CISSP Study Session

Study and become CISSP Certified

We will learn the 10 domains used in the ISC2 and which are tested in the CISSP exam.

Charles Sturt University

IT Masters
itmasters.edu.au

Certified Information System Security Professional

Earn the CISSP certification without breaking your wallet

Class Information

Webinars run on Wednesdays

- First session from 12:00pm – 1:30pm
- Second session from 3:00pm – 4:30pm
- Webinars will be uploaded within 24 hours of running

CISSP Short Course

A compressed version of subject

ITE514: Professional Systems Security

Part of the

- ***Master of Information Systems Security***
- ***Master of Management (IT)***

Charles Sturt University

IT Masters
itmasters.edu.au

Master of IS Security

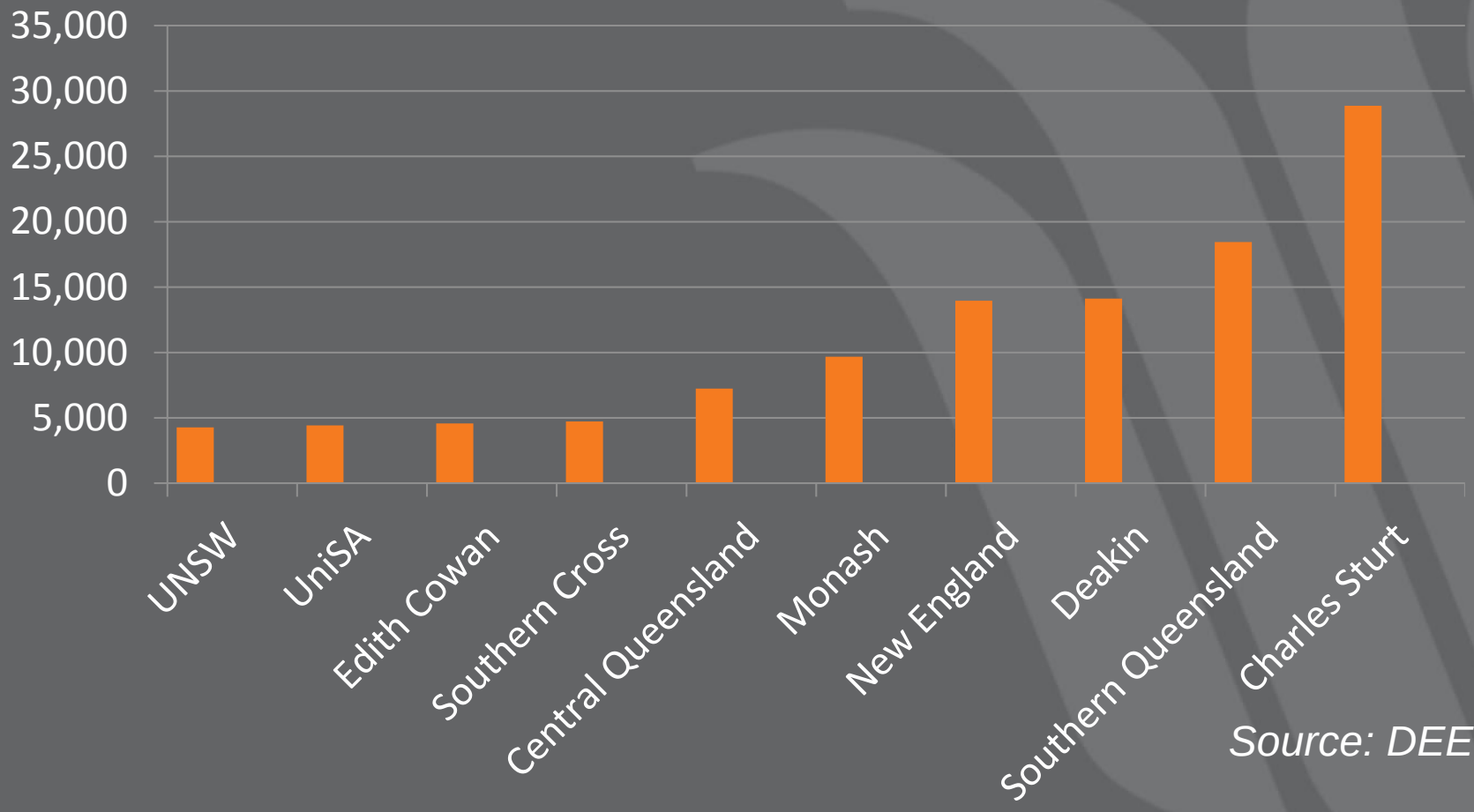
Core Subjects (5 Subjects):	Industry Electives (choose 3)
ITC596 IT Risk Management	ITE514 Professional Systems Security
ITC593 Network Security	ITE511 Digital Forensic Security Essentials (Credit only)
ITC506 Topics in IT Ethics	ITE515 Forensic Analysis (Credit only)
ITC595 Information Security	ITE516 Hacking Countermeasures
ITC597 Digital Forensics	ITI551 Virtual Private Network and Firewall Management I (Credit only)
ITE512 Incident Response	MGI511 Project Management Fundamentals
ITE513 Forensic Investigation	MGI512 The Project Lifecycle
ITE525 Cyber Law	MGI513 Enterprise Project Management
Elective Subjects (Choose 1):	ITI581 Network Security Fundamentals
ITC516 Principles of Database Development	MGI522 Developing Solutions
ITC514 Network and Security Administration	
ITC563 IT Management Issues	
ITC513 Wireless Networking Concepts	

- CISSP certification = credit for 2 subjects
- To find out additional credit, fill out Eligibility Form at www.itmasters.edu.au
- To contact Charles Sturt University Course Director: jhowarth@csu.edu.au

Charles Sturt University

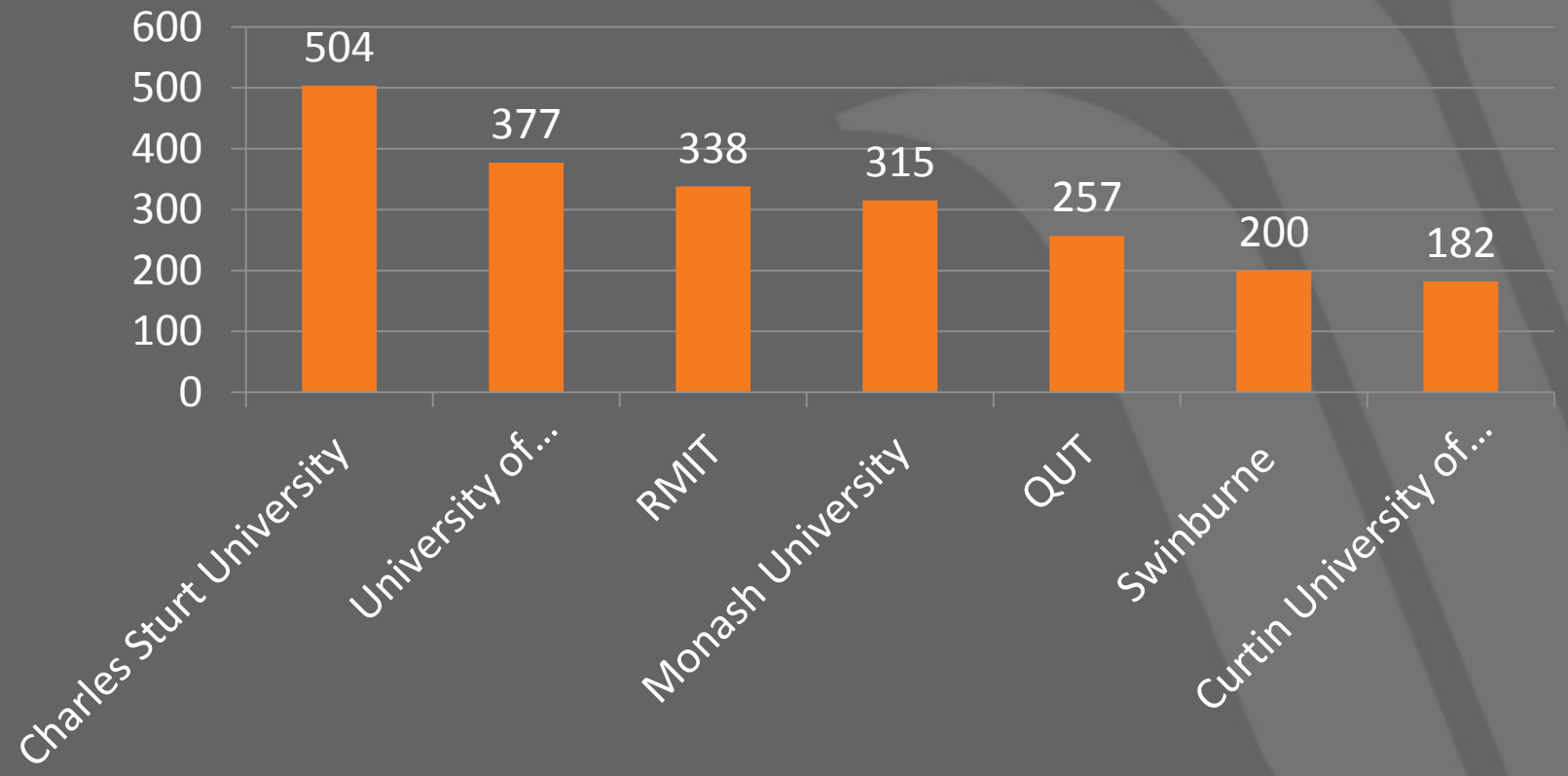
IT Masters
itmasters.edu.au

Market Leader: Distance Ed



Source: DEET

Market leader – IT, PG, Domestic



Information

- Dr. Craig S Wright GSE MSTAT LLM GSC GSM MInfoSysSec, MMgmt
- Charles Sturt University

- Craig.Wright@cscss.org
- crwright@csu.edu.au

Overview

- Certification review
- CISSP requirements
- Common Body of Knowledge Areas
- Study Suggestions

- You will get out of this what you put in.

About this Class

I would like to thank all the authors that have worked to add materials to the Internet that we can all use to educate ourselves inexpensively.

This course is based on many sources of materials and links are provided throughout.

About this Class

In this series of lectures, we will use a variety of free and open source materials and present these in a way that aids you in learning the material and gaining the knowledge needed to pass the exam.

Where possible, all materials and links are available without cost.

Who?

- CISSP
  - Certified Information Systems Security Professional
  - ISC² (www.isc2.org)
    - The International Information Systems Security Certification Consortium, Inc.
    - Maintains the CBK® for information security
  - ANSI ISO Accredited
  - Targeted for mid- and senior-level managers who are working toward or have already attained positions as CISOs, CSOs or Senior Security Engineer equivalents

Commonalities in Certification Programs

- Understand a common body of knowledge
- Previous education and/or work experience
- Demonstrate a level of understanding
- Certification time period
- Re-certification procedures
- Reinstatement
- Dues, Fees, or Memberships

Professional Certification

- Body of Knowledge encompasses the majority of the field
- Managed by a non-profit organization
- Exam requires NDA
- Requires commitment to code of ethics
- Requires endorsement and may involve an audit
- Examples:
  - $(ISC)^2$ CISSP
  - ISACA CISA and CISM

ISC2 CISSP Requirements

- Commit to Code of Ethics
- Have required work experience
- Pass the Examination
  - 250 multiple choice questions; Six hours
- Continuing Professional Education
  - 120 credits per three year certification period
- Pay yearly maintenance fee

- ISC2 site holds the details.


Firefox
CSU Forums - Forums
Interact : ITE504 201190 W D : Su...
Recent Announcements
(ISC)² Security Transcends Techn...
CISSP Education & Certification
https://www.isc2.org
TextAloud
Speak
Pause/Resume
Stop
Add Article
Zoom In
Zoom Out
Speed
TextAloud Voice
(ISC)² SECURITY TRANSCENDS TECHNOLOGY
Sign In
Sign In here to pay AMFs, submit CPEs, update profile settings, review transactions, and more.
Home
Education
Certifications
Chapters
Social Responsibility
Careers
Events
Industry Resources
About (ISC)²
Blog
Join InterSeC!
INTERSEC
The community where secure minds meet.
Don't miss out on the conversation. Collaborate with other security professionals for career advice, projects, best practices through groups, wiki's, blogs, etc.
Join InterSeC!
Register Now
Help make the world Cyber safe!
Safe and Secure Online
(Share)
(Download)
(Volunteer)
Employers
How certified employees benefit your organization
Government
Education & certification that meets regulations
(ISC)² Resource Guide
Access key resources in information security
SDLC Professional
Steps to CSSLP certification
I am interested in:
select below
Site Search
Search
Download a FREE case study by (ISC)²
(ISC)² Security Congress Press Conferences
At (ISC)²'s first annual Security Congress, the organization held two press conferences. One to announce new (ISC)² initiatives and one held with ASIS on collaboration to advance all security professionals. Videos from these press conferences are available at www.youtube.com/isc2tv
2011 (ISC)² Global Information Security Workforce Study - Available Now
Download the latest study based on over 10,000 information security respondents globally. Topics include trends in salary, years of experience in information security to the most critical threats to the organizations today.
Why Certify with (ISC)²?
CAP®
(Connect with us on:)
Join the InterSeC Community!
INTERSEC
where secure minds meet
Already an InterSec user?
Log in here.
(Latest Blog Post)
RSS
(News & Media)
October 26, 2011
(ISC)² Safe and Secure Online

CISSP Domains

- https://www.isc2.org/cissp-domains/default.aspx
- Ten domains – this week…

- **Access Control** – a collection of mechanisms that work together to create security architecture to protect the assets of the information system.
  - Concepts/methodologies/techniques
  - Effectiveness
  - Attacks
- **Software Development Security** – refers to the controls that are included within systems and applications software and the steps used in their development.
  - Systems development life cycle (SDLC)
  - Application environment and security controls
  - Effectiveness of application security

Preparing for the Exam

- Collect your study materials
  - Build a library of documents in the subject areas
- Set time aside every day for study
  - Avoid taking too much time off between study

Exam Resources

- CISSP practice tests

  http://www.cccure.org/modules.php?name=Web_Links&l_op=viewlink&cid=168

  Registration is free…

After the Exam

- Must provide resume
- Must state which 2+ domains you have experience in, at which jobs and for how many years.
- Must be sponsored by a current CISSP (preferred) or have a past manager vouch for your experience

In summary...

- You will need to learn the 10 domains well
- You need to have a good knowledge of all areas to do well.

QUESTION AND ANSWER

before we start?

Security Principles

- The three main security principles also pertain to access control:
  - Availability
  - Integrity
  - Confidentiality

Week 1 - Part 1
Access Controls

A collection of mechanisms that work together to create security architecture to protect the assets of the information system.

- Concepts/methodologies/techniques
- Effectiveness
- Attacks

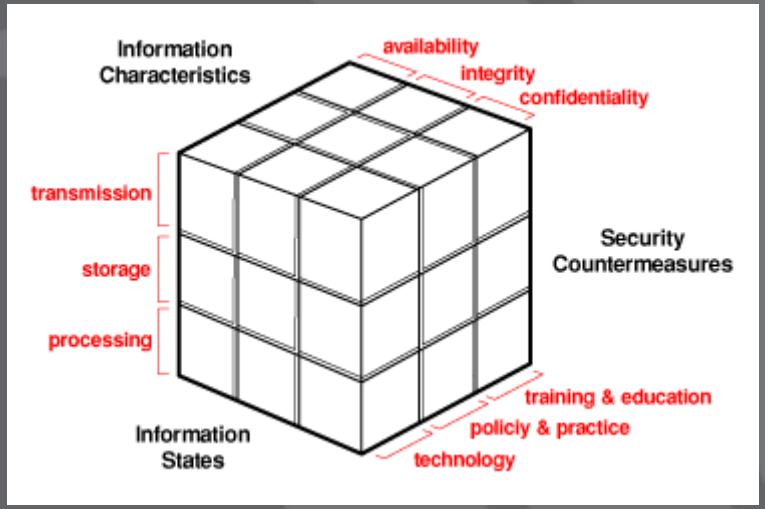
Access Controls

http://en.wikipedia.org/wiki/Access_control

Purpose of Access Control

Information security consists of many components:

- Culture
- Processes
- Policies
- Technologies



Control Combinations

- Preventive/Administrative
  - "Soft" mechanisms that support access control objectives
  - Include organizational policies/procedures, pre-employment background checks, employment agreements
- Preventive/Technical
  - Uses technology to enforce access control policies
  - Include protocols, encryption, smart cards, call-back systems
- Preventive/Physical
  - Intuitive measures intended to restrict physical access
  - Defined by a circular security perimeter that is under access control (fences, badges, man-trap)
- Detective/Administrative
  - Applied for prevention of future security policy violations or to detect existing violations
  - Organizational policies and procedures, increased supervision, behavior awareness
- Detective/Technical
  - Intended to reveal the violations of security policy using technical means
  - Include intrusion detection systems and violation reports from audit trail information
- Detective/Physical
  - Usually require that a human evaluate the input from sensors or cameras

Access Controls

- From (ISC)2 Candidate Information Bulletin:
  - Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system.

Access Controls

- From (ISC)2 Candidate Information Bulletin:
  - The candidate should fully understand access control concepts, methodologies and implementation within centralized and decentralized environments across the enterprise's computer systems. Access control techniques, detective and corrective measures should be studied to understand the potential risks, vulnerabilities, and exposures.

Access control

- From (ISC)2 Candidate Information Bulletin:
  - Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system.

Access Control Overview

- Access Controls: The security features that control how users and systems communicate and interact with one another.
- Access: The flow of information between subject and object
- Subject: An active entity that requests access to an object or the data in an object
- Object: A passive entity that contains information

Identification, Authentication, and Authorization

- Identification, Authentication, and Authorization are distinct functions.
  - Identification
  - Authentication
  - Authorization

- Identity Management: A broad term to include the use of different products to identify, authenticate, and authorize users through automated means.

Identification

- Identification
  - Method of establishing the subject's (user, program, process) identity.
    - Use of user name or other public information.
    - Know identification component requirements.

Authentication

- Authentication
  - Method of proving the identity.
    - Something a person is, has, or does.
    - Use of biometrics, passwords, passphrase, token, or other private information.
- Strong Authentication is important

Authentication

- Biometrics
  - Verifies an identity by analyzing a unique person attribute or behavior (e.g., what a person “is”).
- Most expensive way to prove identity, also has difficulties with user acceptance.
- Many different types of biometric systems, know the most common.

Authentication

- Most common biometric systems:
  - Fingerprint
  - Palm Scan
  - Hand Geometry
  - Iris Scan
  - Signature Dynamics
  - Keyboard Dynamics
  - Voice Print
  - Facial Scan
  - Hand Topography

Authentication

- Biometric systems can be hard to compare.
- Type I Error: False rejection rate.
- Type II Error: False acceptance rate.
  - This is an important error to avoid.
- Crossover Error Rate

Authentication

- Passwords
  - User name + password most common identification, authentication scheme.
  - Weak security mechanism, must implement strong password protections
  - Implement Clipping Levels

Authentication

- Techniques to attack passwords
  - Electronic monitoring
  - Access the password file
  - Brute Force Attacks
  - Dictionary Attacks
  - Social Engineering
- Know difference between a password checker and a password cracker.

Authentication

- Passphrase
  - Is a sequence of characters that is longer than a password.
  - Takes the place of a password.
  - Can be more secure than a password because it is more complex.

Authentication

- One Time Passwords (aka Dynamic Passwords)
  - Used for authentication purposes and are only good once.
  - Can be generated in software (soft tokens), or in a piece of hardware

Authentication

- Two types of Token Devices (aka Password Generator)
  - Synchronous
    - Time Based
    - Counter Synchronization
  - Asynchronous
- Know the different types of devices and how they work.

Authentication

- Smart Cards and Memory Cards
  - Memory Cards: Holds but cannot process information.
  - Smart Cards: Holds and can process information.
    - Contact
    - Contactless
      - Hybrid
      - Combi

Authentication

- Attacks on Smart Cards
  - Fault Generation
  - Microprobing
  - Side Channel Attacks (nonintrusive attacks)
    - Differential Power Analysis
    - Electromagnetic Analysis
    - Timing
    - Software attacks

Authentication

- Hashing & Encryption
  - Hash or encrypting a password to ensure that passwords are not sent in clear text (means extra security)
- Windows environment, know syskey modes.
- Salts: Random values added to encryption process for additional complexity.

Authentication

- Cryptographic Keys
  - Use of private keys or digital signatures to prove identity
- Private Key
- Digital Signature
  - Beware digital signature vs. digitized signature.

Authorization

- Authorization
  - Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources.

Authorization

- Access Criteria can be thought of as:
  - Roles
  - Groups
  - Location
  - Time
  - Transaction Types

Authorization

- Authorization concepts to keep in mind:
  - Authorization Creep
  - Default to Zero
  - Need to Know Principle
  - Access Control Lists

Authorization

- Problems in controlling access to assets:
  - Different levels of users with different levels of access
  - Resources may be classified differently
  - Diverse identity data
  - Corporate environments keep changing

Authorization

- Solutions that enterprise wide and single sign on solutions supply:
  - User provisioning
  - Password synchronization and reset
  - Self service
  - Centralized auditing and reporting
  - Integrated workflow (increase in productivity)
  - Regulatory compliance

Authorization

- Single Sign On Capabilities
  - Allow user credentials to be entered one time and the user is then able to access all resources in primary and secondary network domains
- SSO technologies include:
  - Kerberos
  - Sesame
  - Security Domains
  - Directory Services
  - Dumb Terminals

Access Control Models

- Access Control Models:
- Three Main Types
  - Discretionary
  - Mandatory
  - Non-Discretionary (Role Based)

Access Control Models

- Discretionary Access Control (DAC)
  - A system that uses discretionary access control allows the owner of the resource to specify which subjects can access which resources.
  - Access control is at the discretion of the owner.

Access Control Models

- Mandatory Access Control (MAC)
  - Access control is based on a security labeling system. Users have security clearances and resources have security labels that contain data classifications.
  - This model is used in environments where information classification and confidentiality is very important (e.g., the military).

Access Control Models

- Non-Discretionary (Role Based) Access Control Models
  - Role Based Access Control (RBAC) uses a centrally administered set of controls to determine how subjects and objects interact.
  - Is the best system for an organization that has high turnover.

Access Control Techniques

- There are a number of different access controls and technologies available to support the different models.
  - Rule Based Access Control
  - Constrained User Interfaces
  - Access Control Matrix
  - Content Dependent Access Control
  - Context Dependent Access Control

Access Control Techniques

- Rule Based Access Control
  - Uses specific rules that indicate what can and cannot happen between a subject and an object.
  - Not necessarily identity based.
  - Traditionally, rule based access control has been used in MAC systems as an enforcement mechanism.

Access Control Techniques

- Constrained User Interfaces
  - Restrict user's access abilities by not allowing them certain types of access, or the ability to request certain functions or information
- Three major types
  - Menus and Shells
  - Database Views
  - Physically Constrained Interfaces

Access Control Techniques

- Access Control Matrix
  - Is a table of subjects and objects indicating what actions individual subjects can take upon individual objects.
- Two types
  - Capability Table (bound to a subject)
  - Access Control List (bound to an object)

Access Control Techniques

- Content Dependent Access Control: Access to an object is determined by the content within the object.
- Context Based Access Control: Makes access decision based on the context of a collection of information rather than content within an object.

Access Control Administration

- First an organization must choose the access control model (DAC, MAC, RBAC).
- Then the organization must select and implement different access control technologies.
- Access Control Administration comes in two basic forms:
  - Centralized
  - Decentralized

Access Control Administration

- Centralized Access Control Administration:
  - One entity is responsible for overseeing access to all corporate resources.
  - Provides a consistent and uniform method of controlling access rights.
    - Protocols: Agreed upon ways of communication
    - Attribute Value Pairs: Defined fields that accept certain values.

Access Control Administration

- Types of Centralized Access Control
  - Radius
  - TACAS
  - Diameter

Access Control Administration

- Decentralized Access Control Administration:
  - Gives control of access to the people who are closer to the resources
  - Has no methods for consistent control, lacks proper consistency.

Access Control Methods

- Access controls can be implemented at various layers of an organization, network, and individual systems
- Three broad categories:
  - Administrative
  - Physical
  - Technical (aka Logical)

Access Control Methods

- Administrative Controls
  - Policy and Procedure
  - Personnel Controls
    - Separation of Duties
    - Rotation of Duties
    - Mandatory Vacation
  - Supervisory Structure
  - Security Awareness Training
  - Testing

Access Control Methods

- Physical Controls
  - Network Segregation
  - Perimeter Security
  - Computer Controls
  - Work Area Separation
  - Data Backups
  - Cabling
  - Control Zone

Access Control Methods

- Technical (Logical) Controls
  - System Access
  - Network Architecture
  - Network Access
  - Encryption and protocols
  - Auditing

Access Control Types

- Each control works at a different level of granularity, but can also perform several functions
- Access Control Functionalities
  - Prevent
  - Detect
  - Correct
  - Deter
  - Recover
  - Compensate

Access Control Types

- Security controls should be built on the concept of preventative security
- Preventative Administrative Controls
  - Includes policies, hiring practices, security awareness
- Preventative Physical Controls
  - Includes badges, swipe cards, guards, fences
- Preventative Technical Controls
  - Includes passwords, encryption, antivirus software

Accountability

- Accountability is tracked by recording user, system, and application activities.
- Audit information must be reviewed
  - Event Oriented Audit Review
  - Real Time and Near Real Time Review
  - Audit Reduction Tools
  - Variance Detection Tools
  - Attack Signature Tools

Accountability

- Other accountability concepts…
- Keystroke Monitoring
  - Can review and record keystroke entries by a user during an active session.
  - A hacker can also do this
  - May have privacy implications for an organization
- Scrubbing: Removing specific incriminating data within audit logs

Access Control Practices

- Know the access control tasks that need to be accomplished regularly to ensure satisfactory security. Best practices include:
  - Deny access to anonymous accounts
  - Enforce strict access criteria
  - Suspend inactive accounts
  - Replace default passwords
  - Enforce password rotation
  - Audit and review
  - Protect audit logs

Access Control Practices

- Unauthorized Disclosure of Information
  - Object Reuse
  - Data Hiding
- Emanation Security
  - Tempest
  - White Noise
  - Control Zone

Access Control Monitoring

- Intrusion Detection
  - Three Common Components
    - Sensors
    - Analyzers
    - Administrator Interfaces
  - Common Types
    - Intrusion Detection
    - Intrusion Prevention
    - Honeypots
    - Network Sniffers

Access Control Monitoring

- Two Main Types of Intrusion Detection Systems
  - Network Based (NIDS)
  - Host Based (HIDS)
- HIDS and NIDS can be:
  - Signature Based
  - Statistical Anomaly Based
    - Protocol Anomaly Based
    - Traffic Anomaly Based
  - Rule Based

Access Control Monitoring

- Intrusion Prevention Systems
  - The next big thing
  - Is a preventative and proactive technology, IDS is a detective technology.
  - Two types: Network Based (NIPS) and Host Based (HIPS)

Access Control Monitoring

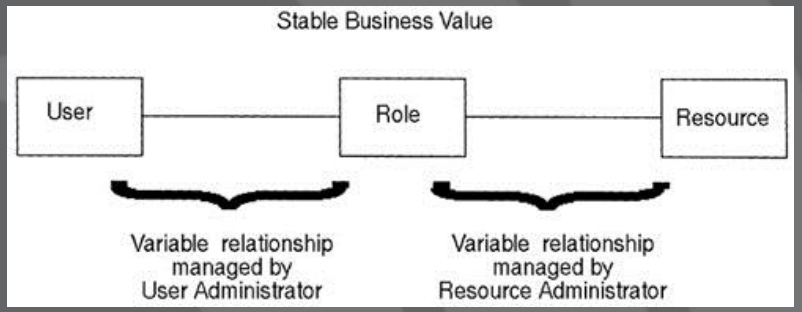
- Honeypots
  - An attractive offering that hopes to lure attackers away from critical systems
- Network sniffers
  - A general term for programs or devices that are able to examine traffic on a LAN segment.

Threats to Access Control

- A few threats to access control
  - Insiders
    - Countermeasures include good policies and procedures, separation of duties, job rotation
  - Dictionary Attacks
    - Countermeasures include strong password policies, strong authentication, intrusion detection and prevention
  - Brute Force Attacks
    - Countermeasures include penetration testing, minimum necessary information provided, monitoring, intrusion detection, clipping levels
  - Spoofing at Logon
    - Countermeasures include a guaranteed trusted path, security awareness to be aware of phishing scams, SSL connection

Role Based Access Control

- Security is managed at a level that corresponds closely to the organization's structure
- Each user is assigned one or more roles, and each role is assigned one or more privileges that are permitted to users in that role



Role Based Access Control

- Security administration: determine the operations that must be executed by persons in particular jobs, and assign employees to the proper roles
- Complexities introduced by mutually exclusive roles or role hierarchies are handled by the RBAC software, making security administration easier

Approaches to RBAC

- Core RBAC
  - Foundation of the model
  - Users, roles, permissions, operations, and sessions are defined and mapped according to the security policy
  - Can also include time of day, location of role, day of week, etc
- Hierarchical RBAC
  - Role relation defining user membership and privilege inheritance
  - Reflects organizational structures and functional delineations
  - Two types
    - Limited hierarchies – one level of hierarchy allowed
    - General hierarchies – allows for many levels of hierarchies
  - Separation of duties provided
    - Static Separation of Duties (cannot be a member of two groups)
    - Dynamic Separation of Duties (can be a member of two groups, but cannot be in both roles at the same time)

Threats to Access Control

We will talk about these later.. But let's review these now

- Dictionary attacks – what is this?
- Sniffers – what is this?
- Brute force attacks – how is this different then a dictionary attack.
- Spoofing login/trusted path
- Phishing
- Identity theft

Summary

- Administrative controls include a security policy, personnel controls, supervisory structure, and security-awareness training
- Physical controls include network segregation, perimeter security, work area separation, and data backups
- Technical controls include system access, network architecture, network access, encryption and protocols
- Identity management uses different products to identify, authenticate, and authorize users through automated means
- Single sign-on technologies include scripts, directory services, Kerberos, SESAME and Thin Clients

Summary - 2

- Access control models can be identity-based, role-based, or label-based
- RADIUS, TACACS+ and diameter are examples of centralized administration
- IDS's can monitor behavior or watch for known attacks
- IDS sensors and monitoring console are the components of a network IDS
- An IPS prevents unwanted traffic from getting to the target

Question and answer

Week 1 - Part 2
Software Development Security

Refers to the controls that are included within systems and applications software and the steps used in their development.

- Systems development life cycle (SDLC)
- Application environment and security controls
- Effectiveness of application security

Application security

http://en.wikipedia.org/wiki/Application_security

Application Development Security

- From (ISC)2:
  - Applications Development & Programming Concepts
  - Audit and Assurance Mechanisms
  - Malware
  - Database and Data Warehousing Environments
  - Web Application Environments

What do we cover

- Software Engineering
- Threats and Countermeasures
- Database Systems security
- Web Application Security

What is in this domain?

From the (ISC)^2 Store:

- Applications Development & Programming Concepts
- Audit and Assurance Mechanisms
- Malware
- Database and Data Warehousing Environments
- Web Application Environments

The Subject Areas

- Software Engineering
- Threats and Countermeasures
- Database Systems security
- Web Application Security

The Basics

Software controls vs environment

Software lifecycle Change control

Object-oriented components

Some technologies

- Java, etc...

Why look at Software Security?

Appliances (e.g., firewalls/toys) do not provide complete security

- Insider attacks
- Bypassed by proxy servers, VPNs

Same software can be used by different users with different privileges

- More security layers help

Security Approaches

Reactive (expensive and slow)

- Vulnerability scanning and patching
- Intrusion detection
- Incident response

Proactive

- More secure software and technologies
  - Designed
  - Configured

Security Approaches

Black Lists
Security Approaches

- Forbid known bad things (or look for them)
- Always one step behind
- Prone to failure as attackers figure out ways around the blocks

White Lists

- Allow only what's known to be safe
- Make it provably safe

Software Engineering Areas

- Requirements
- Design
- Construction
- Maintenance
- See: “Software Engineering Body of Knowledge”
- a.k.a. “SWEBOK”

- http://www.computer.org/portal/web/swebok

Requirements

Security functional

- Logging
- Password quality checks

Security Assurance

- Testing
- Code audits
  - Code checking tools

More Requirements

Threats vs countermeasures (controls)

- Threat modeling
- Threat assessment
- Risk analysis
- Risk assessment

Definition of Controls

- Read as “things that improve security”
  - **Prevent**
  - **Detect**
  - **Correct** **} policy violations**
- Using means
  - Physical
  - Administrative
  - Technical (a.k.a. logical)

Administrative Controls

- Policies
- Procedures
- Standards

e.g., must get approval to make a code change

Physical Controls

Software development and production environments should be secured

Physical access

- Servers, workstations
- Network plugs

Activity monitoring

Logical Controls

Protect data (confidentiality, integrity) and resources (availability)

Database controls

- Accounts
- Roles
- Transactions

File system controls

- Permissions

Risk Analysis

Do the defenses match the risks?

Cost vs risk

- Typically more secure systems cost more to build

–The CISSP test doesn't argue fine points

Security vs functionality

Threats, Vulnerabilities and Attacks

Vulnerabilities and the Software Development Life Cycle

- Object-Oriented Programming
- Capability-Maturity Model

Malware definitions

Detecting attacks

- Expert systems and artificial intelligence

Software Development Life Cycle - SDLC

1. Feasibility study
2. Requirements definition
3. Design
4. Implementation
5. Integration and testing
6. Operations and maintenance

Vulnerabilities & Flaws

Vulnerability: “An instance of an error in the specification, development, or configuration of software such that its execution can violate the security policy" [Krsul 98].

Flaw: a flaw defines or implies what should have been done to prevent policy violations; it is a problem at a higher level of abstraction that may potentially enable several different attacks and create various vulnerabilities.

- example flaw: missing input validation

Vulnerability Classes

It is common to refer to the set of vulnerabilities that enable attack scenario X as “X vulnerabilities”, e.g., “cross-site scripting vulnerabilities”

Sometimes the name of a technology is used instead of the name of an attack, e.g., “format string vulnerabilities”.

Secure Programming

A set of processes, techniques and a way of thinking about software engineering to minimize the occurrence of flaws and vulnerabilities

- In general, fewer bugs mean fewer vulnerabilities

» Software engineering methods that prevent bugs are good for security

Secure Programming

Input validation

- Boundary identification and formation
- Input awareness
- Taint tracking

Secure programming principles

Code checkers

Code integrity with formal methods

Secure Programming Principles

- Least privilege
- Economy of mechanism
- Complete mediation
- Open design
- Separation of privilege
- Least common mechanism
- Psychological acceptability
- Fail-safe defaults (deny by default; white list)

OOP Object Orientated Programming

- Fundamental idea: encapsulate data with the procedures that manipulate it into a logical entity (“object”)
- Forbid direct access to the data, so that Invariants can be enforced
- – Data integrity is stronger
- Only pre-defined actions can be taken
- – Decreases the possibility of malicious or erroneous actions

OOP

Instance

Inheritance

Polymorphism

• Common methods defined by a common parent class (superclass)

Polyinstantiation

Object Request Brokers (ORB)

Capability Maturity Model

Software development processes

- Level 1: Ad Hoc (heroics)
- Level 2: Repeatable
- Level 3: Defined
- Level 4: Quantitatively Managed
- Level 5: Optimizing

- From an artisan approach (1) to an engineering science (5)

Attack code

- Attack code aims at exploiting vulnerabilities, and is commonly found in the form of attack scripts or proof-of-concept exploits. Worms are another example of attack code. Malicious code isn't necessarily attack code, but its mere presence may imply that the system was compromised by a prior attack. Malicious code resident on a victim computer and performing an undesirable function, such as spyware, rootkits or backdoors, is to be differentiated from attack code that exploits vulnerabilities.

Parasitic code

- Parasitic code is code that is attached or included in another document or executable and violates its integrity. Intended or original properties of the document or executable must be identifiable in order to determine the presence, nature and extent of the parasite. Parasitic code is not necessarily attack code.

Back-Door

- A back-door is code bypassing policy-approved user authentication mechanisms. Back-doors are usually hidden, hard to discover, and inserted and used for malicious purposes. For example, a remote user may issue commands as root through a previously installed back-door. Some back-doors are created by programmers for reasons of convenience (e.g., remote maintenance) and so the original intent may not be malicious. However, back-doors that violate security policies must be considered malicious, based on their behavior alone. Remote access mechanisms operating within policy are not to be confused with back-doors.

Trojan

- Code that gets executed by deceiving a user is a Trojan (the deception aspect implies maliciousness, even if it is a mild prank). Trojans can carry and be the initial entry mechanism for malicious code of another nature (e.g., a back-door or keylogger).

Self-Propagating code 1

- Viruses are parasitic and are spread by means of finding new host files (documents or executables) that will presumably also get read or run later. Macro viruses refer to viruses carried by documents which can carry “macros”, essentially a scripting capability which blurs the boundary between data and code.

Self-Propagating code 2

- Worms spread on their own, by duplicating their code to other systems and re-spawning their processes.

Spyware

- Spyware is code that reports user activities and system information to “unauthorized” parties (who is “unauthorized” may depend on perspective). An example is an “unauthorized” keylogger. Spyware could also take “interesting” forms such as being a virus, and reporting when a certain type of document is opened.

Rootkit

- A rootkit is a set of software artifacts that attempts to conceal its existence and execution (and possibly that of other malicious software as well) from the rest of the operating system, other processes or security tools, and consequently from users and administrators. Typically a rootkit subverts or replaces the utilities included with an operating system for the purposes of hiding a compromise and a back-door. A rootkit may include attack code as one of its components and may resist removal.

Botnets

Botnets are organized “networks of robots” or ZOMBIES obeying commands from a particular source, unknown to the owners of the computers

- Often comprise of ill-protected home computers

IDS

- WHAT is an IDS / IPS
- The difference

IDS

Signature

Vs

Anomaly detection

Integrity

E.g. Tripwire

Verify at regular intervals that what is not supposed to change hasn't

- Compute hashes
- Verify system invariants

Database Security

- Database types
- Database access control mechanisms
- Database integrity
- Database attacks and countermeasures

Relational Databases

Tables, rows, primary keys

» Foreign key constraints link a table to another

Database Access Control

Views
Only provide the data needed

Stored Procedures
Code executed in the database

Roles
Avoid errors in the repetitive assignment of permissions to users
Reason about types of users

SQL injection

Countermeasure: Parameterized Queries

- Send the commands and data separately so there can be no confusion

WWW Attacks

- Web Issues

WWW

- CSFR
- XSS
- Browser attacks

XSS

Server-Side Controls

- Strong input validation

» White list approach: define what's allowed and reject everything else

CSRF

Every form should contain a secret value set for each user at every session

» Receiving script should check that this secret is present

Session Fixation

Malory lays out a trap in the form of a URL or HTTP redirect

The trap specifies a session ID; Alice clicks on it

The web server accepts the session ID as valid

Session Fixation

Alice authenticates (gives user name and password)

Session status is now "authenticated" and linked to Alice's user name

Malory can now send commands as Alice because he knows the sessionID

Why?

Why does the attack work?

Is it because the client chose the session-ID?

No: an attacker can first get a valid session-ID from the real server, and keep it alive as long as necessary (until an attack succeeds)

Why?

The server has no proof that Alice received the original session ID directly, and not through Malory

- This shared knowledge is the pitfall
- Resembles a partial Man-In-The-Middle attack

Fix: Authentication Nonce

Remove the possibility of decoupling the identification and authentication

• Assign a proof of authentication nonce to Alice's browser only and directly in response to a successful authentication request

» Request valid nonce for every request afterwards

More reading

- GIAC white papers for the CISSP CBK

- http://www.giac.org/resources/whitepaper/application/

Code Injection Attacks (Web)

- This is a lecture on
  - HTTP Response Splitting
  - XSS,
  - CSRF, and
  - Other code injection attacks

Code Injection Attacks (Web)

- Input flaws are very common
- This is fundamental to well-known attacks such as SQL Injection and Cross Site Scripting.
- Occurs when the developer places too much trust in the client
- Input is accepted without adequate filtering.

Cross Site Scripting (XSS)

- Cross Site Scripting AKA XSS
- It is tricking user into allowing their browser to execute code
- The browser treats the code as part of the local website and runs it in the same context as that page
- XSS attacks targets the browser (user) and not the server

An XSS attack comes in 4 parts

1. The client application which is fooled into running the code,
2. The server which is used to send the code to the client,
3. The attacker who seeks to gain in targeting the user, and
4. The code the attacker seeks to run on the client.

XSS Attacks (common ones)

- Displaying the page differently
- Stealing Cookies
- Phishing (redirection of traffic)
- VPN (End-points) – Dan Kaminsky
- Port scanning

Simple code injection

- <SCRIPT>alert("XSS")</SCRIPT>

- **See:**
- http://ha.ckers.org/xss.html

Types of XSS

- Reflection
  - Easiest to test
  - Place script in URL
- Persistent
  - Requires attacker to input script
  - Then view resulting page
  - Eg.
    - Post a message to a forum
    - View message as another user

XSS - Reflection

- XSS reflection attacks are simple.
- Add <script>alert('XSS')</script> into a URL
- Add the same to a POST to a site and the script is returned immediately on the page.
- **Reflection most common form**

XSS - Persistant

- Persistent XSS uses a web site's message-board features to place scripts in the user's browser.
- Commonly used to attack:
  - guest books,
  - classified ads, and
  - social networking
- Anywhere that user posting is allowed and encouraged.

Cross Site Request Forgery (CSRF)

- **Not related to XSS, but cam make it worse**
- The attacker does not need to inject code into a web application.
- CSRF leverages the web servers trust of an authenticated user

CSRF requires...

- Requires various items in order to succeed
  - The user is logged in with an active session
  - Application contains transactions that have predictable parameters

CSRF Step through (SANS.ORG)

- Attacker determines a link to initiate a transaction that uses predictable parameters
- Attacker posts this link on a site he controls
  - This site could just be a MySpace page or similar
  - Or the attacker could force the users to the site through DNS poisoning
- User logs into the application normally
- While the user is still logged in, they browse the link from the attacker
- This link could be
  - An Image tag
  - An IFRAME
  - CSS or JavaScript import
  - XMLHTTP
- This initiates a transaction as the victim
- The application isn't aware that the user didn't mean to submit the transaction

HTTP Response Splitting (OWASP)

- HTTP response splitting occurs when:
- Data enters a web application through an untrusted source, most frequently an HTTP request.
- The data is included in an HTTP response header sent to a web user without being validated for malicious characters.

- https://www.owasp.org/index.php/HTTP_Response_Splitting

HTTP Response Splitting (OWASP)

- HTTP response splitting is a means to an end, not an end in itself. At its root, the attack is straightforward: an attacker passes malicious data to a vulnerable application, and the application includes the data in an HTTP response header.

- To mount a successful exploit, the application must allow input that contains CR (carriage return, also given by %0d or \r) and LF (line feed, also given by %0a or \n)characters into the header. These characters not only give attackers control of the remaining headers and body of the response the application intends to send, but also allow them to create additional responses entirely under their control.

SQL Injection

- SQL injection is one of the most common attacks on the Web at the moment. The aim of this attack is to gather information from a database. A detailed description is located at http://www.owasp.org/index.php/SQL_Injection
- SQL injection errors transpire when developers allow data entry from untrusted sources and where the data can be used to dynamically construct a SQL query. The two main types of SQL injection attack include Passive SQL Injection (SQP) and Active SQL Injection (SQI).

SQL Injection

- The following sites are recommended to learn more about SQL injection.
- The SQL Injection Cheat Sheet:
  - http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- SQL Injection Walkthrough
  - http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- SQL Injection Attacks by Example
  - http://www.unixwiz.net/techtips/sql-injection.html

Start practicing NOW

We shall provide some of the many free sites that you can use to test yourself.

http://quizlet.com/2398073/cissp-250-500-flash-cards/

QUESTION AND ANSWER

That is week 1