DSci526:
Secure Systems Administration

Course Introduction

Prof. Clifford Neuman

Lecture 1
20 January 2021
Online

Course Identification

- DSci 526
  - Secure Systems Administration (4 units)
- Class meeting schedule
  - 2PM to 5:20PM Wednesday
  - Online
- Class communication
  - inf526@csclass.info
  - Goes to instructor and any assistants and is archived.

General Course Information

- Professor office hours
  - Monday 1PM-2:30PM via Zoom
    - Link to be sent in email
  - Other times by appointment
  - E-mail: dsci526@csclass.info and bcn@isi.edu

- TA for the class
  - Not yet assigned
  - Likely to have a lab assistant assigned instead

Guidelines for Students

- Class will include group projects
- Student deliverables
  - 10% Two homework assignments
  - 10% Class Presentation on Administration Tools
  - 30% Two Group exercises
    - 10% each group Performance
    - 5% each individual performance (presentations)
  - 20% Midterm exams
  - 25% Final exam 25%
  - Class Participation 5%
- Read the assigned readings before class!
  - Responsible for content of assigned reading

Guidelines for Students

- Academic integrity is taken very seriously
  - https://viterbischool.usc.edu/academic-integrity/
    - Viterbi has a site that explains academic integrity and what is meant by plagiarism.
  - https://libguides.usc.edu/c.php?g=234929&p=1559180
    - USC Libraries has additional resources

Letter Grade Assignment

- A letter grade will be assigned for each assignment, project, or exam. The individual assignment scores are based on overall class performance.
- Course grade is determined by weighted calculation from the component grades.

Group Projects

- Two Administration case studies drawn from:
  - Banks
  - Retailer
  - Government
  - Cloud
  - Critical Infrastructure
  - Criminal Enterprise
  - Internet of Things
  - Home Networking
- Each case study (of the two selected) will have a different grouping for students.
  - You will each be part of two groups.
  - Once established, last 20 minute of lecture period will be for group meetings (with the instructor)

Individual Presentation

- On topic from course syllabus
  - 20 minute PPT presentation on aspect of system administration
  - Will select topics from among:
    - Adversarial Security Plan
    - Response Plans
    - Red teaming and penetration testing tools
    - Linux security administration
    - Network Security Components
    - Network Security administration
    - Configuration Management
    - Network Attack Administration (SIEM)
    - Network Monitoring and Attack Forensics
    - Accreditation and acceptance testing
    - (others as proposed by students)

Questions on Course Structure

Initial Reading Assignment
(read before 1/27 class)

- Guidance in writing a security policy

www.GIAC.org/paper/gsec/734/system-security-policy/101613

- Not so much reading, but I want you to all become familiar with installing linux under a virtual machine (e.g. VMWare or VirtualBox). Some good starting points are:
  - https://itsfoss.com/install-linux-in-virtualbox/
  - https://linuxhint.com/install_ubuntu_vmware_workstation/

Course Outline

- Introduction to Secure System Administration
- Generation of Security Requirements
- NIST Best Practices – Linux System Administration
- Composition of systems and protection domains
- Configuration Management, System Updates
- Adversarial Security – Pen Testing – Read Teaming
- Virtualization and Cloud Security
- Incident Response Planning
- Network Administration
- Network Monitoring and Attack Forensics
- Security Incident Event Management
- Group Project Testing and Debrief
- Accreditation and acceptance testing

Introduction to Secure System Administration

- Secure
  - Ability to correctly implement relevant policy
- System
  - A computer?
  - A network?
  - The combination of all system components implementing a particular function
- Administration
  - Selection of components (purchases of products)
  - Architecture – how the pieces fit together
  - Installation and configuration
  - Security Testing
  - Operation
  - Monitoring
  - Repair and Maintenance
  - Threat response

Application Architecture

- What are the functional requirements of the system?
  - This guides equipment needs
    - Processing, Storage, and Network.
  - What are the functional goals of the system.
- This defines the meaning of availability
  - What constitutes a breach of availability – the system no longer meets its functional goals.
  - Critical Infrastructure
  - Critical for you
- Consequences of failure

Positive and Negative Requirements

- Functional requirements are positive.
  - This is what most developers focus on
  - And why our systems are not secure.
  - Functionality over security
- Security requirements tend to be negative
  - What should not be possible (conf and integ)
  - But availability is a positive requirement
- How do we test for negative requirements
  - *absence of evidence is not evidence of absence*

Information Flow and Containment

- Understand your applications Information Flow:
  - What is to be protected
  - Against which threats
  - Who needs to access which apps
  - From where must they access it
- Do all this before you invest in the latest products that salespeople will say will solve your problems.

What is to be protected

- Is it the service or the data?
  - Data is protected by making it less available
  - Services are protected by making them more available (redundancy)
  - The hardest cases are when one needs both.

Classes of Data

- Decide on multiple data classes
  - Public data
  - Customer data
  - Corporate data
  - Highly sensitive data

  (not total ordering)
- These will appear in different parts of the network

Classes of Users

- Decide on classes of users
  - Based on the access needed to the different classes of data.
- You will architect your system and network to enforce policies at the boundaries of these classes.
  - You will place data to make the mapping as clean as possible.
- You will manage the flow of data

Component Selection

- What systems do you need
  - System or VM for different classes of protection domains.
- Network Components
  - To interconnect
  - To Segregate
- Management Components
  - Special tools for management and security

- You will manage the flow of data

Inventory

Conduct an Inventory – of physical assets

- What Kinds of systems do you have
  - E.g. POS terminals, SCADA, servers, network hardware
- Understand the access to each system
  - Employees, customers, etc
- How are the different classes of systems protected from one another
  - Network zones, etc
- How do you contain breaches to particular zones.
- What happens to your business if any of these are compromised or shut down.

Identity Management

- Interrelation of identity with policy
  - Selection of authentication technology
  - Enrollment issues
  - Balancing cost with security
- What is needed for strong audit capability
  - Not just intrusion detection
  - Regulatory and recovery/remediation

Configuration Management

- Catalog of systems
  - What is approved for connection
- Catalog of software
  - What is approved for use
  - Patch management
- Configuration checkers
- Change detectors
  - E.g. tripwire, AFIK

Adversarial Security Plan

- Enumerate goals of attacker
  - Consider likelihood of targets
- Enumerate consequences of various attacks
  - Consider cost to organization of effective attack
- Prioritize deployed resources to defend systems
- Develop attack defense trees

- Consider mitigations

- Design red teams
- System red teams
- Penetration testing

Response
Handling the Inevitable Breach

- Response depends on many factors, but most importantly:
  - Your containment architecture - How the system has been set up according to the information discussed earlier

- But also on your preparation
  - Emergency Response Plan
  - Emergency Response Team
  - How the system has been set up - Backups, Data Collection for Forensics, Baselines

Collect Baseline On all Assets

Software and system checksums

- Used to detect changes to the system
- To identify which assets are affected
- To enable recovery – reinstall those affected systems

Baseline data communication from all assets

- In your network infrastructure, use this to identify anomalous flows
- As they happen to block exfiltration
- From Logs to identify where data went and how much, and over what time periods

After a breach: Containment

- You will need to shut down or take offline those systems affected by the breach (those you can no longer trust) to prevent further loss of data.
- Collect forensic data to assist in assessing impact, to identify attackers, and for prosection.
- Stronger containment (from preparation phase) means fewer critical services that you need to take offline.

After a breach: analysis

- Check for changes to your systems and data.
- Use forensic data collected using technologies in place from your planning phase to identify sources of the attack, and the techniques used.
- Use this information to determine which customers data and which systems were affected.
- Use this information to fix the vulnerabilities in your existing systems.
- Subject to legal requirements, share this information as appropriate with the authorities and the security community.

After a breach: recovery

- Systems/data must be restored to a trusted state.
  - Using backups
  - Legitimate updates to data may need to be reapplied
- Vulnerably used in the attack must be patched before systems are brought back online.
- You need a plan for operating your business for some period without the impacted systems.
  - Part of your planning phase

System Administration

- What must be administered:
  - User accounts – Least Privilege
  - Software
  - Servers
  - Storage
  - Network (next slide)
  - Keys
  - Monitoring
  - Logs and Audit
- Core principles
  - Minimization

Network Administration

- Creation of network protection domains
  - Firewalls
  - VLANs
  - VPNs for access
  - Ipsec
  - Wireless Management
- Network Monitoring
- Network Admission Control

SIEM Monitoring - Forensics

- Network Attack Administration (SIEM)
- Network Monitoring and Attack Forensics

Accreditation and acceptance

- Determining when it is OK to bring your system live
- Certification for government agencies
- Periodic audits
- Certification for customers or upstream parties
  - E.g. PCI Compliance

Administration vs Development

- Different stages in system life cycle
  - Administration is concerned with installation, interconnection, configuration, operation, and decommissioning
  - Administration is concerned with the environment
  - Development addresses the architecture of the system (or part of a system)
    - Depends on assumptions

- Security fails when environmental assumptions are violated.
  - Let’s brainstorm on examples of such assumptions that led to security failures when they no longer held.

Two Scenarios used as Examples

- These are the basis of the exercises throughout the semester.
  - Banking and Retail
  - Criminal Enterprise
- These were chosen because there are differences in the goals (interpretation of the principles) and thus they provide a good way to discuss the principals, policies, and procedures that underly administration.

Banking

- Your organization must:
  - Maintain a database of account holders
  - A database of account balances
  - Enable web access by customers who:
    - Can update their personal information
    - Check their account balance
    - Transfer funds to another account (by number)
    - View transactions on their account
    - Submit an image of a check for deposit
      - (check should be viewable, but you do not need to scan it or process it)
- Access is needed
  - Via web from the open internet
  - Outbound email confirming transactions
  - All other interactions may be limited by information flow policies to internal machines.

Retail (similar to banking)

- Your organization must:
  - Maintain a database of customers
  - A database of products and prices
  - A database of customer orders – and status
  - Support the update of prices in the system
  - Support inquires by customers of order status
  - Allow customers to place orders
  - Accept payment information from customers for submission to a credit card processor
  - Enable web access by customers who:
    - Can place orders
    - Check order status
    - Cancel orders
  - Enable access by employees
    - To set prices
    - Perform customer service functions
- Access is needed
  - Via web from the open internet for customer facing functions
  - For employees
- OUR EXERCISES WILL INCLUDE EITHER BANKING OR RETAIL, WE WILL NOT DO BOTH

Criminal Enterprises (We can adjust this based on CE)

- Chosen because of differences in the high level principles.
  - Not because I expect you to implement these kinds of systems in your future endeavors.
  - But you may be called upon to break some of these systems if later employed by government organizations.
- Your organization must:
  - Accept Bitcoin as payment (not really, but it must accept something that stands in for bitcoin)
  - Manage an inventory of stolen account identifiers with passwords
  - Control access to such information
  - Prevent collection of evidence or intelligence by third parties.
  - Note, do not deal in any illegal goods, but use dummy information to stand in for such goods. Also, do not use terms associated with such illegals goods or information in communications, make up new names for this dummy information.

Pre-Initial Homework Exerise
(due before 1/27 class and discussed now)

- Submit through Drop-box on D2L
- System Structure for Home Network with IoT devices.
  - Enumerate the classes of data
  - Enumerate the classes of users
  - Identify the protection domains
  - Enumerate the systems (hardware)
  - Enumerate the systems (software components)
- This write-up is expected to be about 3 pages in length (could be more or less)
- But we will develop our answer right now (you only need to explain what we discuss).

CSci530 Final Q3 – Fall 2016
Internet of Threats (IoT)

Following last month's denial of service attack on the Dyn Domain Name System infrastructure, we learned how Internet of Things (IoT) Devices in the homes of consumers can be subverted and used as nodes in a Mirai botnet to attack other systems on the Internet (Mirai is the name of the software used by the attackers to create the botnet). While the effects of this particular attack were felt primarily outside the home network on which the compromised attacks were placed, it serves as a wakeup call for users of Internet of Things devices because such compromised devices can do much worse things if the attacker chooses. In this question you will explore the potential impact of compromised / subverted IoT devices, and propose steps you can take to mitigate the impact of such attacks.

– Vulnerabilities (10 points) – Discuss some of the characteristics of IoT devices as they are usually implemented and deployed that makes them more vulnerable to compromise?.

– Impact of compromise (10 points) – List some of the consequences that are possible from an IoT subversion. By this I am asking what are the activities attackers can perform from a compromised IoT device on the typical home network, and how does this affect security.

– Design of IoT Devices (5 points) – If you were hired by a company developing devices that are intended to operate effectively as appliances connected to a home network, list some of the improvements in the design of such devices (i.e. certain requirements for the implementation of these devices) that will reduce the vulnerability of the devices to compromise.

– Securing your home network (15 points) – There will always been devices you want to use in your home that have not been appropriately protected by their manufacturer, In this question, discuss some of the steps that you can take on your home network to improve the resistance of IoT devices to attacks, and also to improve the security of the rest of your systems against attacks that might be initiated through a compromised IoT device.

Ungraded Lab Work for next Week

- Install free version of vmplayer or virtualbox on your own machine
- Configure some version / dist of Linux as a guest OS.
- Run two instances simultaneously
- Configure to allow network communication between the two VMs.
- Install a web server on one of the VMs.
- Configure Dynamic DNS (e.g. no-ip.com) to enable connection to the server from the internet.

Guidance for VMs

- If running windows, use virtualbox or vmware player.
- Workstation 12 Player is licensed for commercial use and is enabled to run restricted virtual machines. If you simply want to learn more about virtual machines or run virtual machines at home in a non-commercial environment you may use Workstation 12 Player at no cost. Download Workstation 12 Player for personal use. - See more at: https://www.vmware.com/products/workstation-player.html
- I have found it less problematic to install the 32 bit version even on a 64 bit machine.
  - If under linux, virtualbox may be easier to install.

Selecting a Linux Distribution

- Distributions are available that are optimized for many functions.
  - http://distrowatch.com/
- You should install LTS (long term support) versions, rather than the latest experimental versions.
- Apply all updates to your selected software.

- End of Lecture 1
- Following material is for lecture 2 but will be covered if time allows during first lecture

Your Oganizations Security Policy

- First step – Establish an Organization Security Policy
  - https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
- Guidance in writing a security policy
  - www.GIAC.org/paper/gsec/734/system-security-policy/101613
- First question for security auditors
- It will guide you in creating categories of data and user

Your Oganization’s Security Policy

- Principles
  - Computer Security Supports the Mission of the Organization
  - Computer Security is an Integral Element of Sound Management
  - Computer Security Should Be Cost-Effective
  - Systems Owners Have Security Responsibilities Outside Their Own Organizations
  - Computer Security Responsibilities and Accountability Should Be Made Explicit .
  - Computer Security Requires a Comprehensive and Integrated Approach
  - Computer Security Should Be Periodically Reassessed
  - Computer Security is Constrained by Societal Factors

Your Oganization’s Security Policy

Guidance in writing a security policy
www.GIAC.org/paper/gsec/734/system-security-policy/101613

- First question for security auditors
- It will guide you in creating categories of data and user and the kinds of access authorized
- It provides specific guidance for security requirements necessary to meet the principles just discussed.
- It will define responsibilities
- It will provide the basis for evaluating your organizations ability to meet the principals discussed earlier.

Security Requirement's

- Information Access
  - Mandatory Policies
  - Discretionary Policies
- Requirements on Security Technology
- Personnel Security
  - Including training
- Physical Security
- Monitoring and Audit
- Vendor Requirements
- Accreditation

Information Access

- Decide on multiple data classes
  - Public data
  - Customer data
  - Corporate data
  - Highly sensitive data
- Access to each class of data
  - Can you support mandatory policies
  - Otherwise what discretionary policies apply.
- Domain boundaries
  - Based on users and locations

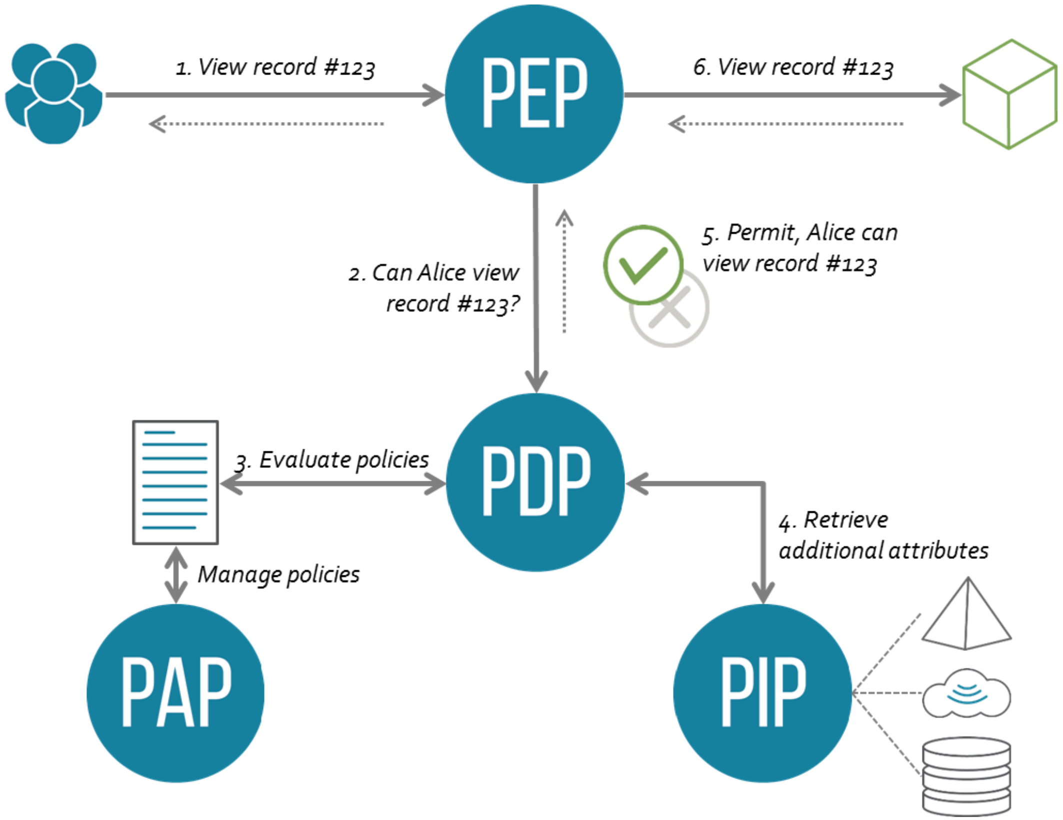
Technological Requirements: Information Access

- Identity Management
  - Factors / Basis for Authentication
  - Enrollment, Exception Handling
  - Other policy conditions

- Containment
  - Firewalls, VLANs
  - Encryption

- Policy
  - Decision points
  - Specification point (or administration)
  - Enforcement point

Points of Policy


1. View record #123
PEP
6. View record #123
2. Can Alice view record #123?
5. Permit, Alice can view record #123
3. Evaluate policies
PDP
4. Retrieve additional attributes
Manage policies
PAP
PIP

- By Axiomatics - Axiomatics, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=48397652

Network Administration

- Creation of network protection domains
  - Firewalls
  - VLANs
  - VPNs for access
  - Ipsec
- Define required characteristics
  - Where is encryption required
  - This is policy and administrations

Personnel Security

- Requirements on credentials and vetting processes for employees with access to different domains.
  - Relates to identity management
  - More as a precursor
- IM about who the user is, PS about vetting and physical access and issuance of ID’s.

Physical Security

- Virtual containment of data to domains is useless if access to protected machines can be achieved by failures of physical security. Define controls on placement of hardware and protection of cables, etc.

Monitoring and Audit

- This is how you will know that you have been attacked.
- It is critical to consider these technologies when designing your deployment.
- The monitoring function is part of administrations.
  - Responding to alerts
  - False positive vs false negatives
  - Volume of alerts and what is of interest.

Vendor Requirements

- Concern with supply chain subversion, and physical access by vendors on site.
  - Apply personnel security constraints to vendors.
  - Restrict access by vendors and visitors.

INF526: Secure Systems Administration

Composition of Systems And Security Domains

Prof. Clifford Neuman

What are you Securing

- The System as a Whole
  - Comprised of Software Components
  - Components have access to information
  - The Composition Problem
    - System must be evaluated as a whole
    - Can only reason about complete encapsulation
      - In which case you are reasoning about the effectiveness of containment.
      - Guard example
      - Firewall example

Containment Technologies

- Network Containment
  - – Firewalls
  - – Virtual Lans (VLANS)
  - – Virtual Private Networks (VPNs)
  - – Encryption
    - SSL, TLS, IPSec, and IPv6 Security
    - End to End
      - – Application encapsulation
      - – Trusted Computing Key Management
      - – Guards
- Network Administration

Containment Technologies

- Containment Within a Computer
  - OS Enforced Access Control
    - MAC or DAC
  - Application Enforced Access Control
    - Database access policies
    - Web access policies (e.g. .htaccess)
  - Specific Technologies
    - Virtual Memory or Segment Architectures
    - Reference Monitory / Access Control
    - User mode vs System Mode
    - Trusted Computing
- System Administration

Containment Technologies

- System Containment
  - Encryption Based
  - Guards
  - Object Encryption

Protection Domain

- The set of objects and operations on those objects that may be performed by a process.
- If access is dynamic, then the concept is amorphous.
  - Generally, if two processes share the same access to objects, we think of them as being in the same protection domain.
  - An object, or collection of information, will usually be part of more than one protection domain.
  - Granularity usually not smaller than that of a process (at a particular point in time) since the process is the only entity capable of accessing data.

Controlling Access to Data by Protection Domains

- General Containment
  - System Boundaries
    - Data exists in memory (V or NonV, Primary or Secondary) of a system.
    - It can only be accessed from outside that system with:
      - Physical Access to the peripheral
      - Assistance by a process running on that system
    - Does this apply to NAS?
    - Does this apply to cloud storage?

Processes and Concentric Protection Domains

- Process Boundaries
  - Managed by OS
  - Limits access by processes to their own memory
  - Limits access to storage according to permissions (DAC,MAC)
  - May assign labels to data based on processes protection domain (labels)
- System has full access, Administrator might have full access
  - MAC and Trusted computing can control admin access

Network Containment

- When data is sent across a network
  - It should be considered accessible by all computer on the network segments traversed
  - Unless that data is encrypted
- When a process on a system can communicate with a process in the network.
  - It should be considered subvertable by any process with which it communicates.
  - A subverted process can not control access to information within its protection domain.
- Network Containment
  - Controls the segments of which data can traverse (outbound)
  - Controls communication (inbound) that is capable of subverting a process or accessing data.

Host Administration Guidance

- Create multiple protection domains
  - Don't run anything as root (or as little as possible)
- Configure access to resources carefully

Network Administration Guidance

- Use firewalls to contain access
  - Distributed Host Based may be okay and more effective for some environments – embedded even better.
- Disallow by default
  - Open a flow only when defined by application and system architecture.
- VLAn's good, but unless enforced by network hardware or encryption, subverted hosts can circumvent.

Administering Encryption

- Encryption can provide containment independent of the integrity of the systems connected physically to the stored or transmitted data.
  - Reduces protection of data to protection of the key
  - Still circumventable when access to plaintext exists.
- Key Management issues
  - Can leverage trusted hardware
    - Smartcards, Secure Elements, TPM's, Intel's Trusted Execution Technology (TXT)
  - Often too complex to manage at level of authorized users