



BITS Pilani

Pilani Campus

Cloud, IoT and Enterprise Security

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



<SS ZG570 , Cloud, IoT and Enterprise Security>

Lecture No. 1: Introduction

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)*

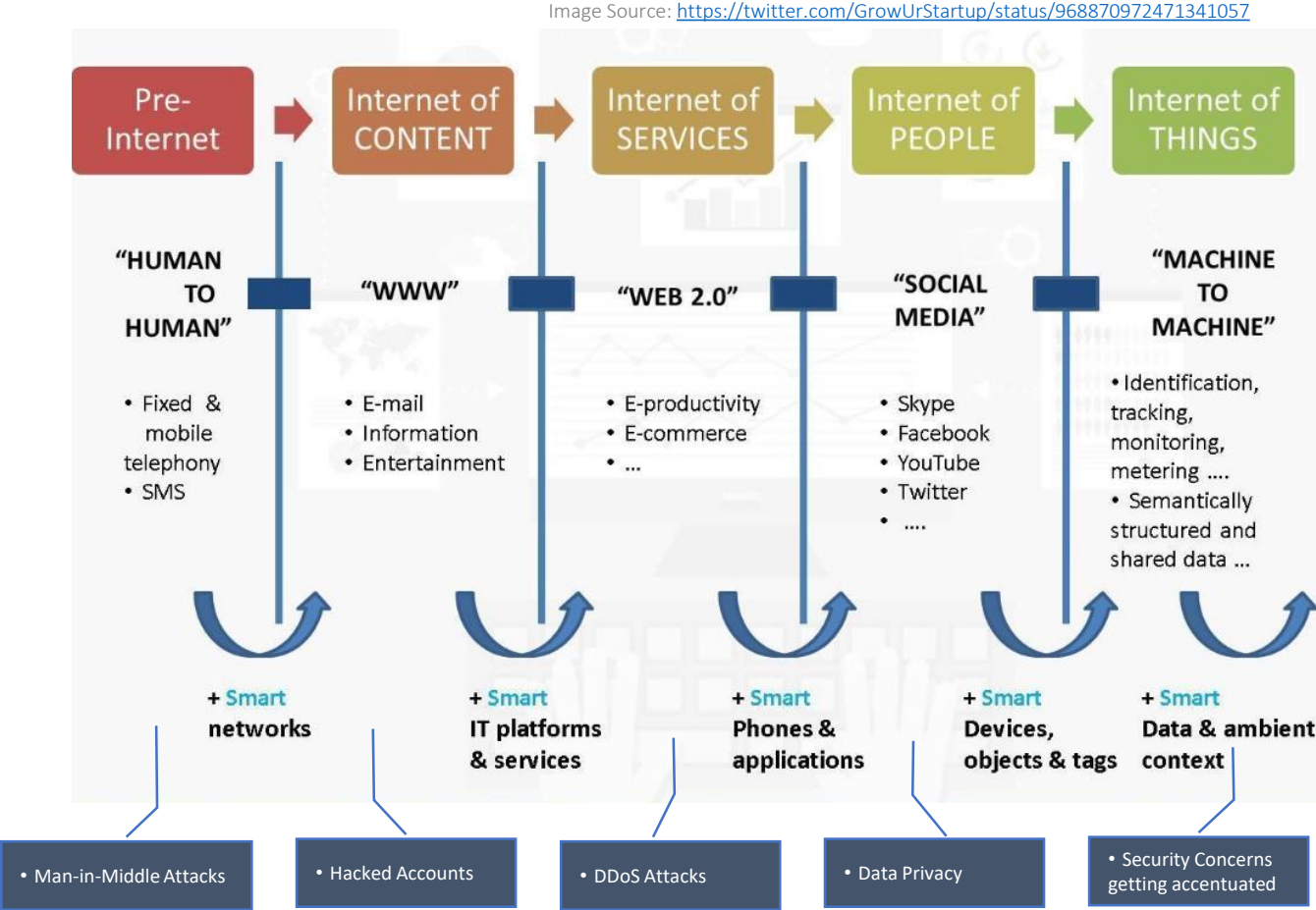


As the world is increasingly interconnected,
everyone shares the responsibility of securing
cyberspace.



- 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

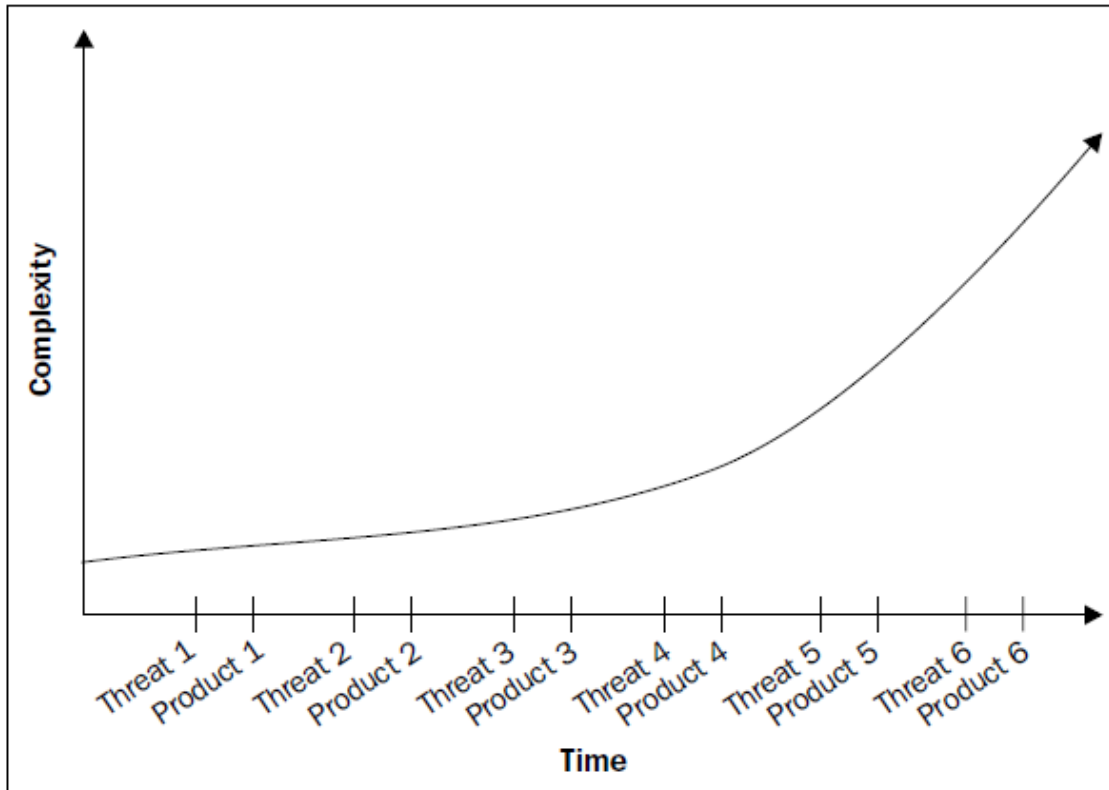
- History of Enterprise Security
 - Older times → no concept of DMZ, as no public Internet existed
 - Only form of Networking in the form of dial-up networking connections → not much security concerns as phone numbers had to be known
 - Modems used to make outbound calls and accept inbound calls to primarily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

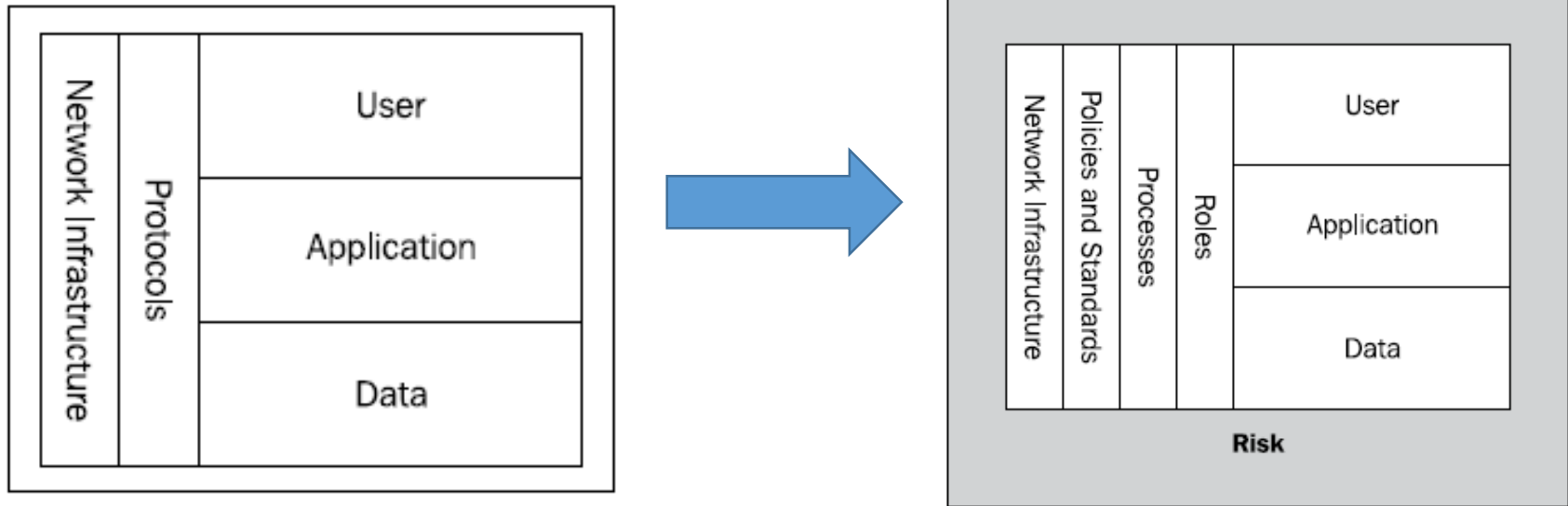
It has led to a relatively secure network perimeter instead of a functioning, extensible, enterprise-wide security architecture



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**