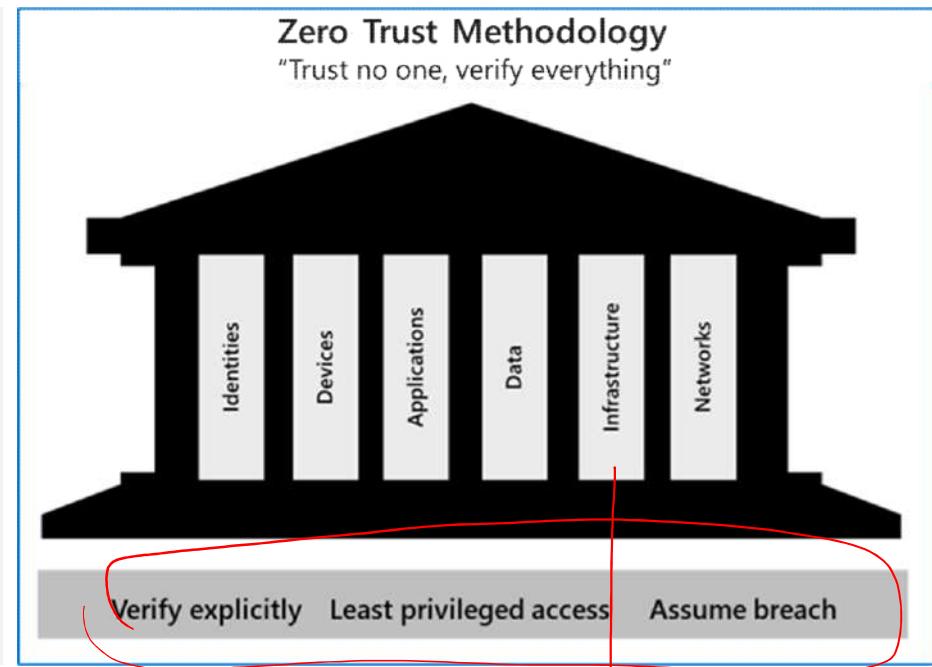
Principle 11: Leveraging Existing Components

- The principle aims to increase cloud system security by leveraging existing components
- In many instances, the security mechanisms of a cloud implementation might not be configured properly or used to their maximum capability.
- Reviewing the state and settings of the security mechanisms and ensuring that they are operating at their optimum design points will greatly improve the security posture of an information system

“the underlying principles that inform good security practices are well established and quite stable” – IoT SF

Cloud Security: The Zero-trust methodology

- Zero Trust guiding principles
 - ✓ Verify explicitly
 - ✓ Least privileged access
 - ✓ Assume breach
- Six foundational pillars
 - **Identities** may be users, services, or devices.
 - **Devices** create a large attack surface as data flows.
 - **Applications** are the way that data is consumed.
 - **Data** should be classified, labeled, and encrypted based on its attributes.
 - **Infrastructure** whether on-premises or cloud based, represents a threat vector.
 - **Networks** should be segmented.



IAM

Data Classif
labeling

Cloud Security: The shared responsibility model

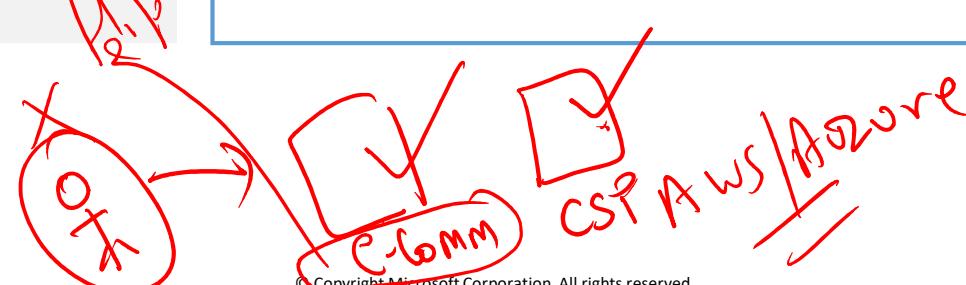
The responsibilities vary based on where the workload is hosted:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)
- On-premises datacenter (On-prem)

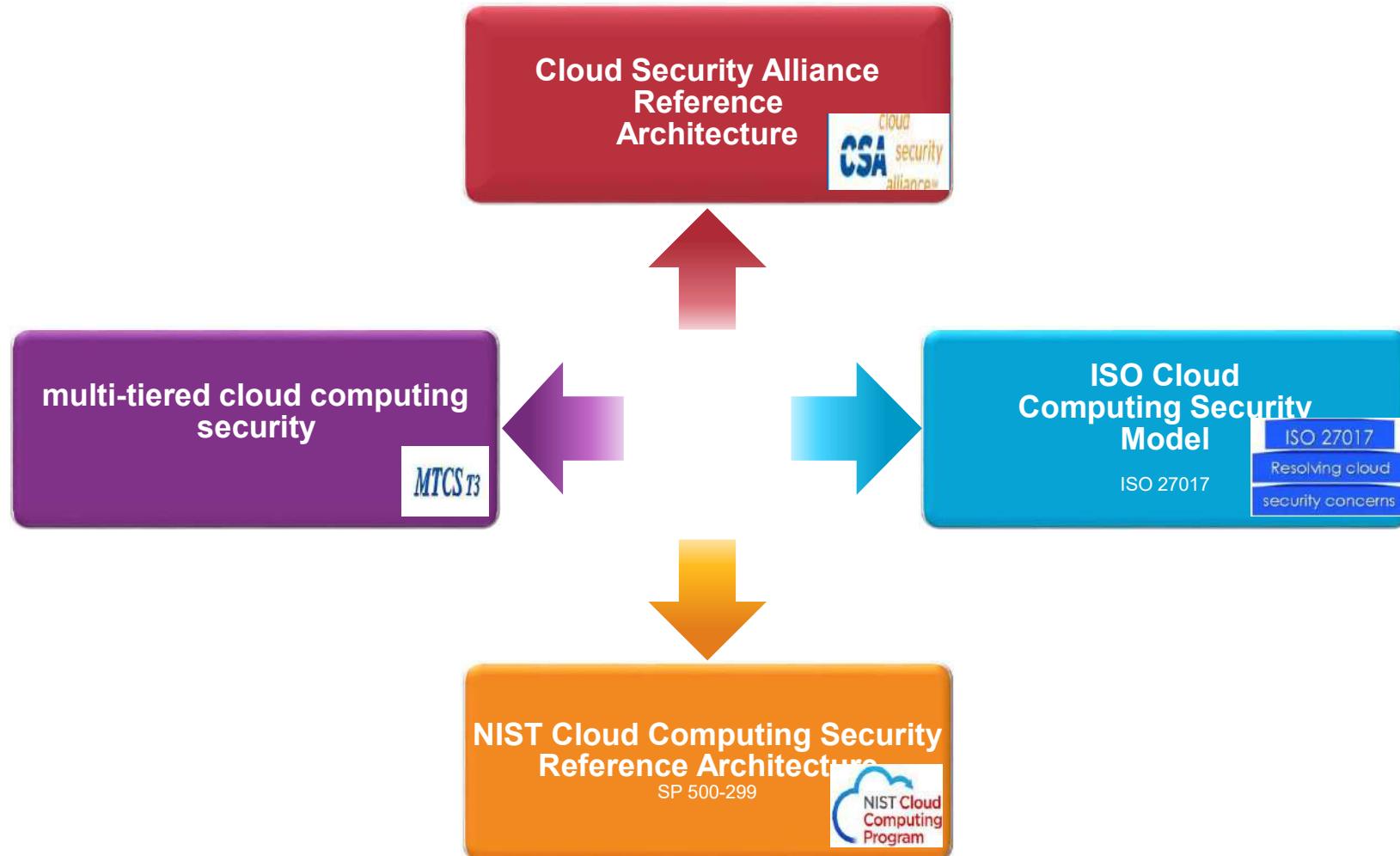
Shared responsibility model

Responsibility	SaaS	PaaS	IaaS	On-Prem
Information and data	Customer	Customer	Customer	Customer
Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
Accounts and identities	Customer	Customer	Customer	Customer
Identity and directory infrastructure	Customer	Customer	Customer	Customer
Applications	Customer	Customer	Customer	Customer
Network controls	Customer	Customer	Customer	Customer
Operating system	Customer	Customer	Customer	Customer
Physical hosts	Microsoft	Customer	Customer	Customer
Physical network	Microsoft	Customer	Customer	Customer
Physical datacenter	Microsoft	Customer	Customer	Customer

Microsoft Customer



RECAP: Cloud Security Reference Architectures & Standards





NIST 33 Security Principles

- NIST Special Publication 800-27
 - “Engineering Principles for Information Technology Security (EP-ITS)
 - It presents 33 security principles that begin at the design phase of the information system or application and continue until the system’s retirement and secure disposal
- Some of the 33 principles that are most applicable to cloud security policies and management are as follows:
 - Principle 1 — Establish a sound security policy as the “foundation” for design.
 - Principle 2 — Treat security as an integral part of the overall system design.
 - Principle 3 — Clearly delineate the physical and logical security boundaries governed by associated security policies.
 - Principle 6 — Assume that external systems are insecure.
 - Principle 7 — Identify potential trade-offs between reducing risk and increased costs and decreases in other aspects of operational effectiveness.
 - Principle 16 — Implement layered security; ensure there is no single point of vulnerability.
 - Principle 20 — Isolate public access systems from mission-critical resources (e.g., data, processes, etc.).
 - Principle 21 — Use boundary mechanisms to separate computing systems and network infrastructures.
 - Principle 25 — Minimize the system elements to be trusted.
 - Principle 26 — Implement least privilege.✓
 - Principle 32 — Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
 - Principle 33 — Use unique identities to ensure accountability



Business Continuity Planning / Disaster Recovery

- Business continuity planning (BCP) and disaster recovery planning (DRP) involve the preparation, testing, and updating of the actions required to protect critical business processes from the effects of major system and network failures
- From the cloud perspective, these important business processes are heavily dependent on cloud-based applications and software robustness and security
- Cloud computing offers an attractive alternative to **in-house** BCP/DRP implementations



DRP

The means of obtaining backup services are important elements in the disaster recovery plan. The typically used alternative services are as follows:

- **Mutual aid agreements** — An arrangement with another company that might have similar computing needs. The other company may have similar hardware or software configurations or may require the same network data communications or Internet access.
- **Subscription services** — Third-party commercial services that provide alternate backup and processing facilities. An organization can move its IT processing to the alternate site in the event of a disaster.
- **Multiple centers** — Processing is spread over several operations centers, creating a distributed approach to redundancy and sharing of available resources. These multiple centers could be owned and managed by the same organization (in-house sites) or used in conjunction with a reciprocal agreement.
- **Service bureaus** — Setting up a contract with a service bureau to fully provide all alternate backup-processing services. The disadvantages of this arrangement are primarily the expense and resource contention during a large emergency.



BCP

- A BCP is designed to keep a business running, reduce the risk of financial loss, and enhance a company's capability to recover promptly following a disruptive event.
- One of the key principle components of the BCP is the BIA:
 - Business impact assessment (BIA) — Assisting the business units in understanding the impact of a disruptive event. This phase includes the execution of a vulnerability assessment.
 - The function of a vulnerability assessment is to conduct a loss impact analysis. Because there are two parts to the assessment, a financial assessment and an operational assessment, it is necessary to define loss criteria both quantitatively and qualitatively



Using the Cloud for BCP/DRP

- Adopting a cloud strategy for BCP/DRP offers significant benefits without large amounts of capital and human resource investments.
- Proper design of a cloud-based IT system that meets the requirements of a BCP and DRP should include the following:
 - Secure access from remote locations
 - A distributed architecture with no single point of failure
 - Integral redundancy of applications and information
 - Geographical dispersion



Redundancy Provided by the Cloud

- Cloud computing offers redundancy in various forms (e.g. physical and virtual infrastructure, data backup etc)
 - Cloud-based BCP and DRP eliminate the need for expensive alternative sites and the associated hardware and software to provide redundancy.
 - Cloud computing provides for low cost and widely available, dynamically scalable, virtualized resources.
 - With a cloud computing paradigm, the backup infrastructure is always in place.
- Another option is to implement a hybrid cloud with collocation of resources and services.
- Cloud service providers also offer organizations the option to support the backup process thorough the use of storage area networks (SANs).
 - Examples of elements that require backup are application data, media files, files that have changed, recent documents, the operating system, and archival files.

Cloud Security

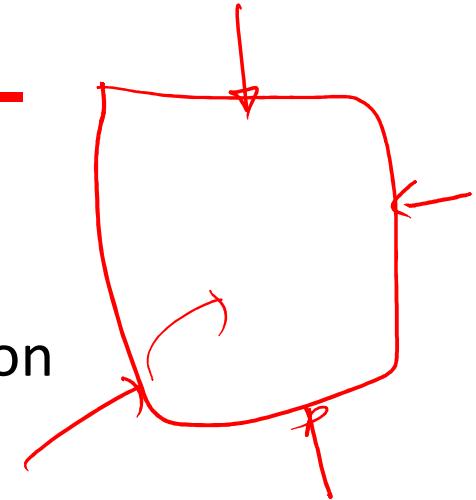
Identity and Access Management (IAM)

Source Disclaimer:

- Content for some of the slides is from the course Textbook:
 - *Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley & Sons, 2010*
- Some of the slides are taken from Microsoft Educator Learn Material (Microsoft Azure Security Technologies)
- Material for some of the other slides is from following book:
 - *Authentication: From Passwords to Public Keys, by Richard E. Smith*

IAM: Overview

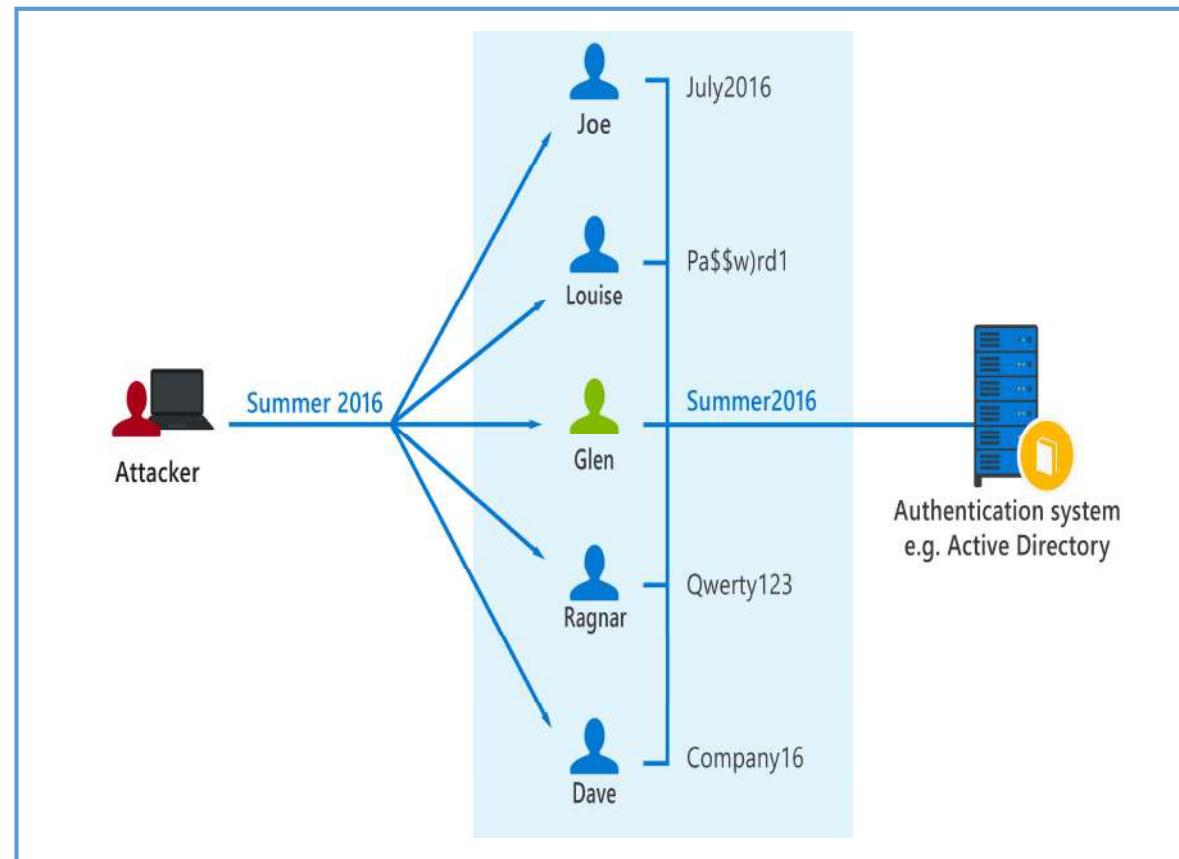
- Why is ***Identity*** important?
 - Concept of identity as a security perimeter
 - Is key behind authentication and authorization
- Why IAM?
 - Improve Operational Efficiency
 - IAM technology and processes can improve efficiency by automating user on-boarding and other repetitive tasks (e.g., self-service for users requesting password resets)
 - Regulatory security compliance management
 - Need to comply with various regulatory, privacy, and data protection requirements



Common identity attacks

Types of security threats:

- Password-based attacks
 - Many password-based attacks employ brute force techniques to gain unauthorized access, often using a dictionary
- Phishing
 - hacker sends an email that appears to come from a reputable source, instructing the user to sign in and change their password
- Spear phishing
 - a variant on phishing. Hackers build databases of information about users, which can be used to create highly credible emails



A password-spray attack – attacker sprays a commonly used password against multiple accounts



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 13: Cloud Security

Identity and Access Management (IAM)

- **Source Disclaimer:** Content for some of the slides is from the course Textbook:
 - *Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley & Sons, 2010*
- Some of the slides are taken from Microsoft Educator Learn Material (Microsoft Azure Security Technologies)
- Material for some of the other slides is from following book:
 - *Authentication: From Passwords to Public Keys, by Richard E. Smith*

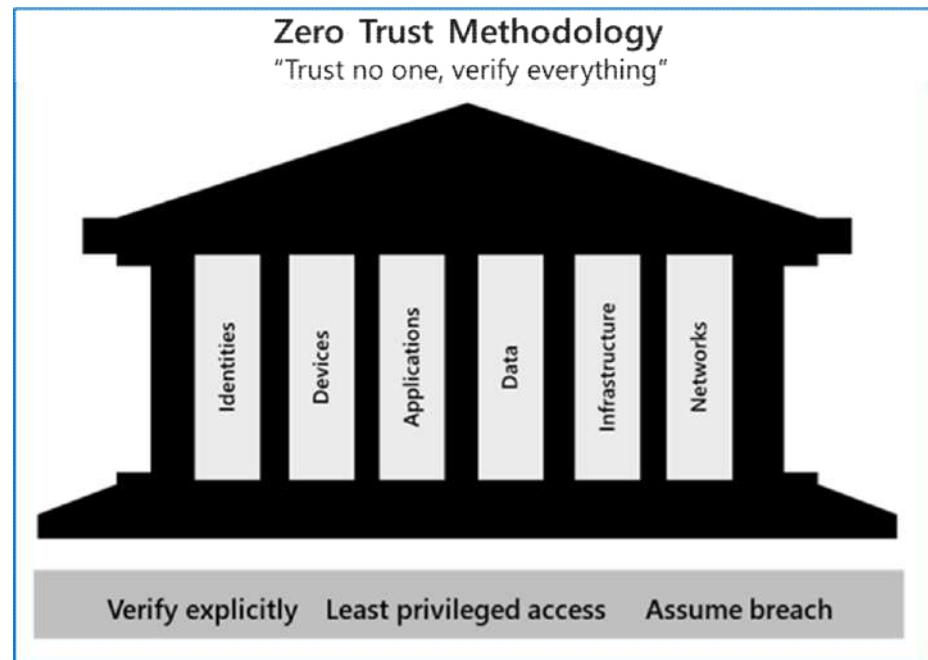


RECAP: AAAA

- *Authentication* is the testing or reconciliation of evidence of a user's identity. It establishes the user's identity and ensures that users are who they claim to be.
 - *Authorization* refers to rights and privileges granted to an individual or process that enable access to computer resources and information assets.
 - Auditing: To maintain operational assurance, organizations use two basic methods: system audits and monitoring. These methods can be employed by the cloud customer, the cloud provider, or both, depending on asset architecture and deployment
 - A *system audit* is a one-time or periodic event to evaluate security.
 - *Monitoring* refers to an ongoing activity that examines either the system or the users, such as intrusion detection
 - An *audit trail or log* is a set of records that collectively provide documentary evidence of different cloud operations
 - *Accountability* is the ability to determine the actions and behaviors of a single individual within a cloud system
 - Accountability is related to the concept of *nonrepudiation*, wherein an individual cannot successfully deny the performance of an action
 - Audit trails and logs support accountability
-

RECAP: The Zero-trust methodology

- Zero Trust guiding principles
- Verify explicitly
- Least privileged access
- Assume breach
- Six foundational pillars
- **Identities** may be users, services, or devices.
- **Devices** create a large attack surface as data flows.
- **Applications** are the way that data is consumed.
- **Data** should be classified, labeled, and encrypted based on its attributes.
- **Infrastructure** whether on-premises or cloud based, represents a threat vector.
- **Networks** should be segmented.





IAM: Overview

- What is IAM?
 - IAM = Identity Management (IdM) and Access Management (AcM)
 - Identity Management (IdM)
 - User Identities (Unique)
 - Account Management
 - Authentication
 - Access Management (AcM)
 - Roles and Privileges
 - Authorization
 - Access Control
-



IAM: Overview (2)

- Why is ***Identity*** important?
 - Concept of ***Identity*** as a security perimeter
 - Is key behind authentication and authorization
- Why IAM (tools and functions)?
 - Improve Operational Efficiency
 - IAM technology and processes can improve efficiency by automating user on-boarding and other repetitive tasks (e.g., self-service for users requesting password resets)
 - Regulatory security compliance management
 - Need to comply with various regulatory, privacy, and data protection requirements

Identity as the primary security perimeter

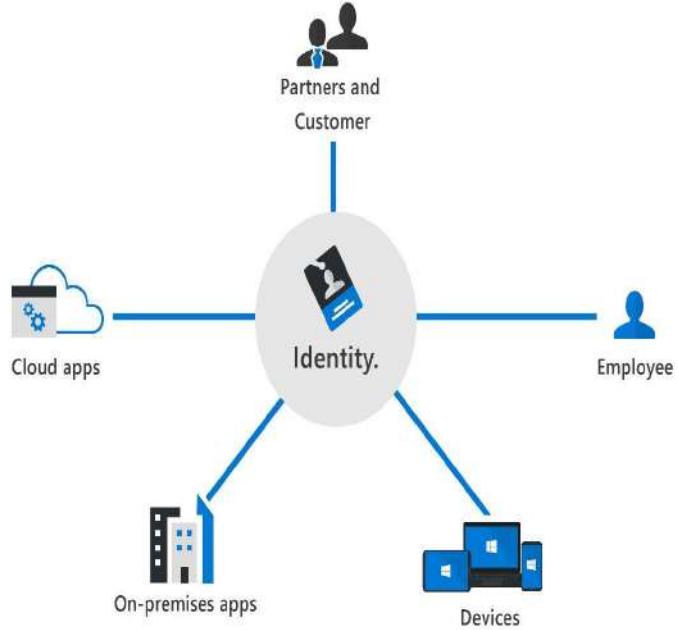
An identity is how someone or something can be verified and authenticated and may be associated with:

- User
- Application
- Device
- Other

Four pillars of identity:

- Administration
- Authentication
- Authorization
- Auditing

Identity is the new security perimeter

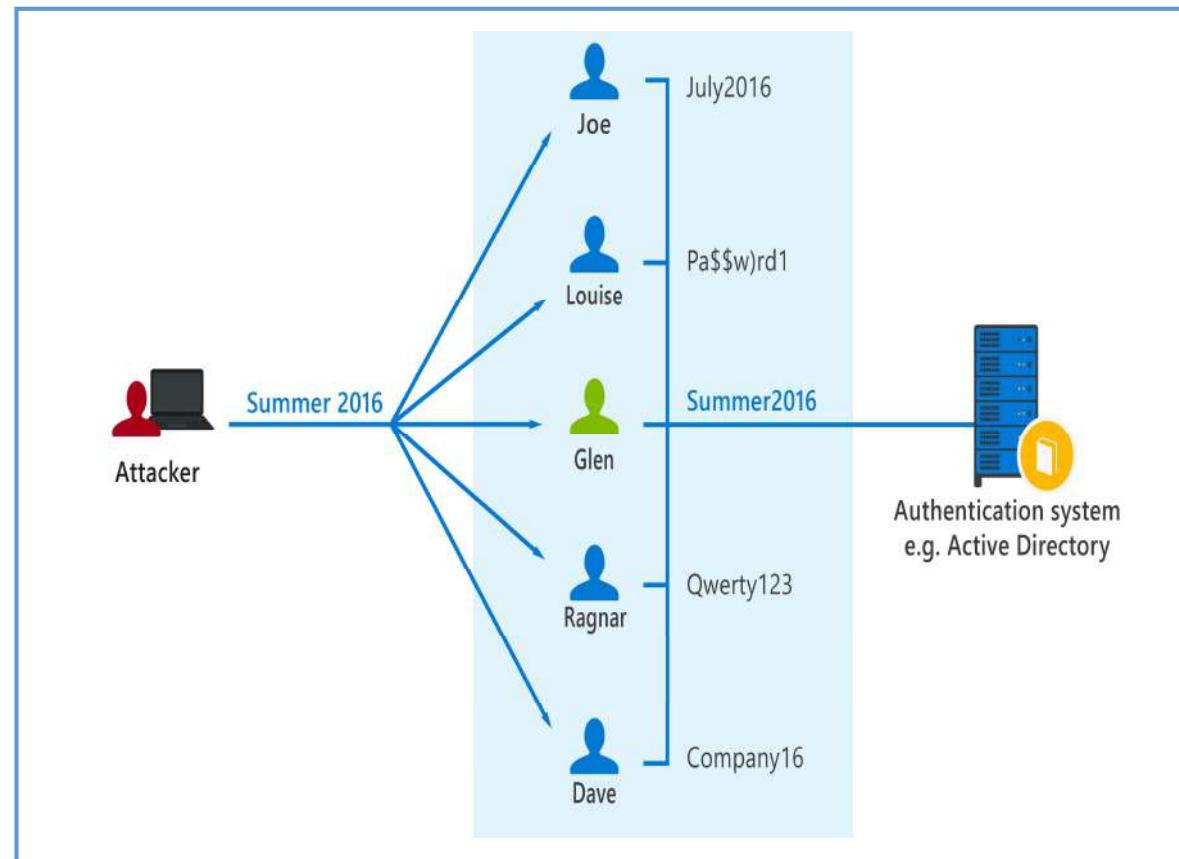


Identity has become the new security perimeter that enables organizations to secure their assets.

Common identity attacks

Types of security threats:

- Password-based attacks
 - Many password-based attacks employ brute force techniques to gain unauthorized access, often using a dictionary
- Phishing
 - hacker sends an email that appears to come from a reputable source, instructing the user to sign in and change their password
- Spear phishing
 - a variant on phishing. Hackers build databases of information about users, which can be used to create highly credible emails



A password-spray attack – attacker sprays a commonly used password against multiple accounts

Modern authentication and the role of the identity provider

- **Modern authentication** is an umbrella term for authentication and authorization methods between a client and a server.

At the center of modern authentication is the role of the **identity provider (IdP)**.



IdP offers authentication, authorization, and auditing services.



IdP enables organizations to establish authentication and authorization policies, monitor user behavior, and more.



A fundamental capability of an IdP and “modern authentication” is the support for single sign-on (SSO).



Microsoft Azure Active Directory is an example of a cloud-based identity provider.



IAM: Overview (3)

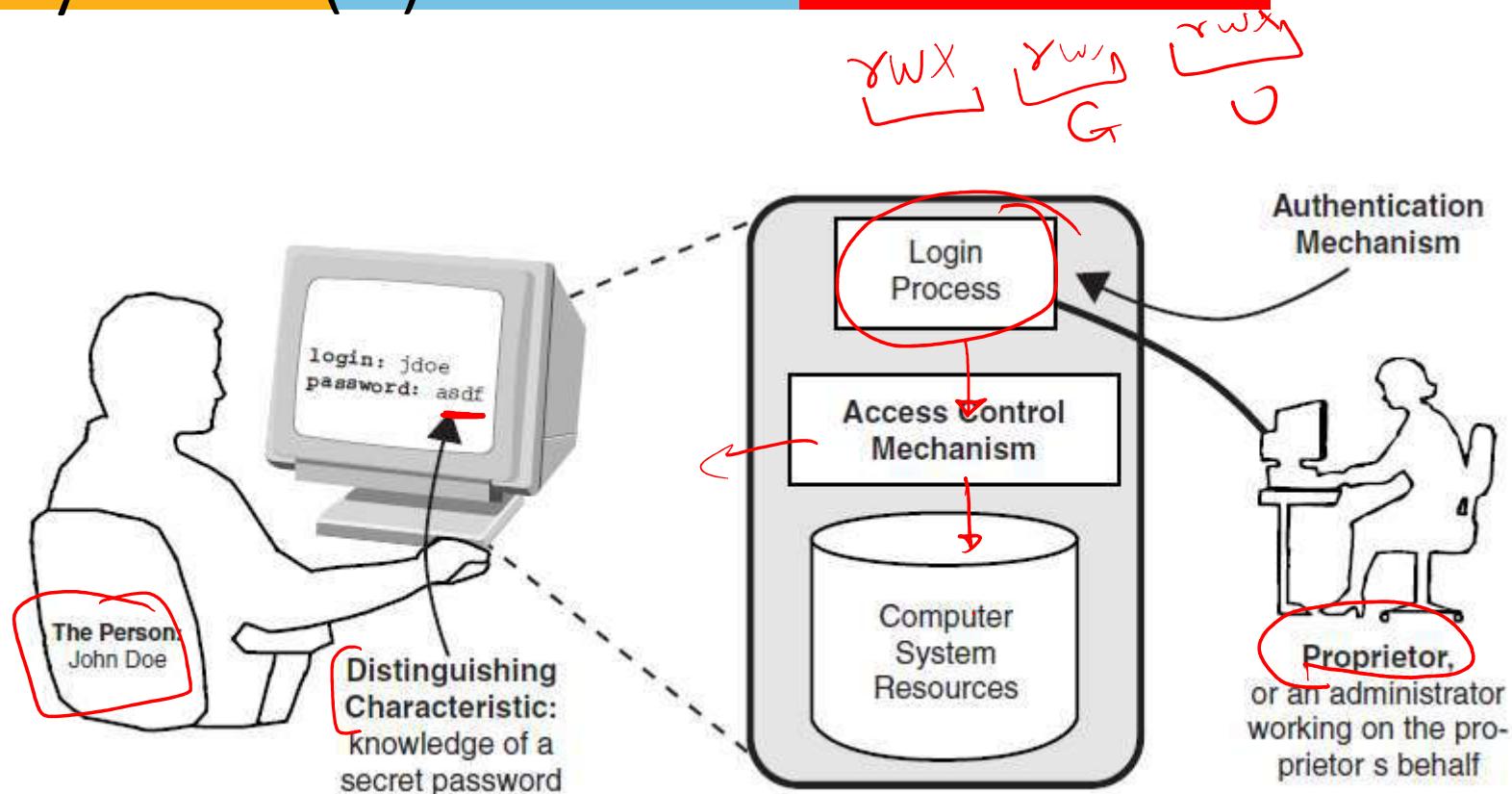
- IAM architecture encompasses several layers of technology, services, and processes.
- At the core of the *deployment architecture is a directory service (such as LDAP or Active Directory) that acts as a repository for the identity, credential, and user attributes of the organization's user pool.*
- The directory interacts with IAM technology components such as authentication, user management, provisioning, and identity services that support the standard IAM practice and processes within the organization.

Elements of an Authentication System

Authentication Element	Cave of the 40 Thieves	Password Login	Teller Machine	Web Server to Client
①	Person, principal, entity	Anyone who knew the password	Authorized user	Web site owner
②	Distinguishing characteristic, token, authenticator	The password "Open, Sesame"	Secret password	Public key within a certificate
③	Proprietor, system owner, administrator	The forty thieves	Enterprise owning the system	Certificate authority
④	Authentication mechanism	Magical device that responds to the words	Password validation software	Certificate validation software
⑤	Access control mechanism	Mechanism to roll the stone from in front of the cave	Login process, access controls	Allows banking transactions Browser marks the page "secure"

Source: "Authentication: From Passwords to Public Keys" by Richard E. Smith

Elements of an Authentication System (2)



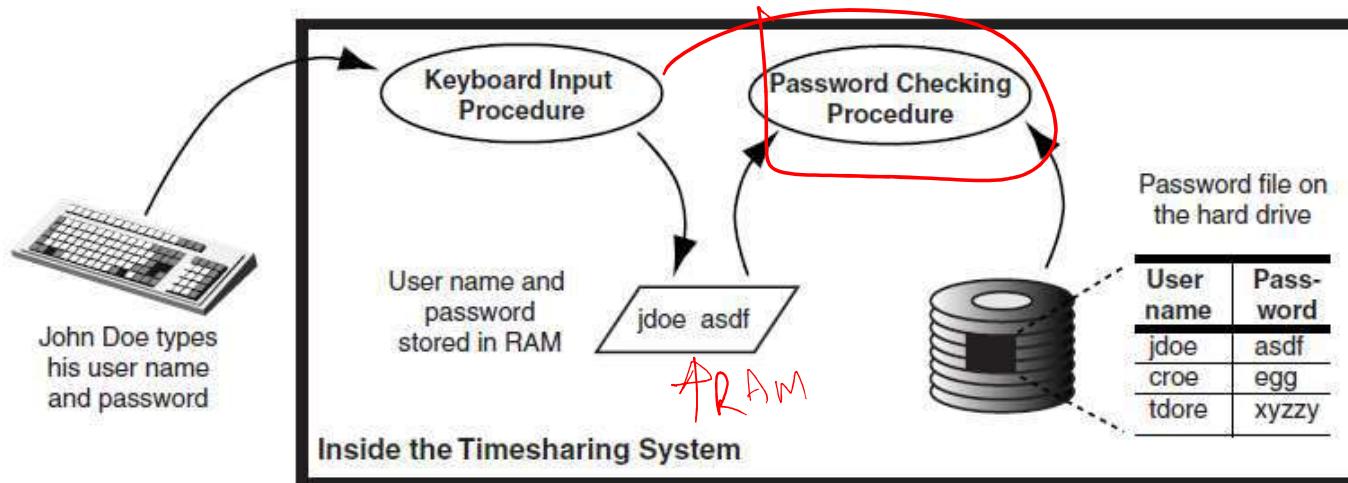
Source: "Authentication: From Passwords to Public Keys" by Richard E. Smith



Authentication Factors

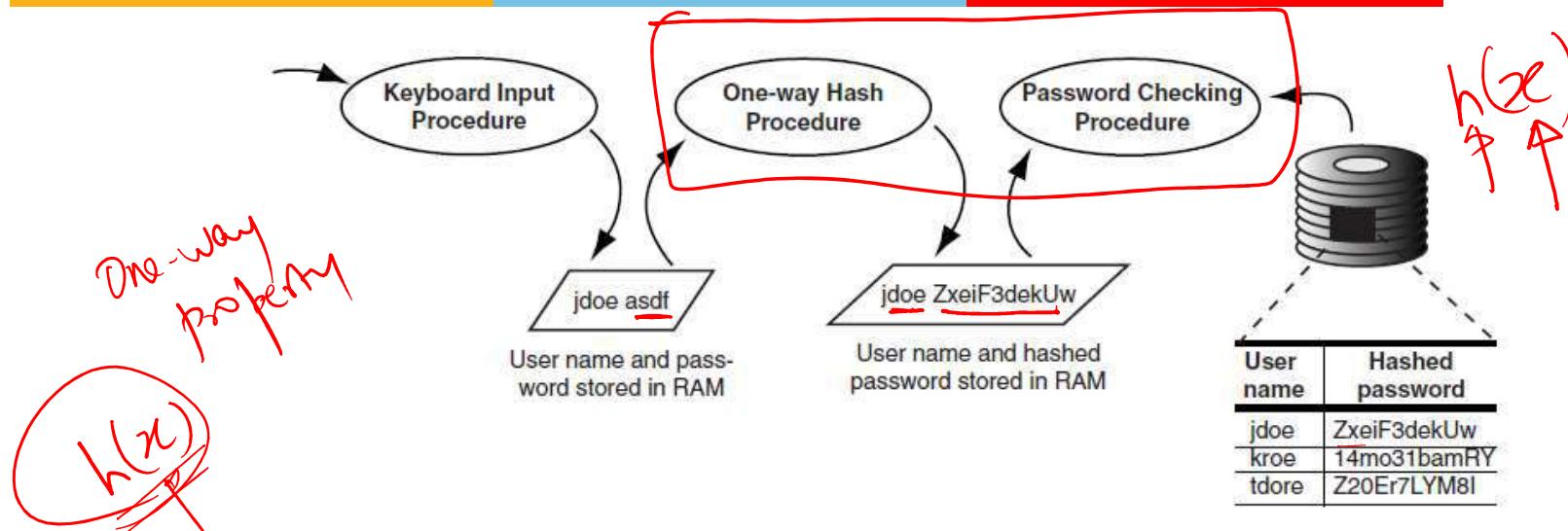
- Authentication can be based on the following three **factor** types:
 - Type 1 — Something you know, such as a personal identification number (PIN) or password
 - Type 2 — Something you have, such as an ATM card or smart card
 - Type 3 — Something you are (physically), such as a fingerprint or retina scan
- 2FA – Two factors are employed
- MFA – More than 2 factors used
 - Factors of the same types are not considered as 2FA or MFA

Authentication via Passwords



- Type 1 Authentication (*Something you know*)
- Passwords can be either:
 - Static: Same password used at each Logon
 - Dynamic: Different password used for each Logon (e.g. OTP)
 - The changing of passwords can also fall between these two extremes (e.g monthly, quarterly etc)

Authentication via Passwords (2)



- Passwords can be stolen from the file-system:
 - Introduction of Hashed Passwords
 - Dictionary Attacks
 - Use of multi-word passwords can be more robust against dictionary attacks as against single word passwords (which are relatively simpler to break)
 - Guessing attacks, Social engineering attacks, Sniffing attacks.....

Authentication via Tokens

Tokens, in the form of small, hand-held devices, are used to provide passwords. The following are the four basic types of tokens:

- Static password tokens
 - 1. Owners authenticate themselves to the token by typing in a secret password.
 - 2. If the password is correct, the token authenticates the owner to an information system.
- Synchronous dynamic password tokens, clock-based
 - 1. The token generates a new, unique password value at fixed time intervals that is synchronized with the same password on the authentication server (this password is the time of day encrypted with a secret key).
 - 2. The unique password is entered into a system or workstation along with an owner's PIN.
 - 3. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is valid and that it was entered during the valid time window.

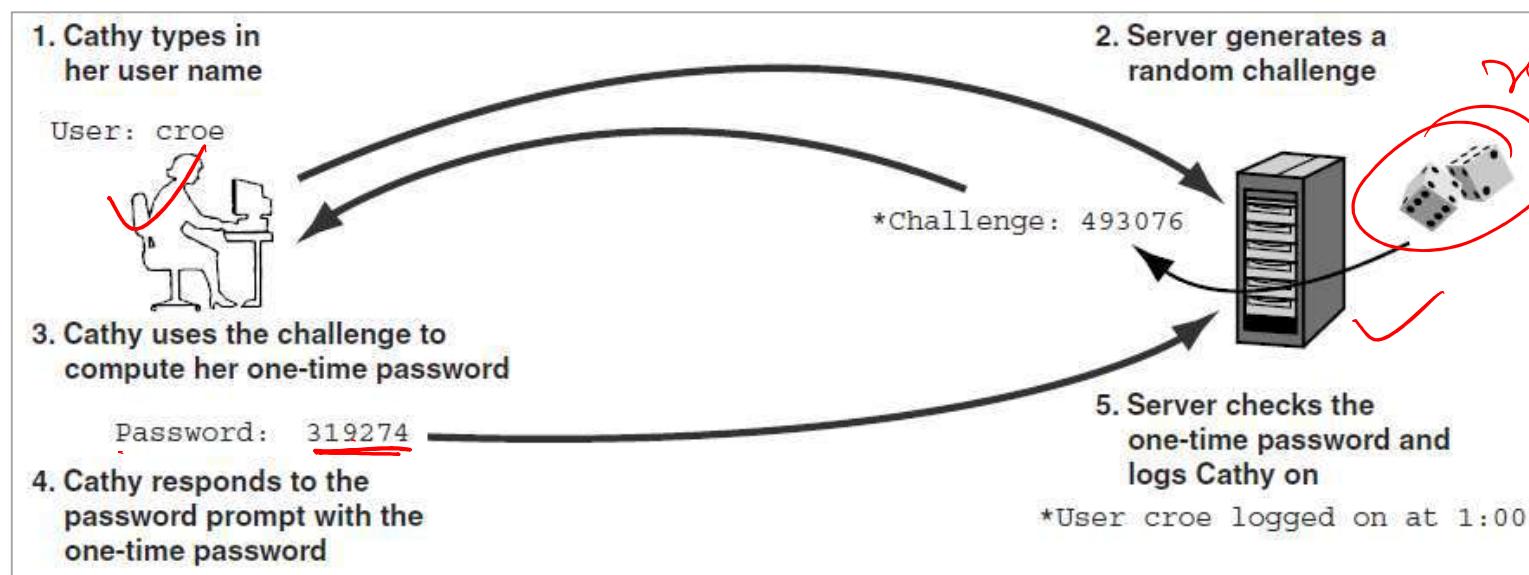


for me
Challenge Sys
Reph

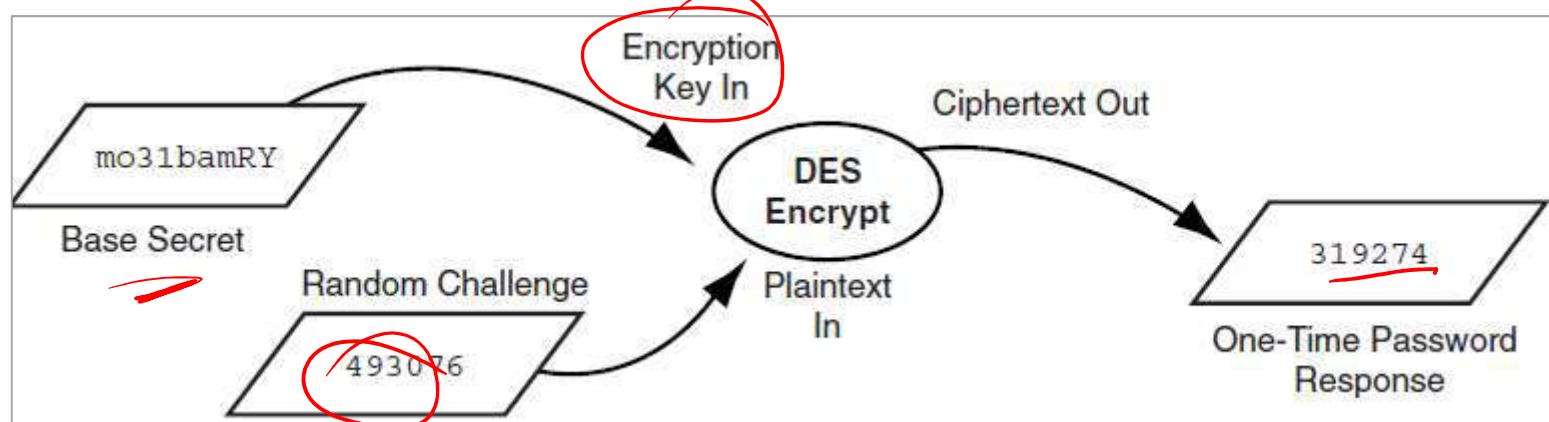
Authentication via Tokens (2)

- Synchronous dynamic password tokens, counter-based
 - 1. The token increments a counter value that is synchronized with a counter in the authentication server.
 - 2. The counter value is encrypted with the user's secret key inside the token and this value is the unique password that is entered into the system authentication server.
 - 3. The authentication entity in the system or workstation knows the user's secret key and the entity verifies that the entered password is valid by performing the same encryption on its identical counter value.
- Asynchronous tokens, challenge-response
 - 1. A workstation or system generates a random challenge string, and the owner enters the string into the token along with the proper PIN.
 - 2. The token performs a calculation on the string using the PIN and generates a response value that is then entered into the workstation or system.
 - 3. The authentication mechanism in the workstation or system performs the same calculation as the token using the owner's PIN and challenge string and compares the result with the value entered by the owner. If the results match, the owner is authenticated.

Challenge-Response



random



Authentication via Memory Cards and Smart Cards

Type 2 Authentication (*Something you have*)

- Memory cards provide nonvolatile storage of information, but they do not have any processing capability
 - A memory card stores encrypted passwords and other related identifying information.
 - An ATM card is an example of memory cards
- Smart cards provide even more capability than memory cards by incorporating additional processing power on the cards
 - These credit-card-size devices comprise microprocessor and memory
 - Are used to store digital signatures, private keys, passwords, and other personal information

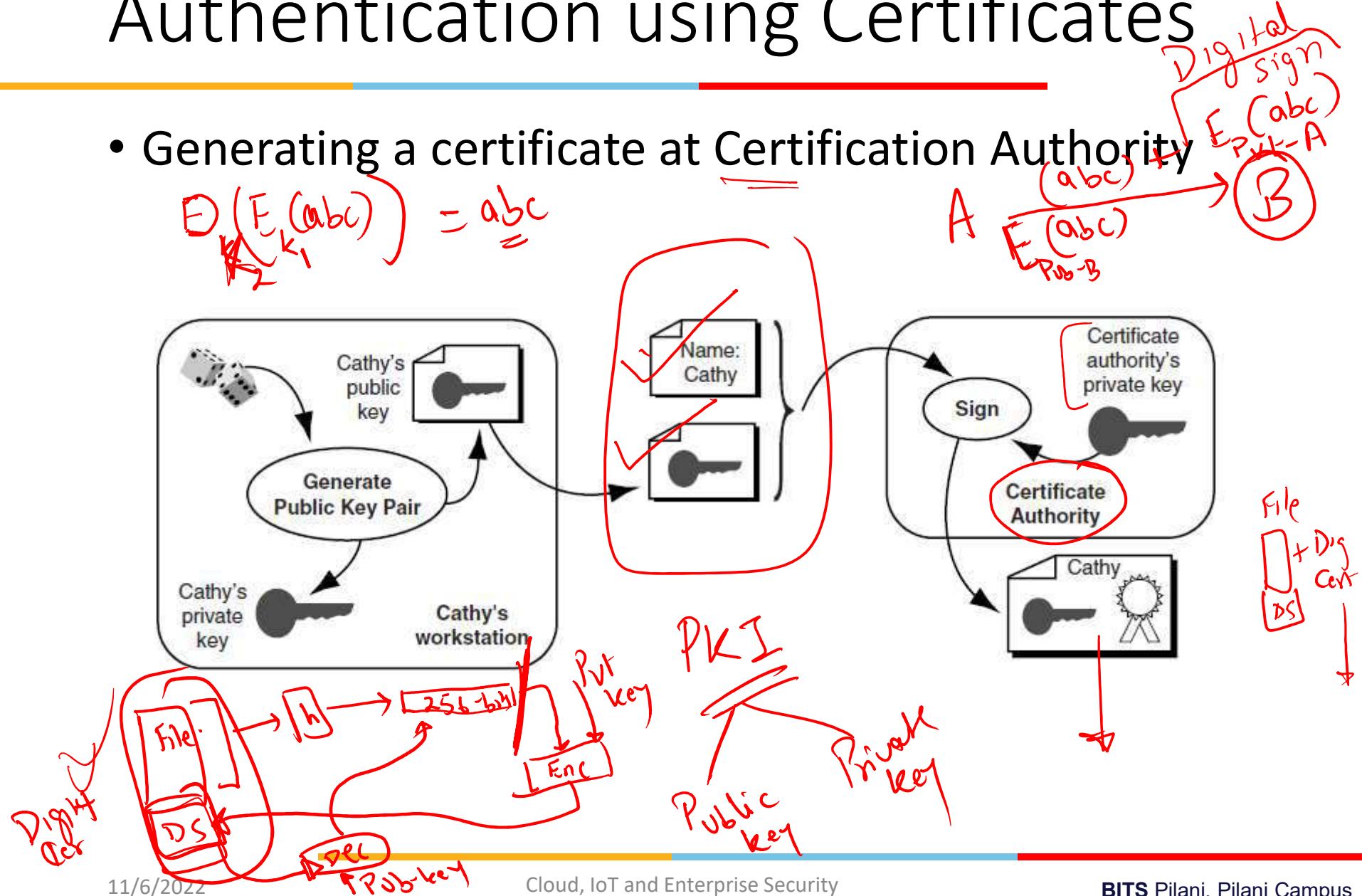


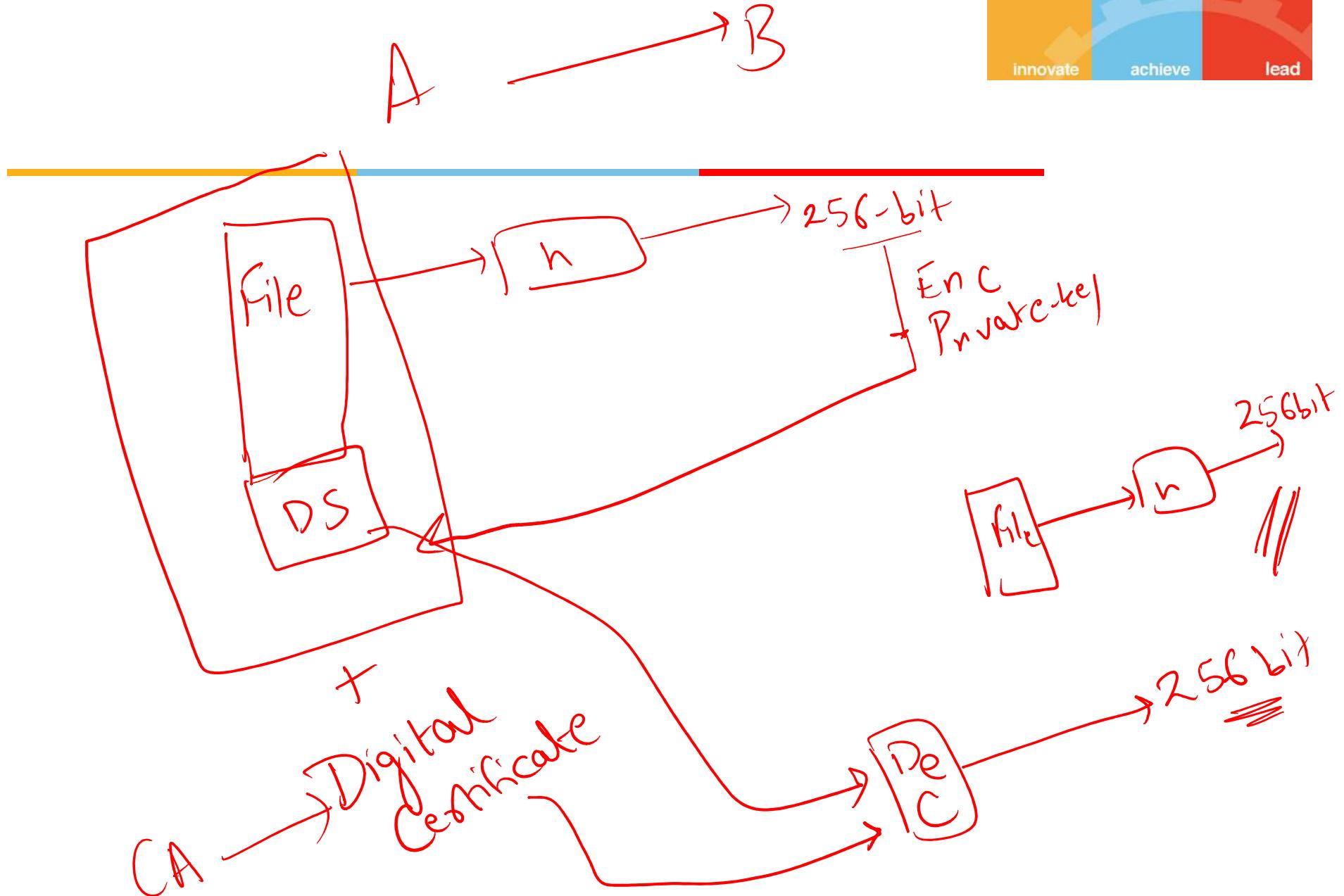
Authentication via Biometrics

- Type 3 authentication(*something you are*)
- In biometrics, identification is a one-to-many search of an individual's characteristics from a database of stored images
- There are three main performance measures in biometrics:
 - False rejection rate (FRR) or Type I Error — The percentage of valid subjects that are falsely rejected.
 - False acceptance rate (FAR) or Type II Error — The percentage of invalid subjects that are falsely accepted.
 - Crossover error rate (CER) — The percentage at which the FRR equals the FAR. The smaller the CER, the better the device is performing.
- In addition to the accuracy of the biometric systems, *Enrollment time, Throughput rate and Acceptability* are also other important measures
 - Enrollment Time is the time that it takes to initially register with a system by providing samples of the biometric characteristic to be evaluated. An acceptable enrollment time is around two minutes
 - The throughput rate is the rate at which the system processes and identifies or authenticates individuals. Acceptable throughput rates are in the range of 10 subjects per minute.
 - Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system. For example, a concern with retina scanning systems might be the exchange of body fluids on the eyepiece.

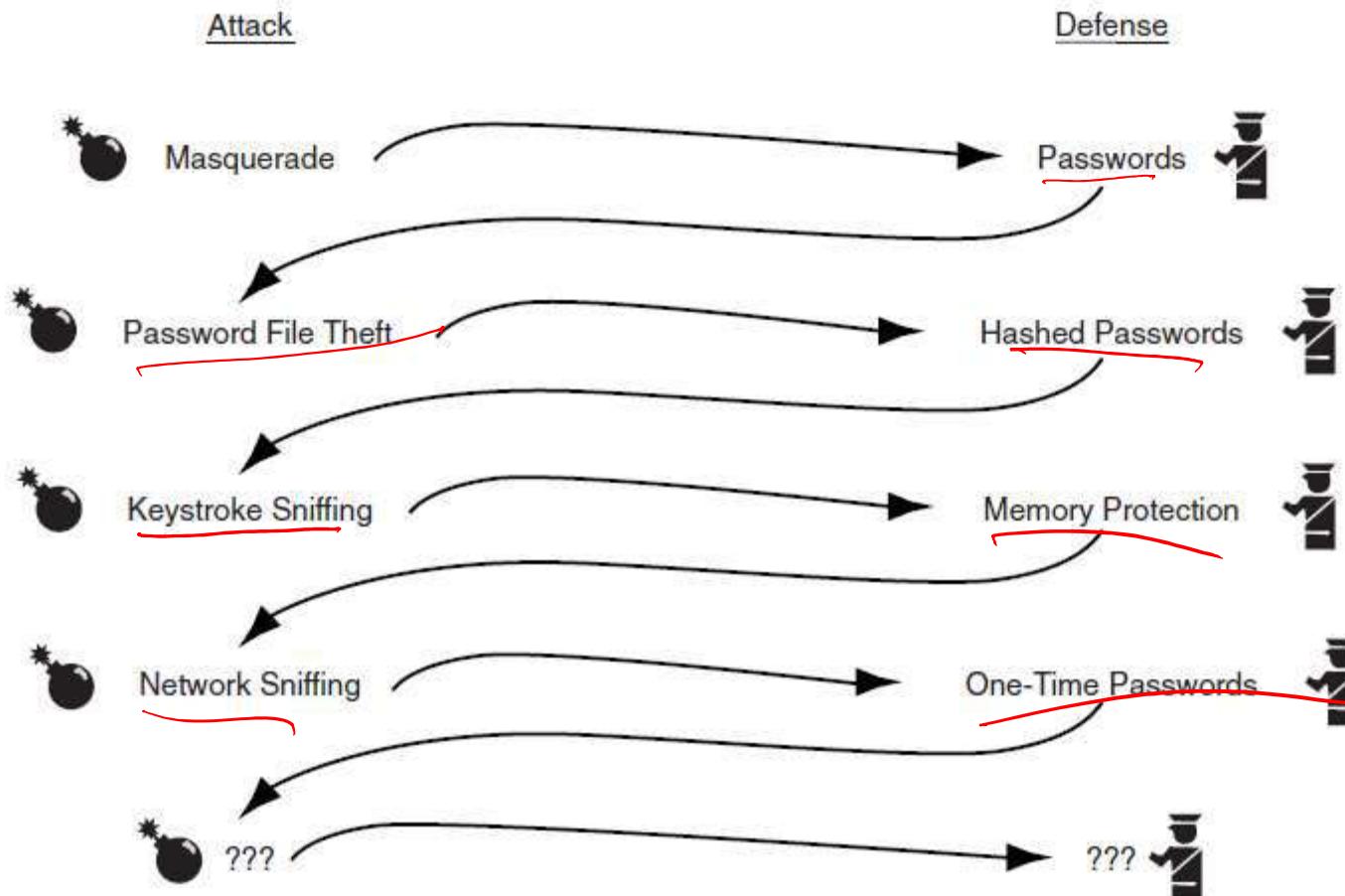
Authentication using Certificates

- Generating a certificate at Certification Authority





Evolving Attacks and Defense Systems



Source: "Authentication: From Passwords to Public Keys" by Richard E. Smith



Authentication Factors: Pros and Cons

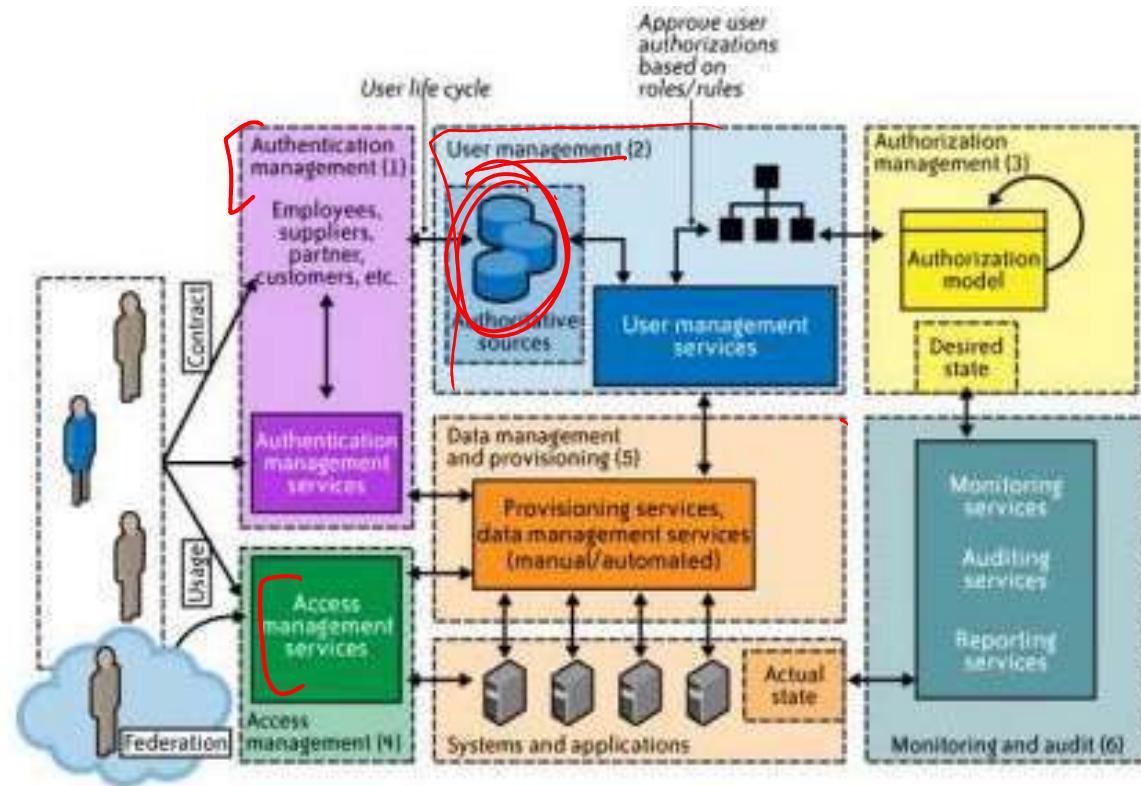
- Summary of strengths and weaknesses of different authentication factors

Factor	Benefits	Weaknesses	Examples
Something you know: password	Cheap to implement, portable	Sniffing attacks, Can't detect sniffing attacks, Passwords are either easy to guess or hard to remember, Cost of handling forgotten passwords	Password, PIN, Safe combination
Something you have: token	Hardest to abuse	Expensive, Can be lost or stolen, Risk of hardware failure, Not always portable	Token, Smart card, Secret data embedded in a file or device, Mechanical key
Something you are: biometric	Easiest to authenticate with, portable	Expensive, Replay threats, Privacy risks, Characteristic can't be changed, False rejection of legitimate users, Characteristic can be injured	Fingerprint, Eye scan, Voice recognition, Photo ID

Implementing IdM

Typical undertakings in putting identity management in place include the following:

- Establishing a database of identities and credentials
- Managing users' access rights
- Enforcing security policy
- Developing the capability to create and modify accounts
- Setting up monitoring of resource accesses
- Installing a procedure for removing access rights
- Providing training in proper procedures



The concept of directory services and Active Directory

A directory is a hierarchical structure that stores information about objects on the network.



A directory service stores directory data and makes it available to network users, administrators, services, and applications.



The best-known service of this kind is Active Directory Domain Services (AD DS), a central component in organizations with on-premises IT infrastructure.



Azure Active Directory is the evolution of identity and access management solutions, providing organizations an Identity as a Service (IDaaS) solution for all their apps across cloud and on-premises.



The concept of Federated Services

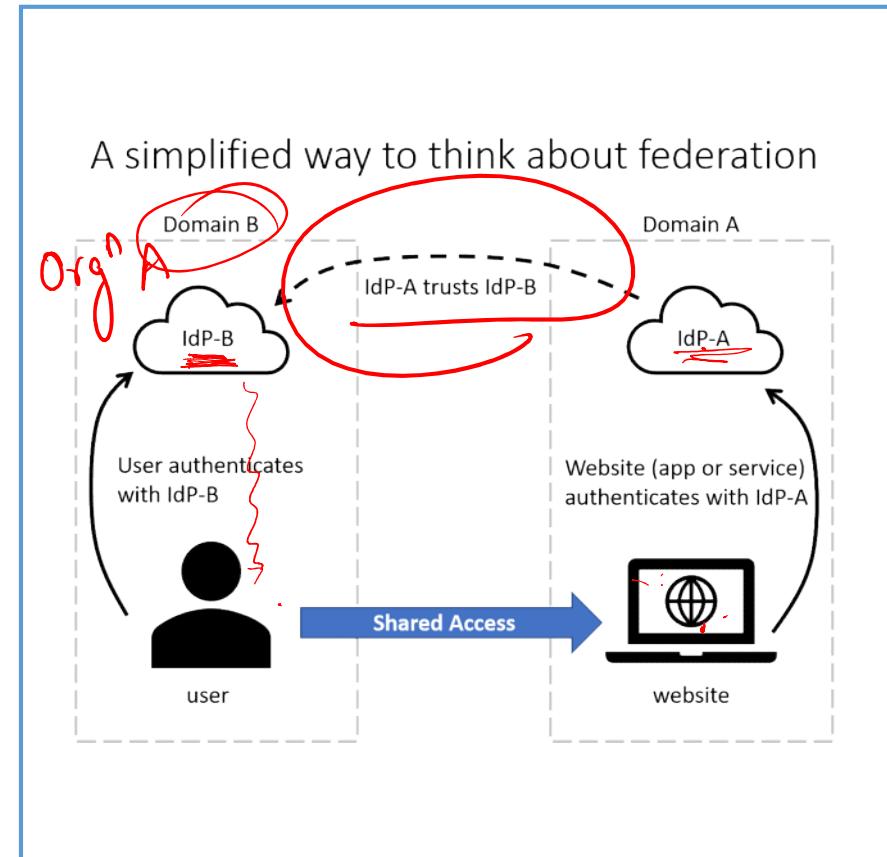
Simplification method of federation scenario:

The website uses the authentication services of IdP-A

The user authenticates with IdP-B

IdP-A has a trust relationship configured with IdP-B

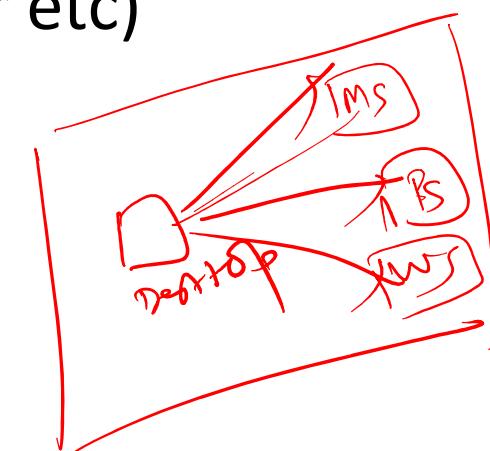
When the user's credentials are passed to the website, the website trusts the user and allows access



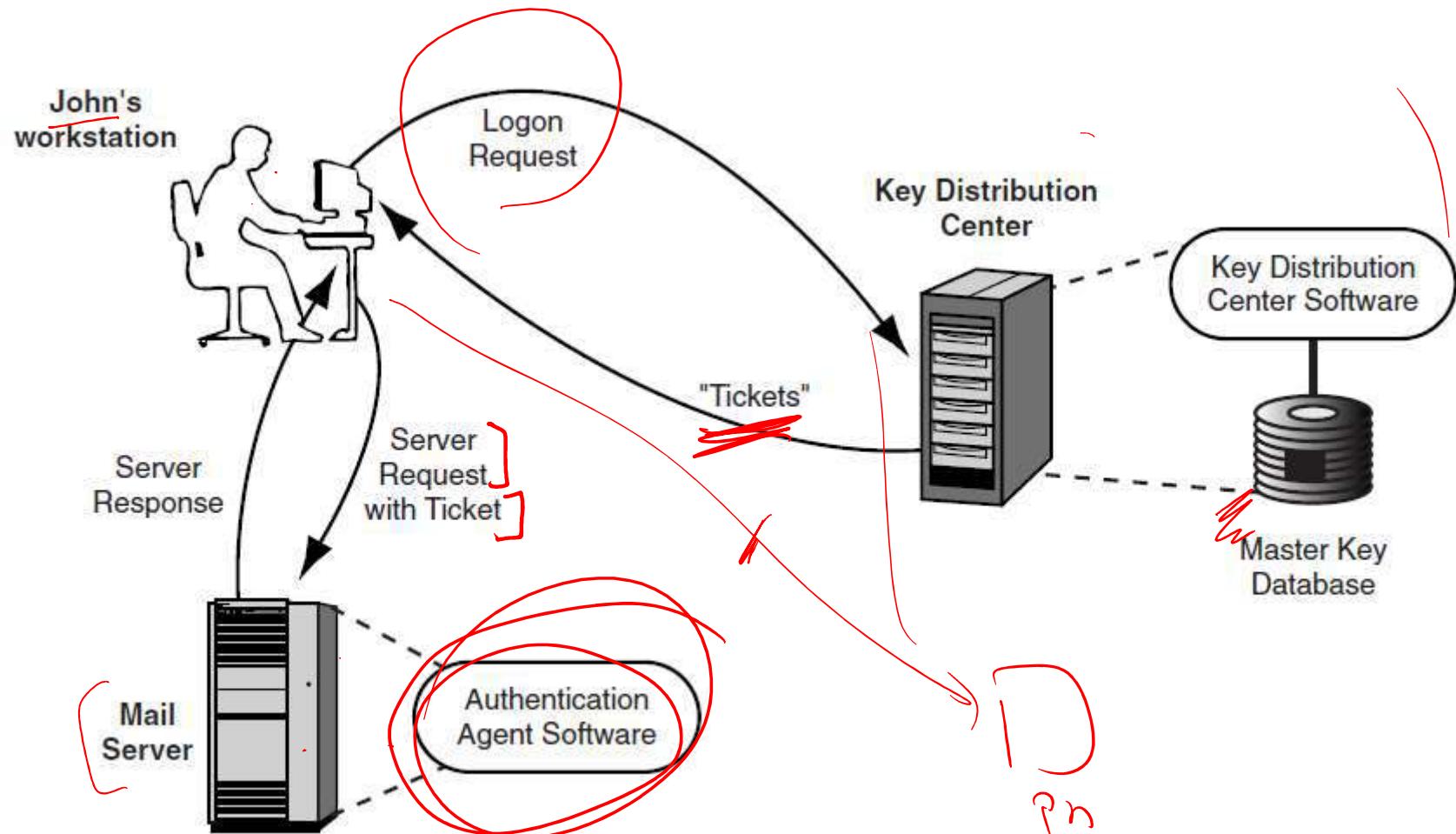
Kerberos and Crypto Tokens

- Kerberos provides a mechanism to authenticate and share temporary secret keys between cooperating processes
- Enables Indirect authentication with a Key Distribution Center (KDC)
- KDC issues tickets for authentication to different services (e.g. a mail server, print server etc)

SSD

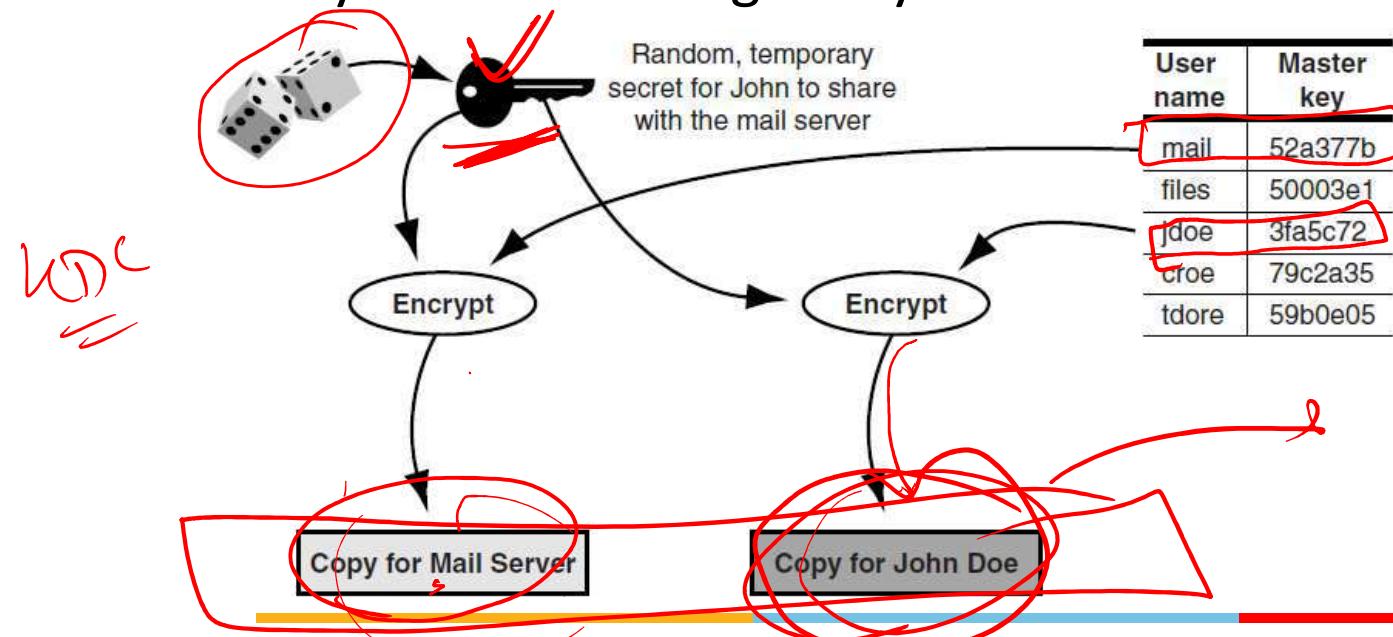


Kerberos KDC



Tickets

- Each trusted site has a unique *master key* that it shares with the KDC
 - The master key allows each site to talk to the KDC safely
 - In addition, the KDC can cryptographically “package” temporary keys using the master keys so that one site can safely forward the right keys to another site

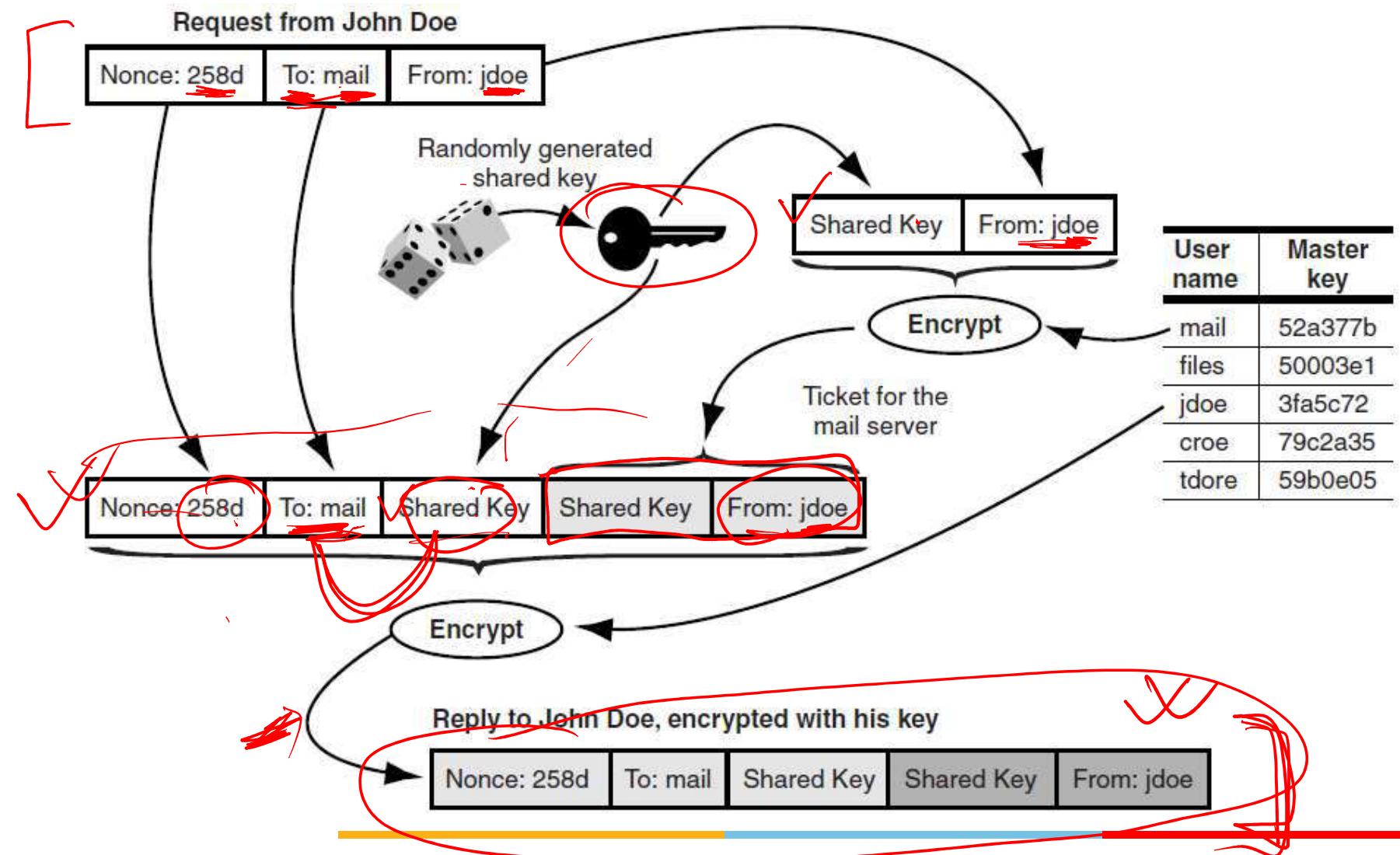




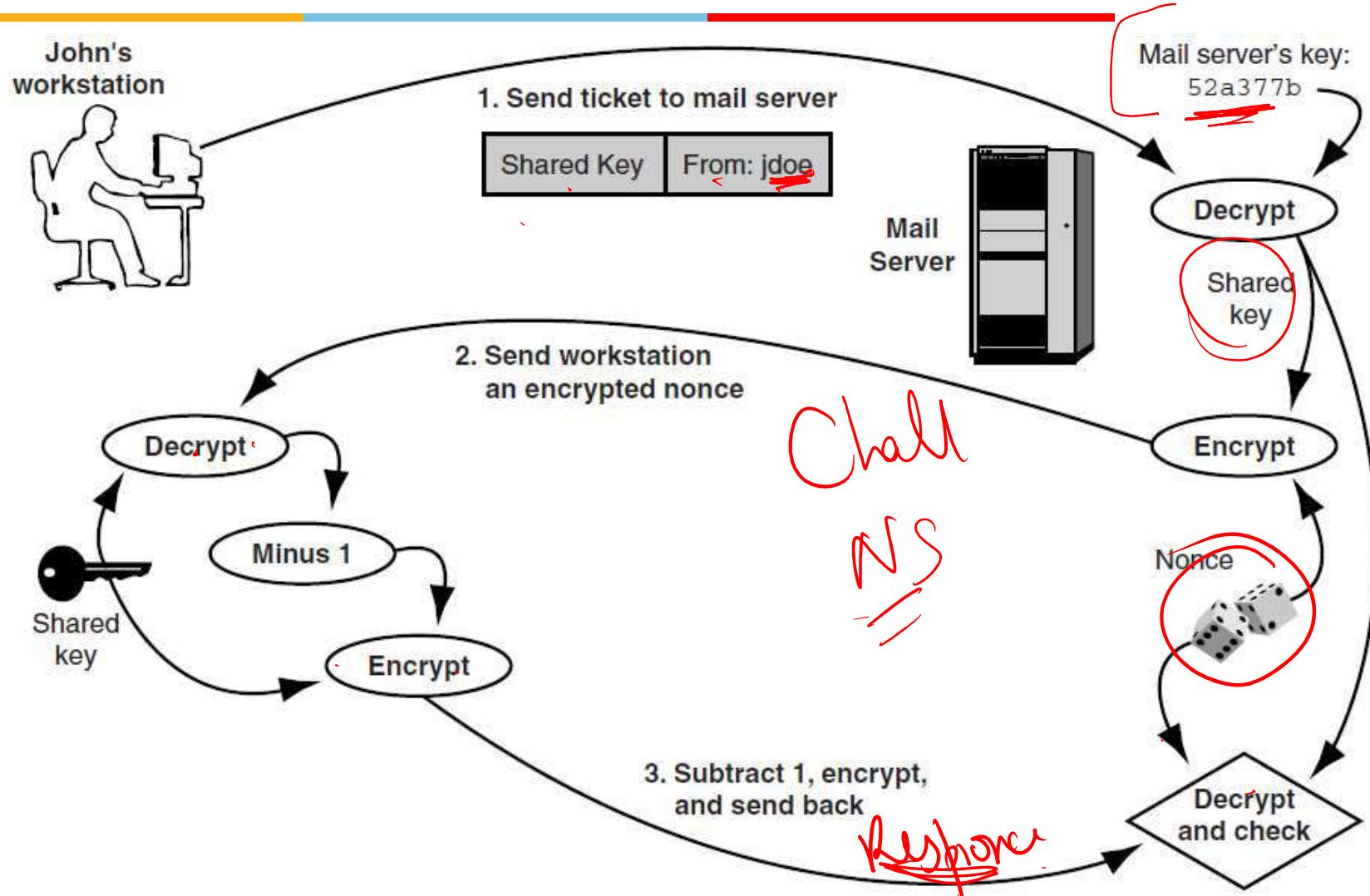
Extensions to Basic KDC

- To combat security problems, the protocol incorporates extra data in key distribution messages, notably message authentication codes, time stamps, and the names of senders and recipients
- In 1978, Needham and Schroeder published a simple protocol to efficiently address forgery problems faced by the KDC
 - This Needham-Schroeder (NS) protocol incorporates nonces and a challenge response to detect forged or replayed messages

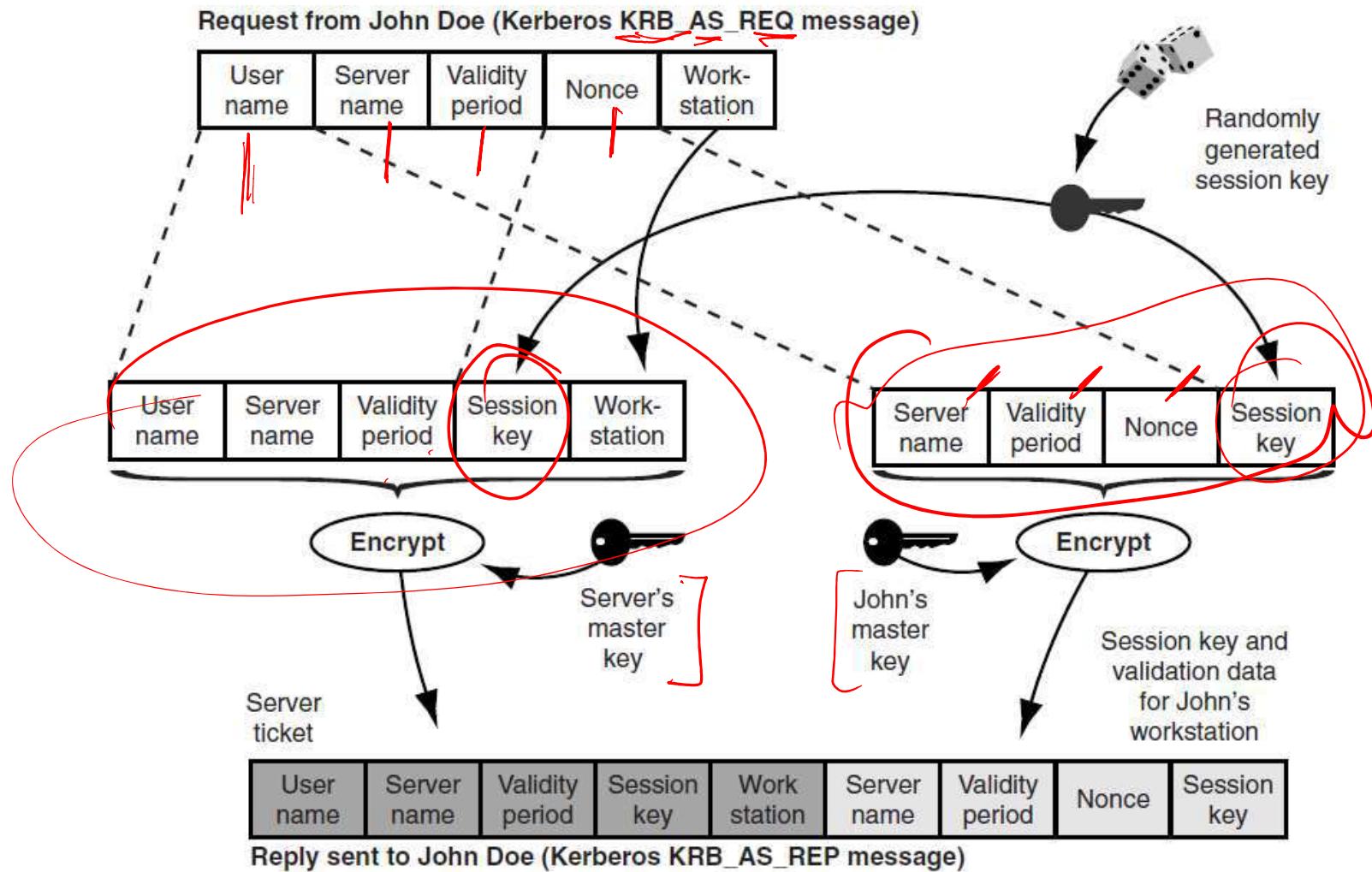
KDC with NS Extensions



Challenge-Response in NS Protocol

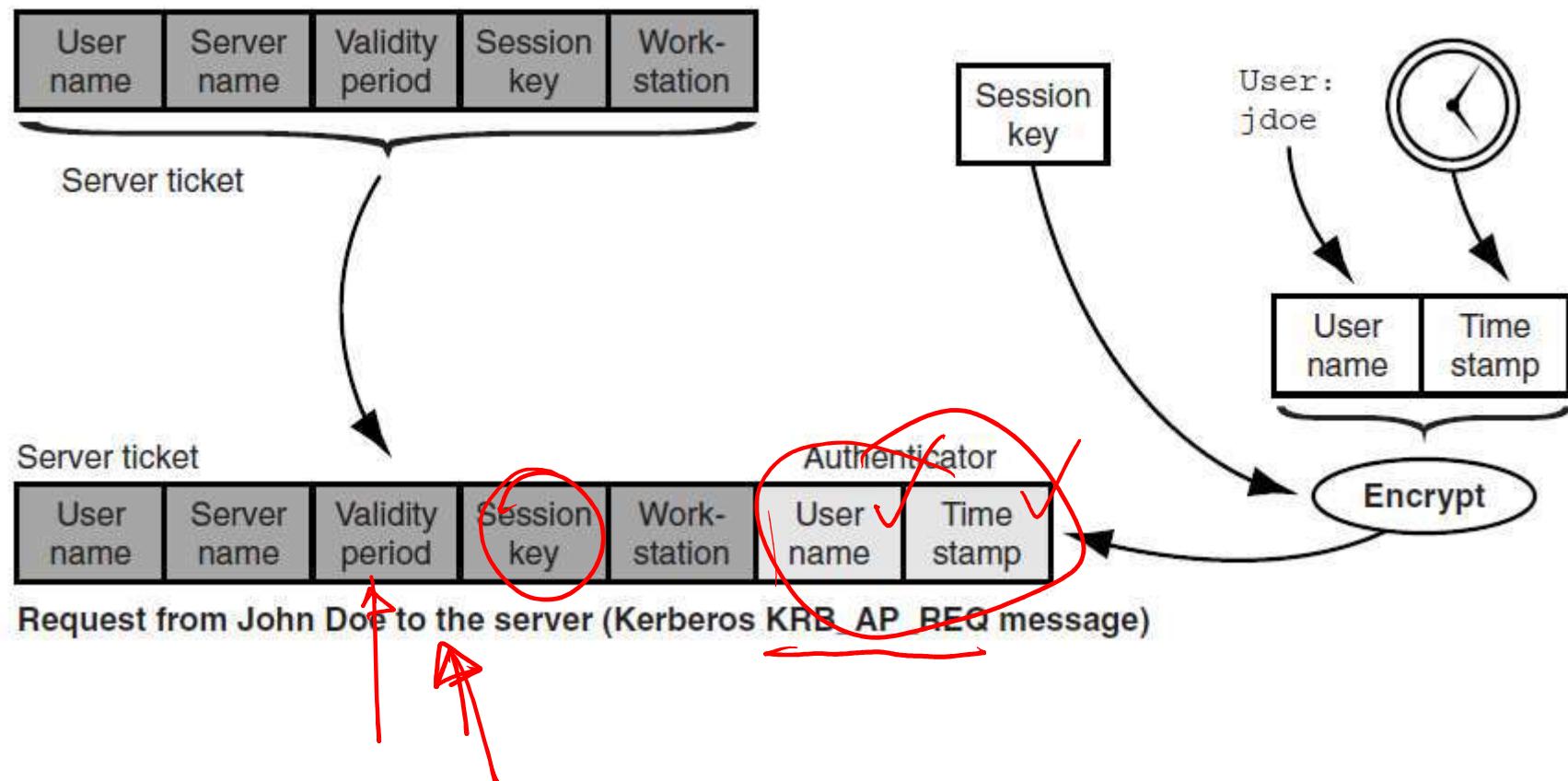


Kerberos Authentication Server



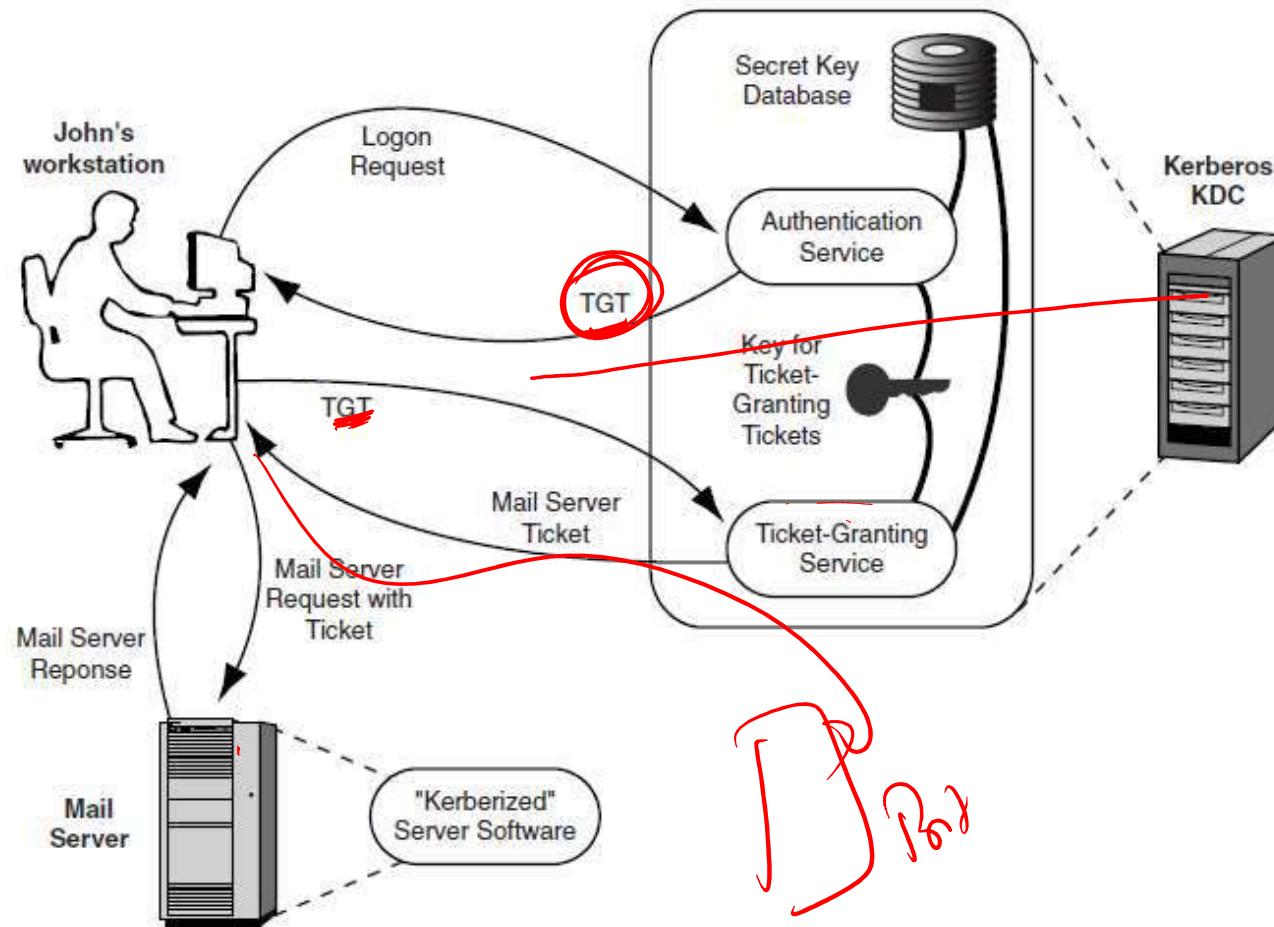


Authenticating to a Kerberized Server



Ticket Granting Ticket

- Kerberos KDC with 2-step ticket granting process





BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

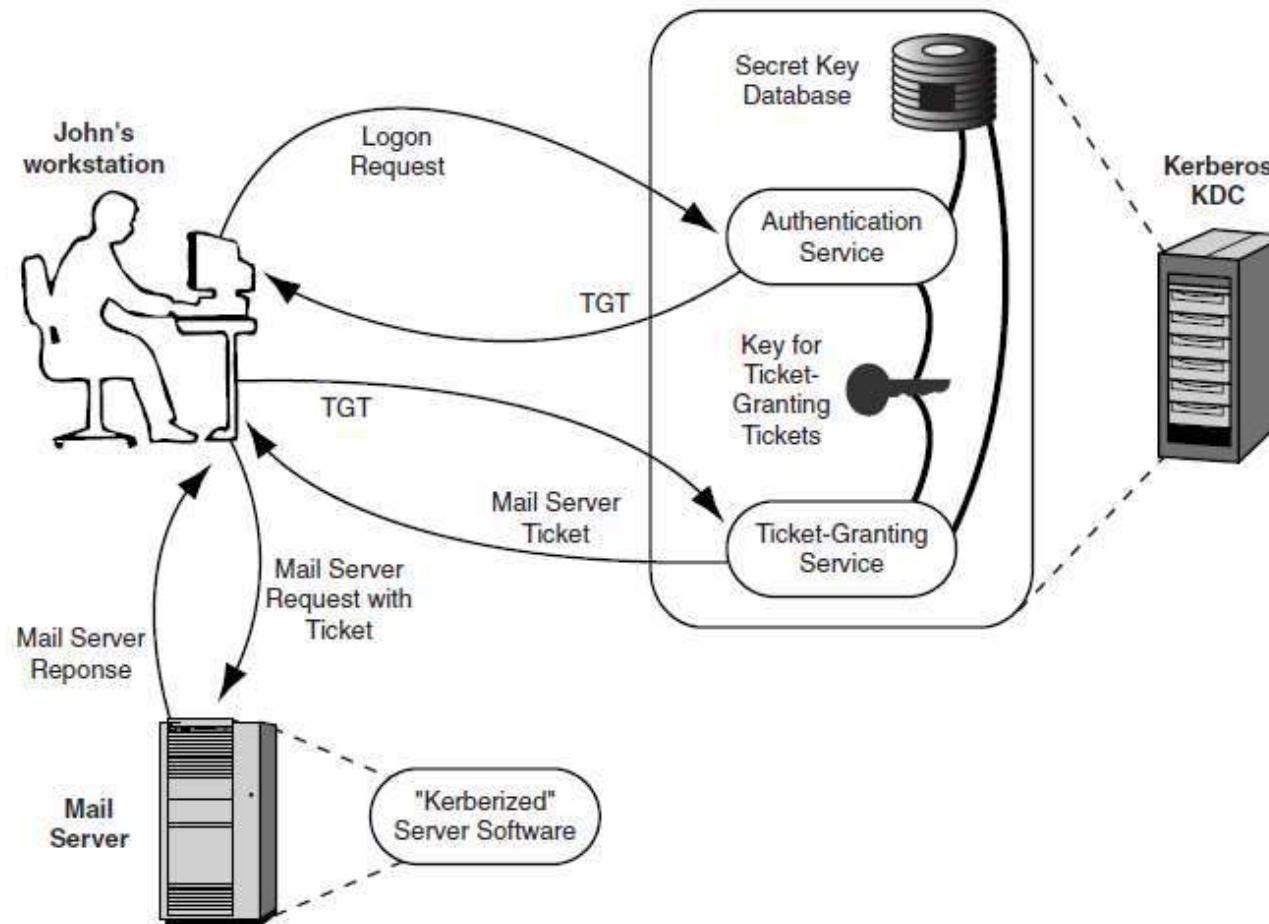
Lecture No. 14: Cloud Security

Identity and Access Management (IAM) - Continued

- **Source Disclaimer:** Content for some of the slides is from the course Textbook:
 - *Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley & Sons, 2010*
- Some of the slides are taken from Microsoft Educator Learn Material (Microsoft Azure Security Technologies)
- Material for some of the other slides is from following book:
 - *Authentication: From Passwords to Public Keys, by Richard E. Smith*

RECAP: Kerberos

- Kerberos KDC with 2-step ticket granting process





BITS Pilani

Pilani Campus



IAM Protocols and Standards for Cloud Services



IAM for Cloud Services

- Lot of Enterprises are embracing and adopting Cloud Services
- Multiple IAM Standards and Protocols help organizations implement efficient User Access Management practices in the cloud
 - Offer a SSO experience and avoid duplication of identity, attributes and/or credentials → [SAML](#)
 - Support automatic (De-)Provisioning of User Accounts → [SPML](#)
 - Enforce privilege and entitlement-based Access Control → [XACML](#)
 - Integrate applications / cloud services without sharing credentials → [OAuth 2.0](#)
 - E.g. Authorize cloud service X to access my data in cloud service Y without disclosing my credentials to X



SAML

- **Security Assertion Markup Language (SAML, pronounced *sam-el*)**
 - An XML-based, open-standard data format for exchanging authentication and authorization data between parties
 - In particular, used between an **identity provider (IdP)** and a **service provider (SP)**
- SAML is a product of the **OASIS*** Security Services Technical Committee

***Organization for the Advancement of Structured Information Standards (OASIS)** is a global nonprofit consortium that works on the development, convergence, and adoption of standards for security, Internet of Things, energy, content technologies, emergency management, and other areas.



SAML Principles

- SAML Roles: the specification defines three roles:
 - the principal (typically a user),
 - the Identity provider (IdP), and
 - the service provider (SP)
- SAML Use Case:
 1. Principal requests a service from the service provider
 2. Service provider requests and obtains an identity assertion from the identity provider
 3. On the basis of this assertion, the service provider can make an access control decision
 - i.e. it can decide whether to perform some service for the connected principal
 4. Before delivering the identity assertion to the SP, the IdP may request some information from the principal – such as a user name and password – in order to authenticate the principal

SAML does not specify the method of authentication at the identity provider; it may use a username and password, or other form of authentication, including multi-factor authentication

One identity provider may provide SAML assertions to many service providers. Similarly, one SP may rely on and trust assertions from many independent IdPs.

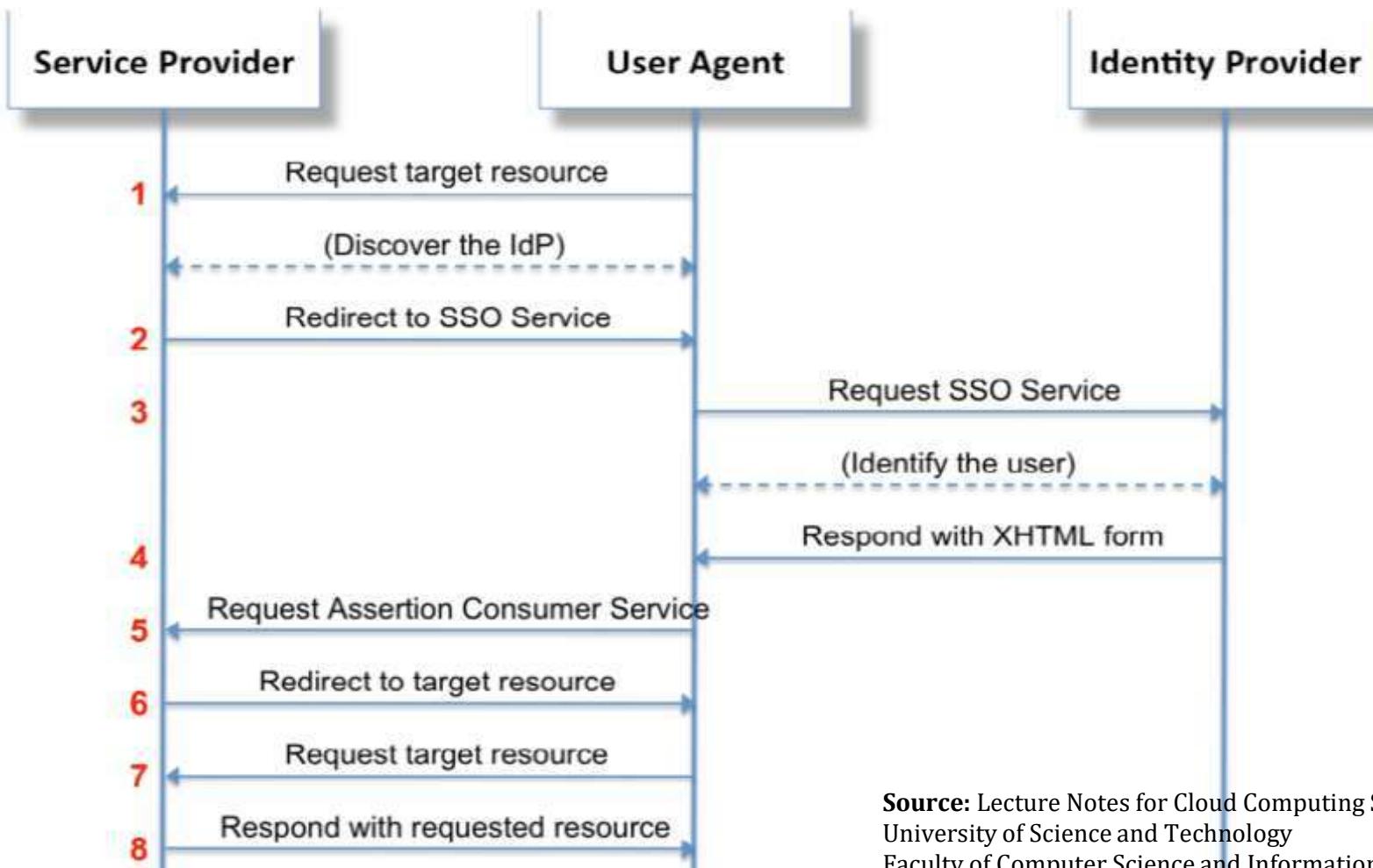


Web Browser SSO using SAML

- The primary SAML use case is the Web Browser Single Sign-On (SSO), where a user using a user agent (usually a web browser) requests a web resource protected by a SAML service provider
- What is SSO?
 - Single sign-on (SSO) is a property of access control of multiple related, yet independent, software systems.
 - With this property, a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system.
 - This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on (directory) servers.

Source: Lecture Notes for Cloud Computing Security
University of Science and Technology
Faculty of Computer Science and Information Technology

Message Flow



Source: Lecture Notes for Cloud Computing Security
University of Science and Technology
Faculty of Computer Science and Information Technology



SPML

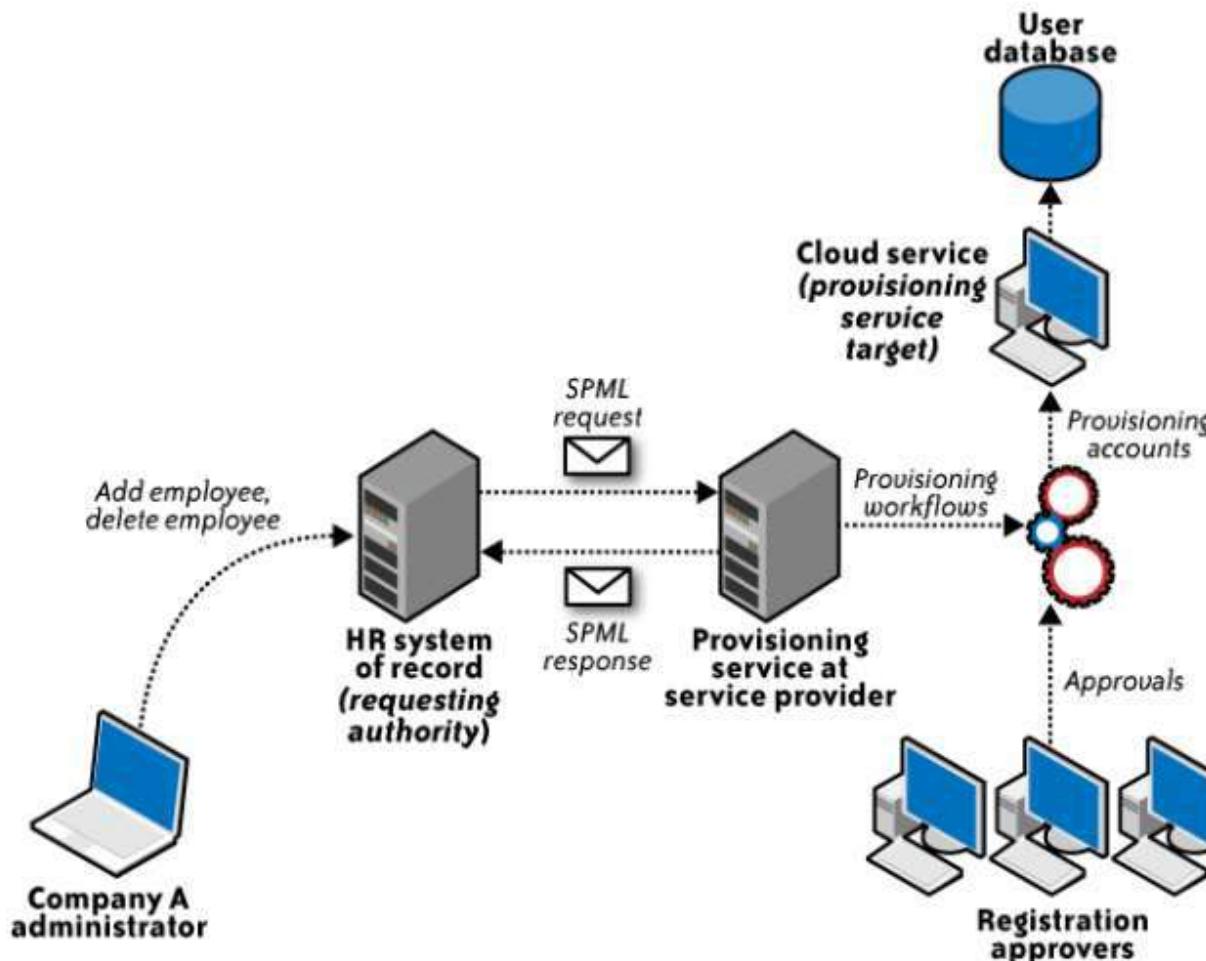
- Service Provisioning Markup Language
 - XML-based framework developed by OASIS
 - Used to provision user accounts and profiles with the cloud service
 - Enables “just-in-time provisioning” to create accounts for new users in real time (instead of pre-registering user accounts)
- SPML helps achieve the below twin objectives:
 - Automate IT tasks for user provisioning
 - Enables interoperability between different provisioning systems using standard SPML interfaces



SPML Principles

- SPML Roles:
 - Requesting Authority (RA)
 - The client in SPML
 - Provisioning Service Point (PSP)
 - listens to the request from the RA, processes it, and returns a response to the RA
 - Provisioning Service Target (PST)
 - the actual resource on which the action is taken
 - E.g. an LDAP directory that stores an organization's user accounts, or a ticketing system used to issue access tickets

SPML Message Flow



Source: Cloud Security and Privacy, by Tim Mather, Subra and Latif

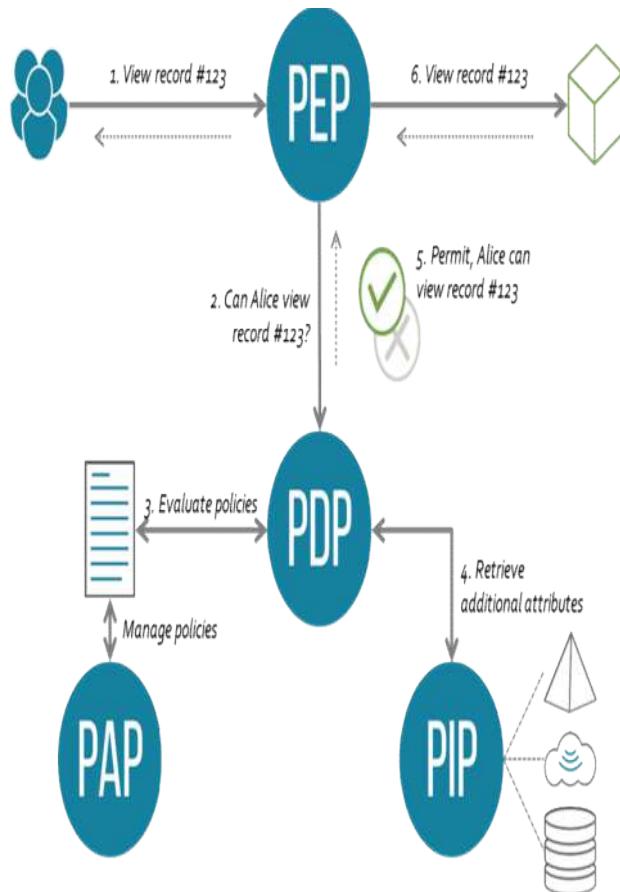


XACML

- eXensible Access Control Markup Language
 - an OASIS, general-purpose, XML-based standard
 - defines a declarative fine-grained, attribute-based access control policy language and architecture
 - Also defines a processing model describing how to evaluate access requests according to the rules defined in policies
- XACML is primarily an attribute-based access control system (ABAC), also known as a policy-based access control (PBAC) system
 - attributes associated with a user or resource are inputs into the decision of whether a given user may access a given resource in a particular way
 - Role-based access control (RBAC) can also be implemented in XACML as a specialization of ABAC

[Source: XACML - Wikipedia](#)

XACML Architecture



Abbr.	Term	Description
PAP	Policy Administration Point	Point which manages access authorization policies
PDP	Policy Decision Point	Point which evaluates access requests against authorization policies before issuing access decisions
PEP	Policy Enforcement Point	Point which intercepts user's access request to a resource, makes a decision request to the PDP to obtain the access decision (i.e. access to the resource is approved or rejected), and acts on the received decision
PIP	Policy Information Point	The system entity that acts as a source of attribute values (i.e. a resource, subject, environment)
PRP	Policy Retrieval Point	Point where the XACML access authorization policies are stored, typically a database or the filesystem.

Source: [XACML - Wikipedia](#)



OAuth (2.0)

Auth in OAuth could imply *Authentication*, but means *Authorization!!*

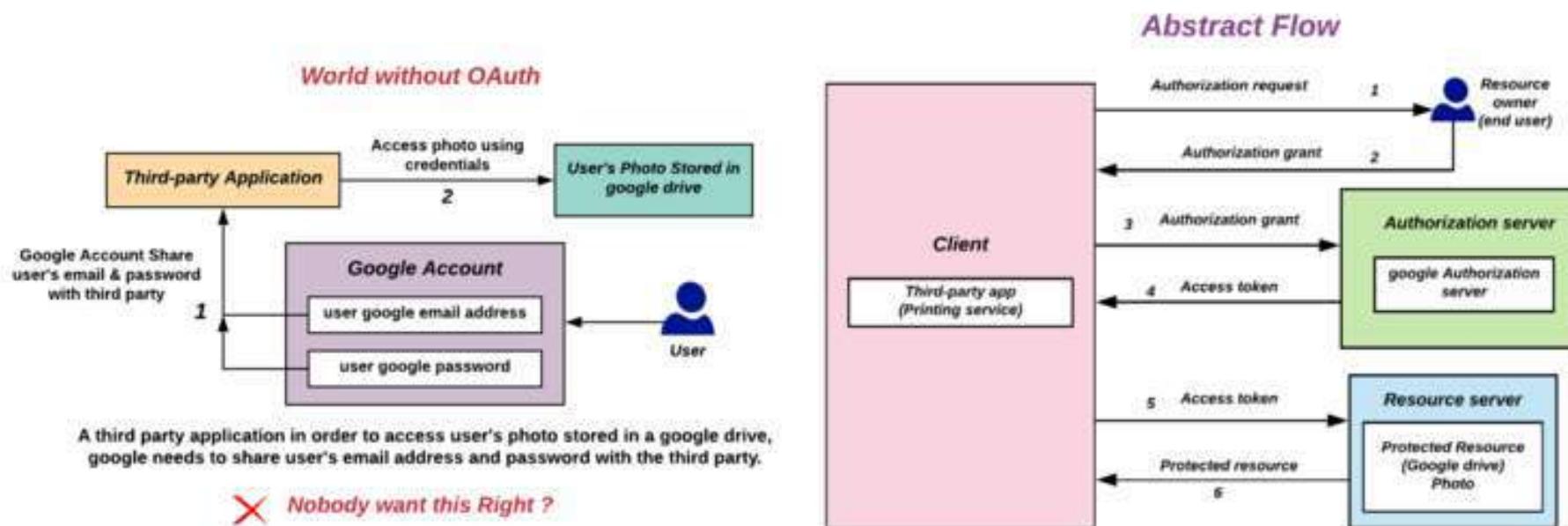
- OAuth (*Open Authorization*) is an open standard for access delegation
 - commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords
 - This mechanism is used by companies such as Amazon, Google, Facebook, Microsoft, and Twitter to permit the users to share information about their accounts with third-party applications or websites
- OAuth enables following use cases
 - delegated access control:
 - I, the user, delegate another user or service access to the resource I own. For instance via OAuth, I grant Twitter (the service) the ability to post on my Facebook wall (the resource).
 - handling the password anti-pattern:
 - Whenever you want to integrate 2 services together, in a traditional, legacy model you have to provide service B with your user credentials on service A so that service B can pretend to be you with Service A. This has many risks of course. Using OAuth eliminates the issues with these patterns and lets the user control what service B can do on behalf of the user with service A.

[Source: XACML - Wikipedia](#)

[Source: OAuth - Wikipedia](#)



OAuth (2.0) Use Case



Source: OAuth - Wikipedia



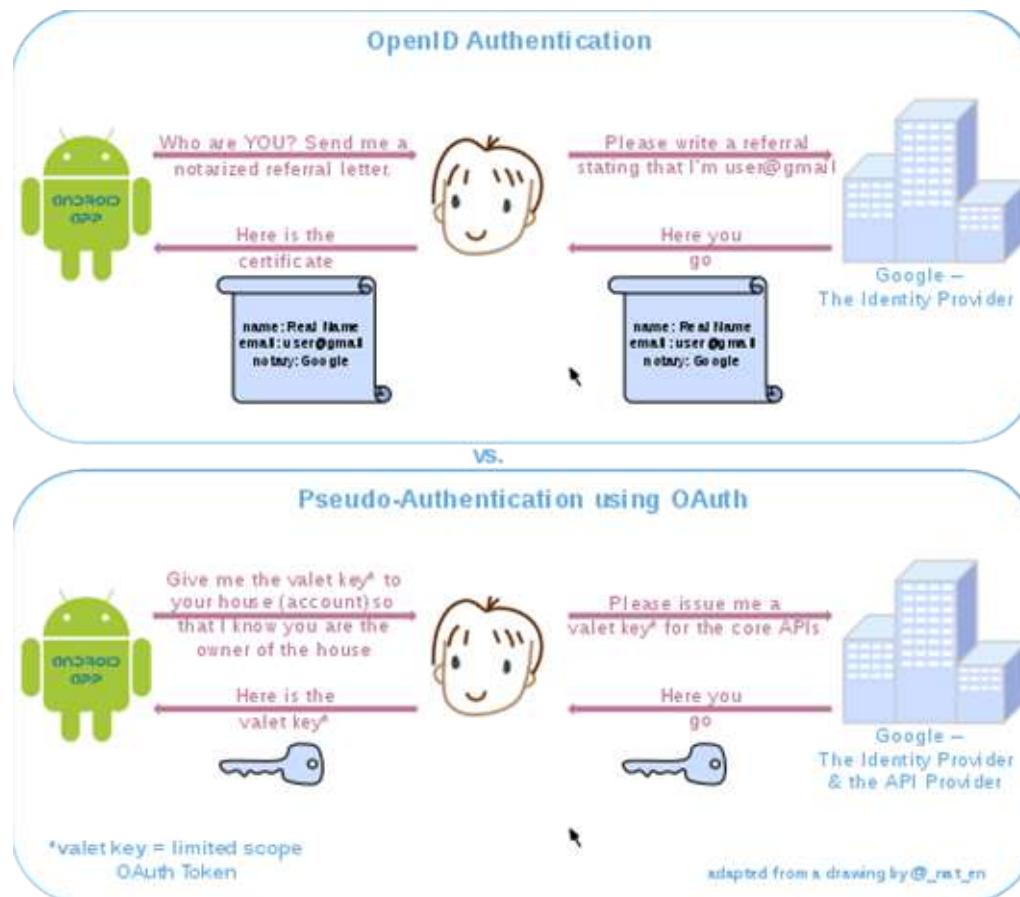
OAuth Vs SAML Vs Open ID

- OpenID Connect is built on the OAuth 2.0 protocol and uses an additional JSON Web Token (JWT), called an ID token
 - standardizes areas that OAuth 2.0 leaves up to choice, such as scopes and endpoint discovery
 - It is specifically focused on user authentication and is widely used to enable user logins on consumer websites and mobile apps
- SAML is independent of OAuth, relying on an exchange of messages to authenticate in XML SAML format, as opposed to JWT
 - It is more commonly used to help enterprise users sign in to multiple applications using a single login

[Source: What's the Difference Between OAuth, OpenID Connect, and SAML? | Okta](#)

OAuth Vs Open ID

- OpenID is specifically designed as an authentication protocol and OAuth for authorization



[Source: OAuth - Wikipedia](#)



BITS Pilani

Pilani Campus



Case Study: Identity and Access in Microsoft Azure



Microsoft
PowerPoint Presentation



BITS Pilani

Pilani Campus



<SSCSZG570 , Cloud, IoT and Enterprise Security>

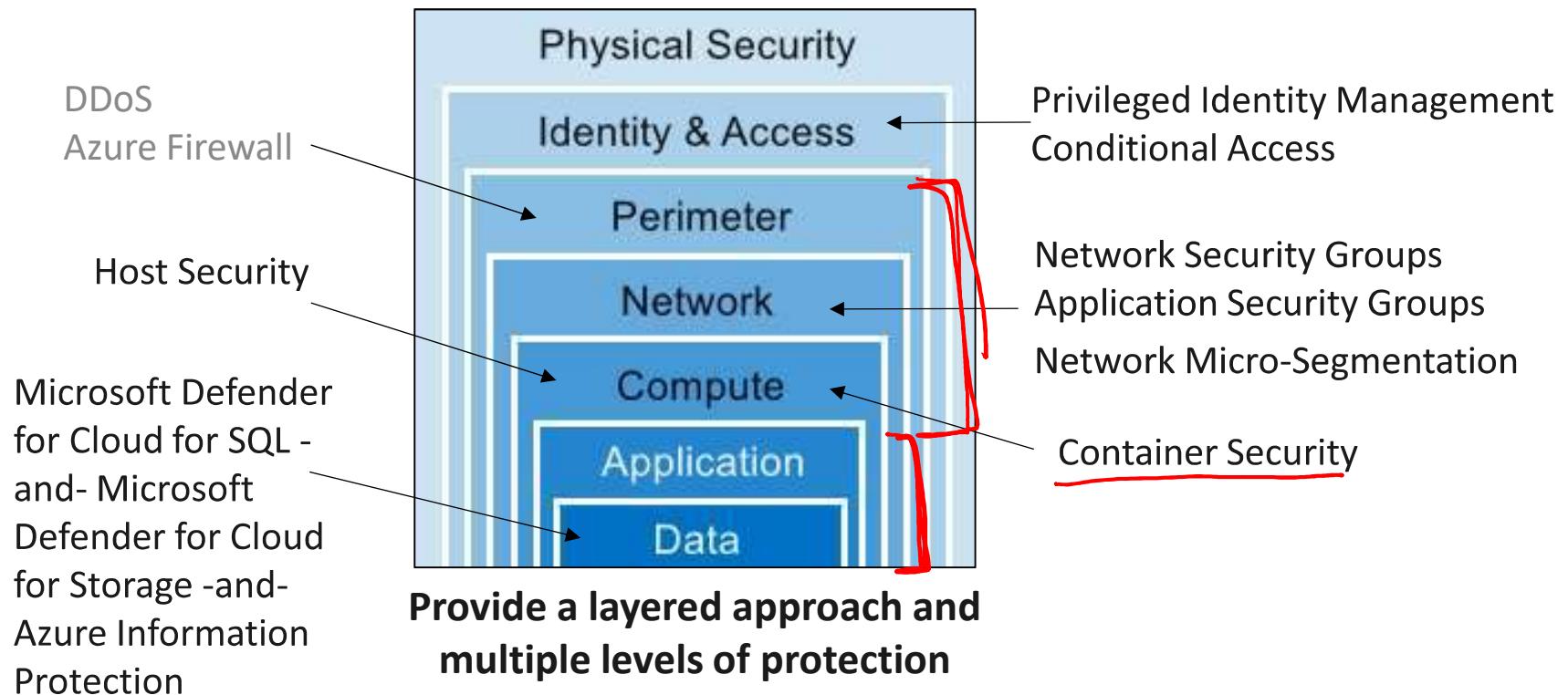
Lecture No. 15: Cloud Security

Infrastructure Security and Application Security

- **Source Disclaimer:** Content for some of the slides is from the course Textbook:
 - *Ronald L. Krutz, Russell Dean Vines, Cloud Security: A Comprehensive Guide to Secure Cloud Computing, John Wiley & Sons, 2010*
- Some of the slides are taken from Microsoft Educator Learn Material (Microsoft Azure Security Technologies)
- Material for some of the other slides is from Kubernetes public documentation:
 - <https://kubernetes.io/docs/concepts/security/>

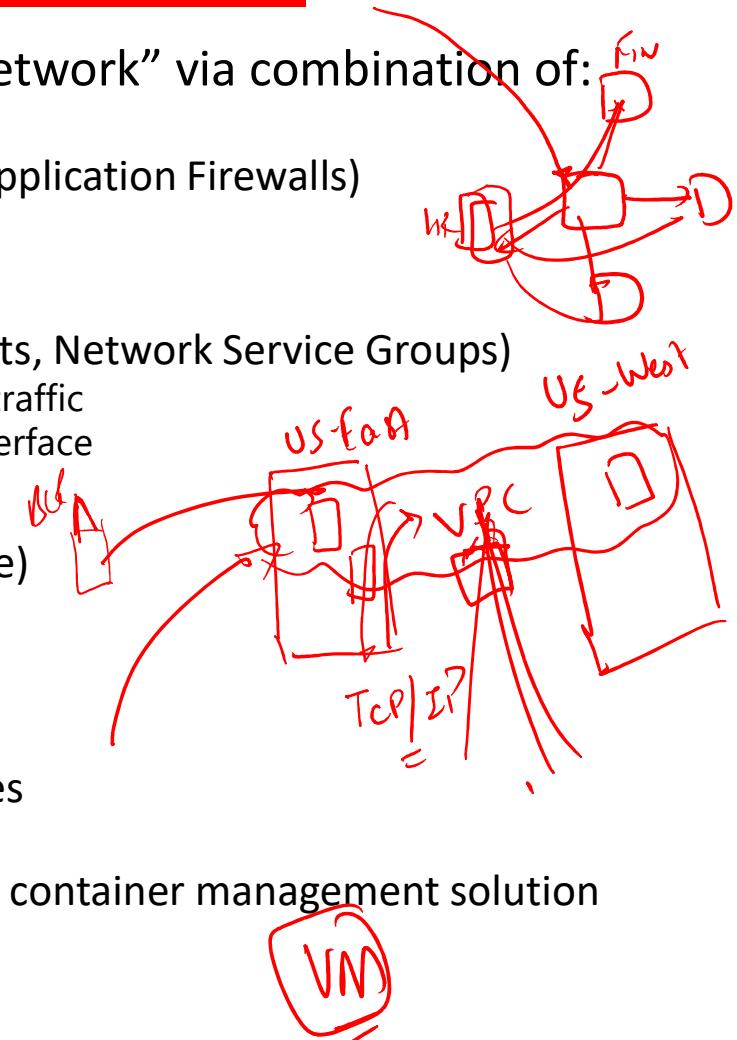


Defense in Depth



Infrastructure Security

- Perimeter Security to protect your “virtual network” via combination of:
 - ✓ DDoS mitigation solutions
 - ✓ Firewall services (Network Firewalls and Web Application Firewalls)
 - ✓ VPN services
- Network Security
 - ✓ Network segmentation (e.g. hub and spoke vnets, Network Service Groups)
 - Use of security rules to allow or deny network traffic
 - Can be associated to a subnet or a network interface
- Host Security
 - End-point protection services (e.g. anti-malware)
 - Disk encryption
 - Update Management
- Container Security
 - Container Registry with Signed Container Images
 - Authenticated access/ RBAC to Registry
 - Network ACL for access of control plane APIs of container management solution (e.g. Kubernetes)



Virtualization Security Management

- The important thing to remember from a security perspective is that there is a more significant impact when a host OS with user applications and interfaces is running outside of a VM at a level lower than the other VMs (i.e., a Type 2 architecture)
- Because of its architecture, the Type 2 environment increases the potential risk of attacks
- For example, a laptop running VMware with a Linux VM on a Windows XP system inherits the attack surface of both OSs, plus the virtualization code (VMM)

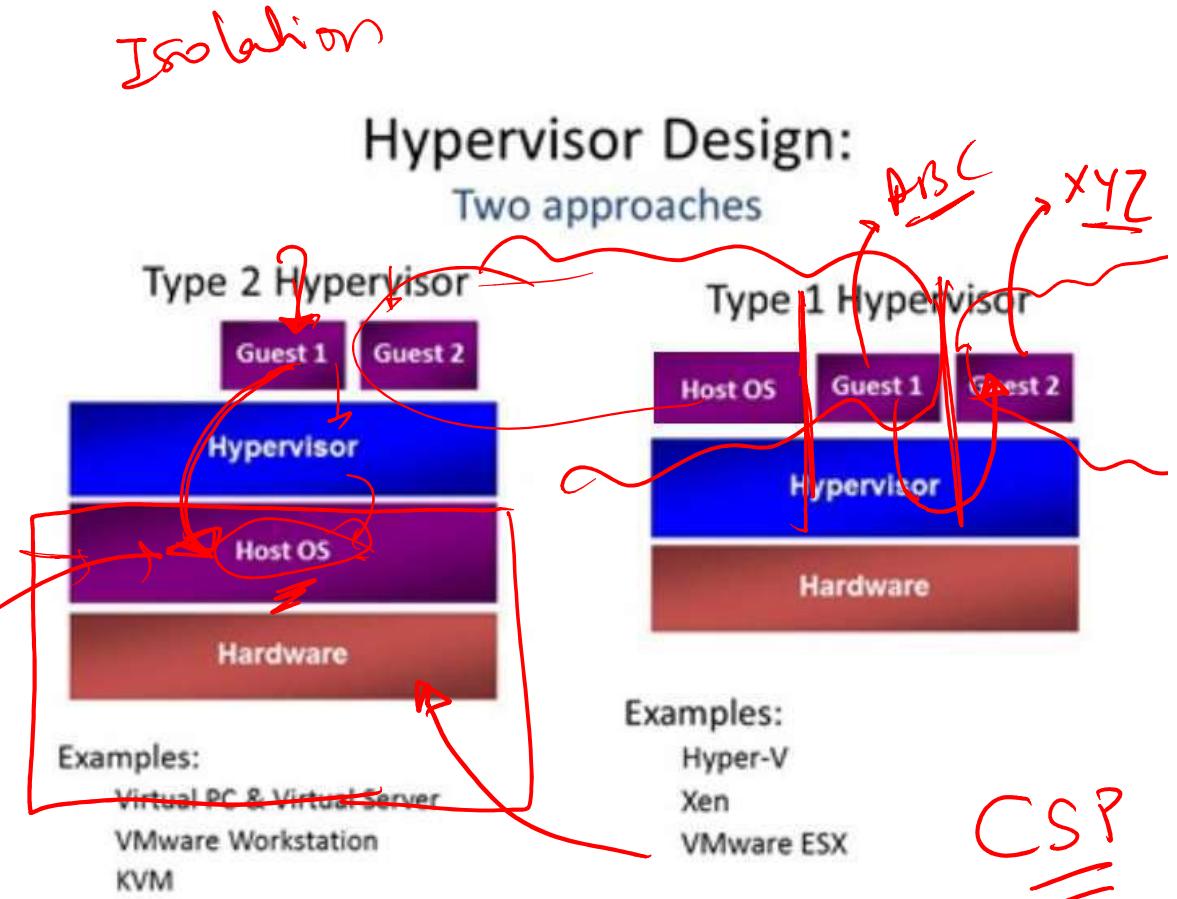


Image Source: <https://www.tenforums.com/virtualization/119469-hypervisor-type-1-type-2-a.html>



Hypervisor Risks

- The ability of the hypervisor to provide the necessary isolation during an attack greatly determines how well the virtual machines can survive risks
- Ideally, software code operating within a defined VM would not be able to communicate or affect code running either on the physical host itself or within a different VM;
- However, several issues, such as bugs in the software, or limitations to the virtualization implementation, may put this isolation at risk
- Major vulnerabilities inherent in the hypervisor consist of rogue hypervisor rootkits, external modification to the hypervisor, and VM escape*

* refers to the attacker's ability to execute arbitrary code on the VM's physical host, by "escaping" the hypervisor

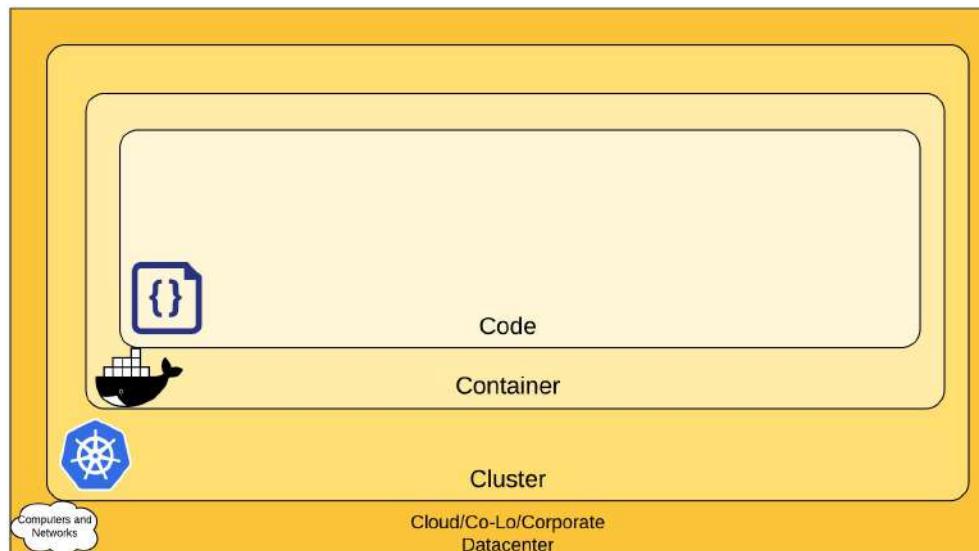


VM Security Practices

- ✓ • Hardening the Host OS and limiting physical access to the host
→ PacS & IaaS
- ✓ • Hardening the VM
- ✓ • Hardening the Hypervisor
→ CSP
- ✓ • Implement only one primary function per VM
- ✓ • Use Unique NICs for Sensitive VMs
- ✓ • Secure VM Remote Access



4Cs of Cloud Native Security



Containers are packages of software that contain all of the necessary elements to run in any environment. Contains all libraries and dependencies required for the application. OS is virtualized. User mode of the OS is included with the containerized application.

The Code layer benefits from strong base (Cloud, Cluster, Container) security layers. You cannot safeguard against poor security standards in the base layers by addressing security at the Code level



Cloud Security

- The Cloud Service Provider (CSP) offers Infrastructure Security across all shared-responsibility models
- There are a variety of compliance frameworks that can serve as a roadmap for security of the cloud environment
- These standards are designed to assure consistency and security for consumers
 - ISO/IEC 27017 and ISO/IEC 27018 are frameworks designed for cloud computing providers for the protection of their clients
 - The first focuses primarily on security controls, the second more on privacy concerns
 - The Service Organization Control (SOC) is a standard of compliance that has three types of certification, named SOC 1, SOC 2 and SOC 3
 - SOC 1 is primarily meant for banks, investment firms and other such companies that house financial data, and SOC 2 is for non-financial companies that house or process data, which could happen to be financial or otherwise
 - It's this latter certification (SOC 2) that software and cloud providers often use to verify their technology controls and processes
 - Obtaining a SOC 2 certification is a rigorous process, since a third-party CPA firm comes to the vendor's datacenter site and performs an assessment of their availability and security stance



Cloud Security (2)

- Security documentation of some of the popular cloud service providers:

IaaS Provider	Link
Alibaba Cloud	https://www.alibabacloud.com/trust-center
Amazon Web Services	https://aws.amazon.com/security/
Google Cloud Platform	https://cloud.google.com/security/
IBM Cloud	https://www.ibm.com/cloud/security
Microsoft Azure	https://docs.microsoft.com/en-us/azure/security/azure-security
Oracle Cloud Infrastructure	https://www.oracle.com/security/
VMWare VSphere	https://www.vmware.com/security/hardening-guides.html

Source: <https://kubernetes.io/docs/concepts/security/overview/>



Infrastructure Security for K8s Cluster

Area of Concern for Kubernetes Infrastructure	Recommendation
Network access to API Server (Control plane)	All access to the Kubernetes control plane is not allowed publicly on the internet and is controlled by network access control lists restricted to the set of IP addresses needed to administer the cluster.
Network access to Nodes (nodes)	Nodes should be configured to <i>only</i> accept connections (via network access control lists) from the control plane on the specified ports, and accept connections for services in Kubernetes of type NodePort and LoadBalancer. If possible, these nodes should not be exposed on the public internet entirely.
Kubernetes access to Cloud Provider API	Each cloud provider needs to grant a different set of permissions to the Kubernetes control plane and nodes. It is best to provide the cluster with cloud provider access that follows the principle of least privilege for the resources it needs to administer. The Kops documentation provides information about IAM policies and roles.
Access to etcd	Access to etcd (the datastore of Kubernetes) should be limited to the control plane only. Depending on your configuration, you should attempt to use etcd over TLS. More information can be found in the etcd documentation.
etcd Encryption	Wherever possible it's a good practice to encrypt all storage at rest, and since etcd holds the state of the entire cluster (including Secrets) its disk should especially be encrypted at rest <small>Source: https://kubernetes.io/docs/concepts/security/overview/</small>



Cluster Security

- Protecting a cluster from accidental or malicious access can be done via:
 - Passing all API calls via Authentication and Authorization
 - Encrypting all API communication in the cluster is with TLS
- Controlling the runtime capabilities of a workload can be done via:
 - Defining Resource quota limits to limit the amount of CPU, memory, or persistent disk a namespace can allocate, and also control how many pods, services, or volumes exist in each namespace
 - Control the privileges associated with containers using the Pod security policies
- Restricting network access
 - Application authors can restrict which pods in other namespaces may access pods and ports within their namespaces



Container Security

Area of Concern for Containers	Recommendation
Container Vulnerability Scanning and OS Dependency Security	As part of an image build step, you should scan your containers for known vulnerabilities.
Image Signing and Enforcement	Sign container images to maintain a system of trust for the content of your containers.
Disallow privileged users	When constructing containers, create users inside of the containers that have the least level of operating system privilege necessary in order to carry out the goal of the container.

Source: <https://kubernetes.io/docs/concepts/security/overview/>



BITS Pilani

Pilani Campus



Case Study: Platform Security Features in Microsoft Azure



Microsoft
PowerPoint Presentat



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

Nishit Narang
WILPD-CSIS
[\(nishit.narang@pilani.bits-pilani.ac.in\)](mailto:nishit.narang@pilani.bits-pilani.ac.in)



<SSCSZG570 , Cloud, IoT and Enterprise Security>

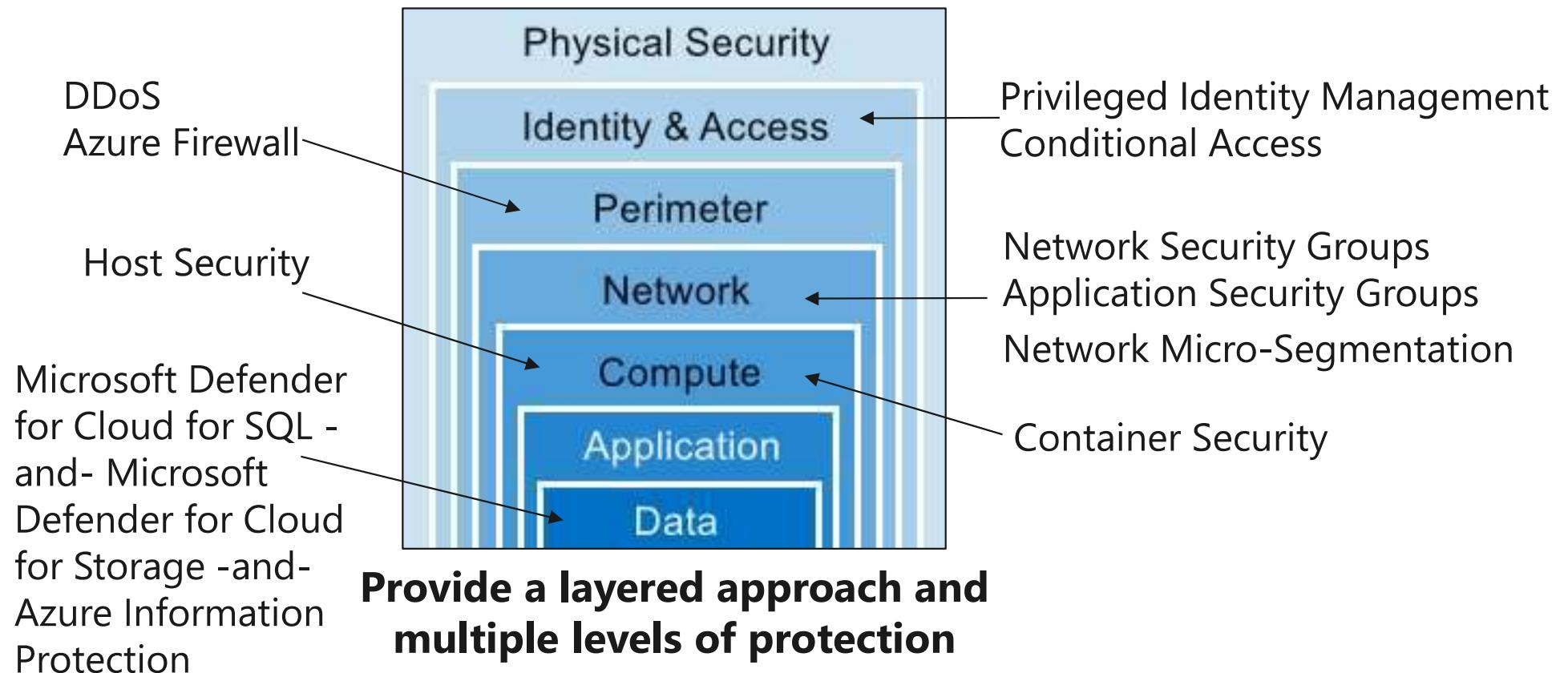
Lecture No. 16: Cloud Security

Application and Data Security + Cloud Forensics

- **Source Disclaimer:** Content for some of the slides is from Wikipedia
- Some of the slides are taken from Microsoft Educator Learn Material (Microsoft Azure Security Technologies)
- Material for some of the other slides is from Kubernetes public documentation:
 - <https://kubernetes.io/docs/concepts/security/>

RECAP: Application and Data Security Layers

Defense in Depth



Application Security

- Most applications are designed and deployed using micro-services architecture and REST APIs
 - REST APIs are designed to be STATELESS
 - Requires secure approach for session management
- OWASP Top 10 vulnerabilities
 - One of the best compilation of vulnerabilities that impact web-applications
 - Must be verified in every application before deployed
- Most applications rely on a variety of security assets (like certificates, API keys, passwords and other secrets)
 - A secure key vault on the cloud is useful to store and manage access to these secrets

Application Security (2)

Area of Concern	Recommendation
Access over TLS only	If your code needs to communicate by TCP, perform a TLS handshake with the client ahead of time. With the exception of a few cases, encrypt everything in transit. Going one step further, it's a good idea to encrypt network traffic between services. This can be done through a process known as mutual TLS authentication or mTLS which performs a two sided verification of communication between two certificate holding services.
Limiting port ranges of communication	Wherever possible, only expose the ports on your service that are absolutely essential for communication or metric gathering.
3rd Party Dependency Security	It is a good practice to regularly scan your application's third party libraries for known security vulnerabilities. Each programming language has a tool for performing this check automatically.
Static Code Analysis	Most languages provide a way for a snippet of code to be analyzed for any potentially unsafe coding practices. Whenever possible you should perform checks using automated tooling that can scan codebases for common security errors.
Dynamic probing attacks	There are a few automated tools that you can run against your service to try some of the well known service attacks. These include SQL injection, CSRF, and XSS. One of the most popular dynamic analysis tools is the OWASP Zed Attack proxy tool.

Source: <https://kubernetes.io/docs/concepts/security/overview/>

Data Security

- Data storage on the cloud is governed by various compliance standards
 - HIPAA, GDPR, PCI-DSS
- Cloud data storage and access must:
 - Support Physical Isolation
 - Support Backup, Recovery, Retention and Disposal Rules, that can be configured as per organizational policies
 - Support Authentication and Authorization of all access
 - Support Encryption of confidential data
 - Support secure transfer of data when required
- Includes both File-based Storage and Databases
 - Database Firewalls, Database Audit Logs..



Case Study: Application and Data Security Features in Microsoft Azure



Microsoft
PowerPoint Presentat



BITS Pilani

Pilani Campus



Compliance Frameworks

HIPAA

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
 - Also known as the Kennedy–Kassebaum Act
 - Is a United States federal statute enacted by the 104th United States Congress and signed into law by President Bill Clinton on August 21, 1996
 - Modernized the flow of healthcare information, stipulates how personally identifiable information maintained by the healthcare and healthcare insurance industries should be protected from fraud and theft, and addressed some limitations on healthcare insurance coverage

Source: [Health Insurance Portability and Accountability Act - Wikipedia](#)

Data Privacy via HIPAA

- HIPAA prohibits healthcare providers and healthcare businesses, called *covered entities*, from disclosing protected information to anyone other than a patient and the patient's authorized representatives without their consent
- With limited exceptions, it does not restrict patients from receiving information about themselves
- It does not prohibit patients from voluntarily sharing their health information however they choose, nor – if they disclose medical information to family members, friends, or other individuals not a part of a covered entity – legally require them to maintain confidentiality

[Source: Health Insurance Portability and Accountability Act - Wikipedia](#)

HIPAA Privacy and Security Rule

- The HIPAA Privacy Rule is composed of national regulations for the use and disclosure of Protected Health Information (PHI) in healthcare treatment, payment and operations by covered entities.
 - The effective compliance date of the Privacy Rule was April 14, 2003
- The Final Rule on Security Standards was issued on February 20, 2003
 - It took effect on April 21, 2003, with a compliance date of April 21, 2005, for most covered entities
- The Security Rule complements the Privacy Rule
 - While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI)
 - It lays out three types of security safeguards required for compliance:
 - **Administrative:** policies and procedures designed to clearly show how the entity will comply with the act
 - **Physical:** controlling physical access to protect against inappropriate access to protected data
 - **Technical:** controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient

[Source: Health Insurance Portability and Accountability Act - Wikipedia](#)

GDPR

- General Data Protection Regulation (GDPR)
 - A regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA)
 - The GDPR is an important component of EU privacy law and of human rights law, in particular Article 8(1) of the Charter of Fundamental Rights of the European Union
 - It also addresses the transfer of personal data outside the EU and EEA areas
 - The GDPR's primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business
 - The GDPR was adopted on 14 April 2016 and became enforceable beginning 25 May 2018

[Source: General Data Protection Regulation - Wikipedia](#)

GDPR Organization

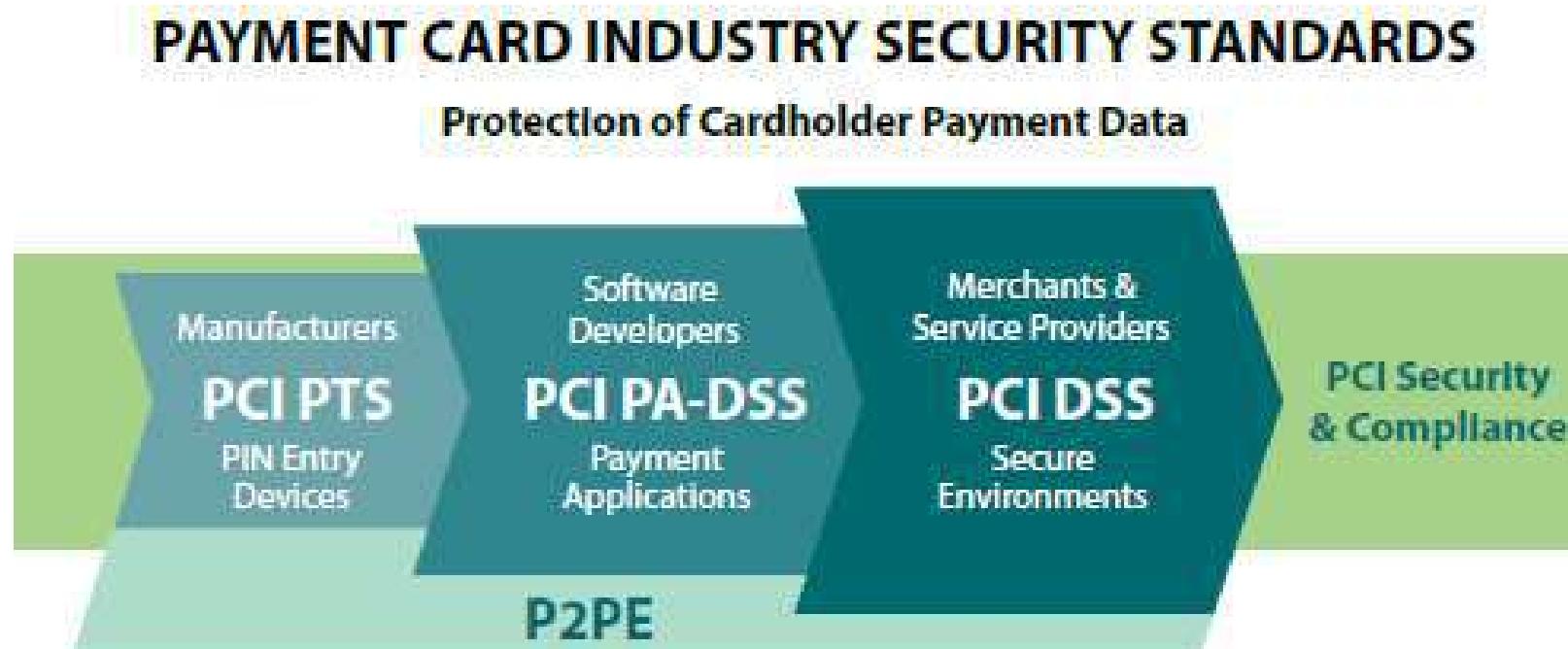
- The GDPR 2016 has eleven chapters, concerning:
 - general provisions, principles, rights of the data subject, **duties of data controllers or processors, transfers of personal data to third countries**, supervisory authorities, cooperation among member states, remedies, liability or penalties for breach of rights, and miscellaneous final provisions
- Duties of Data Controllers or Processors:
 - must clearly disclose any data collection
 - Pseudonymisation is a required process for stored data
 - transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information
 - records of processing activities have to be maintained
 - controllers and processors of personal data must put in place appropriate technical and organizational measures to implement the data protection principles
- Transfer of Personal Data to Third Countries:
 - Chapter V of the GDPR forbids the transfer of the personal data of EU data subjects to countries outside of the EEA — known as third countries — unless appropriate safeguards are imposed, or the third country's data protection regulations are formally considered adequate by the European Commission

PCI-DSS

- Payment Card Industry Data Security Standard (PCI DSS)
 - Is an information security standard for organizations that handle credit cards from the major card schemes
 - The standard was created to increase controls around cardholder data to reduce credit card fraud
- Validation of compliance is performed annually or quarterly, by a method suited to the volume of transactions handled:
 - Self-Assessment Questionnaire (SAQ) — smaller volumes
 - external Qualified Security Assessor (QSA) — moderate volumes; involves an Attestation on Compliance (AOC)
 - firm-specific Internal Security Assessor (ISA) — larger volumes; involves issuing a Report on Compliance (ROC)

[Source: Payment Card Industry Data Security Standard - Wikipedia](#)

PCI Security Standards



PCI Data Security Standard (PCI DSS)

PIN Transaction Security (PTS)

Payment Application Data Security Standard (PA-DSS)

PCI Point-to-Point Encryption Standard (P2PE)

Source: PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1.

PCI-DSS Requirements

- Twelve requirements for compliance, organized into six logically related groups
 - Build and Maintain a Secure Network and Systems
 - Protect Cardholder Data
 - Maintain a Vulnerability Management Program
 - Implement Strong Access Control Measures
 - Regularly Monitor and Test Networks
 - Maintain an Information Security Policy

[Source: Payment Card Industry Data Security Standard - Wikipedia](#)

PCI-DSS Requirements (2)

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information security for all personnel



PCI-DSS Quick Reference Guide

Source: PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1.



PCI-DSS Adherence Steps

Three steps for adhering to the PCI-DSS:

- **Assess** — identifying all locations of cardholder data, taking an inventory of IT assets and business processes for payment card processing and analyzing them for vulnerabilities that could expose cardholder data.
- **Repair** — fixing identified vulnerabilities, securely removing any unnecessary cardholder data storage, and implementing secure business processes.
- **Report** — documenting assessment and remediation details, and submitting compliance reports to the acquiring bank and card brands (or other requesting entity, in case of a service provider).

Source: PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1.



Cloud Forensics

References:

- <https://www.infosecurity-magazine.com/opinions/cloud-complicates-digital-crime/>
- <https://blog.eccouncil.org/cloud-forensics-is-it-important-to-your-cybersecurity-plan/>

Introduction

- Lot of difference between traditional computer forensics and cloud forensics
- While the cloud is becoming more widely used by companies across the globe, few of these companies have included cloud forensics in their cyber-security investments
- Many companies still mistakenly believe that traditional forensics is enough.
- However, without investment into cloud forensics, businesses could find themselves unable to prosecute attackers, collect evidence on what actually happened, and or have their case fully presented in court.
- To help put things into perspective, look at a recent report by Netrix:
 - 39% of healthcare organizations suffered ransomware attacks in the cloud in 2020.
 - Due to a cloud breach, one in four healthcare organizations was fined for non-compliance and 1 in 10 was sued.

Traditional Vs Cloud Forensics

- Cloud forensics is a blend of digital forensics and cloud computing.
- It involves investigating crimes that are committed using the cloud.
- Traditional computer forensics is a process by which media is collected at the crime scene, or where the media was obtained; it includes the practice of preserving the data, the validation of said data, and the interpretation, analysis, documentation, and presentation of the results in the courtroom.
- In most traditional computer forensics, any evidence that has been discovered within the media will be under the control of the relevant law enforcement. This is where the divide between cloud and traditional forensics begins.
- In the cloud, the data can potentially exist anywhere on earth, and potentially outside of your law enforcement jurisdiction. This can result in control of the evidence (and the process of validating it) becoming incredibly challenging.



Cloud Forensics Overview

- Cloud forensics combines the realities of cloud computing with digital forensics, which focuses on collecting media from a cloud environment.
- This requires investigators to work with multiple computing assets, such as virtual and physical servers, networks, storage devices, applications, and much more.
- For most of these situations, the cloud environment will remain live and capable of change.
- Despite this wide array of different assets and jurisdiction challenges, the end result must stay the same: evidence must be presented in a court of law.

Top 5 Cloud Forensics Challenges

The chief concern for any cloud forensics investigator is the preservation of evidence, especially against tampering by any third parties. This is what allows evidence to be admissible in court.

- 1) In SaaS and PaaS cloud models, customers are dependent on cloud service providers for access to any usage logs as they do not have access to the physical hardware (let alone control over it).
- 2) In some instances, cloud service providers have been known to hide logs from customers or hold policies that state logs cannot be collected.
 - This is a strange business practice, given how concerned most consumers are with control over their data, privacy, and anonymity online, but it is an obstacle faced by consumers nonetheless.
 - It is because of this that maintaining a clear chain of custody in a cloud infrastructure is extremely difficult. In traditional forensics, investigators would have complete control of the evidence concerned.



Cloud Forensics Challenges (Contd.)

- 3) In cloud forensics, the investigators may not have full control over who the cloud service provider allows to collect evidence.
 - If the person(s) allowed aren't properly trained, the chain of custody or evidence may be inadmissible in court.
 - This could lead to companies or individuals' entire case being thrown out, even if they were an entirely innocent victim of a damaging cloud-based crime.
- 4) As cloud servers are often located in multiple different counties, the data required by forensic investigators can be as well.
 - This immediately presents the investigators with the obstacle of legal jurisdiction.
- 5) Cloud services can also be reluctant to help you when it comes to conducting an investigation.
 - After all, what may be an issue for you might not be an issue at all for them, and your investigation could further cost them time and money.

Cloud Forensics Tool Capabilities

4 Capabilities Required for Cloud Forensics Tools :

- *Forensic data collection*—Tools must be able to identify, label, record, and acquire data from the cloud.
- *Elastic, static, and live forensics*—To meet the elastic nature of clouds, tools must be able to expand and contract their data storage capabilities as the demand for services changes.
- *Evidence segregation*—Clouds are set up for **multitenancy**, meaning many different unrelated businesses and users share the same applications and storage space., So forensics tools must be able to separate each customer's data.

Tool Capabilities (Contd.)

- *Investigations in virtualized environments*—Because cloud operations typically run in a virtual environment, forensics tools should have the capability to examine virtual systems.

Although most cloud architecture is composed of virtual machines, the actual cloud is much more complex. The failover capability is necessary in case a VM fails, and there are virtualized switches and routers along with multi-tenant and multi-cloud environments.

Cloud Forensics Tools

- In the early days of the cloud, very few tools designed for cloud forensics were available, but many digital, network, and e-discovery tools were used to handle collecting and analyzing data from the cloud.
- Some vendors with integrated tools that can be applied to cloud forensics include the following:
- Guidance Software EnCase eDiscovery and its incident response and EnCase Cybersecurity tools
- AccessData Digital Forensics Incident Response services and AD eDiscovery can collect cloud data from Office 365, SharePoint, and OneDrive for Business
- Specific forensics tools for the cloud are FROST for OpenStack IaaS platforms, F-Response's cloud server utility, and Magnet AXIOM's Cloud module.