Mississippi State UNIVERSITY

J. A. "Drew" Hamilton, Jr., Ph.D.

Director, Center for Cyber Innovation

Professor, Computer Science & Engineering

CCI
Post Office Box 9627
Mississippi State, MS 39762

Voice: (662) 325-2294
Fax: (662) 325-7692
hamilton@cci.msstate.edu

Architecture Frameworks and Secure Network Architectures
Architecture & Design

Reference:

Drew Hamilton Lecture Notes
William Lee

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Architecture & Design

Reference:

Drew Hamilton Lecture Notes
William Lee

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Domain Outline

- Architecture Frameworks and Secure Network Architectures
- Secure Systems Design and Deployment
- Embedded Systems
- Application Development and Deployment
- Cloud and Virtualization
- Resiliency and Automation Strategies
- Physical Security Controls

Architecture and Frameworks

- **Industry-standard frameworks**
  - An overview of the objective and the methods to achieve that objective.
- **Reference architectures**
  - More detailed than a framework.
  - Specifies components, technologies, and protocols to achieve an objective.
- **Types of frameworks/ architectures**
  - Regulatory
  - Non-regulatory
  - National vs. international
  - Industry specific frameworks

Types of Frameworks/ Architectures

- **Regulatory**
  - When supervisory bodies create and approve standards for industries that are regulated by the government.
  - Together these standards provide a reference framework/ architecture for regulated services.
- **Non-regulatory**
  - Are generally technology focused and are considered optional.
  - They can be used by the government, but aren't government driven.

Types of Frameworks/ Architectures

- National
  - Frameworks and architecture that are only used within ones country.
- International
  - Frameworks and architectures that have become the standard for several countries.
  - These countries tend to created the framework or architecture together so that all sides are in agreement.
- Industry specific frameworks
  - Frameworks developed to address the needs of a particular industry.

Models Capturing Security Architecture

- Designing a security architecture requires capturing the architecture in an appropriate way.
- The representation should be clear, concise and consistent to facilitate easy analysis and comparison of architectures.

Models for capturing architecture:

1) The Domain Approach is easy to understand and would allow a concise representation of an organization's discrete information sets along with any appropriate physical elements such as buildings, server rooms, and printers.
2) The Defense Architecture Framework (DoDAF) does not deal specifically with information security, and is likely too broad to be ideally suited to architecture capture.
3) 3) The International Common Criteria's Protection Profiles are formal documents that could certainly capture security architecture, but perhaps at an unnecessary level of detail.

Benchmark/ Secure Config. Guides

- **Definition**
  - Provide guidance and documentation on how to set up and operate a computer system with security in mind.
- **Type of guides**
  - Web server
    - Connection between users and a webpage.
  - Operating system
    - Interface between an application and computer hardware.
  - Application server
    - Handles specific IT system tasks.
  - Network infrastructure devices
    - Devices like switches, routers, firewalls, etc.

Defense-in-Depth/ Layered Security

- **Definition**
  - Multiple methods of security are implemented in order to increase the overall security of the system
- **Types of layered security**
  - Vendor diversity
  - Control diversity
  - Administrative
  - Technical
  - User training

Types of Layered Security

- **Vendor diversity**
  - Having multiple suppliers reduces the risk of failure if one vendor has a problem.
- **Control diversity**
  - Having both technical and administrative controls in place.
  - Administrative controls are polices created by management.
  - Technical controls are technological methods placed on a system like user authentication.
- **User training**
  - Help users recognize safe and unsafe work behaviors.

Zones/ Topologies

- **Definition**
  - Having different layers of security with varying amounts of protection. Similar to how a castle has a moat, walls, etc.
- **Types of topologies**
  - DMZ
  - Extranet
  - Intranet
  - Wireless
  - Guest
  - Honeynets
  - NAT
  - Ad Hoc

Types of Topologies

- **DMZ**
  - Creates a buffer in the network between trusted zones and untrusted zones by using firewalls.
- **Extranet**
  - Semi-private network that shares data through the network with other organizations.
- **Intranet**
  - Completely private network that can only share data with people within the organization.
- **Wireless**
  - Transmission of packets of data through non direct links.

Types of Topologies

- **Guest**
  - Section of a network that guests should not have access to so it is usually separated.
- **Honeynets**
  - Collection of honeypots used to mimic an actual site, but is designed to attract attackers.
- **NAT**
  - Translates private IP address to public IP address.
- **Ad Hoc**
  - Directs packets without the use of a central router or switch.

Segregation, Segmentation, Isolation

- **Definition**
  - **Isolation of specific areas of a network, which allows different levels of trust.**
- **Types**
  - **Physical**
  - **Logical (VLAN)**
  - **Virtualization**
  - **Air Gaps**
  - **Tunneling/ VPN**
  - **Site to Site**
  - **Remote Access**

Types of Segregation

- **Physical**
  - Physically separates equipment to handle different classes of traffic.
- **Logical (VLAN)**
  - Virtual version of a LAN that lets computers believe that they are on the same physical network when they are not.
- **Virtualization**
  - Separates equipment logically even if they are in the same location.
- **Air Gaps**
  - Physical and logical separation of a network from other networks.

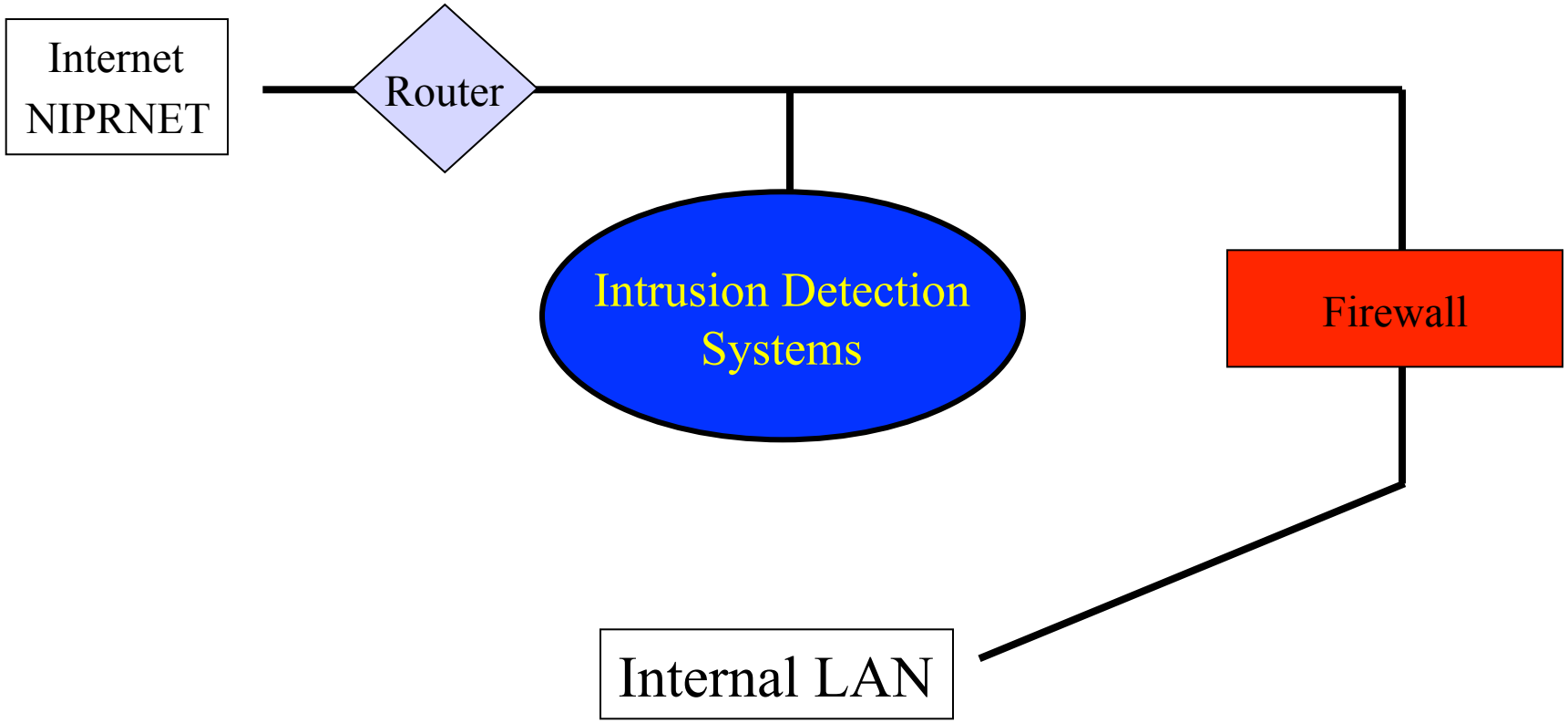
Types of Segregation

- **Tunneling/ VPN**
  - Connects two networks securely across an unsecure network.
- **Site to Site**
  - Links multiple networks through the internet, while using encryption or a VPN to secure data.
- **Remote Access**
  - Connecting to a network while not being there physically through tunneling or VPN.

Security Device/ Tech. Placement

- **Definition**
  - The strategic placement of security devices based on its purpose and required environment
- **Type of devices**
  - Sensors
  - Collectors
  - Correlation engines
  - Filters
  - Proxies
  - Firewalls
  - VPN concentrators
  - SSL accelerators
  - Load balancers
  - DDoS mitigator
  - Aggregation switches
  - Taps and port mirror
  - SDN

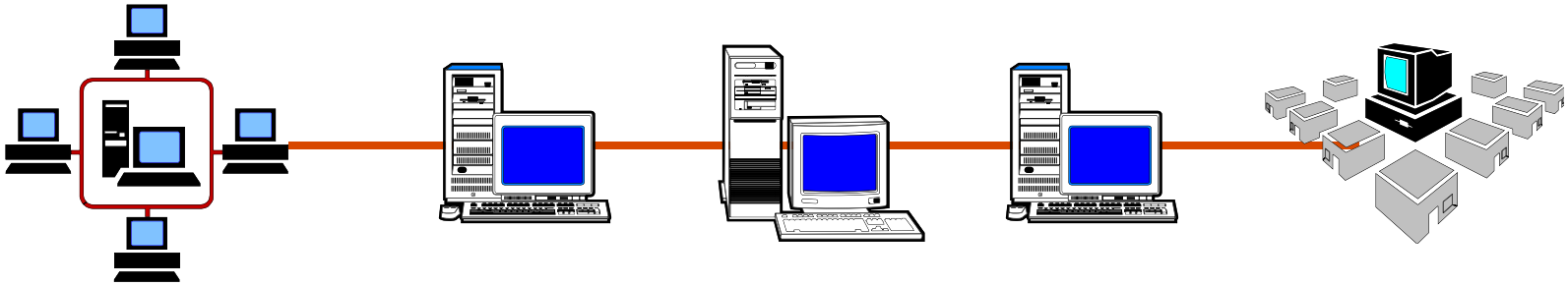
Intrusion Detection Architecture (Simplified)



[**] MISC Large ICMP Packet [**]
04/08-14:35:06.317821 VVV.WWW.XXX.YYY -> AAA.BBB.CCC.DDD
ICMP TTL:108 TOS:0x0 ID:30676 IpLen:20 DgmLen:**65008**
Type:8 Code:0 ID:512 Seq:13792 ECHO
61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop

Multiple Layer Architecture

- In a multiple layer architecture, the firewall functions are distributed among a small number of hosts, typically connected in series, with DMZ networks between them.
- This approach is more difficult to design and operate, but can provide substantially greater security by diversifying the defenses you are implementing.
- The most common design approach for this type of architecture is an Internet firewall composed of two hosts interconnected with one DMZ network.



corporate n/w <--------> firewall <-------> DMZ <------> firewall<-------> Internet

Type of Devices

- **Sensors**
  - Capture data and act upon it by reporting, creating an event log, etc.
- **Collectors**
  - Group of sensors that are being used by another system.
- **Correlation engines**
  - Takes sets of data and compares to other patterns to find a match.
- **Filters**
  - Protects a network by not allowing the passage of unwanted traffic.

Type of Devices

- **Proxies**
  - Servers that are between the client and other systems.
- **Firewalls**
  - Determine if traffic can pass or not based on predefined rules.
- **VPN concentrators**
  - Terminates multiple VPN connection into a single point of concentration.
- **SSL accelerators**
  - Provides SSL/ TLS encryption and decryption to reduce the load on the webserver.

Type of Devices

- **Load balancers**
  - Distributes traffic across multiple network operations.
- **DDoS mitigator**
  - Protects the network from being flooded with unwanted traffic.
- **Aggregation switches**
  - One switch that several other switches can connect to which reduces the number of connections.
- **Taps and port mirror**
  - Can copy the activity of one or more ports.
- **SDN**
  - Manages the network control layer.

Secure Systems Design and Deployment
Architecture & Design

Reference:

Drew Hamilton Lecture Notes

William Lee

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Hardware/ Firmware Security

- **Definition**
  - **Methods used to protect against unauthorized access to hardware.**
- **Types of hardware/ firmware security**
  - **FDE/ SED**
  - **TPM**
  - **HSM**
  - **UEFI/ BIOS**
  - **Secure boot and attestation**
  - **Supply chain**
  - **Hardware root of trust**
  - **EMI/ EMP**

Types of Hardware/ Firmware Security

- **FDE/ SED**
  - Cryptographic protection on the hard disk to protect it even if it is taken out of the machine.
- **TPM**
  - Allows for storing encryption keys in a way so that they are physically separated from the hard drive.
- **HSM**
  - External devices used to manage encryption keys.
  - Comes with tamper protections to prevent physical access to key data.
- **UEFI/ BIOS**
  - All new BIOS are UEFI based, which increases security.

Types of Hardware/ Firmware Security

- **Secure boot and attestation**
  - Using UEFI only signed drivers and OS loaders are invoked at boot time which prevents malware from initializing during the boot cycle.
- **Supply chain**
  - Manufactures typically have a supply chain, which makes it hard to track where each individual component of a device originates from.
- **Hardware root of trust**
  - If one layer has trusted security functions then these functions can be used at higher layers.
- **EMI/ EMP**
  - Interference that affects an electrical circuit.

Operating Systems

- **Definition**
  - Interface used by an application to communicate with other applications or the computer hardware.
- **Types of operating systems**
  - Network
  - Server
  - Workstation
  - Appliance
  - Kiosk
  - Mobile OS

Types of Operating Systems

- **Network**
  - Provides the configuration and computation of the network.
- **Server**
  - Connects the server hardware with the server applications
- **Workstation**
  - Provides a GUI for users to visually interact with the interface.

Types of Operating Systems

- **Appliance**
  - Devices wired into the network to perform specific tasks on network traffic.
  - Usually run a Linux based OS
- **Kiosk**
  - These OS are usually very limited to restrict the changes that users can make.
  - Usually consists of a browser locked on one webpage.
- **Mobile OS**
  - Allows users to run applications and tasks on there mobile device.

Patch Management

- **Definition**
  - Software updates to an operating system.
- **Types of patch management**
  - Hotfix
    - Small updates, that are developed quickly to address a specific problem.
  - Patch
    - Large update that addresses several problems or bugs.
    - Can contain additional features and enhancements.
    - Developed over a long period of time.
  - Service pack
    - Several patches and hotfixes combined into on update.
    - Brings the original software up to date from one install.

Disabling Ports and Services

- **Definition**
  - Only enable items that are absolutely needed for the system to function.
- **Methods**
  - Least functionality
  - Hardening
  - Trusted operating system
  - Application whitelisting/ blacklisting
  - Disable default accounts

Disabling Ports and Services

- **Least functionality**
  - A system should only do what it is designed to do and nothing else.
- **Hardening**
  - Removing all unnecessary software and services.
- **Trusted operating system**
  - An OS that allows multi-level security.
- **Application whitelisting/ blacklisting**
  - List of applications that should and shouldn't be allowed.
- **Disable default accounts**
  - Disabling default accounts increases security.

Peripherals

- **Definition**
  - External devices that interact with a host system.
  - Many peripherals have embedded computers, which can lead to hacking attempts.
- **Type of peripherals**
  - Mouse
  - Keyboard
  - Displays
  - SD Cards
  - Printers

Sandboxing

- Definition
  - The isolation of a component in a system.
  - Limits interaction with the CPU and other processes.
- Type of sandboxing
  - Development
  - Test
  - Staging
  - Production
- Secure baseline
- Integrity measure

Sandboxing

- **Development**
  - Set up for developer to work on new features for a particular software.
- **Test**
  - After developing the updated software is tested.
  - Testing environment attempts to mimic the production environment.
- **Staging**
  - Optional environment where additional testing can occur.
- **Production**
  - Where the system works in a real world setting.

Embedded Systems Architecture & Design

Reference:

Drew Hamilton Lecture Notes

William Lee

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Embedded Systems

- **Definition**
  - **Essential computers that play a role in a larger system of devices.**
- **Type of embedded systems**
  - **SCADA/ICS**
    - **Designed to control automated systems in cyber-physical environments.**
    - **Has multiple components used together to achieve a certain functionality.**
  - **Smart devices/ IoT**
    - **Devices that have the capability of connecting to other devices and sharing information with each other.**
    - **Examples include: wearable technology, home automation, HVAC system, SoC, and RTOS.**

What is SCADA/ICS

- **Supervisory Control and Data Acquisition (SCADA) systems:**
  - **monitor, control, and collect data for industrial systems like gas pipelines, oil refineries, and transmission lines, which are remotely accessible.**
  - **Systems like SCADA, Industrial Control Systems (ICS) and Programmable Logic Controllers (PLC) are used in many places to remotely control valves and other industrial devices.**
  - **The basic SCADA architecture begins with programmable logic controllers (PLCs) or remote terminal units (RTUs). PLCs and RTUs are microcomputers that communicate with an array of objects such as factory machines, HMIs, sensors, and end devices, and then route the information from those objects to computers with SCADA software.**
    - **The SCADA software processes, distributes, and displays the data, helping operators and other employees analyze the data and make important decisions.**

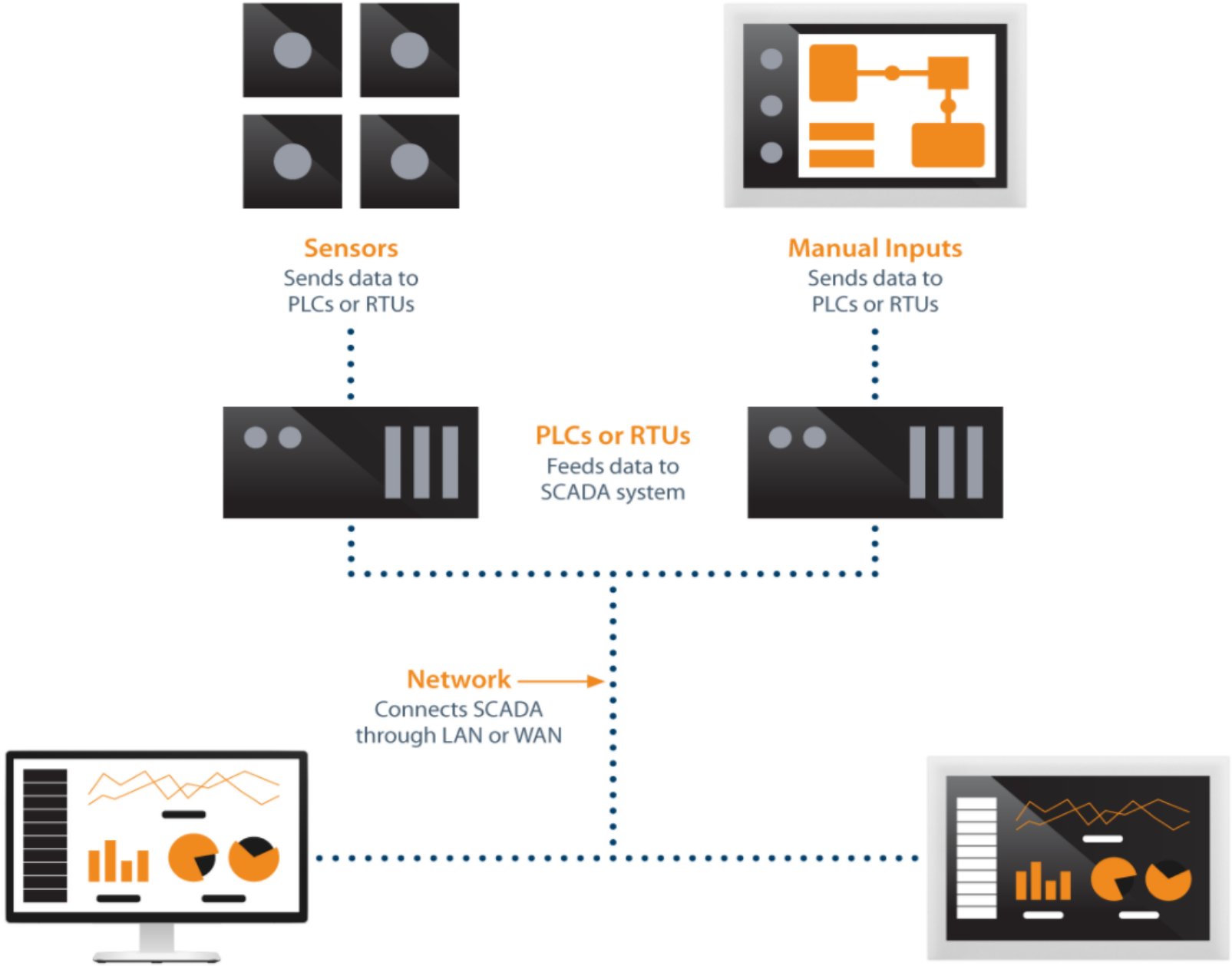
Vulnerabilities

- Simple SCADA architectures have limited vulnerabilities, but companies want ease of access and often intertwine them with corporate networks, vendor connects, websites, and other connections multiplying vulnerabilities.
- Cyber threats can target vulnerabilities and cause temporary disruptions or catastrophic failures that could have greater impacts. Terrorist activity via SCADA or PLC access could cause disruptions to the energy supply chain, and initiate environmental crisis' that would also generate economic pressure.
- SCADA/PLCs systems are the backbone of many modern industries spread across the 16 Critical Infrastructures in valves for damns, pipelines, rail systems, telecommunications, energy, etc.

Scale of the Problem

- A study by Cambridge University found greater than 10,000 control systems connected to the internet and only 17% had some sort of access control.
- Many of these devices are wide open with use of hard coded user and passwords.
- The Energy Supply Chain is at risk due to cyber vulnerabilities jeopardizing U.S Energy Security and we are in a race to prevent disruption .

Reference: Rajeev Kumar, M.L. Dewal, Kalpana Saini, Utility in Power Generation and Distribution System Online, IEEEXplore, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05564689, pg 648, (accessed May 21 2014)


Sensors
Sends data to
PLCs or RTUs
Manual Inputs
Sends data to
PLCs or RTUs
PLCs or RTUs
Feeds data to
SCADA system
Network
Connects SCADA
through LAN or WAN
HMI / SCADA Computer
Supervise and control
from a workstation
inductive
automation
HMI / SCADA Panel View
Supervise and control from
an operator terminal

16 National Critical Infrastructures

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

Threats

- 1st Shot in Cyber War has been fired already!
- People are #1 Vulnerability…7 out of 10 people will click on phishing attack exploit without extensive training.
- A state-actor can get into almost all networks.
  - Our Energy Security is at risk!
  - Critical Infrastructure is at risk!
- Attack Surface is growing exponentially
- Liange & Xiangsui – China PLA "The first rule of unrestricted warfare is that there are no rules, with nothing forbidden"
- Cyber Crime is growing: A 2016 study estimated that the costs of cybercrime could be as high as 2.1 trillion by 2019

Weaknesses

- Attack Surface is growing
  - ubiquitous network, IoT, 5G, Cloud, autonomous…cars, UAV, UGV, etc.
- Easy of Attack vs. Defense
  - Far easier and less costly to attack than to defend a network.
  - Old ICS Systems built for convenience.
- Only 17% of ICS Systems have access control (Cambridge Study of 10,000 systems)
- Hard coded User Name and Passwords
- Never ending Zero Day potential exploits

Opportunities (Services…)

- Service: Cyber Penetration and Vulnerability Testing (Critical Infrastructure, DoD Weapon Systems – Ball model)
- Network development, Defense in Depth
- Service: Network Monitoring, Local/Virtual
  - Subscription - Big Data –massive amounts of data about networks, typical exploits, and create a baseline, and automate standard mitigation steps until the Cavalry can arrive.
- Service: Training
- $100M initial DoD set-aside to understand Cyber Vulnerabilities.
- Critical Infrastructure is basically an Opt In for Do

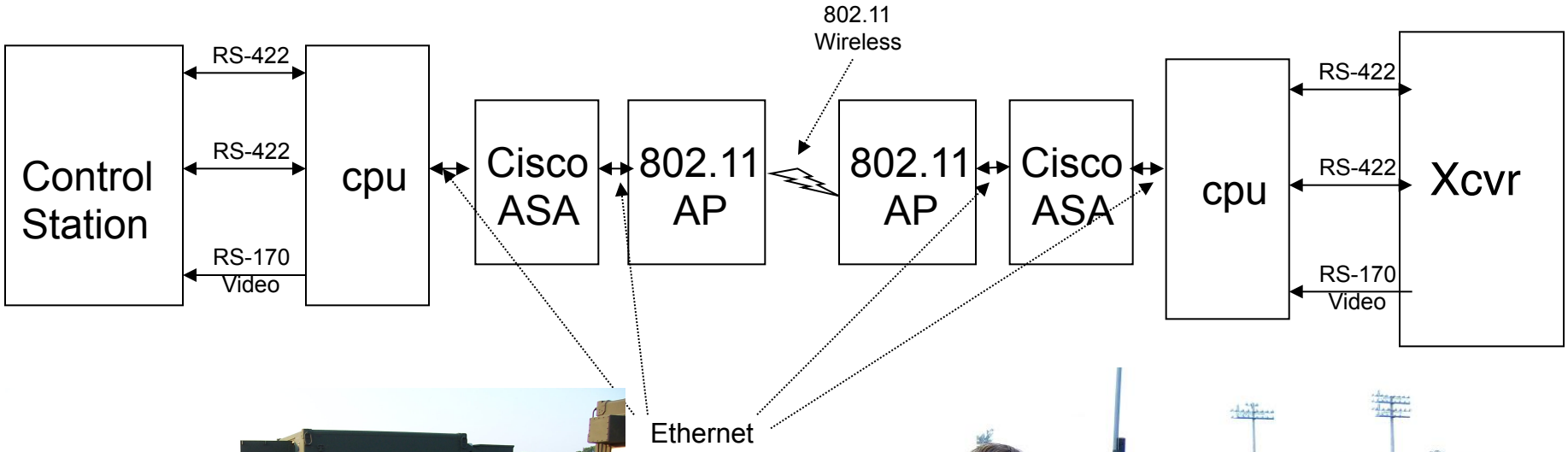
Strengths Required

- Vision & Leadership
- Cyber Expertise – Industry recognized standards to include CISSP, CISM, PMP, Certified Ethical Hacking and Penetration testing, MSCE, CCNA, Network & Network Security Expertise, etc.
- Cyber Security & DoD Network
  - ICS Network, HLD/HLS Power, Gas, Oil, Rail, Communications
- Big Data Software – anticipate/react
- Knowledge to build a team and grow a business

Special Purpose Systems

- **Definition**
  - Systems that are designed to solve a specific problem.
  - Each comes with there own security concerns as well.
- **Types of special purpose systems**
  - Medical devices
  - Vehicles
  - Aircraft/ UAV

Wireless test system for secure UAV ground communications



Application Development and Deployment Architecture & Design

Reference:

Drew Hamilton Lecture Notes

William Lee

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Development Lifecycles

- **Definition**
  - The process of producing software, from its conception to production.
- **Types of lifecycles**
  - Waterfall
  - Agile
  - Scrum
  - XP

Types of Lifecycles

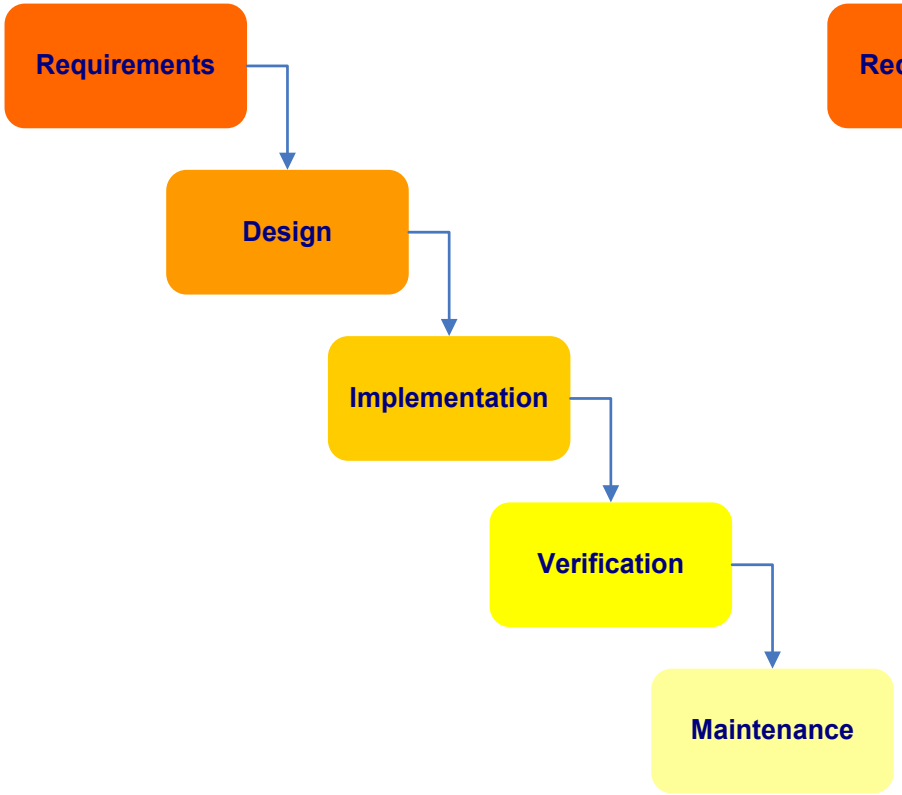
- **Waterfall**
  - Rigid traditional lifecycle where one step leads to the next.
- **Agile**
  - Uses small development cycles so that teams can react to change quickly at the end of a cycle.
- **Scrum**
  - Keep software always ready for release by only having quick, incremental changes.
- **XP**
  - Iterative process that uses acceptance tests to create incremental changes.

System Development Life Cycle (SDLC) Models and Processes

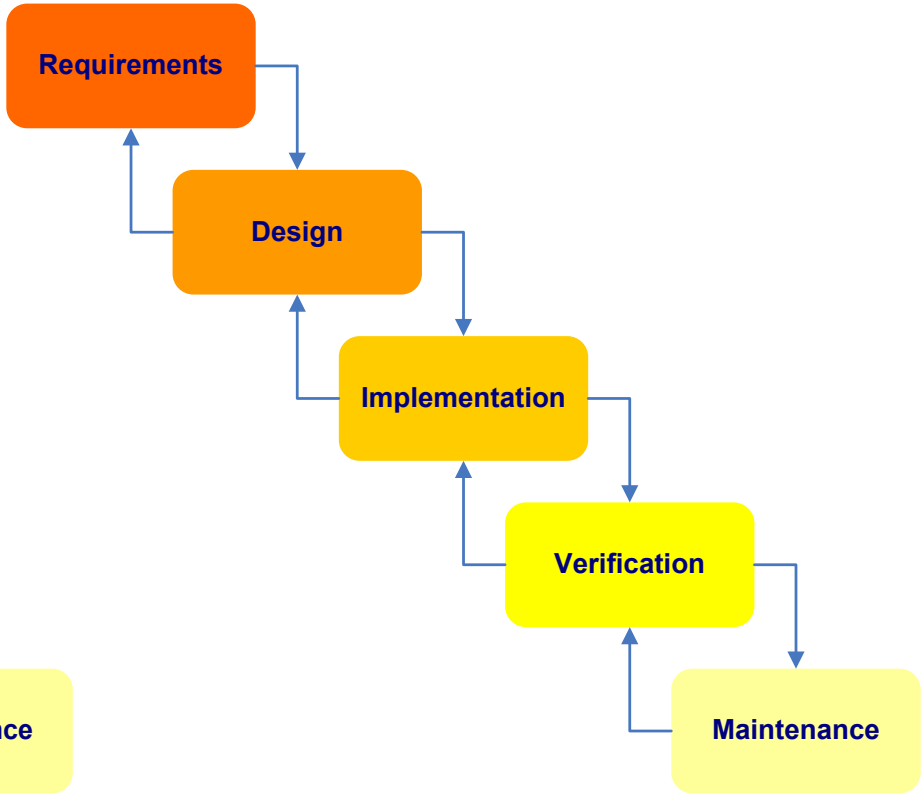
- **Waterfall Development Models**
  - Waterfall: DoD-STD-2167A (replaced by MIL-STD-498 on 11/1994).
  - Modified Waterfall: MIL-STD-498 (cancelled on 5/1998)
- **Iterative Development Models**
  - Boehm's Spiral Model.
  - Rapid Application Development (RAD) & Joint Application Development (JAD)
- **SDLC Processes**
  - ISO/IEC 12207, *Software Life Cycle Processes* (IEEE/EIA 12207 US implementation) (based on MIL-STD-499B)
  - ISO/IEC 15288, *Systems Engineering – System Life Cycle Processes* (IEEE std 1220 – 2005, US implementation)

Waterfall Development Models

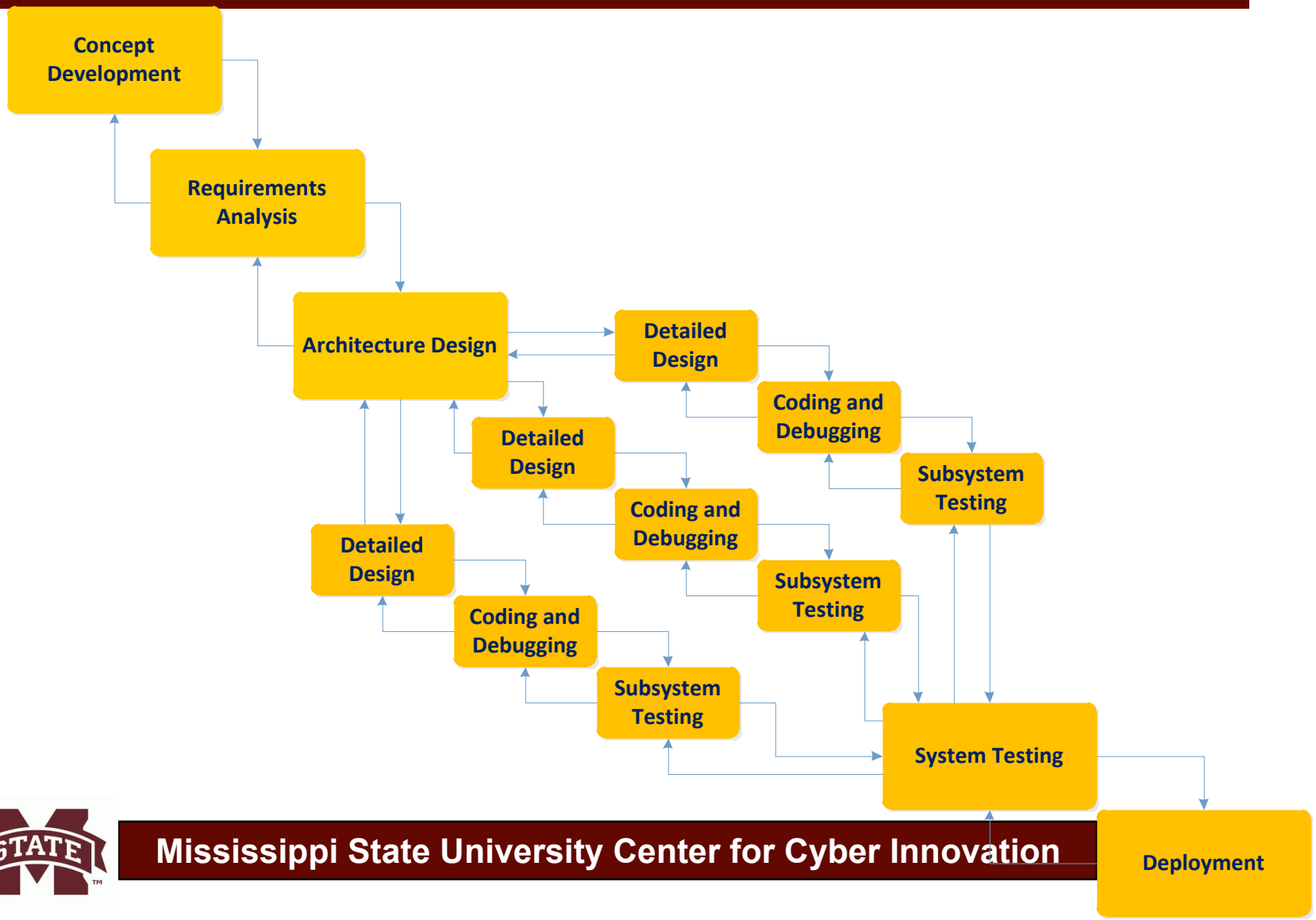
- **Classic Waterfall: DoD-STD-2167A**



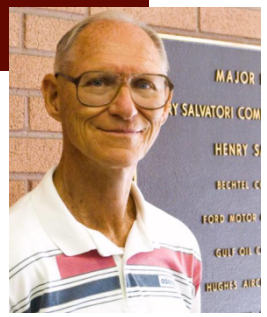
- **Modified Waterfall: MIL-STD-498**

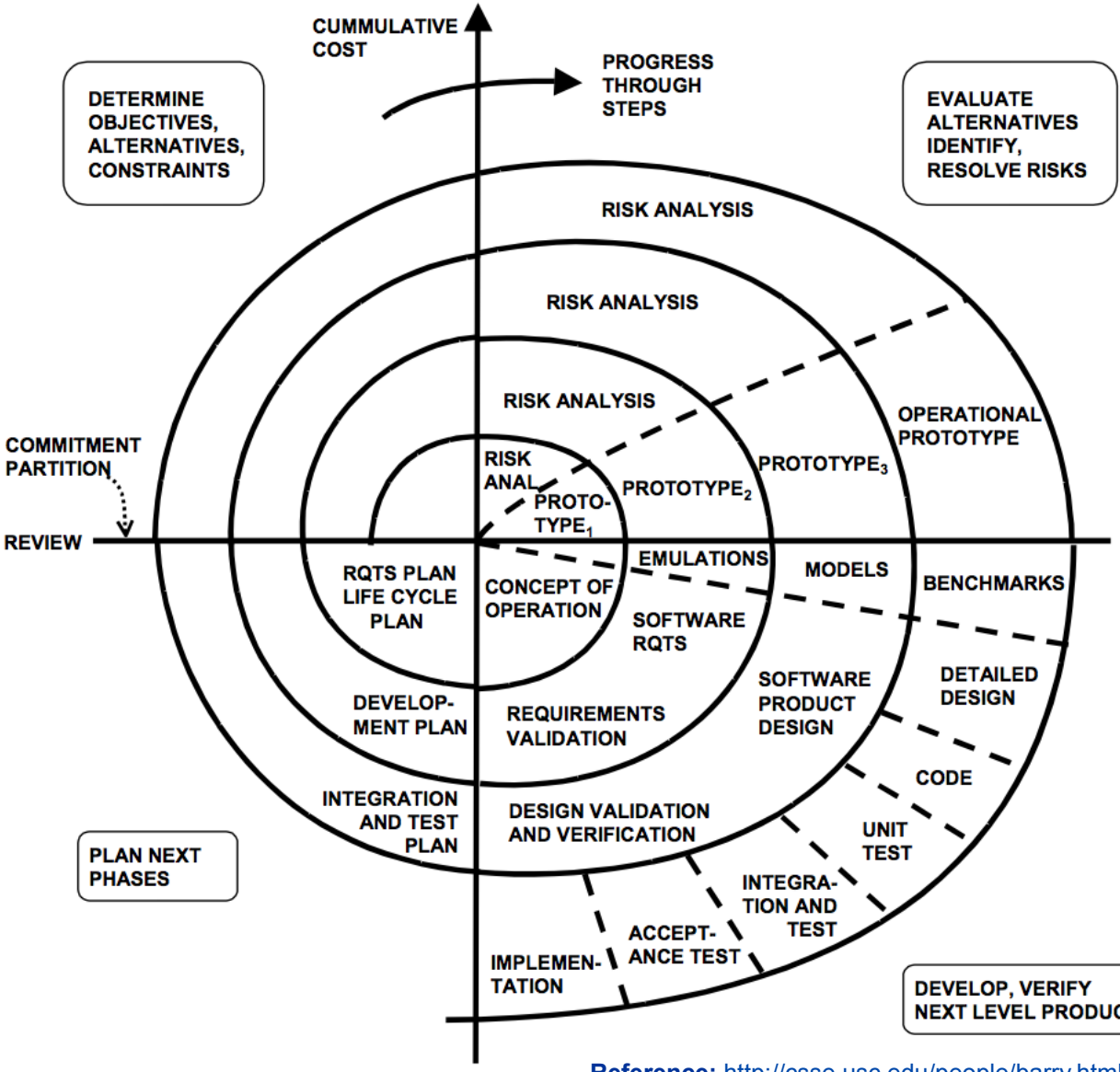


Other SDLC Models – Modified Waterfall w/ Subprojects



Boehm's Spiral Model

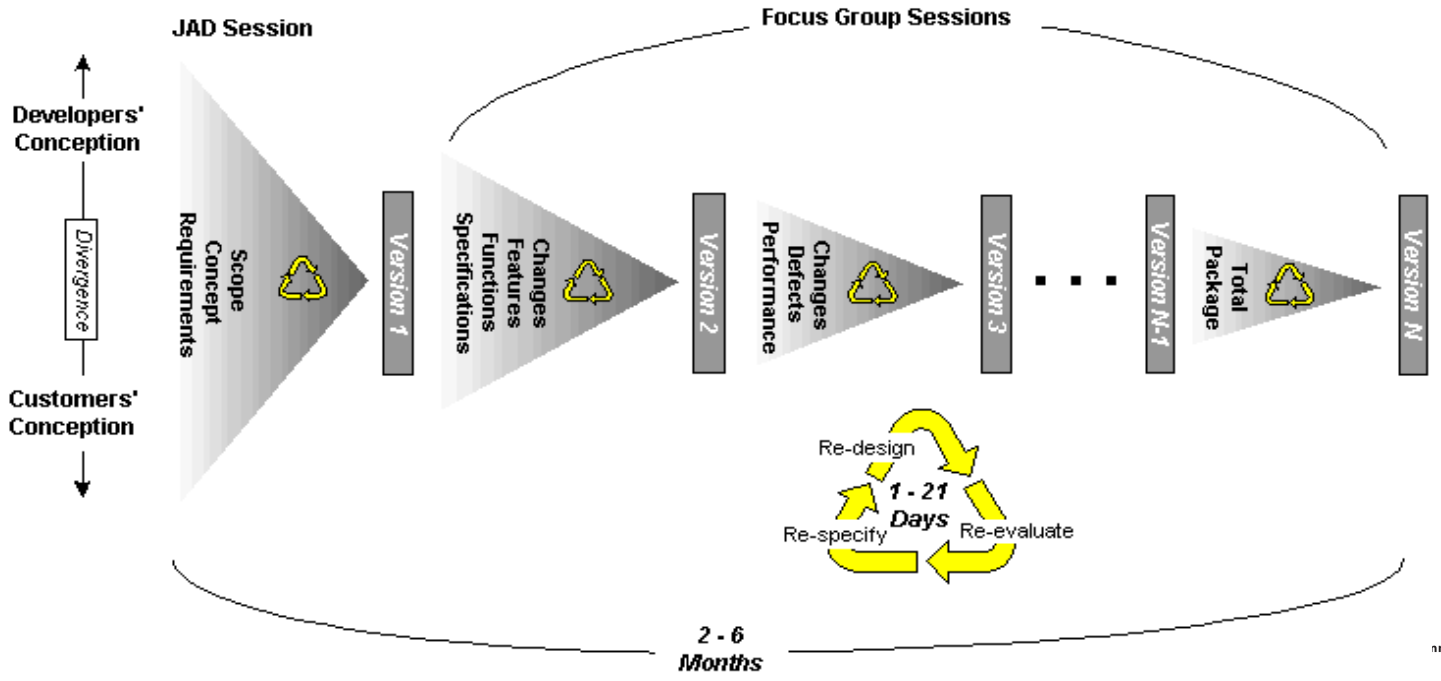




Reference: http://csse.usc.edu/people/barry.html

Rapid Application Development (RAD)

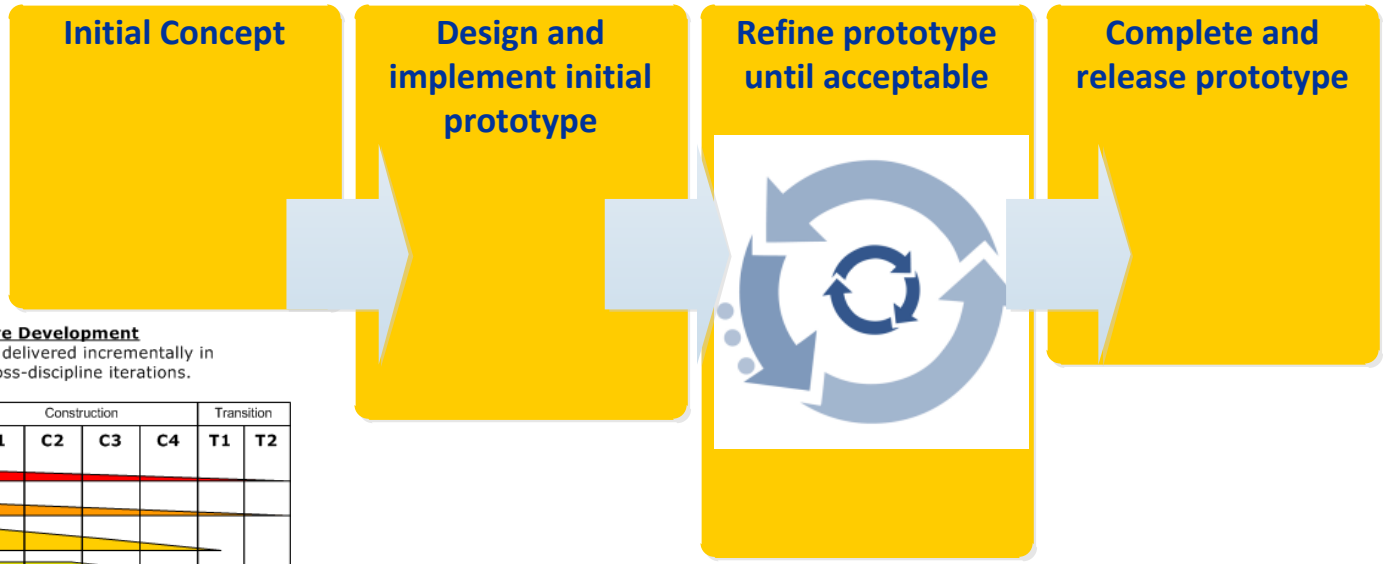
- Iterative, but spiral cycles are much smaller.
- Risk-based approach, but focus on "good enough" outcome.
- SDLC fundamentals still apply…
  - Requirements, configuration, and quality management, design process, coding, test & integration, technical and project reviews etc.

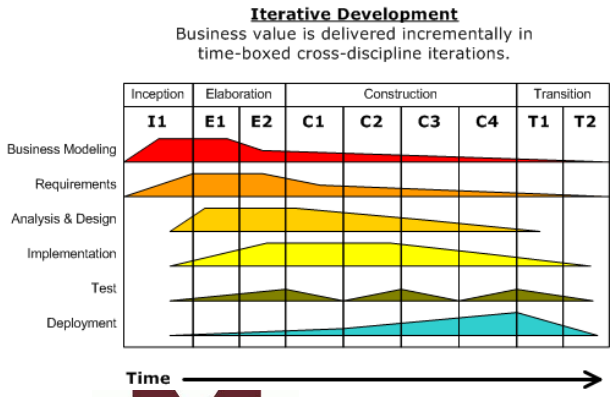


Reference:
- S. McConnel, *Rapid Development: Taming Wild Software Schedules*
- http://www.cs.bgsu.edu/maner/domains/RAD.htm

Evolutionary Prototyping Model

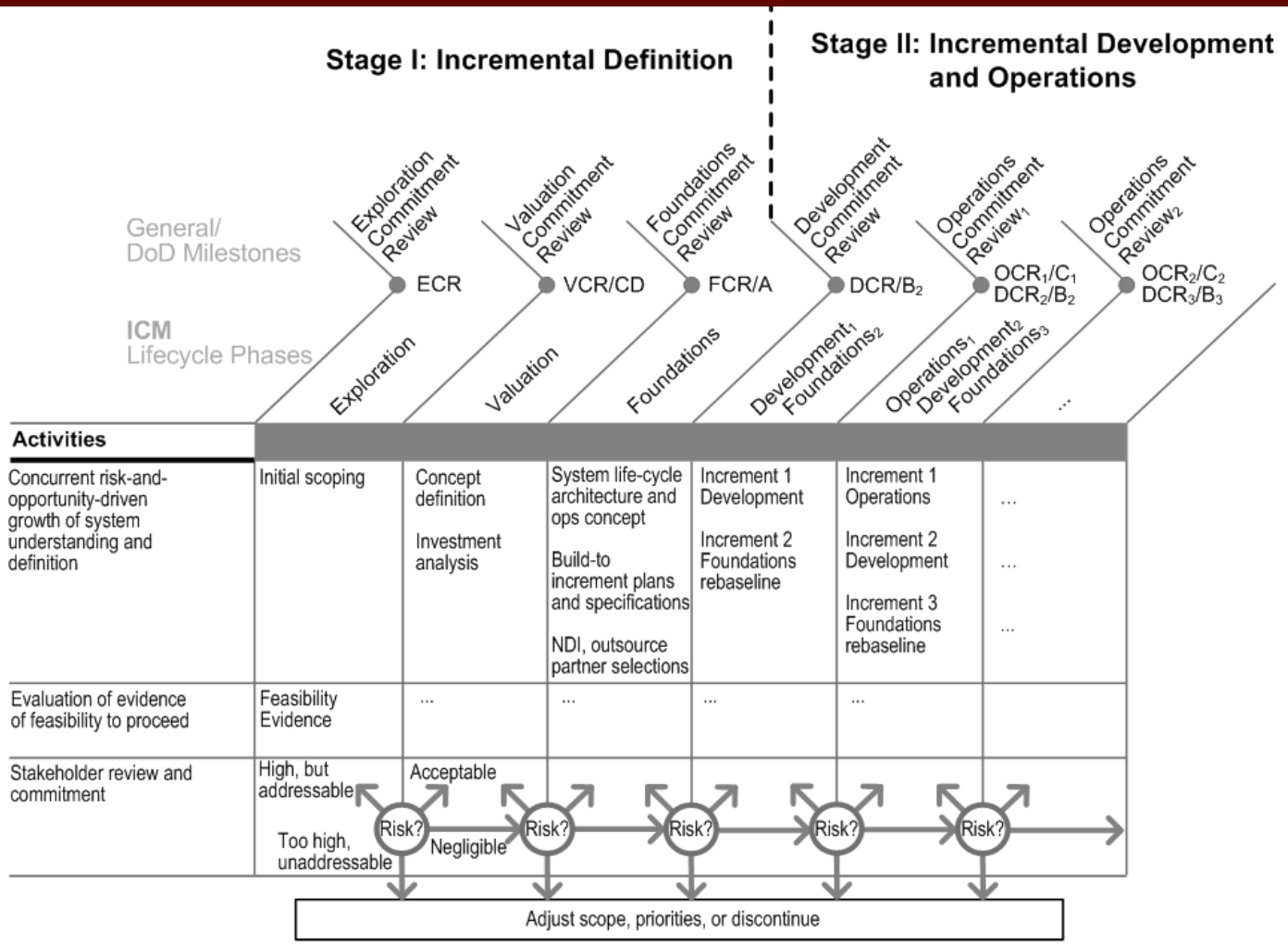
- **The system concept is refined continuously…**
  - **The focus is on "good enough" concept, requirements, and prototype.**
  - **However, it is difficult to determine level of effort (LOE), cost, and schedule.**





Reference: *Rapid Development: Taming Wild Software Schedules*, Steve McConnell, Microsoft Press, 1996

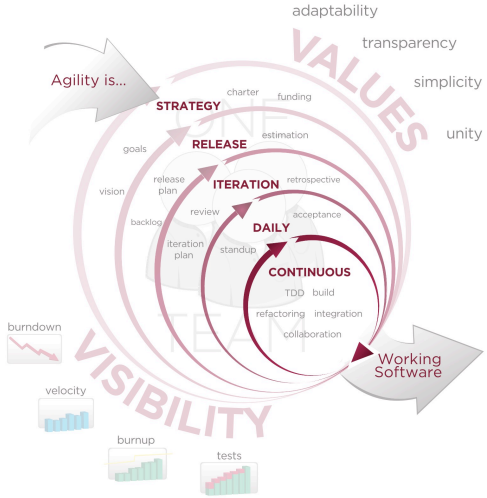
Incremental Commitment Model

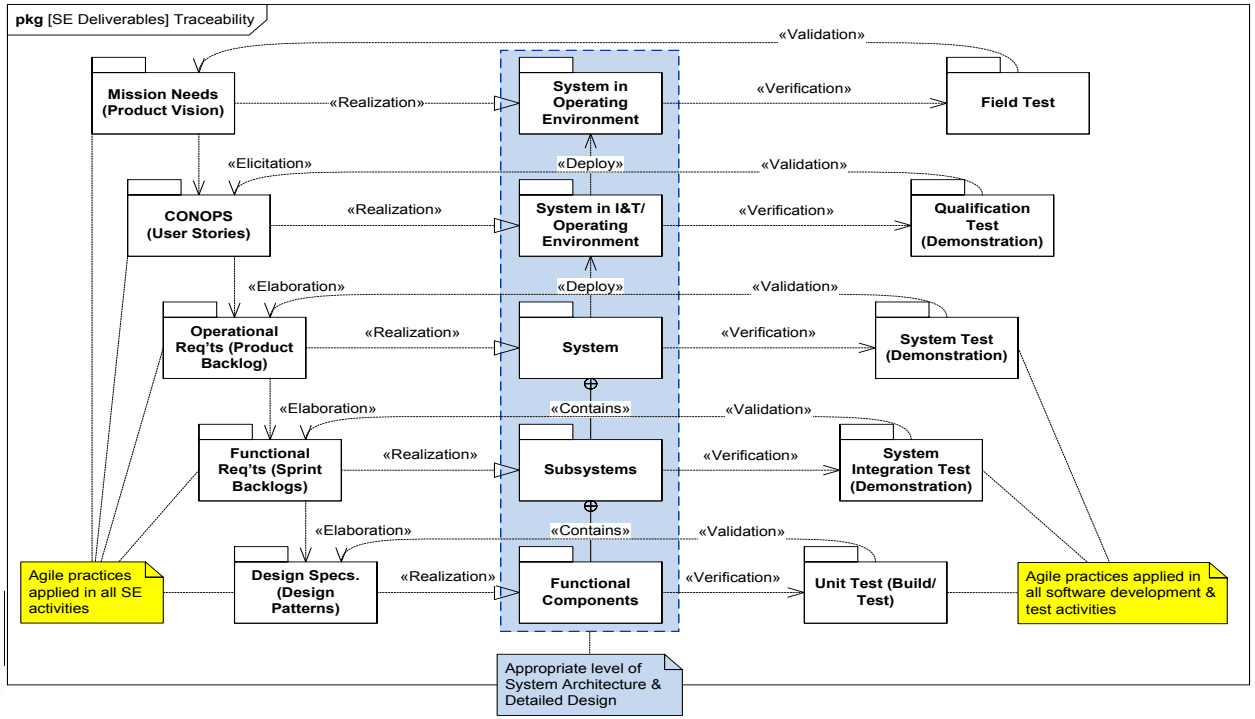


Reference: B. Boehm, J.A. Lane, *Using the Incremental Commitment Model to Integrate System Acquisition, Systems Engineering, and Software Engineering,* CrossTalk, October 2007.

Agile Development Approach

Project Terms	Agile Terms
MNS	Vision
CONOPS	User Stories
SDP	Release & Iteration Plans, Backlogs
PMR/MS Reviews	Retrospectives, Product Demo





Agile SDLC Model – Scrum

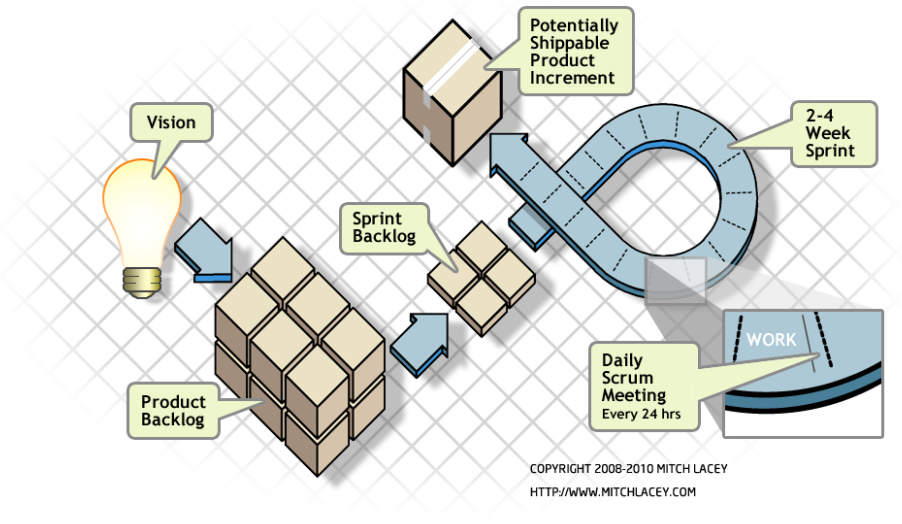
- **Scrum is an agile software development methodology and model that is both iterative and incremental.**
- **The concept derived from the development of commercial products, where:**
  - **Product owner provides the vision and roadmap;**
  - **Scrum master specifies activities and ensures deliverables meet the sprint and iteration goals;**
  - **Team executes the specified scrum activities.**
- **The process is executed in a series of "time-boxed" sprints and iterations, where:**
  - **A "sprint" is usually 2 to 4 weeks; and**
  - **The end-product is a "iteration".**

Reference:

- T. Hirotaka, N. Ikujiro, *The New Product Development Game*, Harvard Business Review, January, 1986. (http://hbr.org/product/new-new-product-development-game/an/86116-PDF-ENG)
- J. Sutherland, *Agile Development: Lessons Learned from the First Scrum*, 2004-10. (http://www.scrumalliance.org/resources/35)
- R. Carlson, P.J. Matuzic, R.L. Simons, *Applying Scrum to Stabilize Systems Engineering Execution*, CrossTalk, May/June 2012.

Agile SDLC Model – Scrum

- The product vision is translated into a list of project requirements;
- This "list" is called the product backlog. It encompasses all the project requirements and work;



- The scrum master works with the the product backlog into a series of sprint backlog.
- The self-organized team composed of domain and SMEs. The team is empowered to select, plan, and make decisions on its work task
- The daily stand-up team meeting is called the daily-scrum. It keeps the team members focused on their tasks. Both product owner and scrum master are required to participate.

Reference:

- R. Carlson, P.J. Matuzic, R.L. Simons, *Applying Scrum to Stabilize Systems Engineering Execution*, CrossTalk, May/June 2012.

Are there other SDLC models?

DevOps*

- Idea observed from cloud computing...
- 2009, Flickr reported doing 10 deployments per day
- Amazon EC2 reported in May 2011:**
  - Mean time between deployments: 11.6 seconds
  - Maximum # of deployments in an hour: 1,079
  - Mean # of hosts can simultaneously receive a deployment: 10k
  - Maximum # of hosts can simultaneously receive a deployment: 30k
  - http://youtu.be/o7-luYS0iSE ***

Reference:

* J. Gorman, G. Kim, *Security is Dead. Long Live Rugged DevOps: IT at Ludicrous Speed*, RSA Conference 2012 (http://www.slideshare.net/realgenekim/security-is-dead-long-live-rugged-devops-it-at-ludicrous-speed)

** Jon Jenkins, Velocity Culture, O'Reilly Velocity 2011, (http://www.youtube.com/watch?v=dxk8b9rSKOo)

*** D. Edwards, *The (Short) History of DevOps*, Sept. 17, 2012. (http://youtu.be/o7-luYS0iSE)

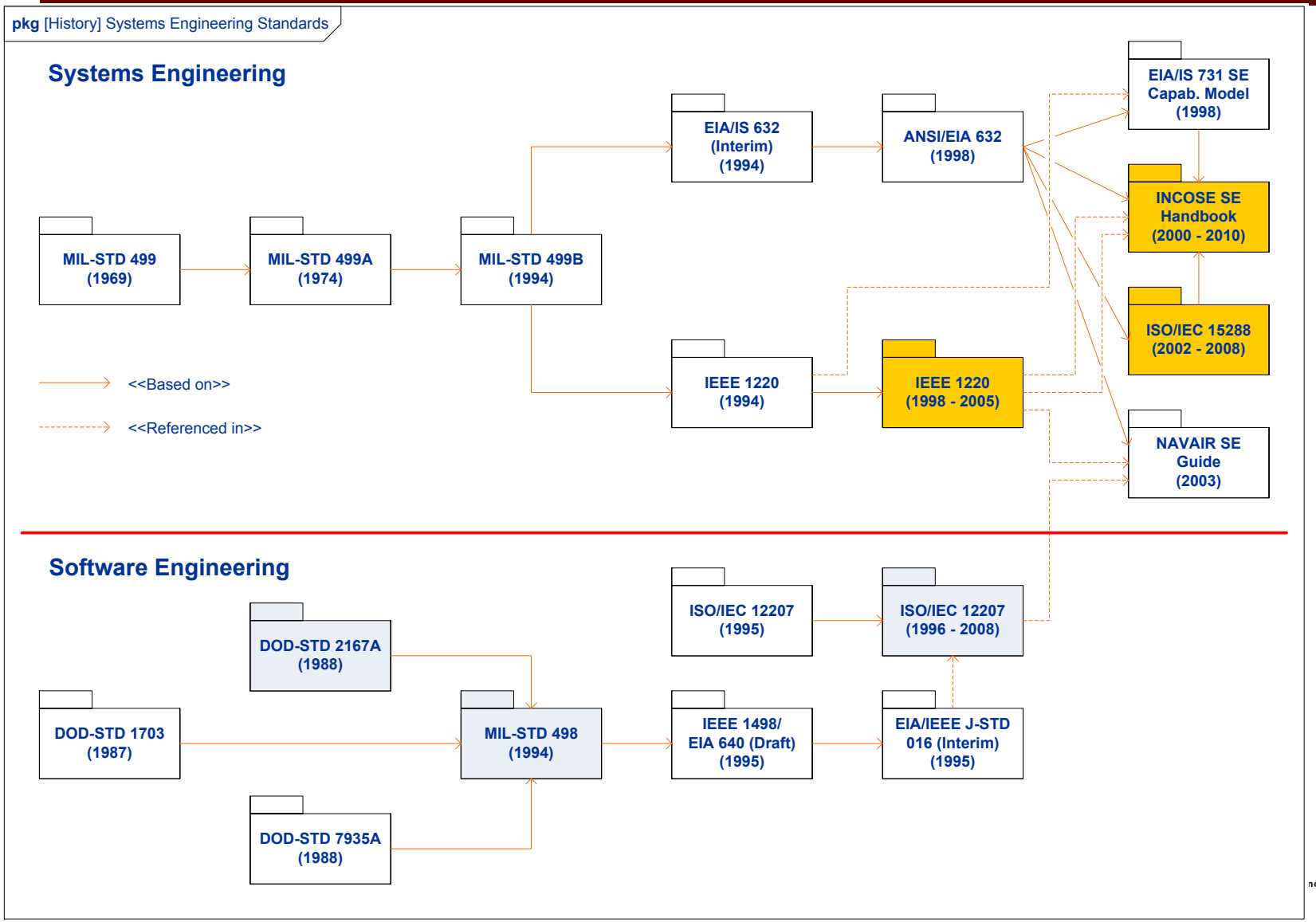
Philosophy behind the Rugged DevOps

- Seamless integration of software development and IT operations
- Focus on the "big picture" rather than security controls
  - Standard configuration
  - Process discipline
  - Controlled access to production systems
- Results
  - 75% reduction in outages triggered by software deployment since 2006
  - 90% reduction in outage minutes triggered by software deployments
  - Instantaneous automated rollback
  - Reduction in complexity
- Back to our study...

Reference:

- Jon Jenkins, *Velocity Culture*, O'Reilly Velocity 2011, (http://www.youtube.com/watch?v=dxk8b9rSKOo)

History of Systems/Software Engineering Process Standards



Secure DevOps

- **Definition**
  - The coordination between developers and the operation team to increment small, quick updates to a system.
- **Types of DevOps**
  - Security automation
  - Continuous integration
  - Baselining
  - Immutable systems
  - Infrastructure as code

Secure DevOps

- **Security automation**
  - Replacing manual security tasks with scripts that can automate tasks.
- **Continuous integration**
  - Continually updating the software with small changes.
- **Baselining**
  - Standard set of functionality and performance for a system.
- **Immutable systems**
  - Once deployed the system is never modified.
- **Infrastructure as code**
  - The use of code to automate the building of systems.

Version Control Management

- **Definition**
  - A way to keep track of changes within a system and allows for a system to revert back to a previous version.
- **Provisioning**
  - Assigning users the permissions to access certain objects.
- **Deprovisioning**
  - Removal of permissions the access certain objects.

Types of Secure Coding Techniques

- **Proper error handling**
  - Handle errors so that secure information is not displayed to the user.
- **Proper input validation**
  - Insure that the user input is not malicious.
- **Normalization**
  - Converts all inputs to one encoding format.
- **Stored procedures**
  - Precompiled methods that are stored in a database.
- **Code signing**
  - Providing a digital signature to code so that the user can verify that it has not been altered.

Types of Secure Coding Techniques

- **Encryption**
  - Converting data with some algorithm so that only specific users can decipher the original data.
- **Obfuscation/ camouflage**
  - Making elements of the code obscure so that attackers cannot easily understand it.
  - This may prevent other developers from understanding the code too.
- **Code reuse/ dead code**
  - Reusing code saves time and reduces development costs.
  - Dead code is code that is executed but never used in the software.

Types of Secure Coding Techniques

- Server vs. client execution/ validation
  - Regardless if the input is validated on the client side it should still be validated again on the server side.
- Memory management
  - Methods used to control computer memory allocation and deallocation.
- Third party libraries
  - Using already created/ tested software within your system.
- Data exposure
  - Loss of control over data in a system.

Code Quality and Testing

- **Definition**
  - Ensure that the code functions correctly, does not have vulnerabilities, and meets the original requirements.
- **Type of testing**
  - Static and dynamic analyzers
    - Static analyzers examine the code without execution.
    - Dynamic analyzers execute the code.
  - Stress testing
    - Tests how the system behaves under high load.
  - Sandboxing
    - Executes code in an isolated environment.
  - Model verification
    - Makes sure the code functions properly.

Compiled vs. Runtime

- **Compiler**
  - Code that is written in a programming language can be converted into executable code to be run on a system.
  - Good for running code that will remain static.
- **Interpreters**
  - Converts high level code into the machine as it is needed.
  - Good for running code that will dynamically change during runtime.

Cloud and Virtualization Architecture & Design

Reference:

Drew Hamilton Lecture Notes

William Lee

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Hypervisor

- **Definition**
  - Allows for more the on OS to be present on a system and allow sit to run in tandem with another OS.
- **Type I**
  - Runs on system hardware and designed for speed/ efficiency in mind.
- **Type II**
  - Run on top of a host OS.
  - Oracle VirtualBox or VMware.
- **Application Cells**
  - Eliminates the need for multiple independent OSs
  - Allows for OSs to store data that needs to be separated.

VM Sprawl Avoidance

- **Definition**
  - Having several VMs in a disorganized structure, which can lead to losing track of a VM file.
  - VM Sprawl Avoidance focuses on techniques to maintain a structure to VM files.
    - Name them appropriately.
    - Proper storage architectures.
  - Virtual machine tools like VMware can prevent sprawl because they automatically structure the VMs.

VM Escape Protection

- **Definition**
  - VM escape is when a program gains access to the host OS without the users permission.
  - This can allow viruses or malware to jump from the M to the host.
  - VM systems are designed to detect and provide protection against VM escape.

Cloud Storage

- **Definition**
  - Computer storage provided over the network.
- **Cloud deployment models**
  - SaaS
  - PaaS
  - IaaS
  - Private vs Public
  - Hybrid
  - Community

Cloud Storage

- SaaS
  - Software as a service offers the service to users within the cloud infrastructure.
- PaaS
  - Platform as a service offers an entire computer platform to users within the cloud infrastructure.
- IaaS
  - Infrastructure as a service is a cloud based system, which allows it to be dynamic and scalable.
- Security as a service
  - Outsourcing security functions from a third party vendor.

Cloud Storage

- **Private vs Public**
  - Private cloud are suitable for organizations with highly sensitive resources.
  - Public cloud has less security restrictions and is more suitable for a system that needs public use.
- **Community**
  - Several organizations use the same cloud due to a common need.
- **Hybrid**
  - Uses public, private, and community features.
  - Private information stays in the private cloud, common information stays on the community cloud, and everything else is stored in the public cloud.

Cloud Residence

- **On-Premise**
  - Cloud server is hosted locally.
- **Hosted**
  - Cloud server is hosted in another location, usually in a shared environment.
- **Cloud**
  - Cloud server is hosted by a third party service.
  - Allows for dynamic scaling since storage is cost based.

Desktop Environment

- Virtual desktop infrastructure (VDI)
  - All the components needed to set up an environment.
- Virtual desktop environment (VDE)
  - The actual user environment, which is what the user will visually see.
- Cloud access security broker
  - The security between the cloud provider and their customers.

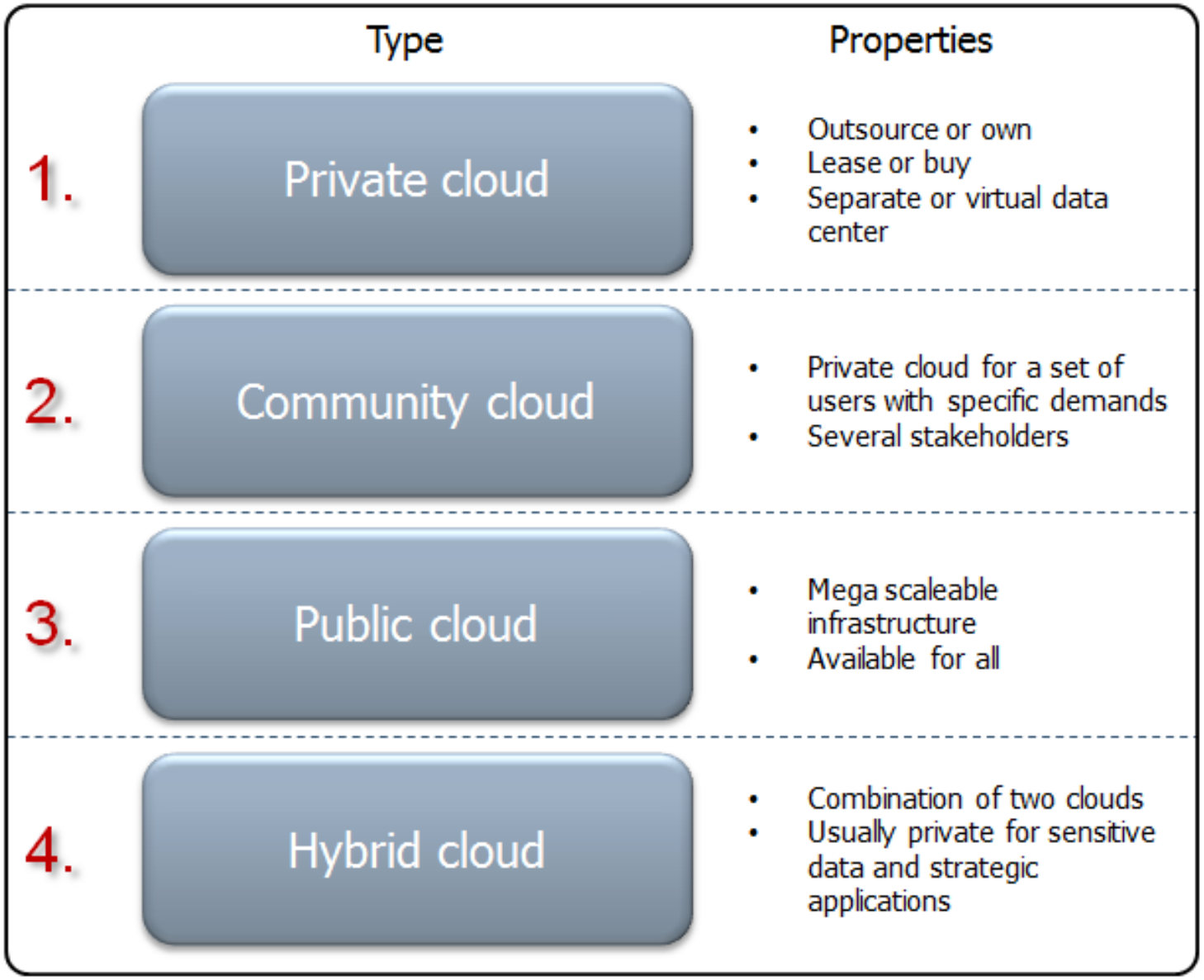
Cloud Computing Background

- Features
  - Use of internet-based services to support business process
  - Rent IT-services on a utility-like basis
- Attributes
  - Rapid deployment
  - Low startup costs/ capital investments
  - Costs based on usage or subscription
  - Multi-tenant sharing of services/ resources
- Essential characteristics
  - On demand self-service
  - Ubiquitous network access
  - Location independent resource pooling
  - Rapid elasticity
  - Measured service
- "Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs, and just-in-time availability of resources"

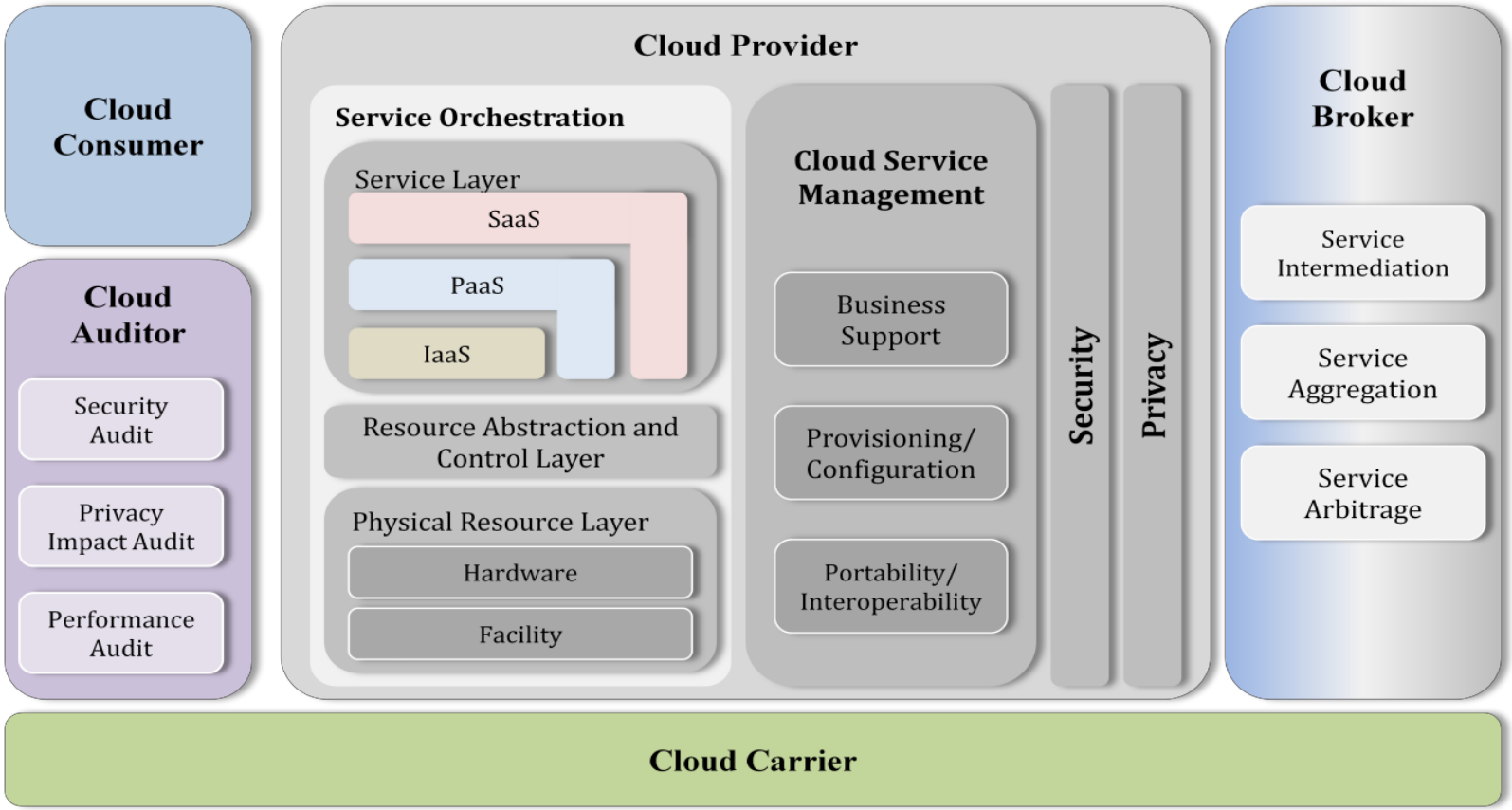
Cloud Delivery Models

- SaaS
  - Software as a service is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted.
    - It is sometimes referred to as "on-demand software", and was formerly referred to as "software plus services" by Microsoft.
- PaaS
  - Platform as a service (PaaS) or application platform as a service (aPaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.
- IaaS
  - Infrastructure as a Service (IaaS) is a form of cloud computing that provides virtualized computing resources over the Internet. IaaS is one of three main categories of cloud computing services, alongside Software as a Service (SaaS) and Platform as a Service (PaaS)

Cloud Deployment Models



NIST SP 500-292 Reference Architecture for Cloud Computing

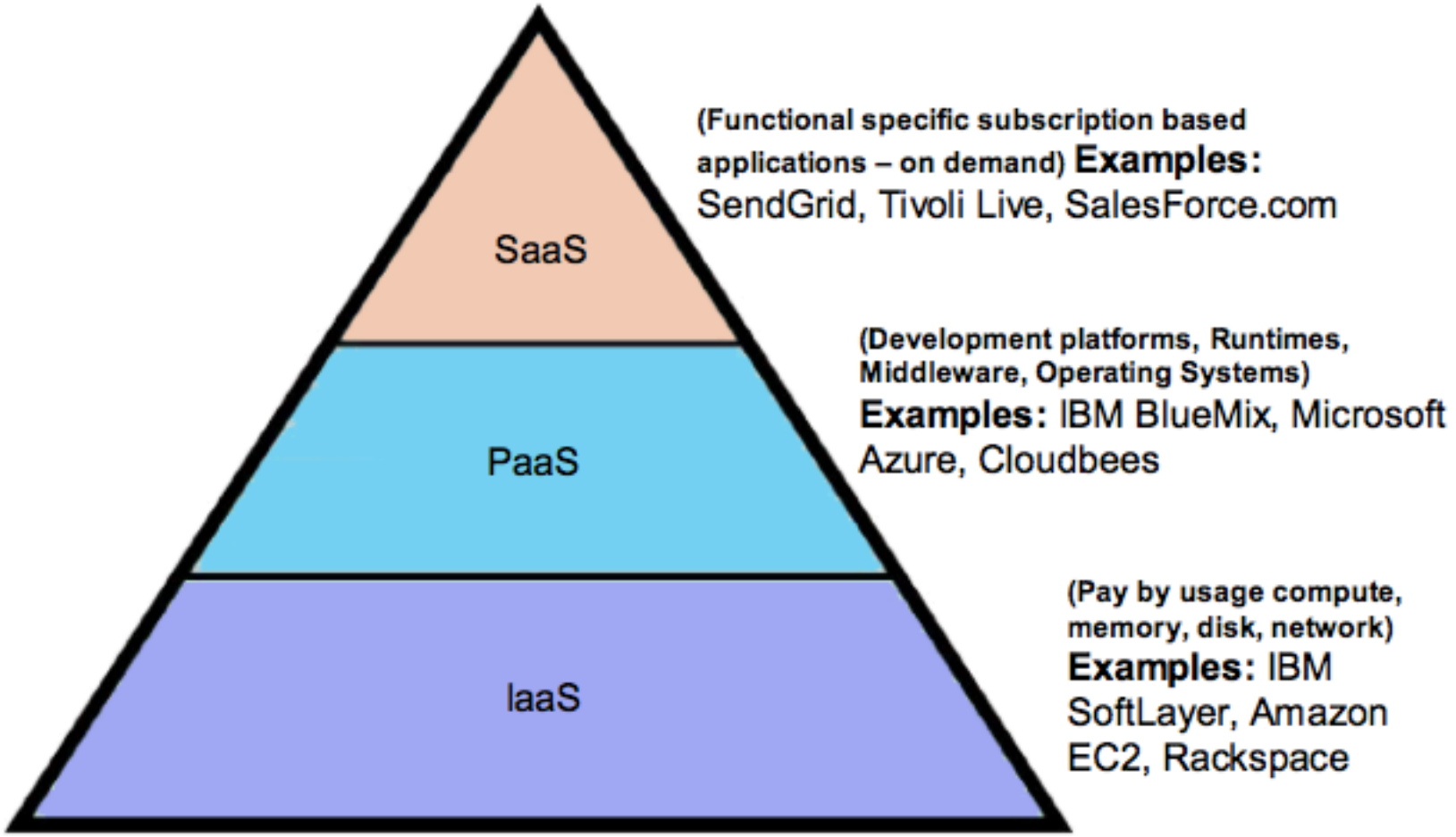


- **NIST Conceptual Reference Model**

SP 500-292 Actors in Cloud Computing

Actor	Definition
Cloud Consumer	A person or organization that maintains a business relationship with, and uses service from, *Cloud Providers*.
Cloud Provider	A person, organization, or entity responsible for making a service available to interested parties.
Cloud Auditor	A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
Cloud Broker	An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between *Cloud Providers* and *Cloud Consumers*.
Cloud Carrier	An intermediary that provides connectivity and transport of cloud services from *Cloud Providers* to *Cloud Consumers*.

Cloud Layers



Cloud Layers

Cloud Computing Limitations

- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

Causes of Problems Associated with Cloud Computing

- **Most security problems stem from:**
  - **Loss of control**
  - **Lack of trust (mechanisms)**
  - **Multi-tenancy**
- **These problems exist mainly in 3rd party management models**
  - **Self-managed clouds still have security issues, but not related to above**

Loss of Control in the Cloud

- **Consumer's loss of control**
  - Data, applications, resources are located with provider
  - User identity management is handled by the cloud
  - User access control rules, security policies and enforcement are managed by the cloud provider
  - Consumer relies on provider to ensure
    - Data security and privacy
    - Resource availability
    - Monitoring and repairing of services/resources

Lack of Trust in the Cloud

- A brief deviation from the talk
  - (But still related)
  - Trusting a third party requires taking risks
- Defining trust and risk
  - Opposite sides of the same coin (J. Camp)
  - People only trust when it pays (Economist's view)
  - Need for trust arises only in risky situations
- Defunct third party management schemes
  - Hard to balance trust and risk
  - e.g. Key Escrow (Clipper chip)
  - Is the cloud headed toward the same path?

Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
  - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
  - Can tenants get along together and 'play nicely'?
  - If they can't, can we isolate them?
- How to provide separation between tenants?

- Cloud Computing brings new threats
  - Multiple independent users share the same physical infrastructure
  - Thus an attacker can legitimately be in the same physical machine as the target

Taxonomy of Fear

- **Confidentiality**
  - Fear of loss of control over data
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromises leak confidential client data
  - Will the cloud provider itself be honest and won't peek into the data?
- **Integrity**
  - How do I know that the cloud provider is doing the computations correctly?
  - How do I ensure that the cloud provider really stored my data without tampering with it?

From www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- **Availability**
  - **Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?**
  - **What happens if cloud provider goes out of business?**
  - **Would cloud scale well-enough?**
  - **Often-voiced concern**
    - **Although cloud providers argue their downtime compares well with cloud user's own data centers**

From www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- **Privacy issues raised via massive data mining**
  - **Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients**
- **Increased attack surface**
  - **Entity outside the organization now stores and computes data, and so**
  - **Attackers can now target the communication link between cloud provider and client**
  - **Cloud provider employees can be phished**

From www.cs.jhu.edu/~ragib/sp10/cs412

Taxonomy of Fear (cont.)

- Auditability and forensics (out of control of data)
  - Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don't maintain data locally
- Legal quagmire and transitive trust issues
  - Who is responsible for complying with regulations?
    - e.g., SOX, HIPAA, GLBA ?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

From www.cs.jhu.edu/~ragib/sp10/cs412

Resiliency and Automation Strategies Architecture & Design

Reference:

Drew Hamilton Lecture Notes

William Lee

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Redundancy and Fault-Tolerant Systems

- Avoid single points of failure
- Direct Access Storage Device (DASD): a general term for magnetic disk storage devices, historically used in mainframe and minicomputer environments

Automation/ Scripting

- **Definition**
  - Performing tasks automatically instead of manually.
  - Increases efficiency, accuracy, and reduces risk.
- **Automated courses of action**
  - Enabled by scripts which can be written to run complex tasks drastically faster than a human.
  - Essentially several tasks can be performed with one command.
- **Continuous monitoring**
  - A system that was designed with automated event monitoring in mind.
  - Users will be alerted of non-standard events, which allows them to better focus on actual issues

Automation/ Scripting

- **Continuous Validation**
  - **Automated scanning of a system to ensure that functions properly, meets security standards, and does not have any added, unnecessary functionality.**
  - **As the system changes with software updates and changes it needs to be validated again.**

Templates

- **Definition**
  - Standard arrangement of data that can be reused to expedite future tasks
- **Template methods**
  - Master Image
  - Non-persistence
  - Snapshots
  - Revert to known state
  - Rollback to known configuration
  - Live boot media

Template Methods

- **Master Image**
  - Fully patched premade image of a system.
  - Allows for quick replacements to a corrupt or broken system.
  - Provides a backup for OS and applications, but not data.
- **Non-persistence**
  - Systems that do not allow permeant changes or persistent files.
  - Only approved application will remain after a restart.
- **Snapshots**
  - Saving a virtual machine's state at a particular time.
  - Can be used to reset a system back to a previous state.

Template Methods

- **Revert to known state**
  - Similar to a snapshot, but used for host operating systems.
  - Saves an OS's machine state as a restore point so that it can be reverted back to that state.
- **Rollback to known configuration**
  - Saves an OS's configuration state and allows users to revert back to the last working configuration
- **Live boot media**
  - A complete bootable system stored on a CD or USB.
  - Enables the ability to boot a system from an external OS source.

Elasticity and Scalability

- **Elasticity**
  - The ability for a system to dynamically increase/ decrease its workload capacity depending on need.
  - These type of dynamic changes benefit from cloud environments.
- **Scalability**
  - Scale up by making the hardware stronger
  - Scale out by adding additional nodes to the server

Allocation and Redundancy

- **Distributive allocation**
  - The method of spreading work across several different servers.
  - Stateful work has to be handled by the same server until completion
  - Stateless work can be handled by sever different servers
- **Redundancy**
  - Having several independent elements to perform a function.
  - If one element fails, several other elements can still continue without it.

Fault Tolerance and High Availability

- **Uninterrupted access**
  - The goal of both methods is to have constant access
- **Fault tolerance**
  - Mirrors the data and hardware systems on a second device.
  - If an error occurs on the first device the mirrored system can handle requests until there is a fix
- **High availability**
  - Similar to fault tolerance's mirror technique except the mirrored system should have the same power and processing as the original
  - Allows for the mirrored system to maintain both data and services.

RAID

- **Definition**
  - Several methods of storing the contents of a single disk onto multiple disks
- **Types of RAID**
  - RAID 0
  - RAID 1
  - RAID 2
  - RAID 3
  - RAID 4
  - RAID 5
  - RAID 6

Types of RAID

- **RAID 0**
  - Spreads data across several disks to reduce the time it takes to read data.
  - Loss of a single disk will cause all data to be lost.
- **RAID 1**
  - Copies data across several disks to improve reliability.
  - Loss of a single disk is insignificant because the same information is stored elsewhere.
- **RAID 2**
  - Spreads data at a bit level to allow for the recovery of a single disk by error correcting techniques
  - Not used often

Types of RAID

- **RAID 3**
  - Spreads data at a bit level, but has one disk dedicated to parity bits for error checking.
  - Not used often due to the fact that inputs and outputs need to access the same disk, which prohibits overlap.
- **RAID 4**
  - Similar to RAID 3 except it spreads data in larger stripes.
  - Suffers from the same issues as RAID 3.
- **RAID 5**
  - Spreads data at a block level and has parity data spread on multiple disks.
  - Provides reliability and increased speeds
  - Most commonly used

Types of RAID

- **RAID 6**
  - **Similar to RAID 5, but completely duplicates the parity data across multiple disks.**
- **RAID 10**
  - **A combination of RAID 1 and RAID 0.**
  - **Mirrors data onto two or more disk drives to avoid the issues with RAID 0.**

Physical Security Controls Architecture & Design

Reference:

Drew Hamilton Lecture Notes

William Lee

Security+ Exam Guide, 5th ed.

Conklin, White, Cothren, Davis and Williams

Introduction to Physical Security

Physical threats to an organization are broken into four broad categories:

- Natural environmental threats – floods earthquakes, storms and tornadoes, fires, extreme temperature
- Supply system threats – power outages, communications interruptions, interruption of natural resources such as water, steam, and gas
- Manmade threats – unauthorized access (internal or external), explosions, damage by employees, employee errors and accidents, vadalism, fraud, and theft
- Politically motivated threats – strikes, riots, civil disobedience, terrorist attacks, and bombings

Physical Security

- **Lighting**
  - Good lighting can detour intruders and allows for cameras to clearly see unauthorized activities.
- **Signs**
  - Provide users with visual information to differentiate secured areas from public spaces.
- **Fencing**
  - Physical barrier to protect property from outside forces
- **Security guards**
  - Monitor entrances and exits in order to secure the facility.

Physical Security

- **Alarms**
  - Alert users to unauthorized activities.
- **Safe**
  - Used to secure objects from unauthorized access.
- **Protected cabling**
  - Protective tubing to shield cables from physical damage and malicious attacks like wire tapping.
- **Airgap**
  - Physical and logical separation of a network from other networks.
  - Prevents unauthorized data transfers from the network.

Physical Security

- **Mantrap**
  - Placing two doors close together, which both require authenticated access.
  - Prevents someone from gaining access by following an authorized user.
- **Faraday cages**
  - Blocks electromagnetic fields by using conductive materials.
  - Does not allow the use of WIFI, cellular data, etc.
- **Locks**
  - Restricts access to an object without the proper key.

Physical Security

- **Biometrics**
  - Human biology is used to gain access to an object.
  - An optical scanner will scan a users eye to see if they have access.
- **Barricades/ bollards**
  - Buffer between someone and a particular object.
- **Tokens/ cards**
  - Objects that are required for a user to be authenticated and given access.
  - Key cards can log users access to specific rooms when they scan in.

Physical Security

- Cable locks
  - Used to secure items that are being transported.
- Screen filters
  - Optical filters that limit the viewability so that individuals surround the user cannot clearly see the screen.
- Cameras and motion detectors
  - Record unauthorized activity
- Logs and key management
  - Keep track of user activity, which can be used as a reference if there is an attack.
- Infrared detections
  - Detects objects that cannot normally be seen.

Environmental Controls

- HVAC
  - It is important to control the temperature and humidity of server rooms to create ideal run conditions.
  - Air conditioning should offset the heat produced by servers and keep humidity levels in check.
- Hot and cold aisles
  - Method of arranging servers so that cold air is brought in and hot air is expelled, while not letting the two mix.
- Fire suppression
  - In the event of a fire have methods in place to limit the overall damage caused from it.
  - Done through fire alarms, fire extinguishers, water suppression devices, and CO_2 suppression devices.

Perimeter Security

- **Highlighted note: It is also important to have a diversity of controls. For example, if one key works on four different door locks, the intruder has to obtain only one key. Each entry should have its own individual key or authentication combination.**

Perimeter Security

Locks

- Considered delaying devices
- Mechanical locks
  - Warded Locks: the basic padlock
  - Spring-loaded bolt with notches cut in it
  - Tumbler locks
    - Pin tumbler lock
    - Wafer tumbler lock
    - Lever tumbler lock

Perimeter Security

Locks (cont'd)

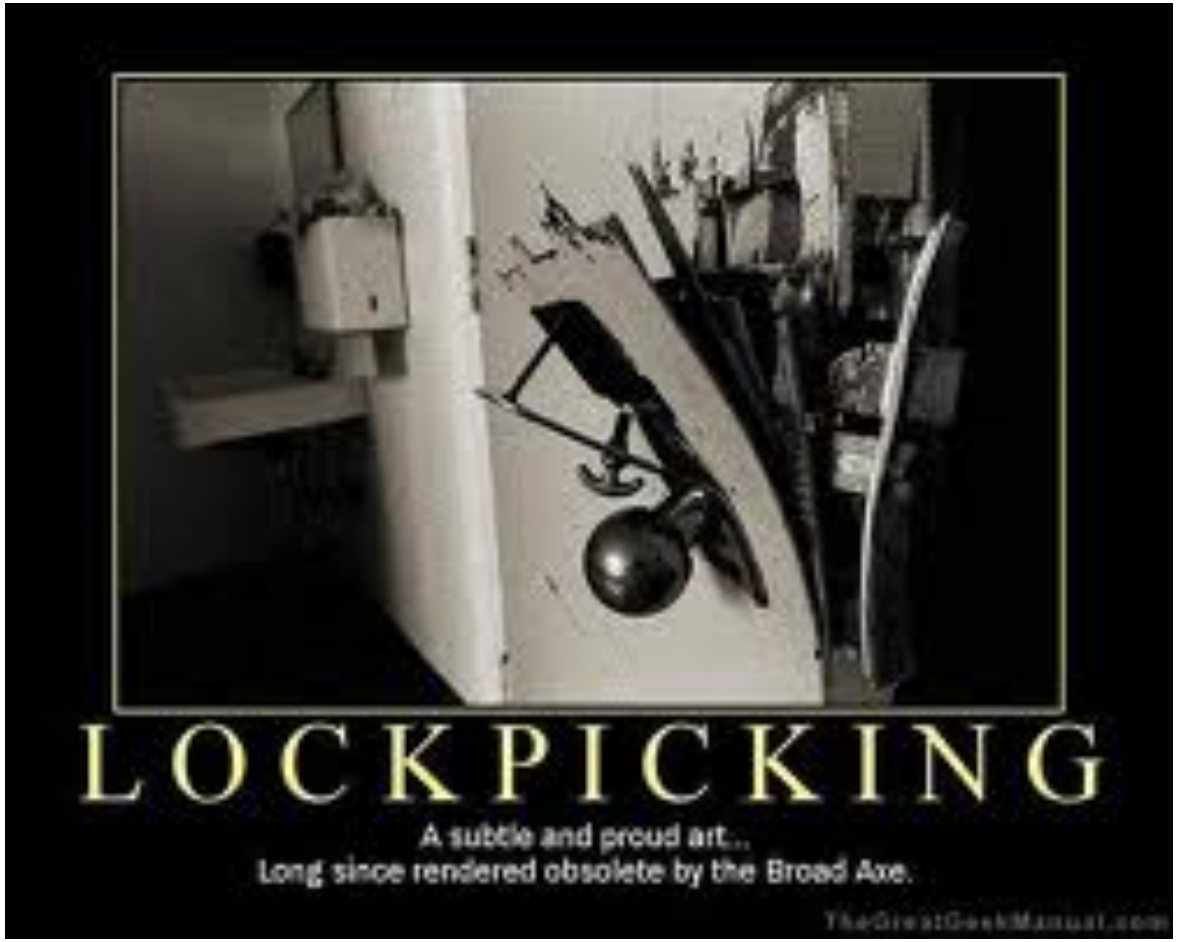
- **Pin tumbler lock**
  - Most common tumbler lock
  - Requires the key to have just the right grooves to put all the spring-loaded pins in the right position
- **Wafer tumbler lock**
  - Also called disc tumbler locks
  - Use flat discs instead of pins
  - Easily Circumvented

Perimeter Security

Locks (cont'd)

- Highlighted note: The delay time provided by the lock should match the penetration resistance of the surrounding components (door, door frame, hinges). A smart thief takes the path of least resistance, which may be to pick the lock, remove the pins from the hinges, or just kick down the door

Perimeter Security



Perimeter Security

Locks (cont'd)

- Highlighted note: Some locks have interchangeable cores, which allow for the core of the lock to be taken out. You would use this type of lock if you wanted one key to open several locks. You would just replace all the locks with the same core

Perimeter Security

Locks (cont'd)

- Combination locks
  - Require the proper combination
  - Use internal wheels that much line up
  - Electronic combination locks have a key pad to type in the combination instead of wheels
- Cipher locks
  - Also called programmable locks
  - Requires combination by key pad, and sometimes a swipe card as well

Perimeter Security

Locks (cont'd)

- **Functions of cipher locks**
  - Door delay: after door is open for so long, an alarm triggers
  - Key override: a specific combination can be used to override normal procedures or for supervisory override
  - Master keying: enables supervisory personnel to change access codes and lock features
  - Hostage alarm: a specific combination can be used to open the door and simultaneously transmit a duress message to guards and/or police station

Perimeter Security

Locks (cont'd)

- **Highlighted note: It is important to change the combination of locks and to use random combination sequences.**
  - **Often, people do not change their combinations or clean the keypads, which allows an intruder to know what key values are used in the combination, because they are the dirty and worn keys.**
  - **The intruder then just needs to figure out the right combination of these values**

Perimeter Security

Locks (cont'd)

- Cipher locks that can assign specific codes to unique individuals are sometimes called smart locks
- Highlighted note: Hotel key cards are also known as smart cards. They are programmed by the nice hotel guy or gal behind the counter. The access code on the card can allow access to a hotel room, workout area, business area, and yes – the mini bar

Perimeter Security

Locks (cont'd)

- **Device locks**
  - Cable locks: a vinyl-coated steel cable to connect a device to a stationary object
  - Switch controls: a cover for power switches
  - Slot locks: similar to cable locks mounted to a bracket mounted in a spare expansion slot
  - Port controls: block access to disk drives or unused connection ports
  - Peripheral switch controls: secures a keyboard by placing a power switch between the system and the keyboard port
  - Cable traps: prevents the removal of I/O devices by passing their cables through a lockable unit

Perimeter Security

Locks (cont'd)

- **Lock strengths**
  - Grade 1: Commercial and industrial use
  - Grade 2: Heavy-duty residential/light-duty commercial
  - Grade 3: Residential/consumer expendable
- **Lock cylinder categories**
  - Low security: No pick or drill resistance
  - Medium security: uses tighter and more complex keyways (notch combinations)
  - High security: Pick resistance protection through many different mechanisms (grade 1 & 2 locks only)

Perimeter Security

Locks (cont'd)

- **Circumventing locks**
  - Lock picks / tension wrenches
  - Raking: push lock pick is pushed to the back of a tumbler pin lock and quickly slid out with upward pressure and tension wrench is used to hold set pins in place
  - Lock bumping: a special bump key is used to force the pins of a tumbler pin lock to the open position

Perimeter Security

Perimeter Security

Personnel Access Controls

- Identification and authentication can be verified by anatomical attribute (biometric), smart or memory card (swipe card), presenting photo ID, using a key, or providing a card and entering a password or PIN
- Piggybacking: an individual gains unauthorized access by using someone else's legitimate credentials (often by following closely through a door)

Perimeter Security

Personnel Access Controls (cont'd)

- Highlighted note: Electronic access control (EAC) tokens is a generic term used to describe proximity authentication devices, such as proximity readers/transponders, programmable locks, or biometric systems, which identify and authenticate users before allowing them entrance into physically controlled areas

Perimeter Security

External Boundary Protection Mechanisms

- **Control pedestrian and vehicle traffic flow**
- **Various levels of protection for different security zones**
- **Buffers and delaying mechanisms to protect against forced entry attempts**
- **Limit and control entry points**

Perimeter Security

Perimeter Security

External Boundary Protection Mechanisms (cont'd)

- Services provided by the following control types:
  - Access control mechanisms: locks, electronic card access, personnel awareness
  - Physical barriers: fences, gates, walls, doors, windows, protected vents, vehicular barriers
  - Intrusion detection: perimeter sensors, interior sensors, annunciation mechanisms
  - Assessment: guards, CCTV cameras
  - Response: guards, local law enforcement
  - Deterrents: signs, lighting, environmental design

Perimeter Security

Fences (cont'd)

- **Perimeter Intrusion Detection and Assessment System (PIDAS) is a type of fencing that has sensors located on the wire mesh and at the base of the fence.**
  - **It is used to detect if someone attempts to cut or climb the fence.**
  - **It has a passive cable vibration sensor that sets off an alarm if an intrusion is detected.**
  - **PIDAS is very sensitive and can cause many false alarms**

Perimeter Security

Fences (cont'd)

- Gates come in four distinct classifications
  - Class I: Residential
  - Class II: Commercial where general public access is expected
  - Class III: Industrial where limited access is expected
  - Class IV: Restricted access
- Highlighted note: UL standards can be found at www.ul.com. A good introduction to the UL-325 standard, which deals with gates, can be found at www.abrpaint.com/services/GatesFencing/ul325intro.htm

Perimeter Security

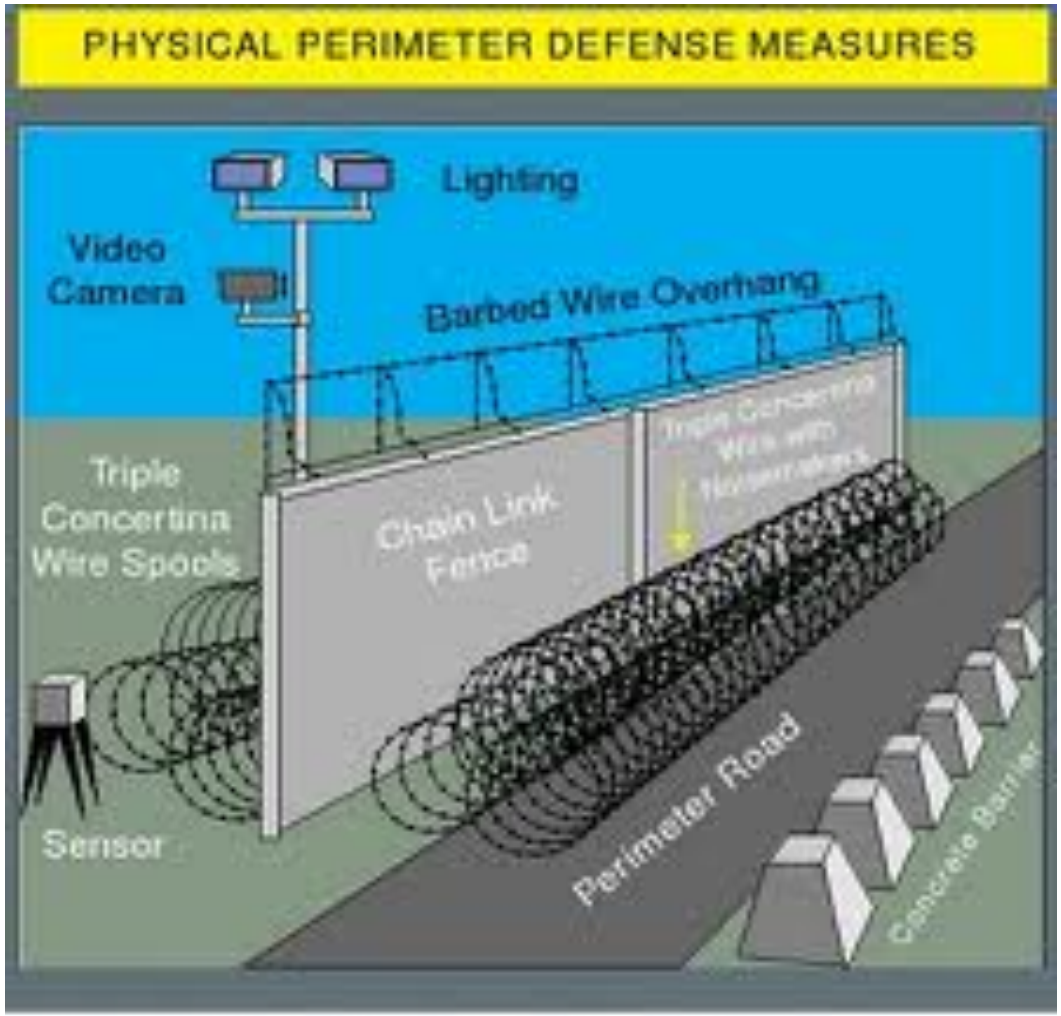


Figure IV-7. Physical Perimeter Defense Measures

Perimeter Security

- **Bollards Lighting**
  - Should overlap
  - Glare protection: security lights should point away from security guard posts and toward gates or exterior access points
  - Continuous lighting: array of lights that provides even illumination across an area
  - Standby lighting: configurable to turn on and off at predetermined times
  - Responsive area illumination: IDS detects suspicious activity and turns on the lights in a specific area

Perimeter Security

- Lighting (cont'd)
  - Highlighted note: Critical areas need to have illumination that reaches at least eight feet with the illumination of two foot-candles
  - Highlighted note: Redundant or backup lights should be available in case of power failures or emergencies. Special care must be given to understand what type of lighting is needed in different parts of the facility in these types of situations. This lighting may run on generators or battery packs

Perimeter Security

- **Closed-circuit television (CCTV)**
  - **The purpose of CCTV is to detect, assess, and/or identify intruders**
  - **Made up of cameras, transmitters, receivers, a recording system, and a monitor**
  - **Most modern CCTV cameras use light-sensitive chips called charged coupled devices (CCDs) in the lens which converts the light received into an electrical signal**
  - **Two types of lenses: fixed focal length and zoom (varifocal)**

Perimeter Security

CCTV (cont'd)

- Highlighted note: CCTVs should have some type of recording system. Digital recorders save images to hard drives and allow advanced search techniques that are not possible with videotape recorders. Digital recorders use advanced compression techniques, which drastically reduce the storage media requirements

Perimeter Security

CCTV (cont'd)

- Highlighted note: Fixed focal length lenses are available in various fields of view – wide, medium, and narrow. A lens that provides a "normal" focal length creates a picture that approximates the field of view of the human eye. A wide-angle lens has a short focal length, and a telephoto lens has a long focal length. When a company selects a fixed focal length lens for a particular view of an environment, it should understand that if the field of view needs to be changed (wide to narrow), the lens must be changed.

Perimeter Security

CCTV definitions

- Focal length: effectiveness in viewing objects from a horizontal and vertical view
- Zoom lens: allow the viewer to change the field of view
- Depth of field: portion of the environment that is in focus
- Manual iris lens: a lens with a ring around the lens that can be manually turned and controlled
- Automatic iris lens: a lens that senses brightness and adjusts itself accordingly
- Fixed mounting: camera cannot move in response to security personnel commands
- PTZ capabilities: ability for a camera to pan, tilt, and zoom

Perimeter Security

- **Intrusion detection systems**
  - **Electromechanical or volumetric**
  - **Volumetric IDSs are more sensitive**
  - **IDSs can detect changes in:**
    - **Beams of light**
    - **Sounds and vibrations**
    - **Motion**
    - **Different types of fields (microwave, ultrasonic, electrostatic)**
    - **Electrical circuits**

Perimeter Security

IDSs (cont'd)

- Electromechanical systems work by detecting a change or break in a circuit
  - Strips of foil embedded or connected to windows
  - Vibration detectors
  - Magnetic contact switches
  - Pressure pads

Perimeter Security

IDSs (cont'd)

- **Volumetric systems**
  - **Photoelectric or photometric: detects changes in a beam of light**
  - **Passive infrared (PIR): identifies changes in heat waves**
  - **Acoustical detection: detects sounds with very sensitive microphones (Vibration sensors??)**
  - **Wave-pattern motion detectors: monitors a microwave, ultrasonic, or low frequency wave**
  - **Proximity detector or capacitance detector: detects changes in an emitted magnetic field caused by static electricity of subatomic particles**

Perimeter Security

IDSs (cont'd)

- Characteristics
  - Expensive and require human intervention to respond to alarms
  - A redundant power supply and emergency backup power are necessary
  - Can be linked to a centralized security system
  - Should have a fail-safe configuration that defaults to "activated"
  - Should detect and be resistant to tampering

Perimeter Security

Other security measures

- **Bollards**
- **Patrol force and security guards**
- **Dogs**
- **Audits of physical access**
- **Testing and drills**

Summary

- Architecture Frameworks and Secure Network Architectures
- Secure Systems Design and Deployment
- Embedded Systems
- Application Development and Deployment
- Cloud and Virtualization
- Resiliency and Automation Strategies
- Physical Security Controls