Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

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

innovate achieve lead

BITS Pilani

Pilani Campus

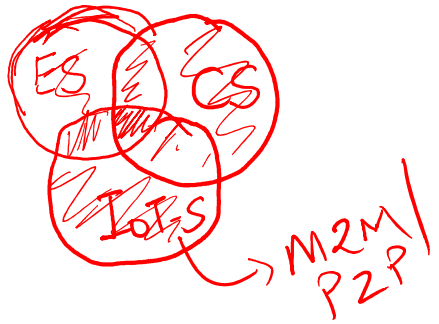
<SS ZG570 , Cloud, IoT and Enterprise Security>

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.

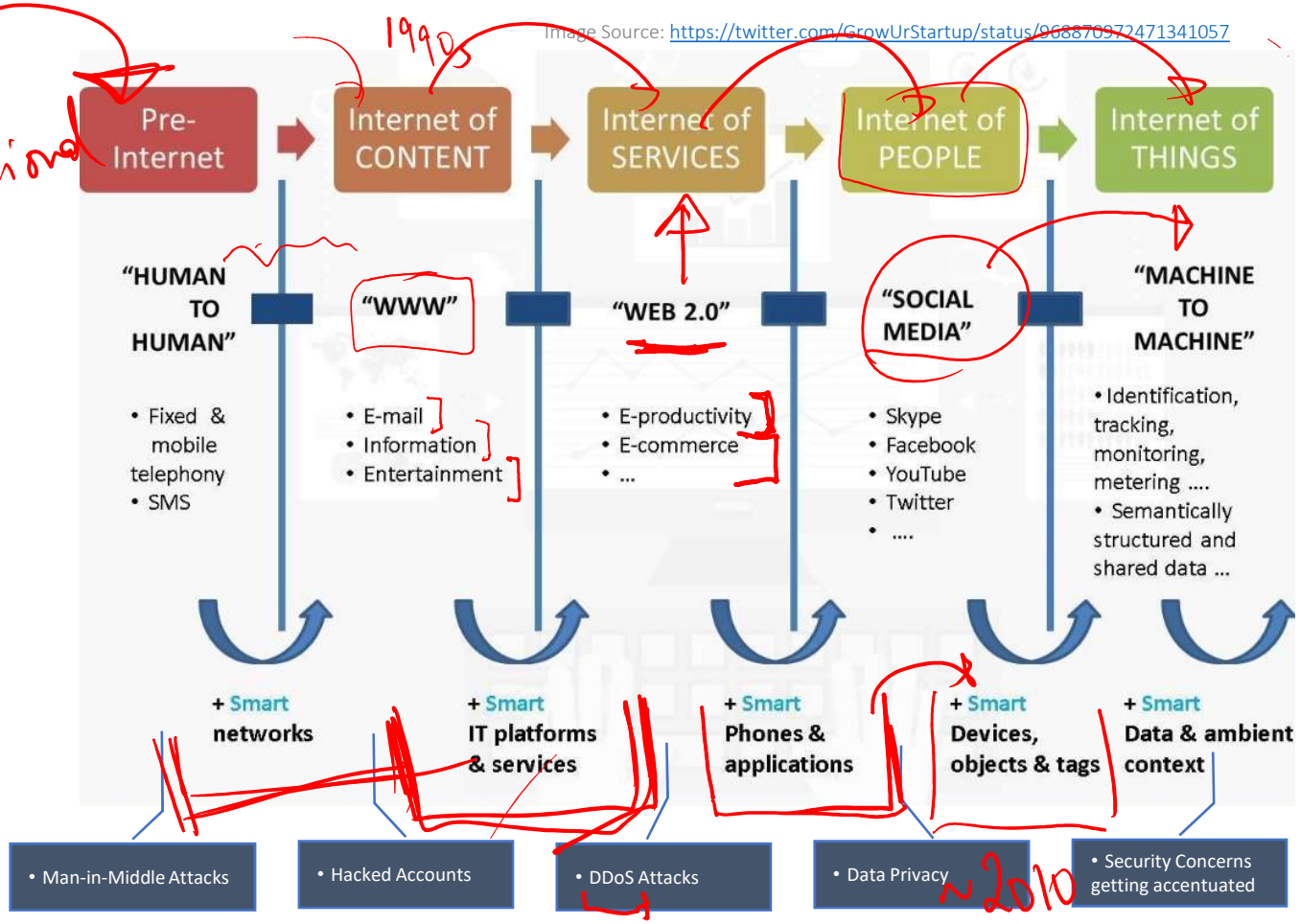
- Dwight D. Eisenhower, 34th President of the United States

"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

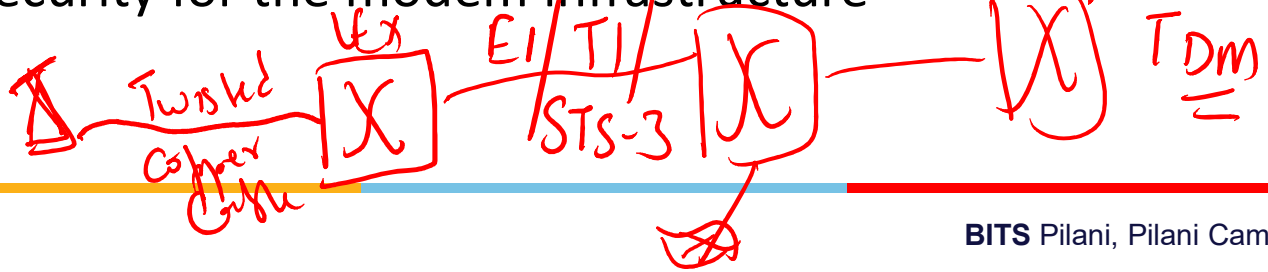
- Enterprise Security

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

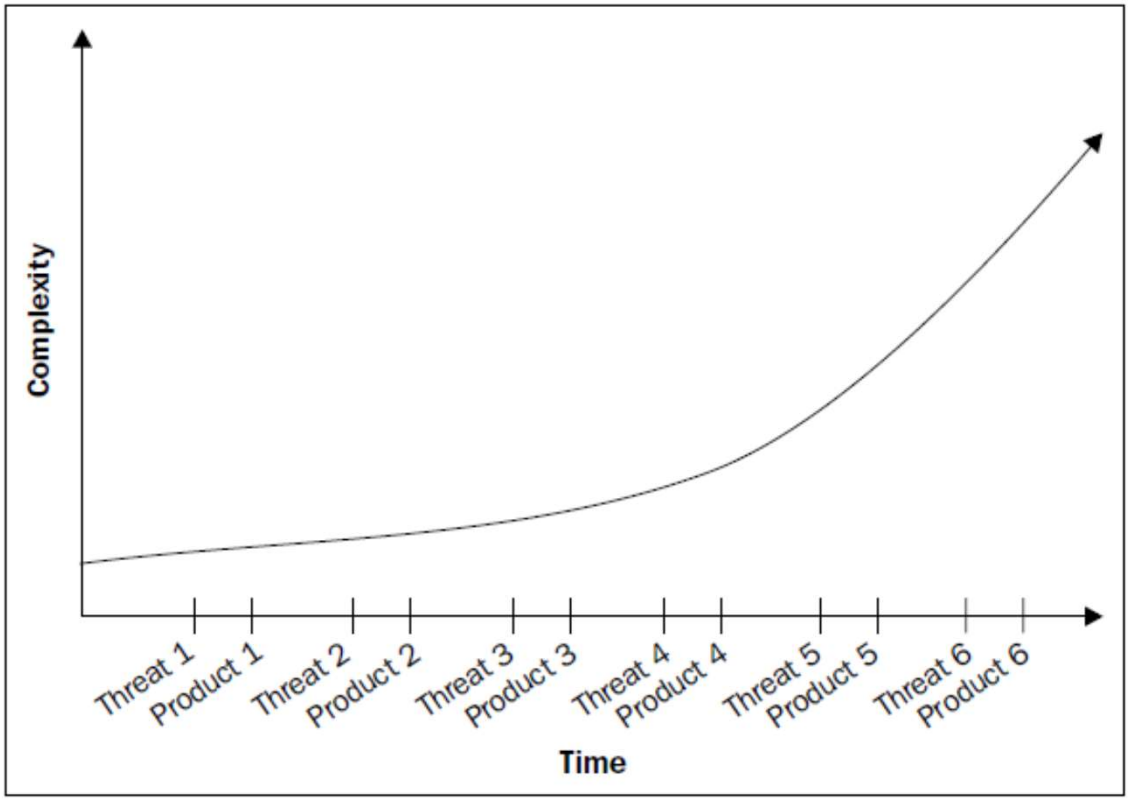
- History of Enterprise Security
  - Older times → no concept of DMZ, as no public Internet existed
  - Only form of Networking in the form of dial-up networking connections → not much security concerns as phone numbers had to be known
  - Modems used to make outbound calls and accept inbound calls to 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



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

A myriad collection of security tools

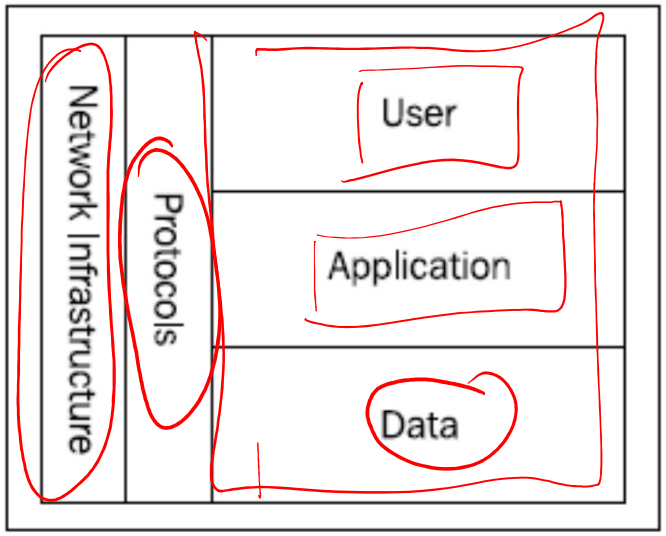
Band-Aid Approach

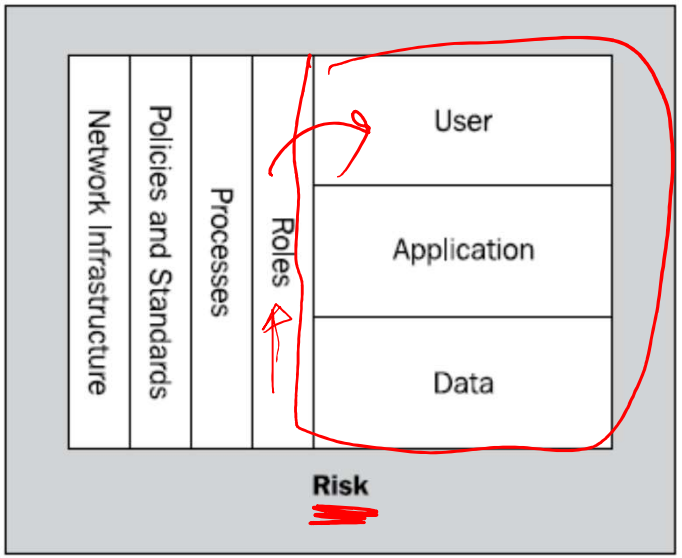
It has led to a relatively secure network perimeter instead of a functioning, extensible, enterprise-wide security architecture

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**

Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

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

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

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

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

Enterprise Security

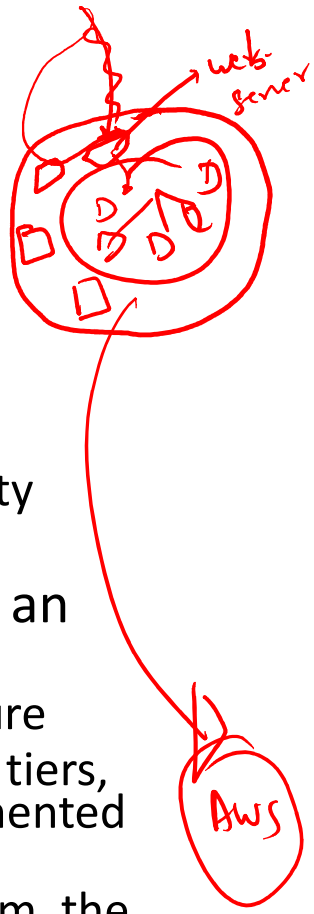
The Roadmap to Securing the Enterprise: Method and Approach

Security Architecture Models

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

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

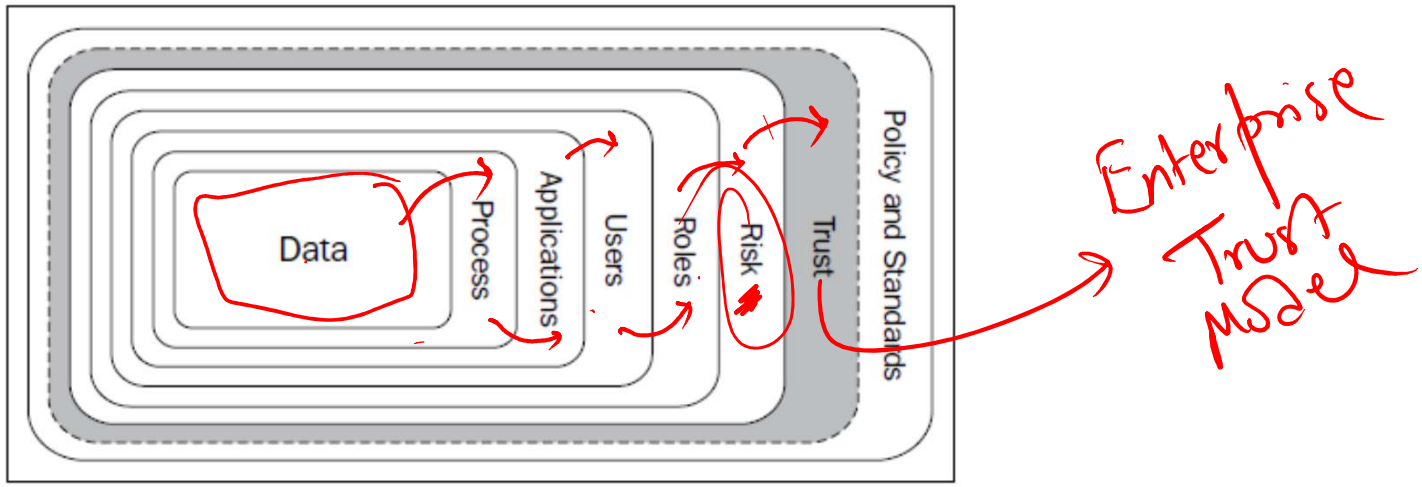
Micro Architectures



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

Data-centric Security Architectures

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



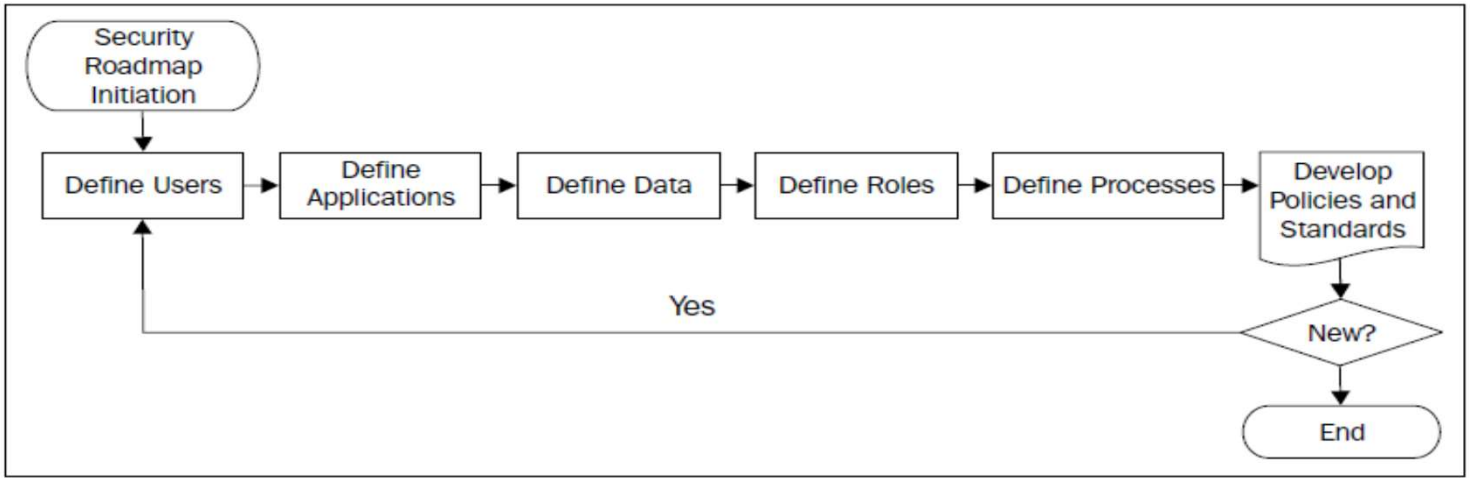
Determination of trust and how risk dictates trust and trust influences policies and standards

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

Data Risk-centric Architectures

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

Architecture Roadmap: Overview



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

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

Defining Data in a Trust Model

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

Example: Data for Common Industries

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

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

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

Defining Processes in a Trust Model

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

Defining Applications in a Trust Model

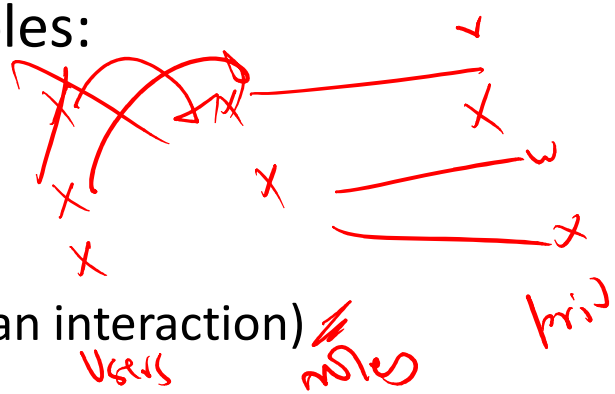
- After identification of the enterprise data and processes, we need to define the applications that transmit, process, or store the defined data
  - see the picture of "use and access"
  - Applications can be any application in the enterprise from e-mail clients to complex sales processing applications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

Defining Users in a Trust Model

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

Defining Roles in a Trust Model

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



Defining Policies and Standards

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

Enterprise Trust Models

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

Example Case Study

Building an Enterprise Trust Model

Trust Model Building Blocks: Sample

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

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

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

Application User (External)

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

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

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

Application Owner (Business Partner)

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

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

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

System Owner (Contractor)

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

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

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

Data Owner (Internal)

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

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

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

Automation

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

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

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

Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

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

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 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

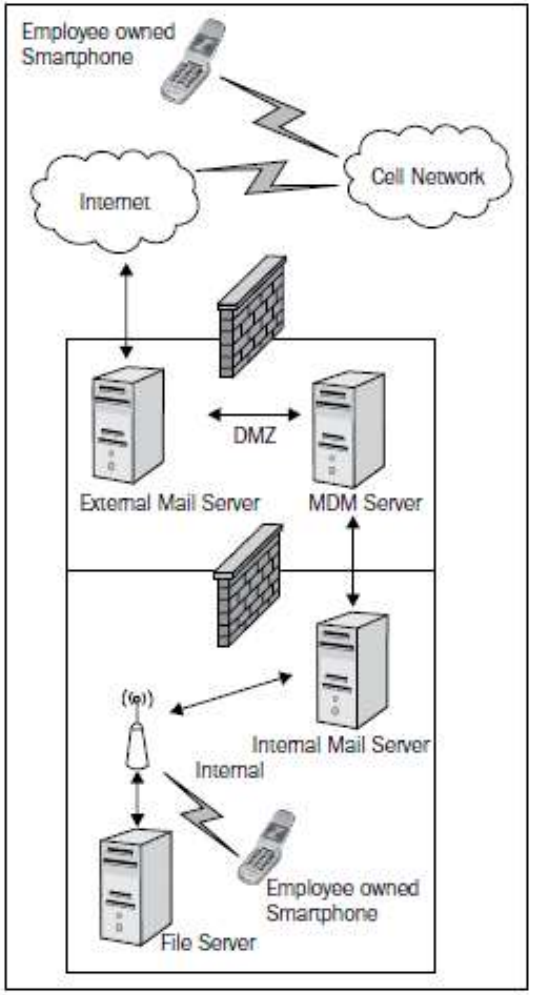
Modern Initiatives and Impacts to Security Architectures

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

BYOD: Personal Computers

Exploring the
uture of Desktop Virtuali

- 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 (ALE) - $50,000 (COP) = $33,000 (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)

innovate achieve lead

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

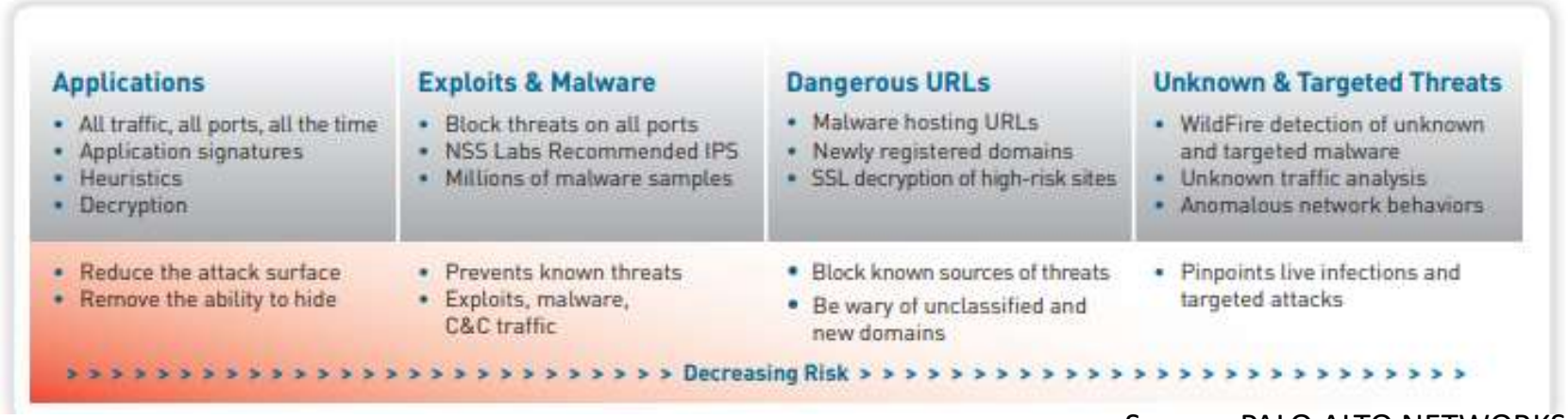
Next Generation Firewalls

- 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)

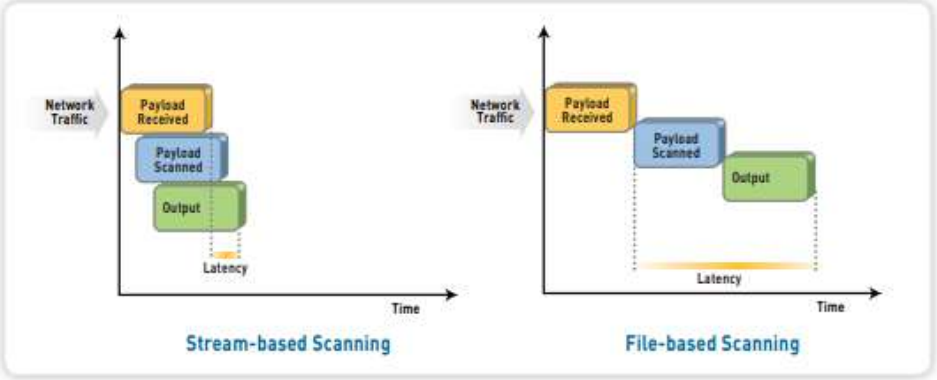
Palo Alto Networks - ContentID

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

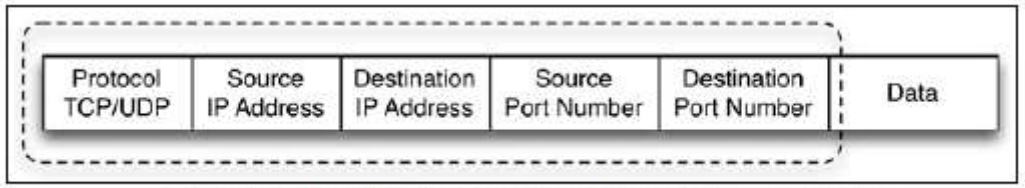


NGFW: Benefits and Challenges

- **+** 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

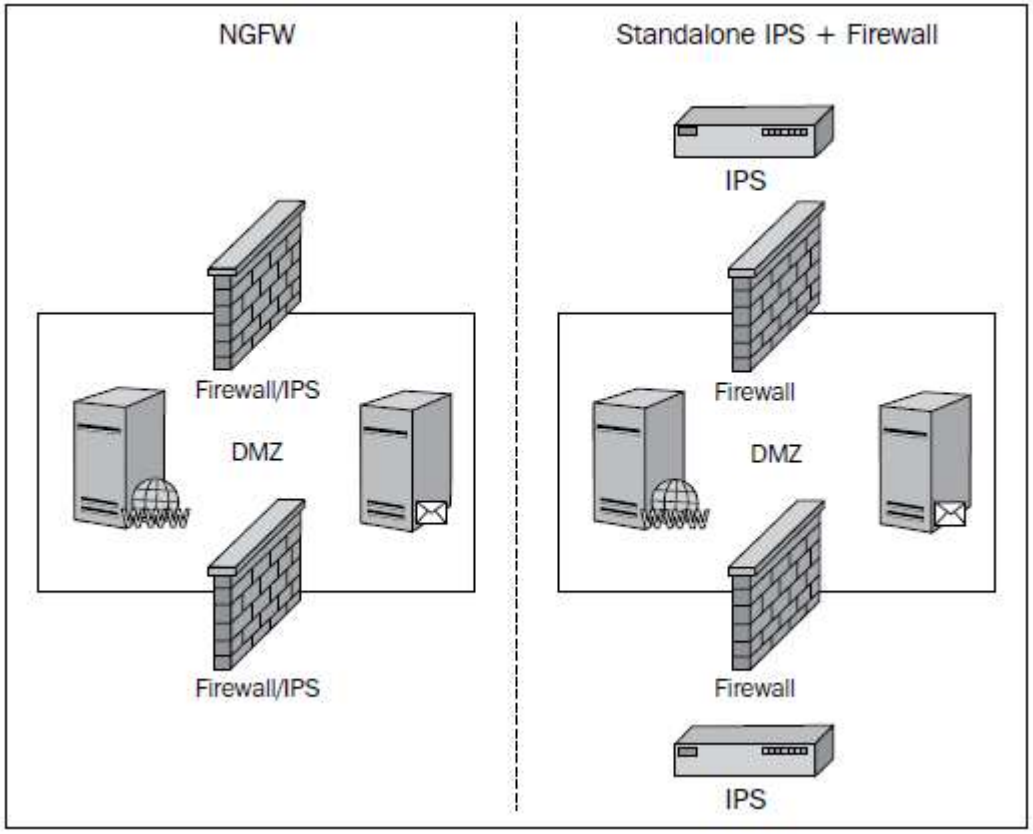


Simplified TCP packet with IP header with header inspection only

- 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

Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

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

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 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

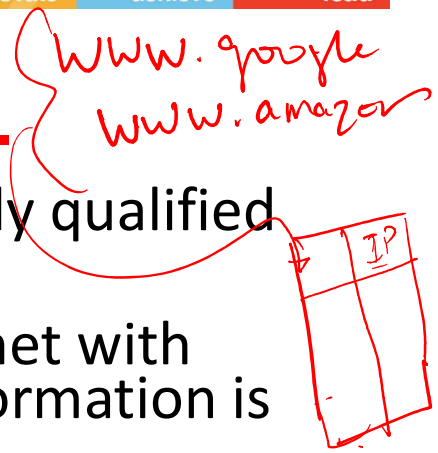
- APT = **Advanced Persistent Threat**
- Are complicated and well disguised malware
  - use complicated zero-day vulnerabilities, multi-encoded malicious payloads, encryption, obfuscation, and clever masquerading techniques
- APT mitigation solutions work by providing a safe environment
  - usually virtualized 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

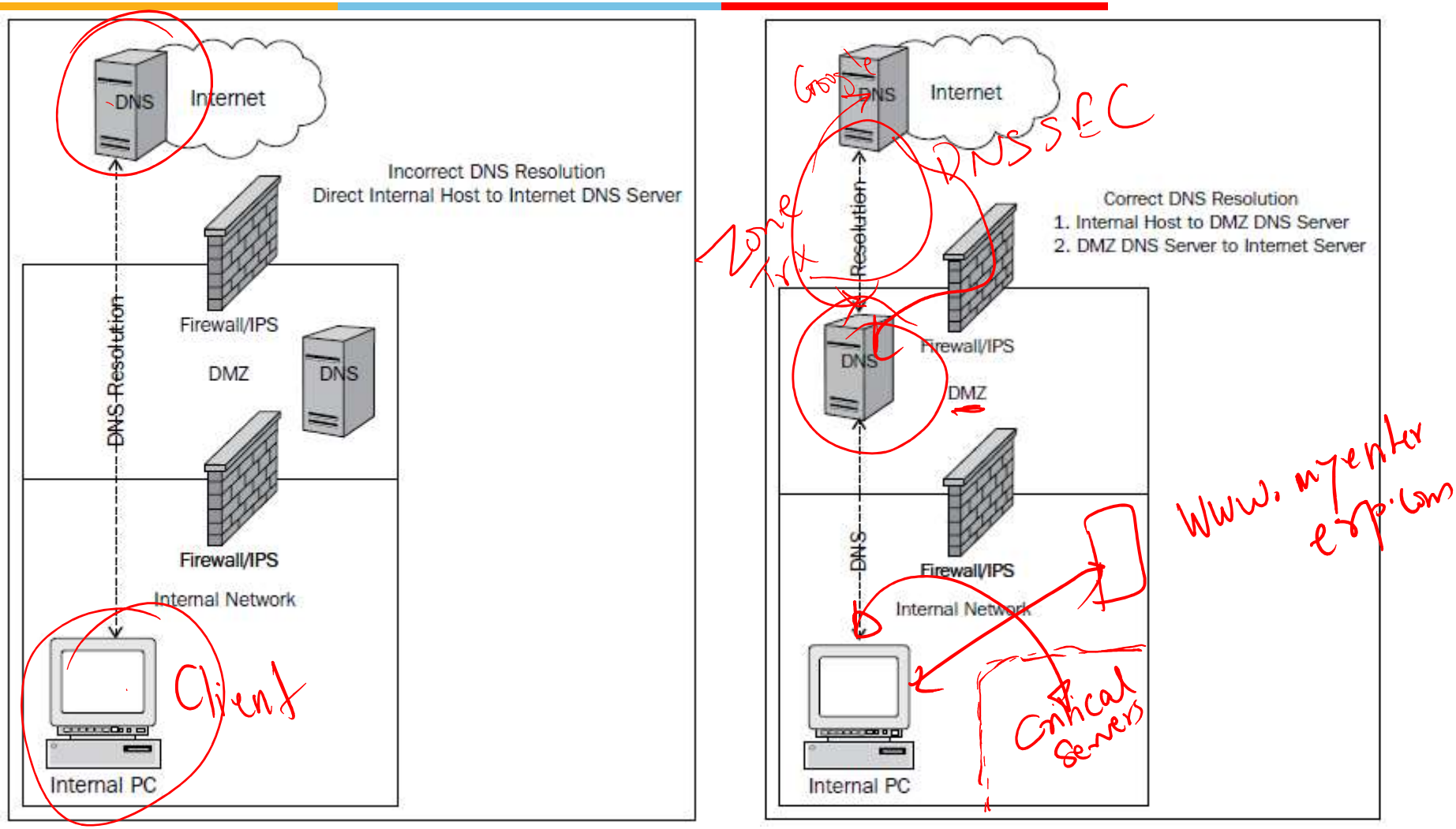


- DNS provides a mapping of an IP address to a fully qualified domain name
- A system can be directed anywhere on the Internet with DNS, so the authenticity of the source of this information is critical
- This is where **DNS Security Extensions** (**DNSSEC**) come into play
  - provide authenticity for 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

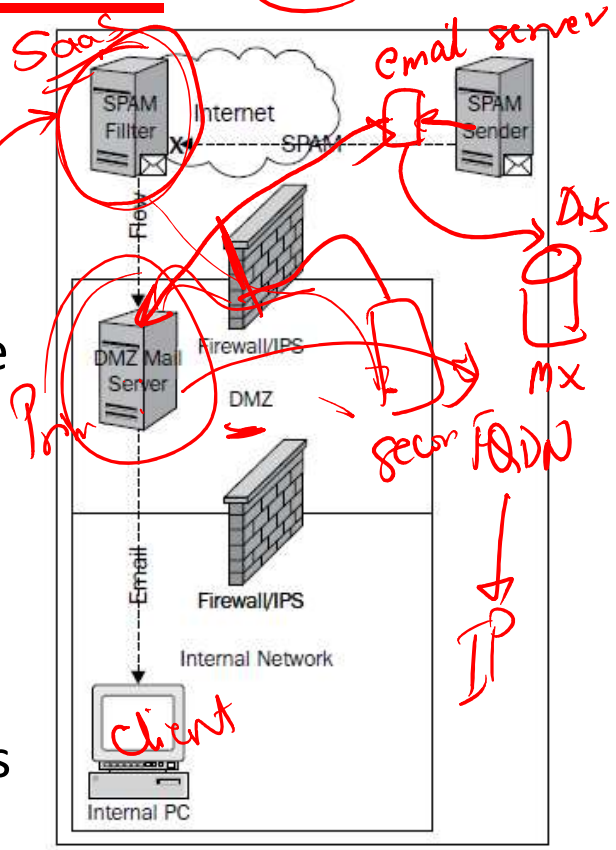
- Email service is a critical business function
- With the increased growth and acceptance of cloud-based services, e-mail is amongst the first to be leveraged
- Some enterprises have already moved their e-mail implementation to the cloud
  - + Enables lower cost and *as-a-service* implementation
  - - 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

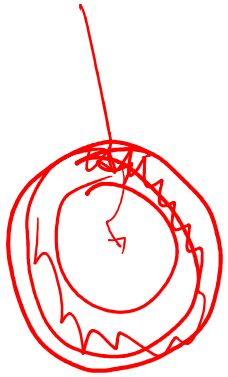
A mail exchanger record (MX record) specifies the mail server responsible for accepting email messages on behalf of a domain name. It is a resource record in the Domain Name System (DNS). It is possible to configure several MX records, typically pointing to an array of mail servers for load balancing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

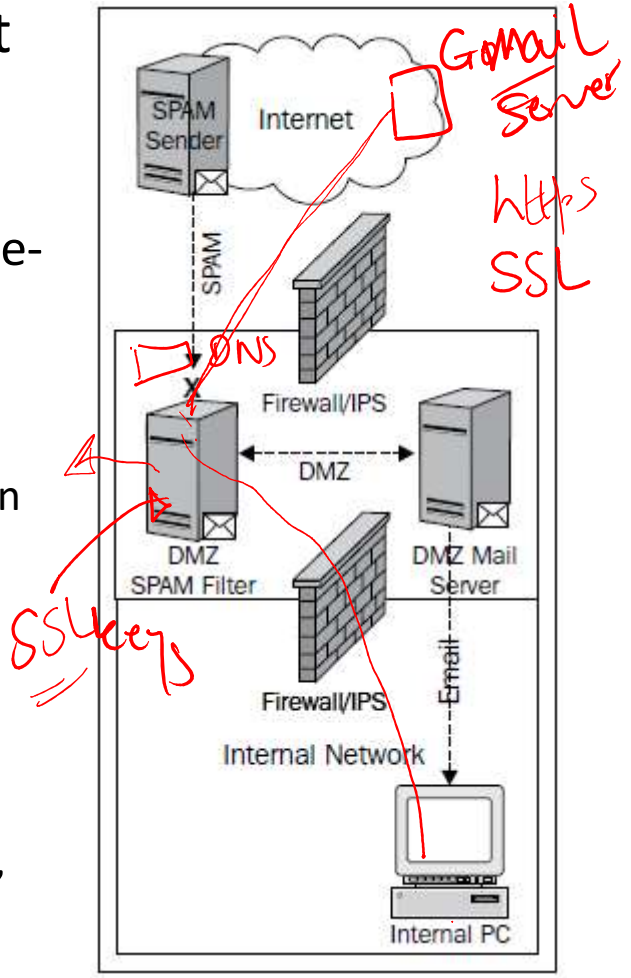
NS: Spam Filtering @ Cloud (2)

- 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)

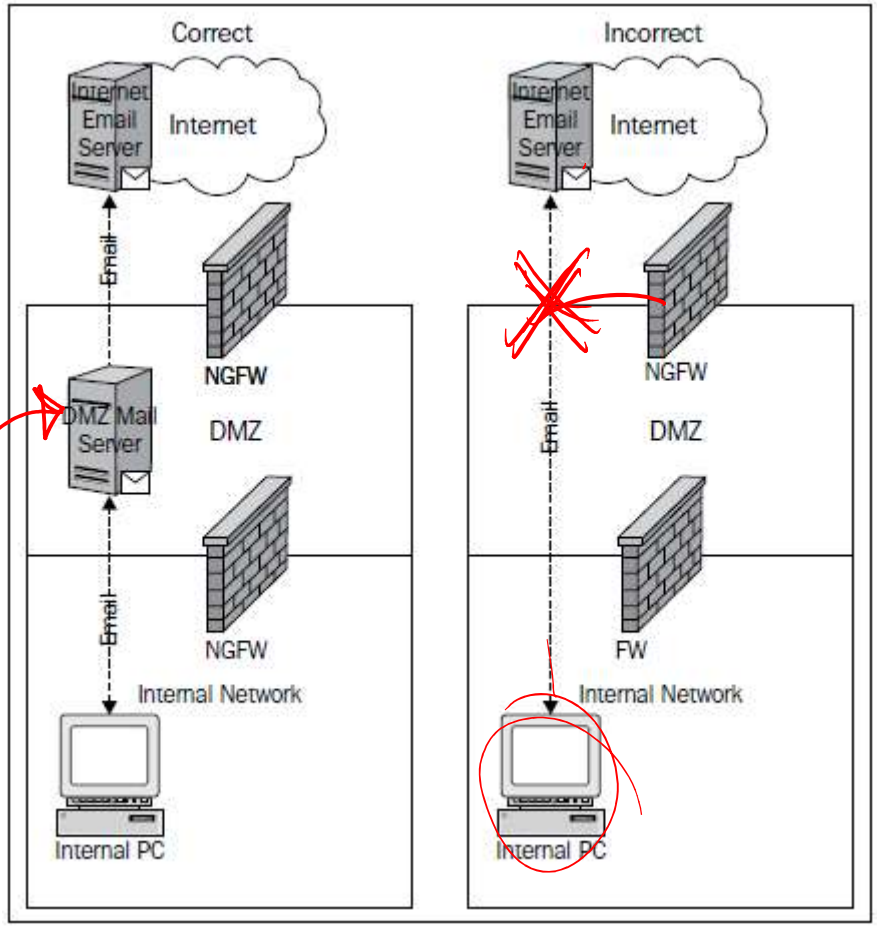
- Pros and Cons:
  - + more control over configuration of filters
  - + vendor continuously updates the appliance to include new block list updates and signatures
  - + ability to also own the DNS infrastructure that tells other e-mail systems where to send e-mail
    - In the event of appliance failure, 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

Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

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

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 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

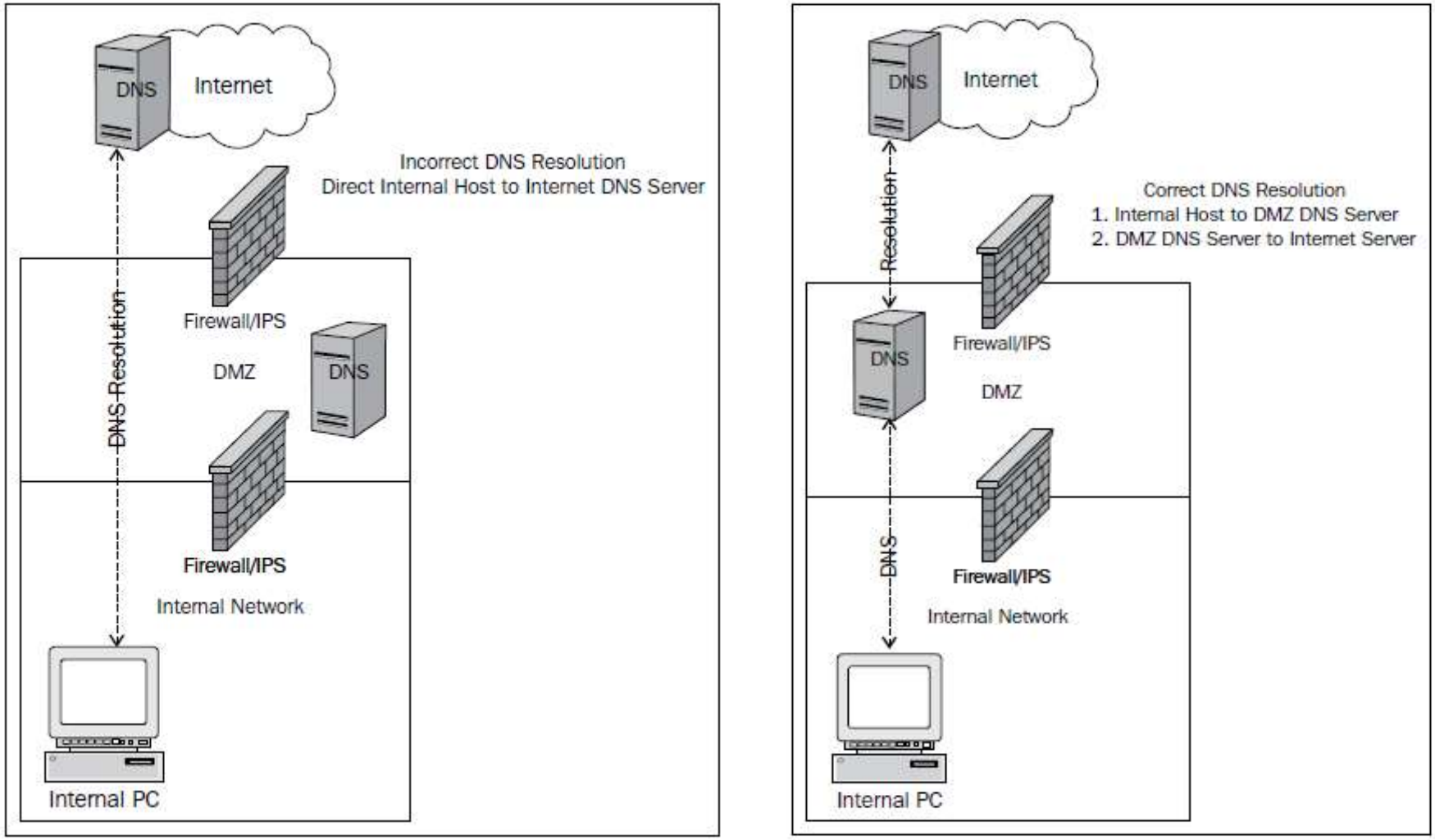
NS: DNS Service Security

- 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

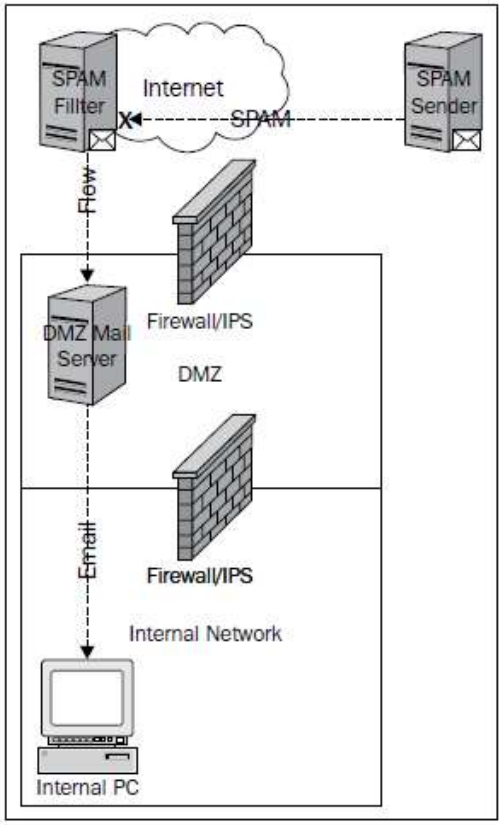
- Email service is a critical business function
- With the increased growth and acceptance of cloud-based services, e-mail is amongst the first to be leveraged
- Some enterprises have already moved their e-mail implementation to the cloud
  - + Enables lower cost and *as-a-service* implementation
  - - 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

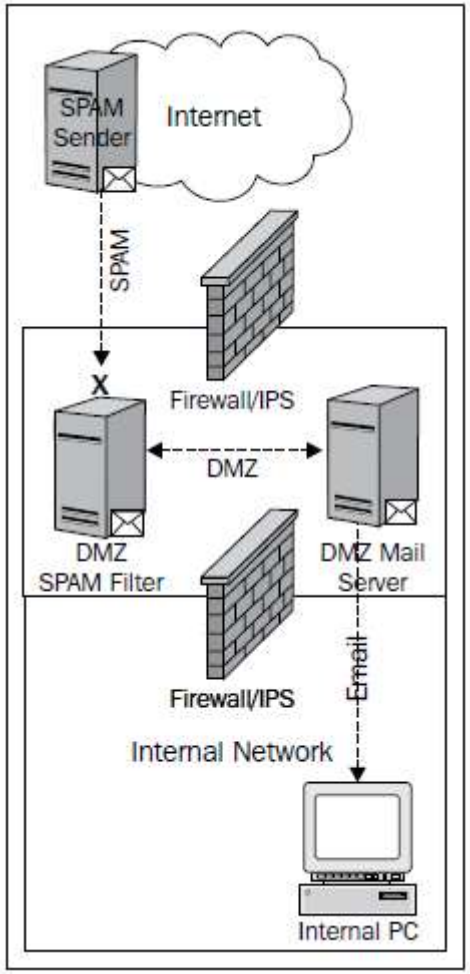
A mail exchanger record (MX record) specifies the mail server responsible for accepting email messages on behalf of a domain name. It is a resource record in the Domain Name System (DNS). It is possible to configure several MX records, typically pointing to an array of mail servers for load balancing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

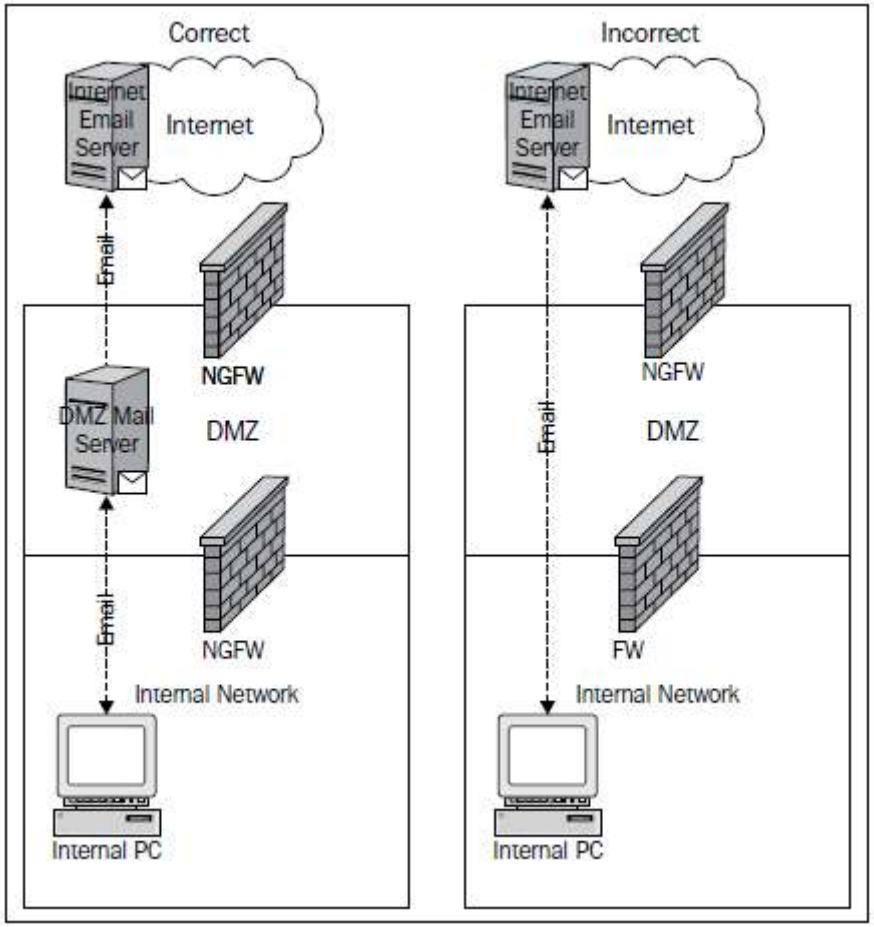
- Pros and Cons:
  - + more control over configuration of filters
  - + vendor continuously updates the appliance to include new block list updates and signatures
  - + ability to also own the DNS infrastructure that tells other e-mail systems where to send e-mail
    - In the event of appliance failure, 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)

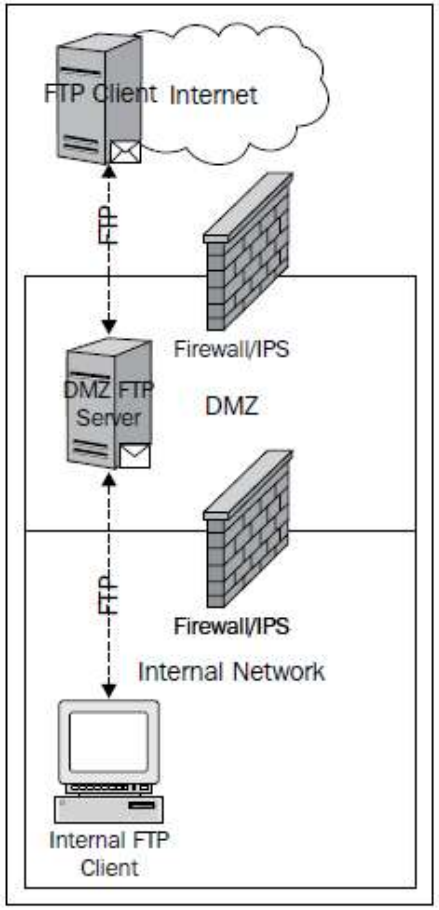
- Prevention:
  - Implement e-mail controls at the firewall to ensure that only the internal mail servers are able to directly send e-mails to the Internet
  - This method reduces the potential impact of end system malware, designed to send SPAM from inside the network
  - Some malware is specifically 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



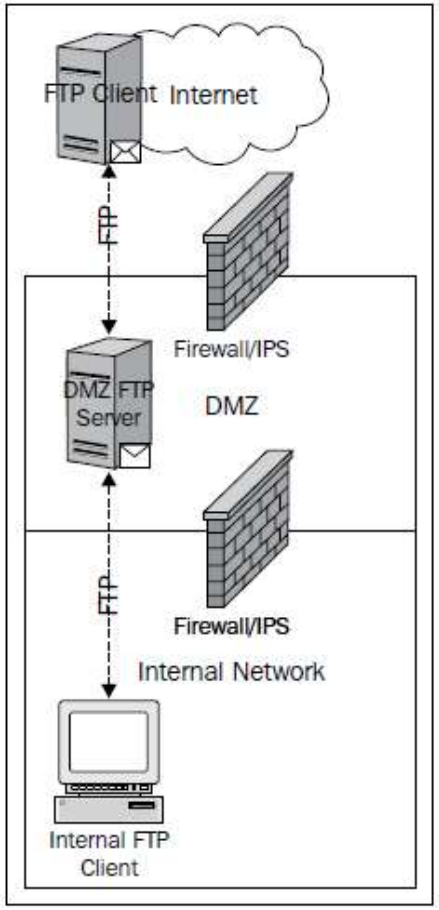
Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

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

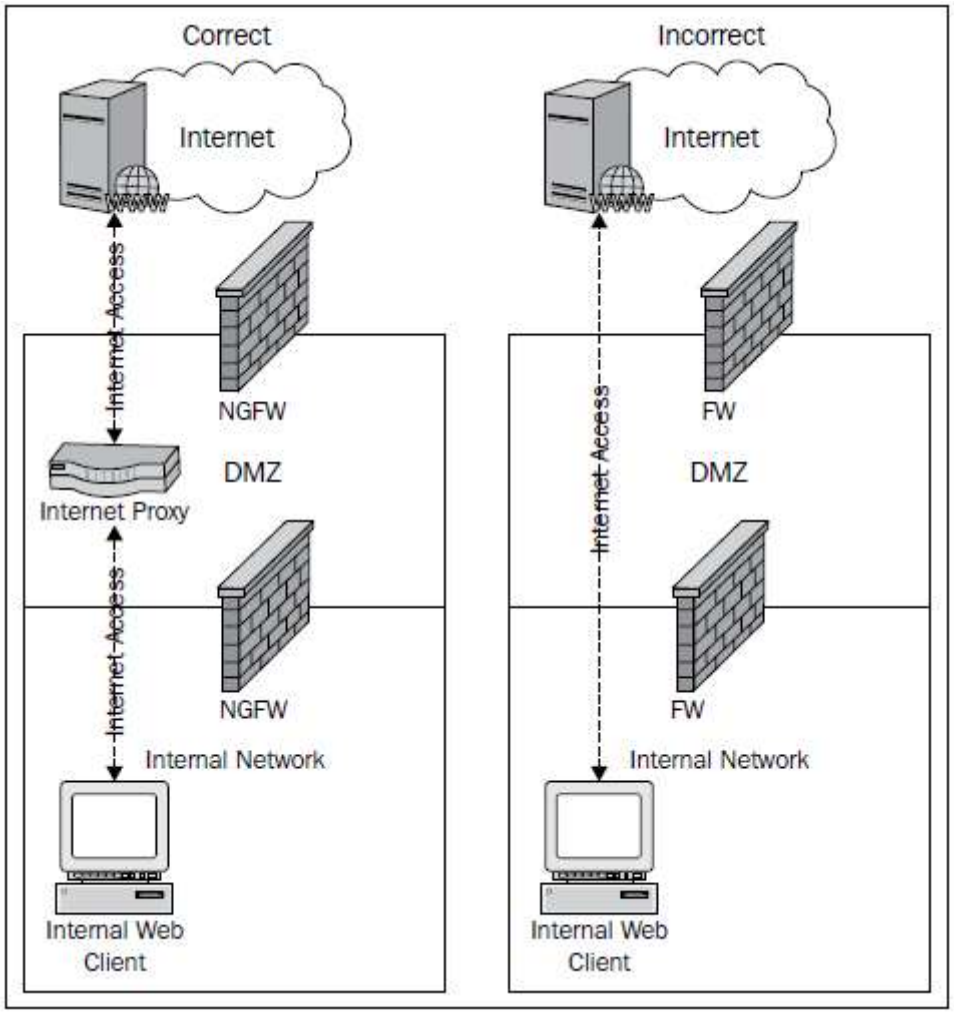
- Not all enterprises that have implemented secure protocols use a secure file transfer
  - Choice by design, such as credit card authorizers, where the risk is accepted due to the overhead and complexity of managing secure communications for a high number of clients
- It can be challenging to implement 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

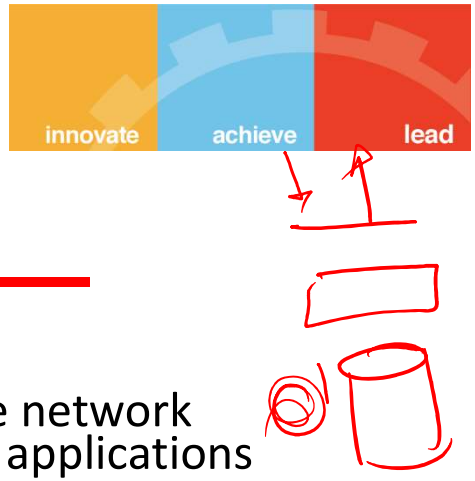
NS: Websites: Secure Coding

- 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



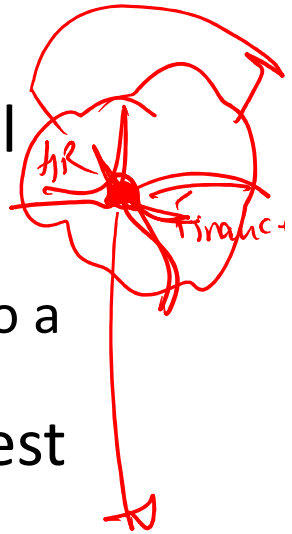
- IPS
  - Intrusion prevention may also be implemented at the network perimeter to mitigate known attack patterns for web applications
  - IPS can provide excellent denial of service protection and block exploit callbacks
- Web-application Firewalls:
  - designed to specifically mitigate attacks against 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



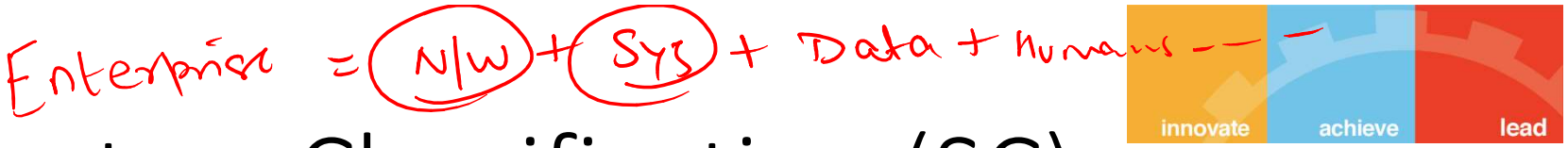
- Before any network segmentation can occur, critical data, processes, applications, and systems must be identified
  - helps determine the complexities of moving the assets to a network segment separated by a firewall
- Network segmentation using a firewall is the simplest network-based security control
- 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



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)

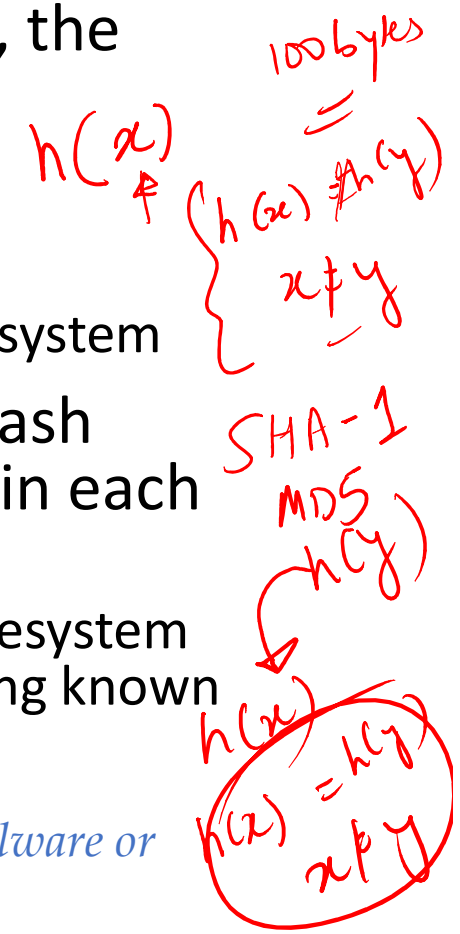
- System patching may be based on
  - A) criticality of the system,
  - B) the severity of the vulnerability, or
  - C) impact of an unpatched software package
- System classification plays a significant role in the patching cycle of systems and must be integrated in the patch and vulnerability management 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

Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

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

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 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?

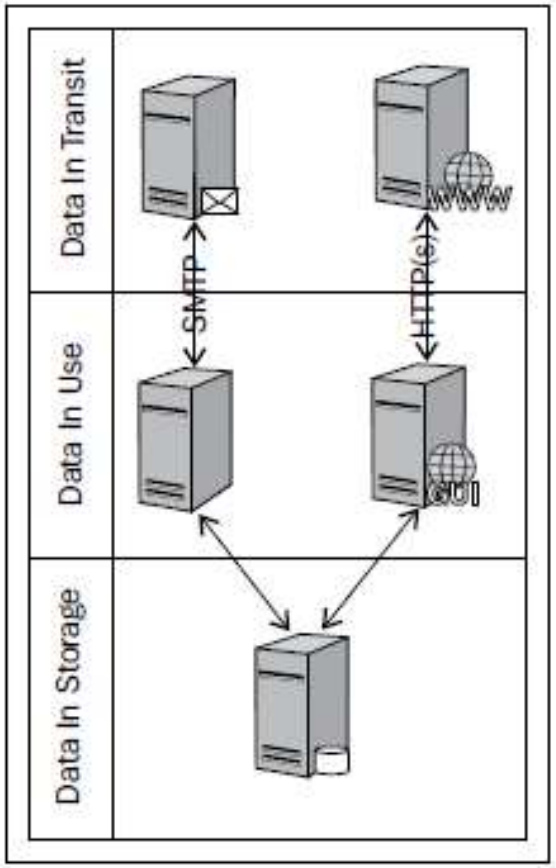
- Developing and enforcing a data classification model is a foundational component to securing enterprise data
- This lecture will focus on the steps required to develop functional data classification and how to protect high-value data in the enterprise
- We shall cover:
  - Data identification and classification ✓
  - 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	Customer: • CC# • PII Employee: • SSN# • PII Company: • Merger Plans • New product	Customer: • PII Employee: • PII Company: • Internal documents	• 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

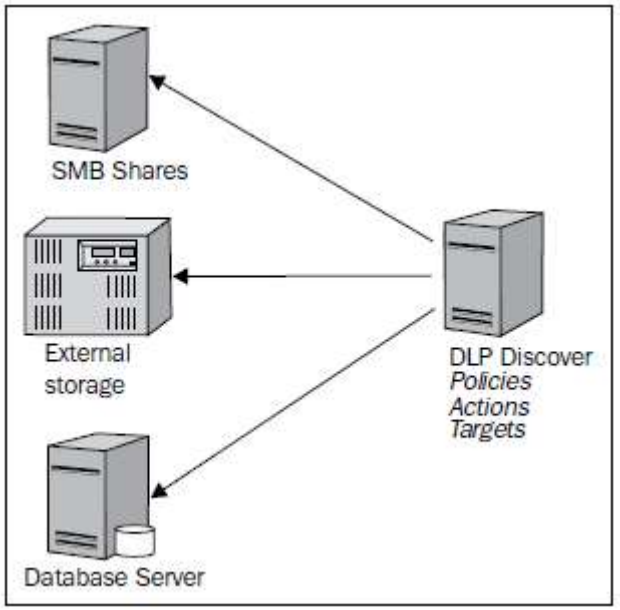
Data Loss Prevention

- **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

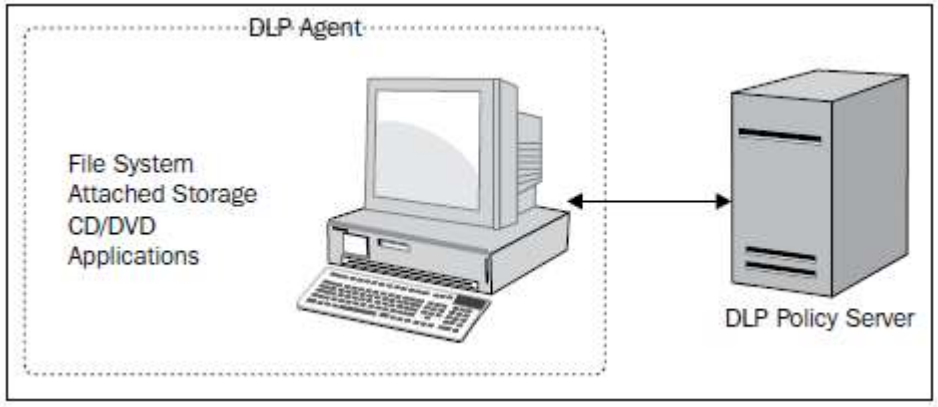
- Data can be stored in network shares, databases, document repositories, online storage, and portable storage devices
- Most DLP solutions have the ability to scan data stores and also provide an agent that can be deployed on end systems to monitor and prevent unauthorized actions for classified enterprise 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

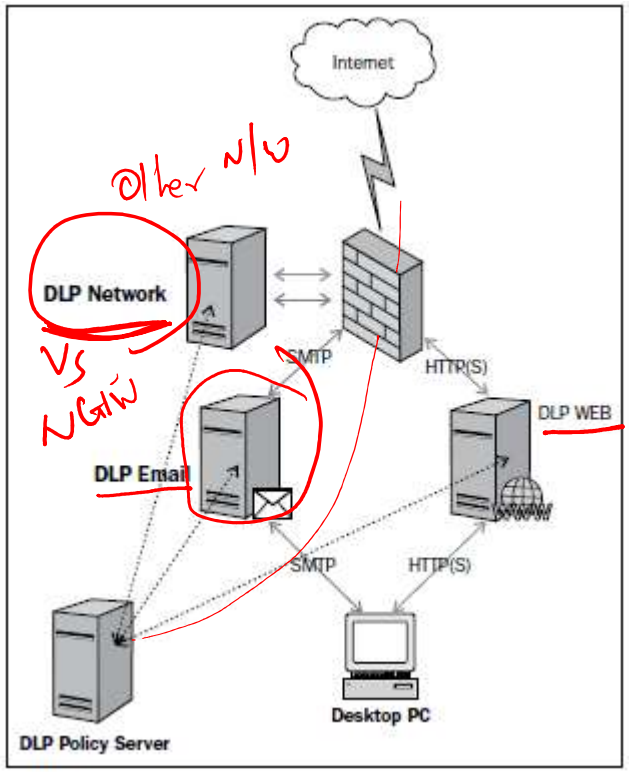
- Data in use is data that is actively processed within an application, process, memory or other location, temporarily for the duration of a function or transaction
  - i.e. enterprise data not stored long term, only long enough to perform a function or transaction
  - there is an application or function 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



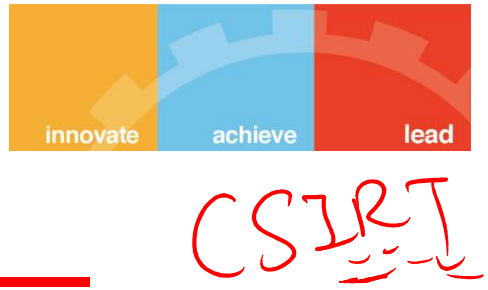
Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

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

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

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, over-flooding 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

Encryption & Hashing

- 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
  - 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

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

Cloud, IoT and Enterprise Security

BITS Pilani

Pilani Campus

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

innovate achieve lead

BITS Pilani

Pilani Campus

<SSCSZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 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

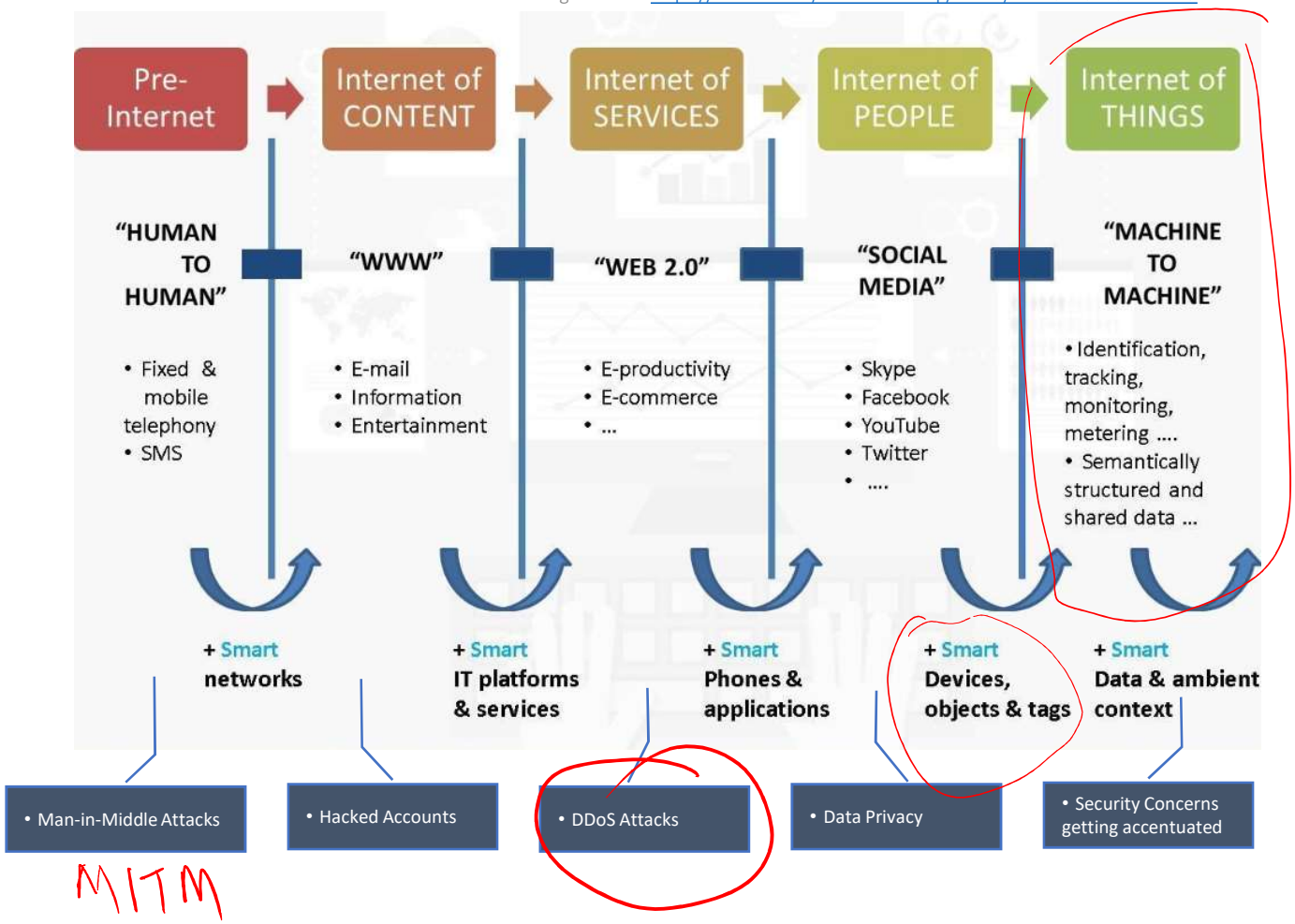
03 The Changing IoT Landscape and What it means for IoT Security

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

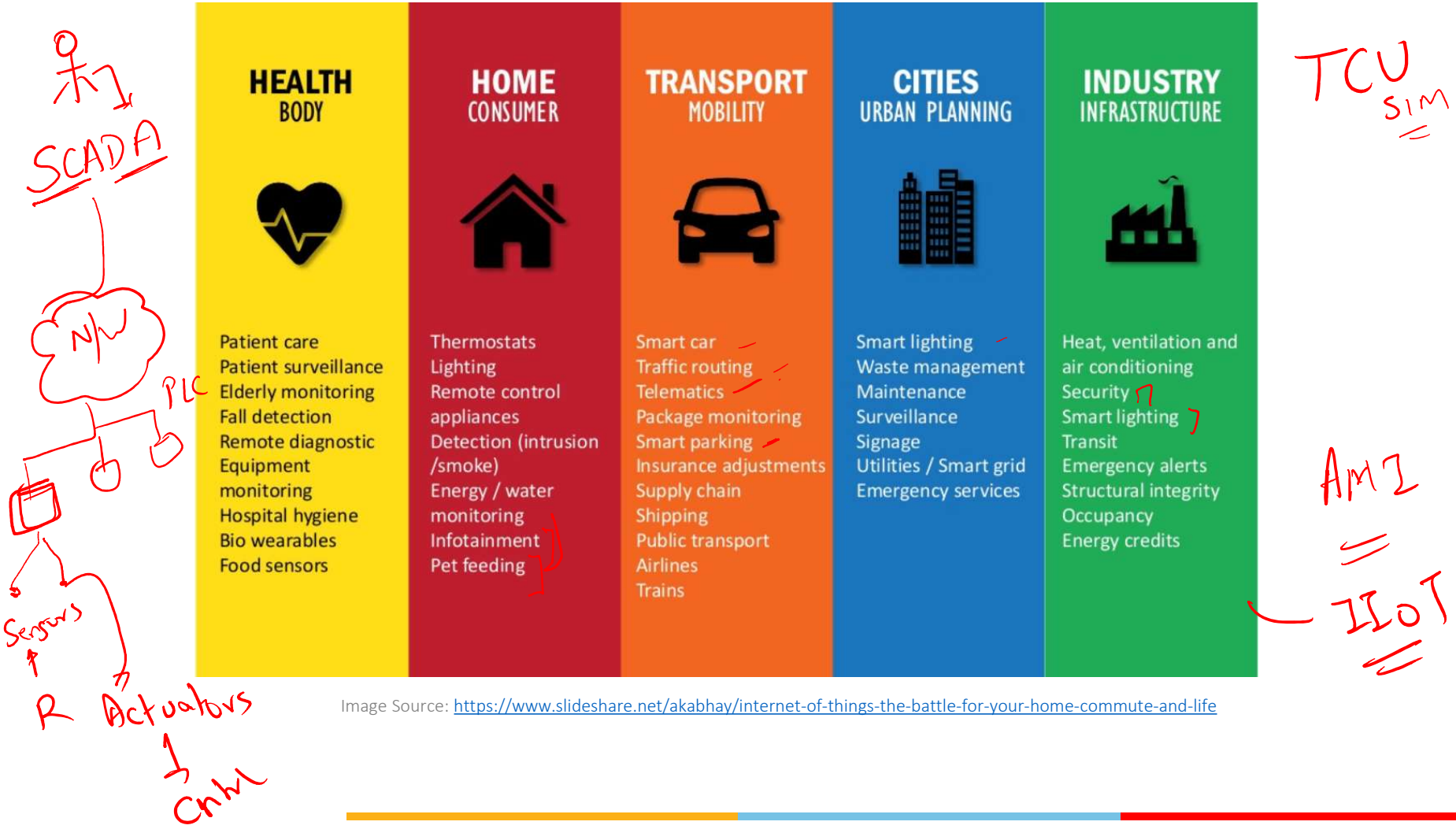
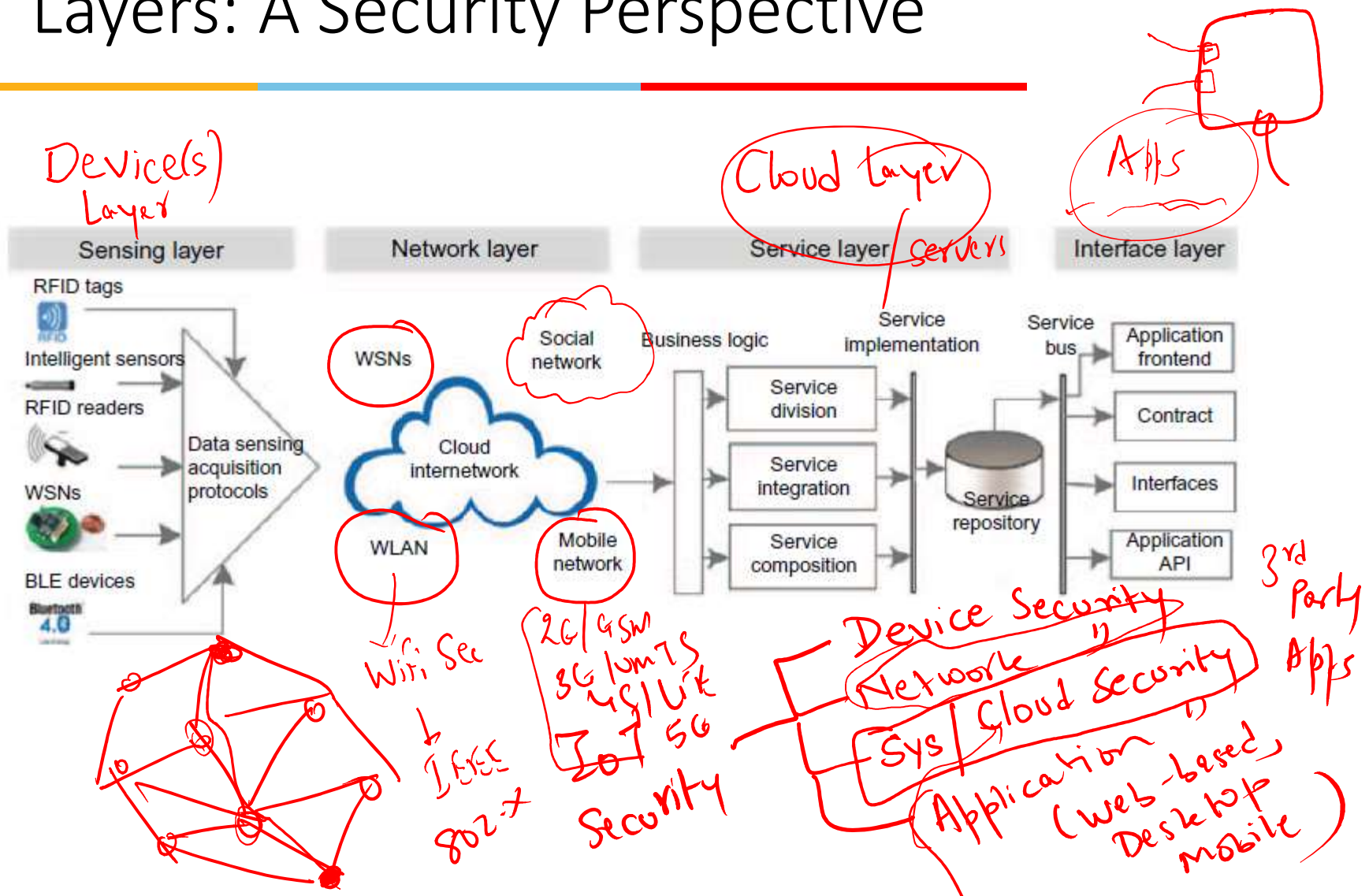


Image Source: https://www.slideshare.net/akabhay/internet-of-things-the-battle-for-your-home-commute-and-life

IoT Layers: A Security Perspective



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

BITS Pilani

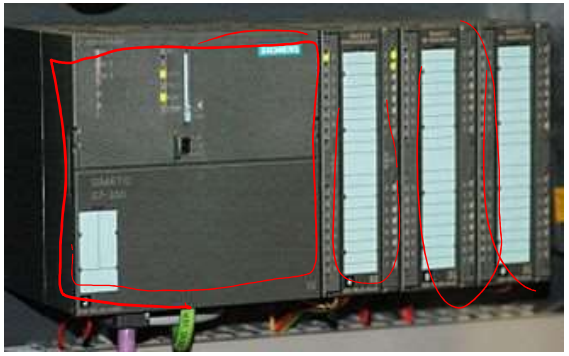
innovate achieve lead

The Stuxnet Attack!

IIoT

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

1100 rpm

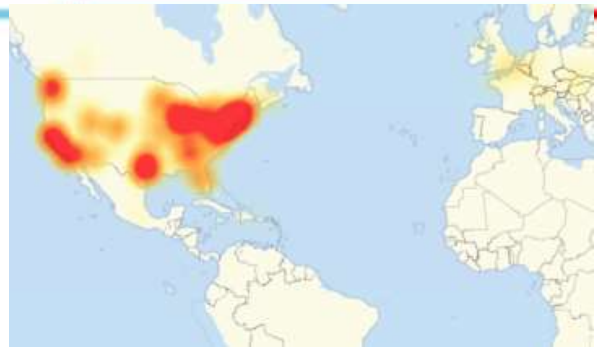
BITS Pilani

innovate achieve lead

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[15]
- *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]
- Pixlr[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

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 fizzle 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?

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

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

HE ECONOMIC TIMES
day

Hackers can track you through your smartband

in.pcmag.com

This randomised address can be decoded with something

- 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

17,129 views | Aug 6, 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 Subex 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-grade 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.

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

Recent, back home….

March 02, 2021

- 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

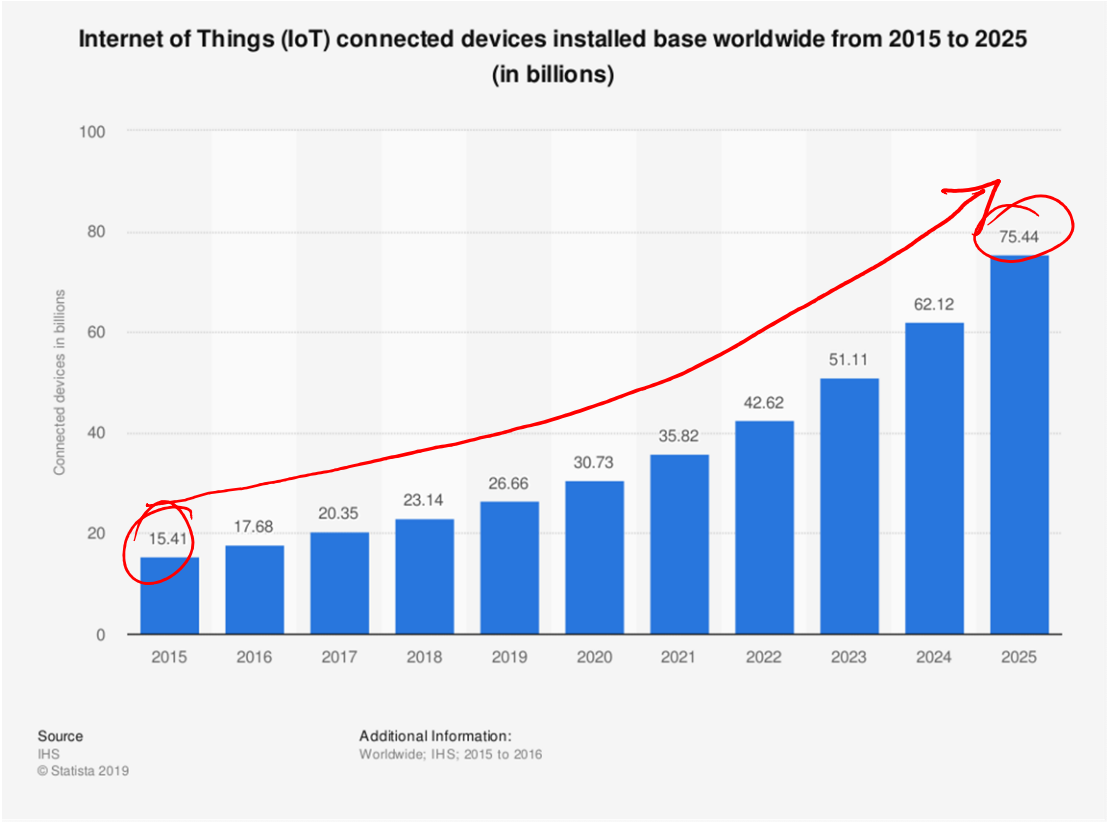


Image Source: https://www.slideshare.net/akabhay/internet-of-things-the-battle-for-your-home-commute-and-life

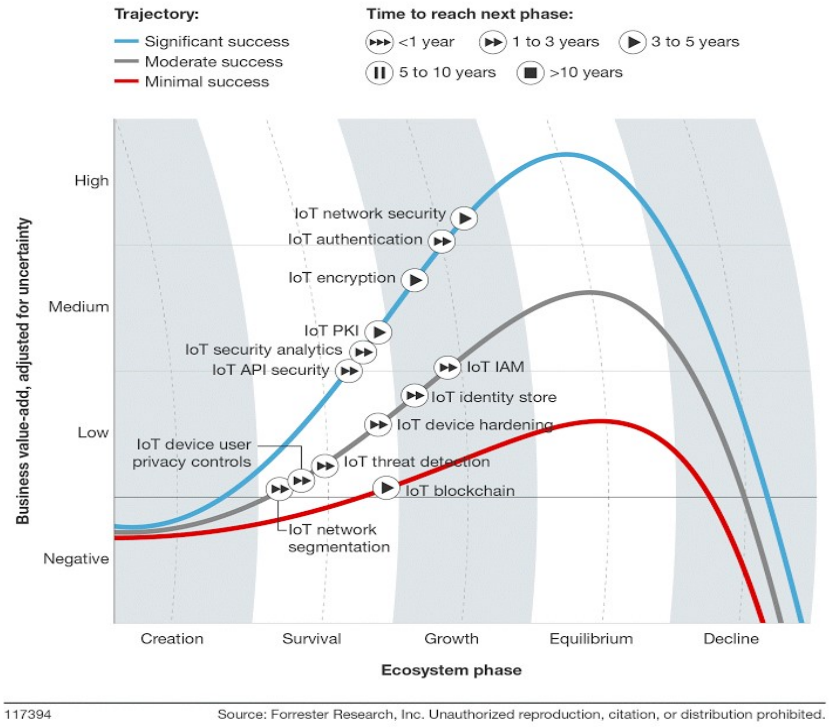
IoT Security: Involved Domains

- 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

FORRESTER® RESEARCH

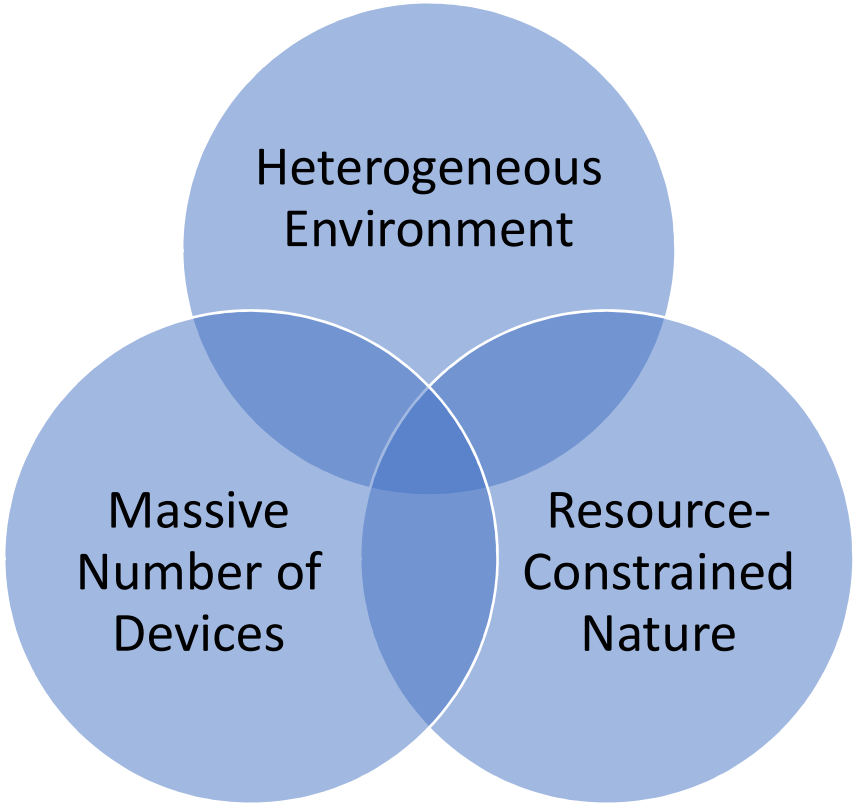
TechRadar™: Internet Of Things Security, Q1 '17

TechRadar™: Internet Of Things Security, Q1 2017



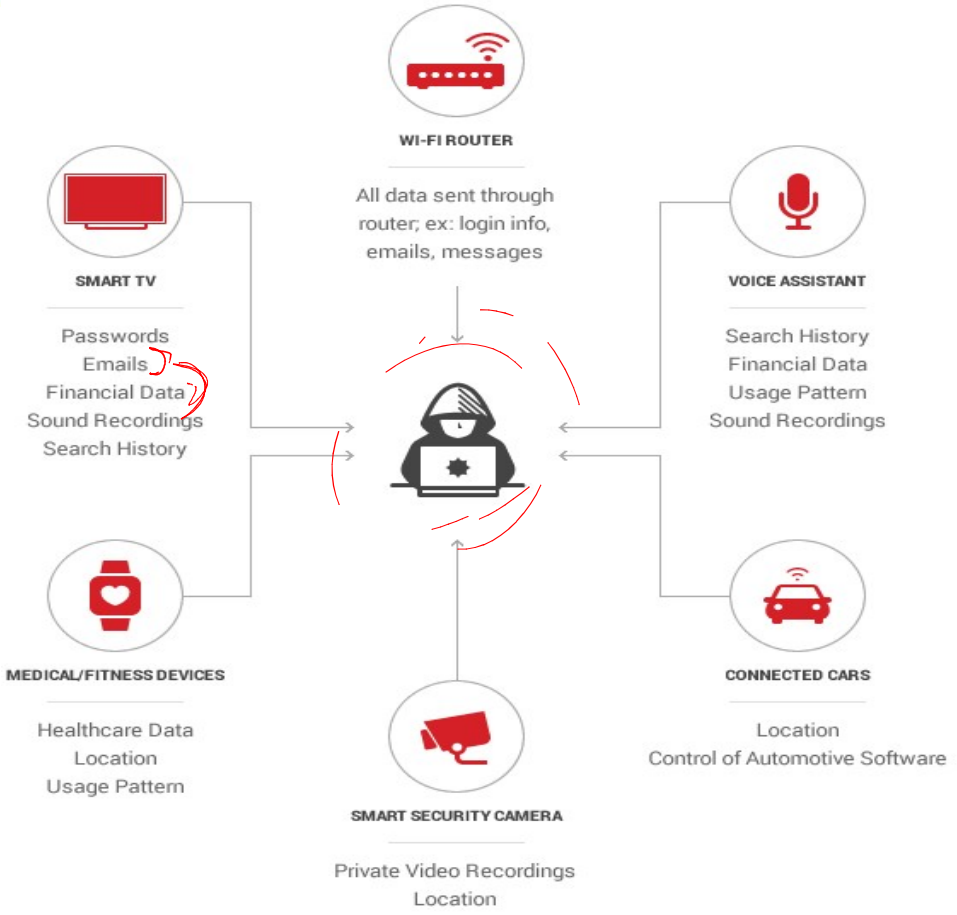
117394 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

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

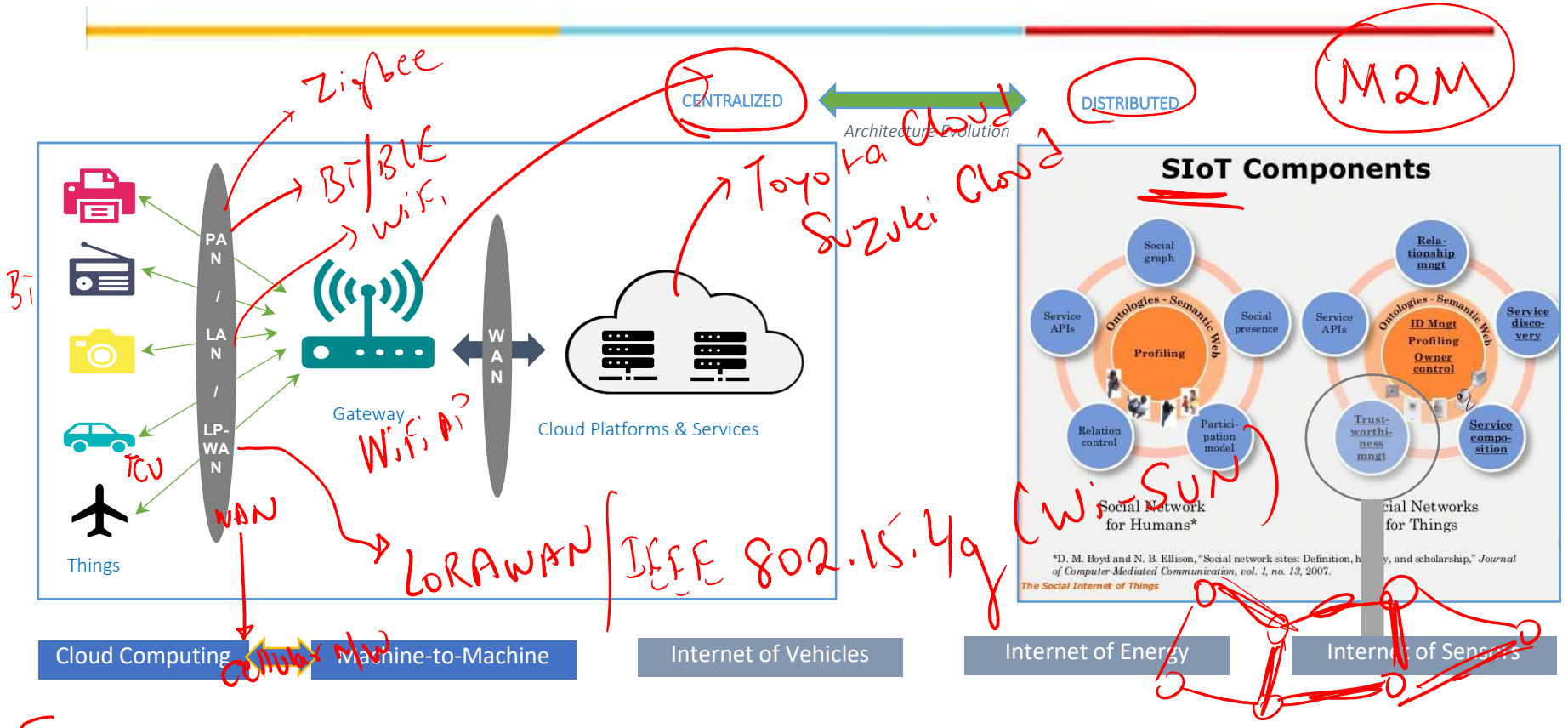


Source: HEIMDAL

BITS Pilani

innovate achieve lead

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

- Unique Device Identification via Secure ID
- Software Integrity: Secure Boot, HW-rooted Trust Chain
- Security Analytics: Identification of Malfunctioning / Compromised Devices
- Data Isolation via defined-access control methods
- Service Management over secure authenticated channels

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