Domain 1 - Security and Risk Management

Concepts (10)

CIA
DAD - NEGATIVE - (disclosure alteration and destruction)
Confidentiality - prevent unauthorized disclosure, need to know, and least privilege. assurance that information is not disclosed to unauthorized programs, users, processes, encryption, logical and physical access control,
Integrity - no unauthorized modifications, consistent data, protecting data or a resource from being altered in an unauthorized fashion
Availability - reliable and timely, accessible, fault tolerance and recovery procedures, WHEN NEEDED
IAAA – requirements for accountability
Identification - user claims identity, used for user access control
Authentication - testing of evidence of users identity
Accountability - determine actions to an individual person
Authorization - rights and permissions granted
Privacy - level of confidentiality and privacy protections

Risk (12)

Not possible to get rid of all risk.
Get risk to acceptable/tolerable level
Baselines – minimum standards
ISO 27005 – risk management framework
Budget – if not constrained go for the $$$

Responsibilities of the ISO (15)

Written Products – ensure they are done
CIRT – implement and operate
Security Awareness – provide leadership
Communicate – risk to higher management
Report to as high a level as possible
Security is everyone's responsibility

Control Frameworks (17)

Consistent – approach & application
Measurable – way to determine progress
Standardized – all the same
Comprehension – examine everything
Modular – to help in review and adaptive. Layered, abstraction

Due Care Which means when a company did all that it could have reasonably done to try and prevent security breach / compromise / disaster, and took the necessary steps required as countermeasures / controls (safeguards). The benefit of "due care" can be seen as the difference between the damage with or without "due care" safeguards in place. AKA doing something about the threats, Failing to perform periodic security audits can result in the perception that due care is not being maintained
Due Diligence means that the company properly investigated all of its possibly weaknesses and vulnerabilities AKA understanding the threats

Intellectual property laws (24)

Patent - grants ownership of an invention and provides enforcement for owner to exclude others from practicing the invention. After 20 years the idea is open source of application
Copyright protects the expression of ideas but not necessarily the idea itself ex. Poem, song @70 years after author dies
Trade Secret - something that is propriety to a company and important for its survival and profitability (like formula of Coke or Pepsi) DON'T REGISTER – no application
Trademarks - words, names, product shape, symbol, color or a combination used to identify products and distinguish them from competitor products (McDonald's M) @10 years
Wassenaar Arrangement (WA) – Dual use goods & trade, International cryptographic agreement, prevent destabilizing
Computer Crimes – loss, image, penalties

Regulations

SOX, Sarbanes Oxley, 2002 after ENRON and World Online debacle Independent review by external accountants.
Section 302: CEO's CFO's can be sent to jail when information they sign is incorrect. CEO SIGN
Section 404 is the about internal controls assessment: describing logical controls over accounting files; good auditing and information security.

Corporate Officer Liability (SOX)

- Executives are now held liable if the organization they represent is not compliant with the law.

Negligence occurs if there is a failure to implement recommended precautions, if there is no contingency/disaster recovery plan, failure to conduct appropriate background checks, failure to institute appropriate information security measures, failure to follow policy or local laws and regulations.
COSO – framework to work with Sarbanes-Oxley 404 compliance
European laws: TREADWAY COMMISSION
Need for information security to protect the individual.
Privacy is the keyword here! Only use information of individuals for what it was gathered for
(remember ITSEC, the European version of TCSEC that came from the USA/Orange Book, come together in Common Criteria, but there still is some overlap)

- strong in anti-spam and legitimate marketing
- Directs public directories to be subjected to tight controls
- Takes an OPT-IN approach to unsolicited commercial electronic communications
- User may refuse cookies to be stored and user must be provided with information
- Member states in the EU can make own laws e.g. retention of data

COBIT – examines the effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability of high level control objectives. Having controls, GRC heavy auditing, metrics, regulated industry

Data Breaches (27)

Incident – an event that has potential to do harm
Breach – incident that results in disclosure or potential disclosure of data
Data Disclosure – unauthorized acquisition of personal information
Event – Threat events are accidental and intentional exploitations of vulnerabilities.

Laws (28)

ITAR, 1976. Defense goods, arms export control act
FERPA – Education
GLBA, Graham, Leach, Bliley; credit related PII (21)
ECS, Electronic Communication Service (Europe); notice of breaches
Fourth Amendment - basis for privacy rights is the Fourth Amendment to the Constitution.
1974 US Privacy Act - Protection of PII on federal databases
1980 Organization for Economic Cooperation and Development (OECD) - Provides for data collection, specifications, safeguards
1986 (amended in 1996) US Computer Fraud and Abuse Act - Trafficking in computer passwords or information that causes a loss of $1,000 or more or could impair medical treatment.
1986 Electronic Communications Privacy Act - Prohibits eavesdropping or interception w/o distinguishing private/public
Communications Assistance for Law Enforcement Act (CALEA) of 1994 - amended the Electronic Communications Privacy Act of 1986. CALEA requires all communications carriers to make wiretaps possible for law enforcement with an appropriate court order, regardless of the technology in use.
1987 US Computer Security Act - Security training, develop a security plan, and identify sensitive systems on govt. agencies.
1991 US Federal Sentencing Guidelines - Responsibility on senior management with fines up to $290 million. Invoke prudent man rule. Address both individuals and organizations
1996 US Economic and Protection of Propriety Information Act - industrial and corporate espionage
1996 Health Insurance and Portability Accountability Act (HIPPA) – amended
1996 US National Information Infrastructure Protection Act - Encourage other countries to adopt similar framework.
Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) - Congress amended HIPAA by passing this Act. This law updated many of HIPAA's privacy and security requirements. One of the changes is a change in the way the law treats business associates (BAs), organizations who handle PHI on behalf of a HIPAA covered entity. Any relationship between a covered entity and a BA must be governed by a written contract known as a business associate agreement (BAA). Under the new regulation, BAs are directly subject to HIPAA and HIPAA enforcement actions in the same manner as a covered entity. HITECH also introduced new data breach notification requirements

Domain 1 – Security and Risk Management

.Ethics (33)

Just because something is legal doesn't make it right.
Within the ISC context: Protecting information through CIA

ISC2 Code of Ethics Canons

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

Internet Advisory Board (IAB)

Ethics and Internet (RFC 1087)

Don't compromise the privacy of users. Access to and use of Internet is a privilege and should be treated as such
It is defined as unacceptable and unethical if you, for example, gain unauthorized access to resources on the internet, destroy integrity, waste resources or compromise privacy.

Business Continuity plans development (38)

- Defining the continuity strategy
- Computing strategy to preserve the elements of HW/SW/ communication lines/data/application
- Facilities: use of main buildings or any remote facilities

People: operators, management, technical support persons
Supplies and equipment: paper, forms HVAC
Documenting the continuity strategy

BIA (39)

Goal: to create a document to be used to help understand what impact a disruptive event would have on the business

Gathering assessment material

- Org charts to determine functional relationships
- Examine business success factors

Vulnerability assessment

- Identify Critical IT resources out of critical processes, Identify disruption impacts and Maximum, Tolerable Downtime (MTD)
- Loss Quantitative (revenue, expenses for repair) or Qualitative (competitive edge, public embarrassment). Presented as low, high, medium.
- Develop recovery procedures

Analyze the compiled information

- Document the process Identify inter-dependability
- Determine acceptable interruption periods

Documentation and Recommendation

RTO<MTD

Administrative Management Controls (47)

Separation of duties - assigns parts of tasks to different individuals thus no single person has total control of the system's security mechanisms; prevent collusion
M of N Control - requires that a minimum number of agents (M) out of the total number of agents (N) work together to perform high-security tasks. So, implementing three of eight controls would require three people out of the eight with the assigned work task of key escrow recovery agent to work together to pull a single key out of the key escrow database
Least privilege - a system's user should have the lowest level of rights and privileges necessary to perform their work and should only have them for the shortest time. Three types:
Read only, Read/write and Access/change
Two-man control - two persons review and approve the work of each other, for very sensitive operations
Dual control -two persons are needed to complete a task
Rotation of duties - limiting the amount of time a person is assigned to perform a security related task before being moved to different task to prevent fraud; reduce collusion
Mandatory vacations - prevent fraud and allowing investigations, one week minimum; kill processes
Need to know - the subject is given only the amount of information required to perform an assigned task, business justification
Agreements – NDA, no compete, acceptable use

Employment (48)

- staff members pose more threat than external actors, loss of money stolen equipment, loss of time work hours, loss of reputation declining trusts and loss of resources, bandwidth theft, due diligence

Voluntary & involuntary ----------Exit interview!!!

Third Party Controls (49)

- Vendors
- Consultants
- Contractors

Properly supervised, rights based on policy

Risk Management Concepts (52)

Threat – damage
Vulnerability – weakness to threat vector (never does anything)
Likelihood – chance it will happen
Impact – overall effects
Residual Risk – amount left over
Organizations own the risk
Risk is determined as a byproduct of likelihood and impact

ITIL (55)

ITIL – best practices for IT core operational processes, not for audit

- Service
- Change
- Release
- Configuration

Strong end to end customer focus/expertise
About services and service strategy

Risk Management (52)

GOAL - Determine impact of the threat and risk of threat occurring
The primary goal of risk management is to reduce risk to an acceptable level.
Step 1 – Prepare for Assessment (purpose, scope, etc.)
Step 2 – Conduct Assessment

- ID threat sources and events
- ID vulnerabilities and predisposing conditions
- Determine likelihood of occurrence
- Determine magnitude of impact
- Determine risk

Step 3 – Communicate Risk/results
Step 4 – Maintain Assessment/regularly

Types of Risk

Inherent chance of making an error with no controls in place
Control chance that controls in place will prevent, detect or control errors
Detection chance that auditors won't find an error
Residual risk remaining after control in place
Business concerns about effects of unforeseen circumstances
Overall combination of all risks aka Audit risk **Preliminary Security Examination (PSE):** Helps to gather the elements that you will need when the actual Risk Analysis takes place.
ANALYSIS Steps: Identify assets, identify threats, and calculate risk.
ISO 27005 – deals with risk

Risk Assessment Steps (60)

Four major steps in Risk assessment?
Prepare, Perform, Communicate, Maintain

Qualitative (57)

Approval –
Form Team –
Analyze Data –
Calculate Risk –
Countermeasure Recommendations -

REMEMBER HYBRID!

Domain 1 – Security and Risk Management

Quantitative Risk Analysis (58)

- Quantitative VALUES!!
- SLE (single Loss Expectancy) = Asset Value * Exposure factor (% loss of asset)
- ALE (Annual loss expectancy) = SLE * ARO (Annualized Rate of occurrence)

Accept, mitigate(reduce by implementing controls calculate costs-), Assign (insure the risk to transfer it), Avoid (stop business activity)
Loss= probability * cost
Residual risk - where cost of applying extra countermeasures is more than the estimated loss resulting from a threat or vulnerability (C > L). Legally the remaining residual risk is not counted when deciding whether a company is liable.
Controls gap - is the amount of risk that is reduced by implementing safeguards. A formula for residual risk is as follows: total risk – controls gap = residual risk
RTO – how quickly you need to have that application's information available after downtime has occurred
RPO -Recovery Point Objective: Point in time that application data must be recovered to resume business functions; AMOUNT OF DATA YOUR WILLING TO LOSE
MTD -Maximum Tolerable Downtime: Maximum delay a business can be down and still remain viable

MTD minutes to hours: critical
MTD 24 hours: urgent
MTD 72 hours: important
MTD 7 days: normal
MTD 30 days non-essential

PLAN
Accept
Build Risk Team
Review
Once in 100 years = ARO of 0.01
SLE is the dollar value lost when an asset is successfully attacked
Exposure Factor ranges from 0 to 1
NO – ALE is the annual % of the asset lost when attacked – NOT

Determination of Impact (61)

Life, dollars, prestige, market share

Risk Response (61)

Risk Avoidance – discontinue activity because you don't want to accept risk
Risk Transfer – passing on the risk to another entity
Risk Mitigation – elimination or decrease in level of risk
Risk Acceptance – live with it and pay the cost
Background checks – mitigation, acceptance, avoidance

Risk Framework Countermeasures (63)

- Accountability
- Auditability
- Source trusted and known
- Cost-effectiveness
- Security
- Protection for CIA of assets
- Other issues created?

If it leaves residual data from its function

Controls (68)

Primary Controls (Types) – (control cost should be less than the value of the asset being protected)
Administrative/Managerial Policy

- Preventive: hiring policies, screening security awareness (also called soft-measures!)
- Detective: screening behavior, job rotation, review of audit records

Technical (aka Logical)

- Preventive: protocols, encryption, biometrics smartcards, routers, firewalls
- Detective: IDS and automatic generated violation reports, audit logs, CCTV(never preventative)
- Preventive: fences, guards, locks
- Detective: motion detectors, thermal detectors video cameras

Physical (Domain 5) – see and touch

- Fences, door, lock, windows etc.

Prime objective - is to reduce the effects of security threats and vulnerabilities to a tolerable level
Risk analysis - process that analyses threat scenarios and produces a representation of the estimated Potential loss
Main Categories of Access Control (67)

- Directive: specify rules of behavior
- **Deterrent**: discourage people, change my mind
- Preventative: prevent incident or breach
- Compensating: sub for loss of primary controls
- Detective: signal warning, investigate
- Corrective: mitigate damage, **restore control**
- Recovery: restore to normal after incident

Control	Accuracy	Security	Consistency
Preventive	Data checks, validity checks	Labels, traffic padding, encryption	DBMS, data dictionary
Detective	Cyclic Redundancy	IDS, audit trails	Comparison tools
Corrective	Checkpoint, backups	Emergency response	Database controls

Functional order in which controls should be used. Deterrence, Denial, Detection, Delay

Penetration Testing (77)

Testing a networks defenses by using the same techniques as external intruders
Scanning and Probing – port scanners

- Demon Dialing – war dialing for modems
- Sniffing – capture data packets
- Dumpster Diving – searching paper disposal areas
- Social Engineering – most common, get information by asking

Penetration testing
Blue team - had knowledge of the organization, can be done frequent and least expensive
Red team - is external and stealthy
White box - ethical hacker knows what to look for, see code as a developer
Grey Box - partial knowledge of the system, see code, act as a user
Black box - ethical hacker not knowing what to find

4 stages: **planning, discovery, attack, reporting**
vulnerabilities exploited: kernel flaws, buffer overflows, symbolic links, file descriptor attacks
other model: footprint network (information gathering) port scans, vulnerability mapping, exploitation, report scanning
tools are used in penetration tests
flaw hypotheses methodology = operation system penetration testing

Egregious hole – tell them now!

Strategies - External, internal, blind, double-blind

Categories – zero, partial, full knowledge tests

Pen Test Methodology (79)

Recon/discover -
Enumeration -
vulnerability analysis -
execution/exploitation -
document findings/reporting - SPELL OUT AND DEFINE!!!!

Control Assessment 76
Look at your posture

Deming Cycle (83)

Plan – ID opportunity & plan for change
Do – implement change on small scale
Check – use data to analyze results of change
Act – if change successful, implement wider scale, if fails begin cycle again

Domain 1 – Security and Risk Management

Identification of Threat (86)

Individuals must be qualified with the appropriate level of training.

- Develop job descriptions
- Contact references
- Screen/investigate background
- Develop confidentiality agreements
- Determine policy on vendor, contractor, consultant, and temporary staff access

DUE DILIGENCE

Software Licenses (91)

Public domain - available for anyone to use

Open source - source code made available with a license in which the copyright holder provides the rights to study, change, and distribute the software to anyone

Freeware - proprietary software that is available for use at no monetary cost. May be used without payment but may usually not be modified, re-distributed or reverse-engineered without the author's permission

Assurance (92)

Degree of confidence in satisfaction of security requirements
Assurance = other word for security
THINK OUTSIDE AUDIT

Successful Requirements Gathering 92

Don't assume what client wants
Involve users early
Define and agree on scope
MORE

Security Awareness (96)

Technical training to react to situations, best practices for Security and network personnel; Employees, need to understand policies then use presentations and posters etc. to get them aware

Formal security awareness training – exact prep on how to do things

Terms

Wire Tapping eavesdropping on communication -only legal with prior consent or warrant
Data Diddling act of modifying information, programs, or documents to commit fraud, tampers with INPUT data
Privacy Laws data collected must be collected fairly and lawfully and used only for the purpose it was collected.
Water holing – create a bunch of websites with similar names
Work Function (factor): the difficulty of obtaining the clear text from the cipher text as measured by cost/time
Fair Cryptosystems - In this escrow approach, the secret keys used in a communication are divided into two or more pieces, each of which is given to an independent third party. When the government obtains legal authority to access a particular key, it provides evidence of the court order to each of the third parties and then reassembles the secret key.
SLA – agreement between IT service provider and customer, document service levels, divorce; how to dissolve relationship
SLR (requirements) – requirements for a service from client viewpoint
Service level report – insight into a service providers ability to deliver the agreed upon service quality

Legislative drivers?

FISMA(federal agencies)
Phase 1 categorizing, selecting minimum controls, assessment
Phase 2: create national network of secures services to assess

Domain 2- Asset Security

Information classification (110)

Categorization – Process of determining the impact of loss of CIA of information to an organization. Identifies the value of the data to the organization. Not all data has same value, demonstrates business commitment to security, Identify which information is most sensitive and vital

Criteria - Value, age, useful life, personal association

Levels

Government, military
- Unclassified (have FOUO also)
- Sensitive but unclassified
- Confidential (some damage)
- Secret (Serious damage) (Can have Country specific restrictions also – NZAUS SECRET for New Zealand, Australia and US secret)
- Top Secret (Grave damage)

Private sector (113)
- Public; used by public or employees
- Company Confidential; viewed by all employees but not for general use
- Company Restricted – restricted to a subset of employees
- Private; Ex. SSN, credit card info., could cause damage
- Confidential; cause exceptionally grave damage, Proprietary; trade secrets
- Sensitive; internal business

TS = Confidential/Prop, Secret = Private, Confidential = sensitive

Security policies, standards & guidelines (119)

Policies first and highest level of documentation

Very first is called Senior management Statement of Policy, Stating importance, support and commitment

Types
- Regulatory (required due to laws, regulations, compliance and specific industry standards!)
- Advisory (not mandatory but strongly suggested
- Informative to inform the reader

Information policy - classifications and defines level of access and method to store and transmit information

Security policies - authenticates and defines technology used to control information access and distribution

SYSTEM security policy - lists hardware / software to be used and steps to undertake to protect infrastructure

Standards - Specify use of specific technologies in a uniform way

Guidelines - same as standards but not forced to follow

Procedures - detailed steps to perform a task

Baseline - minimum level of security

Security planning - involves security scope, providing security management responsibilities and testing security measures for effectiveness. Strategic 5 years Tactical shorter than strategic Operational day to day, short term

Data Classification Policy (111)

- Who will have access to data?
- How is the data to be secured?
- How long is data to be retained?
- What method(s) should be used to dispose of data?
- Does data need to be encrypted?
- What is the appropriate use of the data?

Proper Assess Man REQUIRES (113)

1. Inventory Management – all things

2. Configuration Management - +patching

IT Asset Management (ITAM) (114)

Full life cycle management of IT assets
- CMBD; holds relationships between system components – incidents, problems, known error, changes, and releases
- Single repository
- Organizationally aligned -scalable

US-EU (Swiss) Safe Harbor (124)

The EU Data Protection Directive To be replaced, in 2018, by the General Data Protection Regulation (GDPR)

Bridge differences in approach and provide a streamlined means for U.S. organizations to comply with European Commissions.

STRENGTHING INDIVIDUALS RIGHTS
- Data obtained fairly and lawfully
- Data only used for original purpose
- Adequate, relevant, and not excessive to purpose
- Accurate and up to date
- Accessible to the subject
- Kept secure
- Destroyed after purpose is complete

Directive on Data Protection; Seven Tenets
- Notice; data subjects should be given notice when their data is being collected
- Choice; data should not be disclosed without the data subject's consent
- Onward Transfer; data subjects should be informed as to who is collecting their data
- Security; collected data should be kept secure from any potential abuses
- Data Integrity; reliable, only stated purpose
- Access; data subjects should be allowed to access their data and make corrections to any inaccurate data
- Enforcement; accountability, data subjects should have a method available to them to hold data collectors accountable for not following the above principles

NOT REASON or RETENTION TIME

US Org is Data Processors when they classify and handle data, EU company would be Business/Mission owners, US org. would also be Data Administrators

Data processors have responsibility to protect privacy of data

Dpt. of Commerce holds list of participants

Can transfer to non-Safe Harbor entities with permission

FTC – overseas compliance framework for organizations wishing to use personal data of EU citizens

Self-certify but Dpt. Of Transportation or FTC can enforce

Gramm/Leach/Bailey Act delaying application to financial markets

Roles and responsibilities

Senior Manager ultimate responsibility

Information security Officer functional responsibility
- Ensure policies etc. are written by app. Unit
- Implement/operate CIRTs
- Provide leadership for security awareness
- Communicate risk to senior management
- Stay abreast of current threats and technology

Security Analyst Strategic, develops policies and guidelines

Data Ownership (128)

Data Life - Creation, use, destruction(**subservient to security policy**)

Data/Information Owner
- Ultimate organizational responsibility for data
- Categorize systems and data, determine level of classification
- Required controls are selected for each classification
- Select baseline security standards
- Determine impact information has on organization
- Understand replacement cost (if replaceable)
- Determine who needs the information and circumstances for release
- Determine when information should be destroyed
- Responsible for asset
- Review and change classification
- Can delegate responsibility to data custodian
- Authorize user privileges

Data Custodian Responsibilities (129)

- Day-to-day tasks, grants permission to users in DAC
- Adhere to data policy and data ownership guidelines
- Ensure accessibility, maintain and monitor security
- Dataset maintenance, , archiving
- Documentation, including updating
- QA, validation and audits
- Run regular backups/restores and validity of them
- Insuring data integrity and security (CIA)
- Maintaining records in accordance to classification
- Applies user authorization
- Implement security controls

System Owners - Select security controls

Administrators
- Assign permission to access and handle data

End-user
- Uses information as their job
- Follow instructions in policies and guidelines
- Due care (prevent open view by e.g. Clean desk)
- Use corporation resources for corporation use

Auditor examines security controls

QC & QA (131)

QC – assessment of quality based on internal standards

QA – assessment of quality based on standards external to the process and involves reviewing of the activities and quality control processes.

Domain 2- Asset Security

Benefits of Data Standards (134)

Increased data sharing

Considerations (134)

Borders
Encryption

Data Modeling (135)

Smallest bits of information the Db will hold – granularity
When do we replace – then think about next one
CRITICAL = AVAILABILITY

Data Remanence (140)

Residual physical representation of data that has been in some way erased. **PaaS deals with it best in Cloud**
Remanence - Residual data left on media after erase attempts
Remove unwanted remnant data from magnetic tapes

- Physical destruction
- Degaussing
- Overwriting
- NOT Reformatting

Sanitizing – Series of processes that removes data, ensures data is unrecoverable by any means. Removing a computer from service and disposed of. All storage media removed or destroyed.
Degaussing – AC erasure; alternating magnetic fields , DC erasure; unidirectional magnetic field or permanent magnet, can erase tapes
Erasing – deletion of files or media, removes link to file, least effective
Overwriting/wiping/shredding – overwrites with pattern, may miss
Zero fill – wipe a drive and fill with zeros
Clearing – Prepping media for reuse at same level. Removal of sensitive data from storage devices in such a way that the data may not be reconstructed using normal system functions or utilities. May be recoverable with special lab equipment. Data just overwritten.
Purging– More intense than clearing. Media can be reused in lower systems. Removal of sensitive data with the intent that the data cannot be reconstructed by any known technique.
Destruction – Incineration, crushing, shredding, and disintegration are stages of this
Encrypt data is a good way to secure files sent through the internet
SSD Data Destruction (142)

- NIST says to "disintegrate"
- SSD drives cannot be degaussed, space sectors, bad sectors, and wear space/leveling may hide nonaddressable data, encrypt is the solution
- Erase encryption key to be unreadable
- Crypto erase, sanitization, targeted overwrite (best)

Buy high quality media – value of data exceeds cost of media
Sanitation is business normal, not destruction for costs reasons
Reuse - Downgrading equipment for reuse will probably be more expensive than buying new
Metadata – helps to label data and prevent loss before it leaves the organization,
Data mart - metadata is stored in a more secure container

Baselines (154)

Select based on the data classification of the data stored/handled

- Which parts of enterprise can be protected by the same baseline?
- Should baseline be applied throughout whole enterprise?
- At what security level should baseline aim?

How will the controls be determined?
Baseline – Starting point that can be tailored to an organization for a minimum security standard. Common security configurations, Use Group Policies to check and enforce compliance

Scoping and Tailoring (157)

Narrows the focus and of the architecture to ensure that appropriate risks are identified and addressed.
Scoping – reviewing baseline security controls and selecting only those controls that apply to the IT system you're trying to protect.
Tailoring – modifying the list of security controls within a baseline so that they align with the mission of the organization.
Supplementation – adding assessment procedures or assessment details to adequately meet the risk management needs of the organization.

Link vs. End to End Encryption (174)

Link - is usually point to point EVERYTHING ENCRYPTED
"Black pipe, black oil, black ping pong balls" all data is encrypted, normally did by service providers
End to End – You can see ALL BUT PAYLOAD, normally done by users
YOU CAN LAYER THESE ENCRYPTION TYPES
Email is not secured unless encrypted
NETSCAPE INVENTED SSL, SSLv3 still used
USE TLSv1.2 now for test
PGP = GnuPG (GNP)– not rely on open
S/MIME – secure email

Nice to Know

Classifying Costs – cost are not a factor in classifying data but are in controls
FTP and Telnet are unencrypted! SFTP and SSH provide encryption to protect data and credentials that are used to log in
Record Retention Policies – how long data retained and maintained
Removable Media – use strong encryption, like AES256, to ensure loss of media does not result in data breach
Personnel Retention – Deals with the knowledge that employees gain while employed.
Record Retention – retaining and maintaining information for as long as it's needed
Label Data – to make sure data is identifiable by its classification level. Some label all media that contains data to prevent reuse of Public media for sensitive data.
Data in RAM is Data in use.
CIS – Center for Internet Security; creates list of security controls for OS, mobile, server, and network devices

Standards Selection (158 - 185)

NIST – National Institute of Standards and Technology
NIST SP 800 series - address computer security in a variety of areas
800-14 NIST SP – GAPP for securing information technology systems
800-18 NIST – How to develop security plans
800-27 NIST SP - Baseline for achieving security, five lifecycle planning phases (defined in 800-14), 33 IT security principles

- Initiation
- Development/Acquisition
- Implementation
- Operation/Maintenance
- Disposal

800-88 - NIST guidelines for sanitation and disposition, prevents data remanence
800-122 - NIST Special Publication – defines PII as any information that can be used to trace a person identity such as SSN, name, DOB, place of birth, mother's maiden name
800-137 - build/implement info security continuous monitoring program: define, establish, implement, analyze and report,
800-145 - cloud computing
FIPS – Federal Information Processing Standards; official series of publications relating to standards and guidelines adopted under the FISMA, Federal Information Security Management Act of 2002.
FIPS 199 – Standards for categorizing information and information systems.
FIPS 200 – minimum security requirements for Federal information and information systems
DOD 8510.01 – establishes DIACAP
ISO 15288 – International systems engineering standard covering processes and life cycle stages

- Agreement
- Organization Project-enabling
- Technical Management
- Technical

Nice to Know

COPPA – California Online Privacy Protection Act, operators of commercial websites post a privacy policy if collecting personal information on CA residents
Curie Temperature – Critical point where a material's intrinsic magnetic alignment changes direction.
Dar – Data at rest; inactive data that is physically stored, not RAM, biggest threat is a data breach, full disk encryption protects it (Microsoft Bitlocker and Microsoft EFS, which use AES, are apps)
DLP – Data Loss/Leakage Prevention, use labels to determine the appropriate control to apply to data. Won't modify labels in real-time.
ECM – Enterprise Content Management; centrally managed and controlled
Non-disclosure Agreement – legal agreement that prevents employees from sharing proprietary information
PCI-DSS – Payment and Card Industry – Security Standards Council; credit cards, provides a set of security controls /standards
Watermark – embedded data to help ID owner of a file, digitally label data and can be used to indicate ownership.

Domain 3 – Security Engineering

Systems Engineering & Modeling (194)

Common Criteria ISO 15408 - Structured methodology for documenting security requirements, documenting and validating ****

A SECURITY PRODUCT MAY BE CERTIFIED

Defines a **protection profile** that specifies the security requirements and protections of a product that is to be evaluated. Organized around TCB entities. Evaluation Assurance Levels (EAL)

- EAL0 –Inadequate assurance
- EAL1 –Functionally tested
- EAL2 –Structurally tested
- EAL3 –Methodically tested and checked
- EAL4 –Methodically designed, tested and reviewed
- EAL5 –Semi formally designed and tested
- EAL6 –Semi formally verified design and tested
- EAL7 –Formally verified design and tested

Target of Evaluation (TOE): the product

Protection Profile (PP): set of security requirements for a category of products that meet specific consumer security needs

Security Target (ST): identifies the security properties of TOE

Security Functional Requirements (SFRs): Specific individual security functions

Engineering Principles for IT Security (194)

NIST SP 800-27

- Initiation; need expressed, purpose documented, impact assessment
- Development/Acquisition; system designed, purchased, programmed, developed or constructed.
- Implementation; system tested and installed, certification and accreditation
- Operation/Maintenance; performs function, security operations, audits

Disposal; disposition of information, HW and SW

Physical controls are your first line of defense, and people are your last.

ISO/IEC 21827:2008 SSE-CMM (Maturity Model) (196)

BIGGEST JUMP IN MATURITY MODEL? 2 – 3. FROM REACTIVE TO PROACTIVE

OS Kernel ()

Loads & runs binary programs, schedules task swapping, allocates memory & tracks physical location of files on computers hard disk, manages IO/OP requests from software, & translates them into instructions for CPU

Common System Components (198)

Primary Storage – is a temporary storage area for data entering and leaving the CPU

Random Access Memory (RAM) – is a temporary holding place for data used by the operating systems. It is volatile; meaning if it is turned off the data will be lost. Two types of RAM are dynamic and static. Dynamic RAM needs to be refreshed from time to time or the data will be lost. Static RAM does not need to be refreshed.

Read-Only Memory (ROM) – is non-volatile, which means when a computer is turned off the data is not lost; for the most part ROM cannot be altered. ROM is sometimes referred to as firmware. Erasable and Programmable Read-Only Memory (EPROM) is non-volatile like ROM, however EPROM can be altered.

Process states:

- Stopped; process finishes or must be terminated
- Waiting; the process is ready for continued execution but is waiting for a device or access request
- Running; executes on the CPU and keeps going until it finishes, its time slice expires, or it is blocked
- Ready; process prepared to execute when CPU ready

Multitasking – execute more than one task at the same time

Multiprocessing – more than one CPU is involved.

Multi-Threading: execute different parts of a program simultaneously

Single state machine – operates in the security environment at the highest level of classification of the information within the computer. In other words, all users on that system must have clearance to access the info on that system.

Multi-state machine – can offer several security levels without risk of compromising the system's integrity.

CICS – complex instructions. Many operations per instruction. Less number of fetches

RISC – reduced instructions. Simpler operations per instruction. More fetches.

Software

1 GL: machine language (used directly by a computer)
2GL: assembler
3GL: FORTRAN. Basic pl/1 and C++
4GL: Natural / focus and SQL
5GL: Prolog, lisp artificial intelligence languages based on logic

Memory Protection (200)

Segmentation – dividing a computer's memory into segments.

Protection Keying – Numerical values, Divides physical memory up into particular sized blocks, each of which has an associated numerical value called a protection key.

Paging – divides memory address space into even size blocks called pages. To emulate that we have more RAM than we have. SYSTEM KERNAL KNOWS THE LOCATION OF THE PAGE FILE

DEP, Data Execution Prevention – a system-level memory protection feature that is built into the OS DEP prevents code from being run from data pages such as the default heap, stacks, and memory pools.

ITIL (208)

The ITIL Core includes five publications addressing the overall life cycle of systems. ITIL as a whole identifies best practices that an organization can adopt to increase overall availability, and the Service Transition publication addresses configuration management and change management processes.

- Service Strategy
- Service Design
- Service Transition
- Service Operations
- Continuous Service Improvement

Types of Security Models (210)

Defining allowed interactions between subjects (active parties) and objects (passive parties) at a particular moment in time.

State Machine Model – describes a system that is always secure no matter what state it is in. If all aspects of a state meet the requirements of the security policy, that state is considered secure. A transition occurs when accepting input or producing output. A transition always results in a new state (also called a state transition). A secure state machine model system always boots into a secure state, maintains a secure state across all transitions, and allows subjects to access resources only in a secure manner compliant with the security policy.

Information Flow Model – focuses on the flow of information. Information flow models are based on a state machine model. The Bell-LaPadula and Biba models are both information flow models. Information flow models don't necessarily deal with only the direction of information flow; they can also address the type of flow. Information flow models are designed to prevent unauthorized, insecure, or restricted information flow, often between different levels of security (these are often referred to as multilevel models). The information flow model also addresses covert channels by specifically excluding all non-defined flow pathways.

Noninterference Model – is loosely based on the information flow model. However, instead of being concerned about the flow of information, the noninterference model is concerned with how the actions of a subject at a higher security level affect the system state or the actions of a subject at a lower security level. Basically, the actions of subject A (high) should not affect the actions of subject B (low) or even be noticed by subject B. The noninterference model can be imposed to provide a form of protection against damage caused by malicious programs such as Trojan horses. **Southerland Model**

Techniques for Ensuring CIA

Confinement – to restrict the actions of a program. Simply put, process confinement allows a process to read from and write to only certain memory locations and resources. This is also known as sandboxing.

Bounds – a process consist of limits set on the memory addresses and resources it can access. The bounds state the area within which a process is confined or contained.

Isolation – When a process is confined through enforcing access bounds that process runs in isolation. Process isolation ensures that any behavior will affect only the memory and resources associated with the isolated process.

Domain 3 – Security Engineering

Models (211)

MATRIX

- Provides access rights to subjects for objects
- Access rights are read, write and execute
- Columns are ACL's
- Rows are capability lists
- Supports discretionary access control

BELL-LAPADULA = MAC SUBJECTS/OBJECTS/CLEARANCES/

- Confidentiality model
- developed by DOD, thus classification
- Cannot read up (**simple** e=**read** security rule)
- Cannot **write** down (***** property rule AKA CONFINEMENT PROPERTY). Exception is a trusted subject.
- Uses access matrix to specify discretionary access control
- Use need to know principle
- **Strong star** rule: read and write capabilities at the same level
- First mathematical model defined
- **tranquility** principle in Bell-LaPadula prevents security level of subjects from being changed once they are created
- Bell-LaPadula is concerned with preventing information flow from a high security level to a low security level.

BIBA – MAC "if I in it INTEGRITY MODEL"

- Integrity model
- Cannot read down (**simple** e=**read** integrity rule)
- Simple integrity property
- cannot **write** up (***** integrity)
- lattice based (least upper bound, greatest lower bound, flow policy)
- subject at one level of integrity cant invoke subject at a higher level of integrity
- Biba is concerned with preventing information flow from a low security level to a high security level.
- Focus on protecting objects from external threat

CLARK WILSON

- integrity model
- Cannot be tampered, logged, and consistency
- Enforces segregation of duty
- Requires auditing
- Commercial use
- Works with SCI Constrained Data items, data item whose integrity is to be preserved
- Access to objects only through programs
- An integrity verification procedure (IVP) is a procedure that scans data items and confirms their integrity.

Information flow model

- Each object is assigned a security class and value, and information is constrained to flow in the directions that are permitted by the security policy. Thus flow of information from one security level to another. (Bell & Biba)

Brewer and Nash

- The Chinese Wall model provides a dynamic access control depending on user's previous actions. This model **prevents conflict of interests** from members of the same organization to look at information that creates a conflict of another member of that organization.

Lipner Model – Confidentiality and Integrity, BLP + Biba
1st Commercial Model

Models (211) (cont)

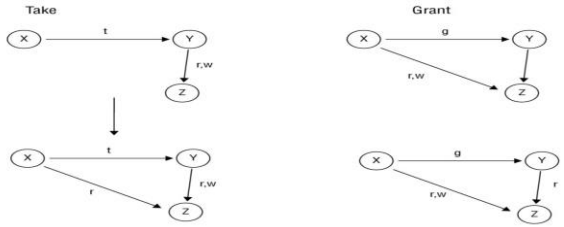
Graham-Denning

- focused on relationship between subjects and objects

TAKE-GRANT

- uses a direct graph to specify the rights that subjects can transfer to objects or that subjects can take from other subjects
- Uses STATES and STATE TRANSTIONS

Take rule	Allows a subject to take rights over an object
Grant rule	Allows a subject to grant rights to an object
Create rule	Allows a subject to create new rights
Remove rule	Allows a subject to remove rights it has



Composition Theories

Some other models that fall into the information flow category build on the notion of how inputs and outputs between multiple systems relate to one another— which follows how information flows between systems rather than within an individual system. These are called composition theories because they explain how outputs from one system relate to inputs to another system.
There are three recognized types of composition theories:

- Cascading: Input for one system comes from the output of another system.
- Feedback: One system provides input to another system, which reciprocates by reversing those roles (so that system A first provides input for system B and then system B provides input to system A).
- Hookup: One system sends input to another system but also sends input to external entities.

MAC – Subjects are labelled as to their level of clearance. Objects are labelled as to their level of classification or sensitivity.
Subjects – Users(perform work task), Data Owners(protect data), and Data Custodians (classify and protect data)

ITSEC (216)

- refers to any system being evaluated as a target of evaluation (TOE).
- does not rely on the notion of a TCB, and it doesn't require that a system's security components be isolated within a TCB.
- includes coverage for maintaining targets of evaluation after changes occur without requiring a new formal evaluation.

Certification and Accreditation (216)

Certification – is evaluation of security features and safeguards if it meets requirements. Certification is the comprehensive evaluation of the technical and nontechnical security features of an IT system and other safeguards made in support of the accreditation process to establish the extent to which a particular design and implementation meets a set of specified security requirements.
Accreditation – the formal declaration by the designated approving authority (DAA) that an IT system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. Once accreditation is performed, management can formally accept the adequacy of the overall security performance of an evaluated system.
System accreditation – a major application or general support system is evaluated.
Site accreditation – the applications and systems at a specific, self-contained location are evaluated.
Type accreditation – an application or system that is distributed to a number of different locations is evaluated.

Product Evaluation Models (216)

Trusted Computer System Evaluation Criteria
TCSEC: (Orange book) From the U.S. DoD, it evaluates operating systems, application and systems. It doesn't touch the network part. It only addresses confidentiality!

ITSEC	TCSEC	Explanation
1	D	minimal protection, any systems that fails higher levels
2	C1	DAC; (identification, authentication, resource protection).
3	C2	DAC; Controlled access protection (object reuse, protect audit trail).
4	B1	MAC; (security labels) based on Bell LaPadula security model. Labeled security (process isolation, devices
5	B2	MAC; Structured protection (trusted path, covert channel analysis). Separate operator/admin roles. Configuration management
6	B3	MAC; security domain (trusted recovery, Monitor event and notification).
7	A	MAC; Formal, verified protection

Operational assurance requirements for TCSEC are:

- System Architecture
- System Integrity
- Covert Channel analysis
- Trusted Facility Management
- Trusted recovery

Rainbow series:
Red = trusted network, Orange = TCSEC evaluation
Brown = trusted facilities management
dcsmmmTan = audit, Aqua = glossary.
Green = password management
Information Technology Security Evaluation Criteria
ITSEC: it is used in Europe only, not USA. Addresses CIA. Unlike TCSEC it evaluates functionality and assurance separately. Assurance from E0 to E6 (highest) and F1 to F10 (highest). Therefore a system can provide low assurance and high functionality or vice-versa.

Domain 3 – Security Engineering

Security Standards (222)

ISO 27001 – focused on the standardization and certification of an organization's information security management system (ISMS), security governance, a standard; ISMS. Info security minimum systems

ISO 27002 – (inspired from ISO 17799) – a guideline which lists security control objectives and recommends a range of specific security controls; more granular than 27001. 14 areas

BOTH INSPIRED FROM BS7799

Control Frameworks (223)

Consider the overall control framework or structure of the security solution desired by the organization.

COBIT – Control Objectives for Information and Related Technology, is a documented set of best IT security practices crafted by the Information Systems Audit and Control Association (ISACA). It prescribes goals and requirements for security controls and encourages the mapping of IT security ideals to business objectives.

COBIT 5 – is based on five key principles for governance and management of enterprise IT:

- Principle 1: Meeting Stakeholder Needs
- Principle 2: Covering the Enterprise End-to-End
- Principle 3: Applying a Single, Integrated Framework
- Principle 4: Enabling a Holistic Approach
- Principle 5: Separating Governance from Management. COBIT is used not only to plan the IT security of an organization but also as a guideline for auditors.

Virtualization (229)

Used to host one or more operating systems within the memory of a single host computer. Such an OS is also known as a guest operating system. From the perspective that there is an original or host OS installed directly on the computer hardware, the additional Oses hosted by the hypervisor system are guests.

- **Virtual machine** – simulated environment created by the OS to provide a safe and efficient place for programs to execute.
- **Virtual SAN** – software-defined shared storage system is a virtual re-creation of a SAN on top of a virtualized network or an SDN.

Timing (233)

TOCTTOU attack - race condition exploits, and communication disconnects are known as state attacks because they attack timing, data flow control, and transition between one system state to another.

RACE - two or more processes require access to the same resource and must complete their tasks in the proper order for normal functions

Memory Components

Register – CPU also includes a limited amount of onboard memory, known as registers, that provide it with directly accessible memory locations that the brain of the CPU, the arithmetic-logical unit (ALU), uses when performing calculations or processing instructions, small memory locations directly in the CPU.

Stack Memory Segment – used by processors to communicate instructions and data to each other

Monolithic Operating System Architecture – all of the code working in kernel mode/system mode in an ad hoc and non-modularized OS

Memory Addressing – When using memory resources, the processor must have some means of referring to various locations in memory. The solution to this problem is known as addressing,

- **Register Addressing** – When the CPU needs information from one of its registers to complete an operation, it uses a register address (for example, "register 1") to access its contents.
- **Immediate Addressing** – is not a memory addressing scheme per se but rather a way of referring to data that is supplied to the CPU as part of an instruction. For example, the CPU might process the command "Add 2 to the value in register 1." This command uses two addressing schemes. The first is immediate addressing— the CPU is being told to add the value 2 and does not need to retrieve that value from a memory location— it's supplied as part of the command. The second is register addressing; it's instructed to retrieve the value from register 1.
- **Direct Addressing –** In direct addressing, the CPU is provided with an actual address of the memory location to access. The address must be located on the same memory page as the instruction being executed. Direct addressing is more flexible than immediate addressing since the contents of the memory location can be changed more readily than reprogramming the immediate addressing's hard-coded data. Indirect Addressing
- **Indirect addressing –** uses a scheme similar to direct addressing. However, the memory address supplied to the CPU as part of the instruction doesn't contain the actual value that the CPU is to use as an operand. Instead, the memory address contains another memory address (perhaps located on a different page). The CPU reads the indirect address to learn the address where the desired data resides and then retrieves the actual operand from that address.
- **Base + Offset Addressing –** uses a value stored in one of the CPU's registers as the base location from which to begin counting. The CPU then adds the offset supplied with the instruction to that base address and retrieves the operand from that computed memory location.

Cloud Service Models (241)

Original service models – SaaS, PaaS; original deployment model- community & hybrid

PaaS – Platform-as-a-Service is the concept of providing a computing platform and software solution stack as a virtual or cloud-based service. Essentially, this type of cloud solution provides all the aspects of a platform (that is, the operating system and complete solution package). The primary attraction of PaaS is the avoidance of having to purchase and maintain high-end hardware and software locally. Customer supplies application code that the vendor then executes on its own infrastructure

SaaS – Software-as-a-Service, is a derivative of PaaS. SaaS provides on-demand online access to specific software applications or suites without the need for local installation. In many cases, there are few local hardware and OS limitations.

IaaS – Infrastructure-as-a-Service, takes the PaaS model yet another step forward and provides not just on-demand operating solutions but complete outsourcing options. This can include utility or metered computing services, administrative task automation, dynamic scaling, virtualization services, policy implementation and management services, and managed/ filtered Internet connectivity.

Deployment Models, parent organization still responsible for patching OS of virtual hosts,

CaaS – not a TERM!

- Private; cloud-based assets for a single organization. Organizations can create and host private clouds using their own resources.
- Community; provides cloud-based assets to two or more organizations. Maintenance responsibilities are shared based on who is hosting the assets and the service models.
- Public; model includes assets available for any consumers to rent or lease and is hosted by an external CSP. Service level agreements can be effective at ensuring the CSP provides the cloud-based services at a level acceptable to the organization.

Hybrid – mix of public and private

Database Security (237)

Aggregation – SQL provides a number of functions that combine records from one or more tables to produce potentially useful information. Aggregation is not without its security vulnerabilities. Aggregation attacks are used to collect numerous low-level security items and combine them to create something of a higher security level or value.

Inference – involve combining several pieces of non-sensitive information to gain access to information that should be classified at a higher level. However, inference makes use of the human mind's deductive capacity rather than the raw mathematical ability of modern database platforms.

Data Warehousing – large databases, store large amounts of information from a variety of databases for use with specialized analysis techniques.

Data Mining – technique allow analysts to comb through data warehouses and look for potential correlated information.

Data dictionary – commonly used for storing critical information about data, including usage, type, sources, DBMS software reads the data

Domain 3 – Security Engineering

Key Encryption Concepts and Definitions (243)

Purpose: protect transmitted information from being read and understood except by the intended recipient

Substitution – like shifting and rotating alphabets, can be broken by statistical looking at repeating characters or repeats

Vernam – cipher (one time pad): - key of a random set of non-repeating characters

Information Theory – Claude Elmwood Shannon

Transposition – Permutation is used, meaning that letters are scrambled. The key determines positions that the characters are moved to, for example vertical instead of horizontal

Null Cipher – used in cases where the use of encryption is not necessary but yet the fact that no encryption is needed must be configured in order for the system to work. Ex. Testing, stenography

Key Length – use with each algorithm based on the sensitivity of information transmitted, longer key the better!

Key space – is the range of values that are valid for use as a key for a specific algorithm. A key space is defined by its bit size. Bit size is nothing more than the number of binary bits (0s and 1s) in the key. The key space is the range between the key that has all 0s and the key that has all 1s. Key space doubles each time you add a bit to key length, which makes cryptanalysis more difficult.

Key Clustering – when different encryption keys generate the same ciphertext from the same plaintext message BAD

Synchronous – each encryption or decryption request is performed immediately

Asynchronous – encrypt/decrypt request are processed in queues.

Hash Function – one-way mathematical operation that reduces a message or data file into a smaller fixed length output. Encrypted using private key of sender.

Registration Authority – performs certificate registration services on behalf of a CA. RA **verifies user credentials**

Certificate Authority – PKI, entity trusted by one or more users as an authority in a network **that issues, revokes, and manages digital certificates.**

Key Space – represents the total number of possible values of keys in a cryptographic algorithm for the encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance. HOW HARD TO BRUTE FORCE

Transposition/permutation – process of reordering plaintext to hide the message rambo = ombar

SP-network – process described by Claude Shannon used in most block ciphers to increase their strength

Confusion – mixing the key values during repeated rounds of encryption, make the relationship between ciphertext and key as complex as possible

Diffusion – mix location of plaintext throughout ciphertext, change of a single bit should drastically change hash, dissipate pattern

Meet in the Middle – Attackers might use a meet-in-the-middle attack to defeat encryption algorithms that use two rounds of encryption. This attack is the reason that Double DES (2DES) was quickly discarded as a viable enhancement to the DES encryption (it was replaced by Triple DES (3DES, TDES, EEE, EDE).

Key Encryption Concepts and Definitions (cont.)

Block Cipher – segregating plaintext into blocks and applying identical encryption algorithm and key

Cipher – cryptographically transformation that operates on characters or bits. DES, word scramble, shift letters

Cipher text or Cryptogram – unintelligible message, encrypt text

Clustering – situation wherein plain text messages generates identical cipher text messages using the same algorithm but with different crypto-variables or keys

Codes – cryptographic transformation that operates at the level of words or phrases**,** one by land, two by sea

Cryptanalysis – breaking the cipher text,

Cryptographic Algorithm – Step by step procedure to encipher plaintext and decipher cipher text

Cryptography – the art and science of hiding the meaning of communications from unintended recipients. (Greek: kryptos=hidden, graphein=to write)

Cryptology: cryptography + cryptanalysis

Cryptosystem – set of transformations from a message space to cipher space

Decipher – To make the message readable, undo encipherment process

Encipher – make message unintelligible

End-to-end encryption – Encrypted information that is sent from point of origin to destination. In symmetric encryption this means both having the same identical key for the session

Exclusive OR – Boolean operation that performs binary addition

Key or Crypto variable – Information or sequence that controls the enciphering and deciphering of messages

Link encryption – stacked encryption using different keys to encrypt each time

One Time Pad – encipher each character with its own unique key that is used only once, unbreakable supposedly

PGP (GPG) – encrypt attached files

Plaintext – message in clear text readable form

Steganography – secret communications where the existence of a message is hidden (inside images for example)

Dumpster Diving – of going through someone's trash to find useful or confidential info –it is legal but unethical in nature

Phishing – act of sending spoofed messages that pretend to originate from a source the user trusts (like a bank)

Social Engineering – act of tricking someone into giving sensitive or confidential info that may be used against the company

Script kiddie – someone with moderate hacking skills, gets code from the Internet.

Red boxing – pay phones cracking

Black Boxing – manipulates toll-free line voltage to phone for free

Blue Boxing – tone simulation that mimics telephone co. system and allows long distance call authorization

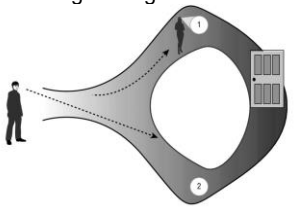
White box – dual tone, multifrequency generator to control phone system

Phreakers – hackers who commit crimes against phone companies

Salami – removal of a small amount of money otherwise known as skimming

Key Encryption Concepts and Definitions (cont.)

Zero-knowledge proof – is a communication concept. A specific type of information is exchanged but no real data is transferred, as with digital signatures and digital certificates. Understand split knowledge. "magic door"



Split knowledge – means that the information or privilege required to perform an operation is divided among multiple users. This ensures that no single person has sufficient privileges to compromise the security of the environment. M of N Control (multiparty key recovery) is an example of split knowledge.

Skipjack – Like many block ciphers, Skipjack operates on 64-bit blocks of text. It uses an 80-bit key and supports the same four modes of operation supported by DES. Skipjack was quickly embraced by the US government and provides the cryptographic routines supporting the Clipper and Capstone encryption chips. However, Skipjack has an added twist— it supports the escrow of encryption keys.

Goals of Cryptography

Confidentiality
Integrity
Proof of origin
Non-repudiation
Protect data at rest
Protect data in transit

Cryptographic Concepts

Key Clustering – when different encryption keys generate the same ciphertext from the same plaintext message

Work Factor – time and effort required to break a protective measure

Kirchhoff's Principle – all but key, secure

Synchronous and self-synchronous

Random Number Generators (RNGs)

Vigenere Cipher – uses key words and numerous rows (traditionally 26), each one of which is offset by one.

Security Monitoring

- Reference Monitor and security kernel are used to determine whether a user should be allowed to access an object
- "complete mediation" means that all subjects must be authenticated and their access rights verified before they can access any object

Domain 3 – Security Engineering

Methods of Cryptography (247)

Stream-based Ciphers – operate on one character or bit of a message (or data stream) at a time. The Caesar cipher is an example of a stream and shift cipher. The one-time pad is also a stream cipher because the algorithm operates on each letter of the plaintext message independently. SUBSTITUTION, real-time
Advantage **– bit by bit substitution with XOR & keystream**
Emulates one time pad
No size difference between plaintext and ciphertext
Disadvantage
Can be difficult to implement correctly
Generally weaker than block mode cipher
Difficult to generate a truly random unbiased keystream
Wireless
Stream Cipher Uses
WEP, WPA – use WEP if you have nothing else
RC4
Audio Visual
Block-based Ciphers – ciphers operate on "chunks," or blocks, of a message and apply the encryption algorithm to an entire message block at the same time. The transposition ciphers are examples of block ciphers. SUBSTITUTION & TRANSPOSITION
No longer common/effective attack on wireless networks

Cipher Modes (249)

- **CBC Cipher Block Chaining** - blocks of 64 bits with
- 64bits initialization vector. Errors will propagate **ECB Electronic Code Book** - right block/left block pairing 1-1. Replication occurs. Secure short messages,
- **Cipher Feedback CFB** - stream cipher where the cipher text is used as feedback into key generation. errors will propagate
- **Output Feedback OFB** - stream cipher that generates the key but XOR-ing the plaintext with a key stream. No errors will propagate
- **Counter (CTR)** – secure long messages

See 111000111000 it's XOR

Symmetric Cryptography (254)

- Both the receiver and the sender share a common secret key.
- Larger key size is safer > 128
- Can be time-stamped (to counter replay attacks)
- Does not provide mechanisms for authentication and non-repudiation

DES (data Encryption Standard) comes from IBM

- DEA Data Encryption Algorithm x3.92, using 64 block size and 56bit key with 8bits parity
- 16-rounds of substitution and transposition cryptosystem
- Adds confusion(conceals statistical connect between cipher text and plaintext) and Diffusion (spread the influence of plaintext characters over many cipher text characters by means of transposition like HIDE IHED) - Triple des = three times encrypted DES, preferably with 3 different keys = DES-EE3. Actual key length = 168 bits. Uses 48 rounds of computations (3x16)
- Replaced by AES Advanced Encryption Standard

Symmetric Cryptography (254) (cont)

AES Advanced Encryption Standard –

- one of the most popular symmetric encryption algorithms
- NIST selected it as a standard replacement for the older Data Encryption Standard (DES) in 2001.
- BitLocker (a full disk encryption application used with a Trusted Platform Module) uses AES
- Microsoft Encrypting File System (EFS) uses AES for file and folder encryption
- AES supports key sizes of 128 bits, 192 bits, and 256 bits, and the US government has approved its use to protect classified data up to top secret
- Larger key sizes add additional security, making it more difficult for unauthorized personnel to decrypt the data.
- Keys are 128, 192, and 256 bits, blocks 128 bits.

Rijndael Block Cipher Algorithm - for speed, simplicity and resistance against known attacks. Variable block length and variable key lengths (128,192 and 256 bits)

Not selected for AES were:

- **RC5 -** variable algorithm up 0 to 2048 bits key size
- Rivest Cipher 5, or RC5, is a symmetric algorithm patented by Rivest, Shamir, and Adleman (RSA) Data Security, the people who developed the RSA asymmetric algorithm. RC5 is a block cipher of variable block sizes (32, 64, or 128 bits) that uses key sizes between 0 (zero) length and 2,040 bits.
- **IDEA -** International Data Encryption Algorithm 64 bit plaintext and 128 key length with confusion and diffusion used in PGP software patented requires licenses fees/free noncom.
- **Two fish -** key lengths 256 bits blocks of 128 in 16rounds BEAT OUT BY Rijndal for AES, based on Blowfish
- **Blowfish -** by Bruce Schneider key lengths 32 to 448 bits, used on Linux systems that use bcrypt (DES alternative)

Asymmetric Cryptography (262)

- Sender and receiver have public and private keys.
- Public to encrypt a message, private to decrypt
- Slower than symmetric, secret key (100 to 1000)

Public Key Algorithms

RSA - (Rivest, Shamir, & Adleman) works with one way math with large prime numbers (aka trap door functions). Can be used for encryption, key exchange and digital signatures)

Diffie Hellman Key exchange - about exchanging secret keys over an insecure medium without exposing the keys

el Gamal – works with discrete logarithms, based on Diffie Hellman

DSA Digital Signature Algorithm – the US Government Equivalent of the RSA algorithm

ECC - Elliptic Curve Cryptosystem - mathematical properties of elliptical curves, IT REQUIRES FEWER RESOURCES THAN RSA. Used in low power systems (mobile phones etc.)

BOTH a hashing and an asymmetric key algorithm; MD5 & ECC

Hybrid Cryptography (266)

Uses both asymmetrical and symmetrical encryption

- asymmetrical for key exchange
- symmetrical for the bulk - thus it is fast
- example: SSL, PGP, IPSEC S/MIME

Message Digest – summaries of a message's content (not unlike a file checksum) produced by a hashing algorithm, checksum?

MAC – Message Authentication Code

Security Assertion Markup Language (SAML) (271)

SAML is an XML-based convention for the organization and exchange of communication authentication and authorization details between security domains, often over web protocols. SAML is often used to provide a web-based SSO (single sign-on) solution. If an attacker can falsify SAML communications or steal a visitor's access token, they may be able to bypass authentication and gain access SAML is a common protocol used for SSO on the Internet.
*Best choice to support a federated identity management system,
Does not have a security mode and relies on TLS and digital signatures
If home organization offline implement a cloud based system
User training about SSO directs a good idea

Service Provisioning Markup Language (SPML) (271)

Allow platforms to generate and respond to provisioning requests It is a newer framework based on XML but specifically designed for exchanging user information for federated identity single sign-on purposes. It is based on the Directory Service Markup Language (DSML), which can display LDAP-based directory service information in an XML format.

Cyber-Physical Systems (CPS) (278)

Smart networked systems with embedded sensors, processors, and actuators that are designed to sense and interact with the physical world.

History of Crypto (284)

Hieroglyphics - sacred carvings
Scythe - wound papyrus around a wooden rod to see message
Substitution character- shifting 3 character (C3) for example in the one (mono-alphabet) alphabet system
Cipher disks - 2 rotating disks with an alphabet around it
Jefferson disks - 26 disks that cipher text using an alignment bar
Unix - uses rot 13 rotate 13 places in the alphabet
Hagelin machine (M-209) - mechanical cryptographic machine
Enigma - poly-alphabetic substitution cipher machine

SABSA – Sherwood Applied business security architecture chain of traceability, 6 layers
TOGAF – method step by step process and framework. These are the tools to go forward FRAMEWORK AND METHOD
Zachman Framework – common context to understand a complex architecture, communication and collaboration

Symmetric vs. Asymmetric Key Systems

Asymmetric Algorithms

-Uses a pair of keys (private and public) for encryption and decryption
-Built upon hard-to-resolve mathematical problem using factorization, discreet logarithms, and the elliptic curve theory.
-Slower than symmetric algorithm.

.Types of Asymmetric Systems

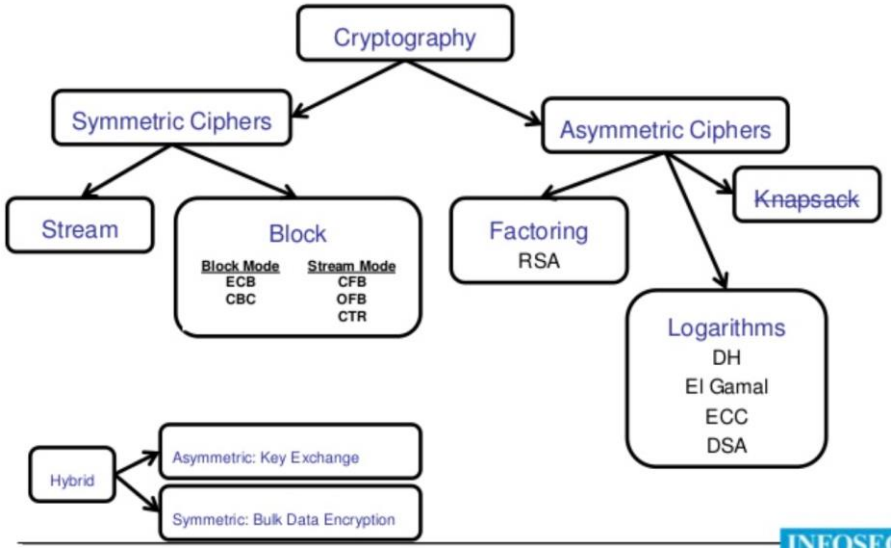
. The Diffie-Hellman Algorithm
. RSA
. El Gamal
. Elliptic Curve Cryptosystems
. LUC
. Knapsack
. Zero Knowledge Proof

Attributes	Symmetric	Asymmetric
Keys	One key is shared between two or more entities	One entity has a public key, and the other entity has a private key
Key Exchange	Out-of-band	Symmetric key is encrypted and sent with message; thus, the key is distributed by in-bound means
Speed	Algorithm is less complex and faster	Algorithm is more complex and slower
Number of Keys	Grows exponentially as users grow	Grows linearly as users grow
Use	Bulk encryption, which means encrypting files and communication paths	Key encryption and distributing keys
Security Service Provided	Confidentiality	Confidentiality, authentication, and non-repudiation

Symmetric Key Cryptography Review

- **Symmetric Algorithms**
  - DES – Data Encryption Standard (56 bits)
  - 3DES – 3 DES keys
  - AES – 128, 192 and 256 bits
  - IDEA – 128 bits
    - International Data Encryption Algorithm
  - Blowfish – up to 448 bits
  - Twofish – up to 256 bits
  - RC4 (variable) – stream cipher
  - RC5 – up to 2048 bits
  - RC6 – up to 2048 bits
  - CAST – 40, 64, 128, and 256 bits
  - SAFER – block cipher developed by the co-creator of IDEA
  - Serpent – Runner-up cipher in the AES competition

Components of Cryptography



Domain 3 – Security Engineering

PKI (289)

Understand the public key infrastructure (PKI). In the public key infrastructure, certificate authorities (CAs) generate digital certificates containing the public keys of system users. Users then distribute these certificates to people with whom they want to communicate. Certificate recipients verify a certificate using the CA's public key.

X.509 standard = PKI.

Serial number, owner, issuer name

Integrity (hash code and message digest), access control, confidentiality (by encryption), authentication (digital certificates) and non-repudiation (digital signatures)

issuer signs a certificate

If you only want to check if a mail is not altered: use digital signature! Proves that the signature was provided by the intended signer

trust anchor = public key that has been verified and that's trusted

Digital signatures (296)

- no modifications allowed
- identity can be derived
- Works with a one-way hash (message digest), like SHA-1 (512 bit blocks) or MD5 (128 bits digest) or HMAC that uses a key
- Acceptable encryption algorithms choices – DSA, RSA, ECDSA

HASH it and ENCRYPT message digest

Correct way to create and use a digital signature – hash the document, encrypt only the hash with the sender's private key, send both the plain text document and the encrypted hash to recipient.

Email Security (297)

S/Mime - Confidentiality (encryption) Integrity (using PKCS X.509 PKI) and non-rep through signed message digests
PEM - Privacy Enhanced Email Encryption (AES) PKI X.509 and RSA
Message Security protocol - Military X.400. Sign, Encrypt, Hash
Pretty Good Privacy - uses IDEA and RSA instead

Digital Certificates

contain specific identifying information and their construction is governed by international standard **(X.509),** creation and validation of digital certificates
Who signs a digital certificate – someone vouching for person not the person.
CRLs - Certificate Revocation Lists are maintained by the various certificate authorities and contain the serial numbers of certificates that have been issued by a CA and have been revoked along with the date and time the revocation went into effect.

Hashing (300)

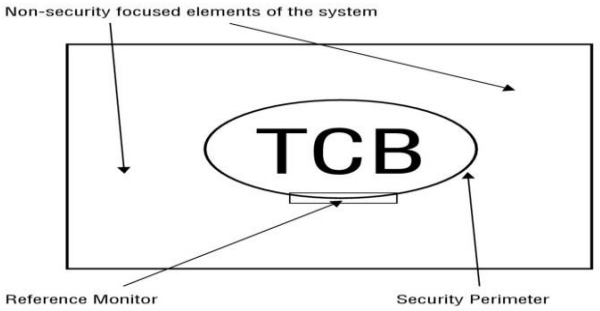
ATTACK HASH BY **BRUTE FORCE** and **dictionary**
CRYPTANALYSIS
Basic Technique –
BRUTE Force will win with no constraints
input of any length and generate a fixed length output
Hash algorithms (Message Digests)
Requirements for HASH

- works on non-fixed length input
- must be relatively easy to compute for any input
- function must be one way
- function must be one way

Most used are MD5 (message Digest 128 bits) and SHA1 (signature hashing algorithm 160 bits)
MD5 – hashing algorithm. It also processes 512-bit blocks of the message, but it uses four distinct rounds of computation to produce a digest of the same length as the MD2 and MD4 algorithms (128 bits). MD5 has the same padding requirements as MD4— the message length must be 64 bits less than a multiple of 512 bits. MD5 implements additional security features that reduce the speed of message digest production significantly. Unfortunately, recent cryptanalytic attacks demonstrated that the MD5 protocol is subject to collisions, preventing its use for ensuring message integrity. it is possible to create two digital certificates from different public keys that have the same MD5 hash.
CRL's of a PKI environment holds serial numbers
SHA1 - was designed by NIST and NSA to be used in digital signatures
Standard is SHA3 most still use SHA2
root Certificate Authority (CA) must certify its own public key pair
cross certification does not check authenticity of the certificates in the certificates path; MD5 not good for securing passwords
Traffic analysis - inference of information from analysis of traffic
Traffic padding - generation of spurious data units
Collision - Same message digest as a result of hashing.
Cryptographic Attacks
Ciphertext Only - attacker sees only the ciphertext, one of the most difficult
Known Plaintext - attacker knowns both cipher and plaintext
Chosen Plaintext - offline attack (attacker prepares list of plaintexts) **-lunch box attack**
online attack - (attacker chooses the plaintext based on the ciphertext already received)
Chosen ciphertext - attacker chooses both the plaintext values and the ciphertext values, cherry picking, feed info and based on what you learned get key
Birthday Attack - Collisions appear much fasters, birthdays match
POODLE - (Padding Oracle on Downgraded Legacy Encryption) attack helped force the movement from SSL 3.0 to TLS because it allowed attackers to easily access SSL encrypted messages.
CRIME/BEAST - earlier attacks against SSL
STUXNET – worm aimed at Iranian nuclear capability

Other things to know

Objects of sensitivity labels are: single classification and component set
'dominate' in access control means access to higher or equal access class
Security perimeter = line between TCB and outside



Validating TCB = formal for system integrity

Digital Rights Management (298)

uses encryption to enforce copyright restrictions on digital media. serves to bring U.S. copyright law into compliance with terms of two World Intellectual Property Organization (WIPO) treaties. The first major provision of the DMCA is the prohibition of attempts to circumvent copyright protection mechanisms placed on a protected work by the copyright holder.
Skip - s a distribution protocol
RC4 - is a stream cipher
RC5 and RC6 are block cipher

FIPS 140 hardware and software requirements

Applets

Applets – these code objects are sent from a server to a client to perform some action. In fact, applets are actually self-contained miniature programs that execute independently of the server that sent them.
Java applets – are simply short Java programs transmitted over the Internet to perform operations on a remote system.
ActiveX – controls are Microsoft's answer to Sun's Java applets. Operate in a similar fashion, but they are implemented using a variety of languages(C, C + +, Java). Two key distinctions between Java applets and ActiveX controls. First, ActiveX controls use proprietary Microsoft technology and, therefore, can execute only on systems running Microsoft browsers. Second, ActiveX controls are not subject to the sandbox restrictions placed on Java applets. They have full access to the Windows operating environment and can perform a number of privileged actions.

Domain 3 – Security Engineering

Threats (317)

Natural environment threats (earthquakes floods, tornadoes)
Supply system threats (power communications water gas)
Manmade threats (vandalism, fraud, theft)
Politically motivated threats (terroristic attacks, riots bombings)
Life safety takes precedence!!
Layered defense model: all physical controls should be work together in a tiered architecture (stacked layers)
Vulnerability=weakness threat = someone will identify the weakness and use it against you and becomes the threat agent
Risk analysis-->Acceptable risk level -->baseline>implement countermeasures
Major sources:
Temperature, Gases, Liquids
Organism: viruses, bacteria
Projectiles: cars, trucks, bullets
Movement: Collapse, earthquakes Energy: radio, radiation

Nice to Know

SMSD - Switched Multimegabit Data Service, a connectionless packet-switching technology. Often, SMDS is used to connect multiple LANs to form a metropolitan area network (MAN) or a WAN. SMDS was often a preferred connection mechanism for linking remote LANs that communicate infrequently, a forerunner to ATM because of the similar technologies used.
DHCP Snooping – used to shield networks from unauthenticated DHCP clients
ICS - industrial control system is a form of computer-management device that controls industrial processes and machines. ICSs are used across a wide range of industries, including manufacturing, fabrication, electricity generation and distribution, water distribution, sewage processing, and oil refining.
There are several forms of ICS, including distributed control systems (DCSs), programmable logic controllers (PLCs), and (SCADA).
SCADA - supervisory control and data acquisition
Kerchoff principle - a cryptographic system should be secure even if everything about the system, except the key, is public knowledge.
Input and Parameter Checking - limit how much data can be proffered as input. Proper data validation is the only way to do away with buffer overflows.
Side-channel attack - is a passive, noninvasive attack intended to observe the operation of a device. When the attack is successful, the attacker is able to learn valuable information contained within the smartcard, such as an encryption key.

Trust – ()

Transitive Trust – Transitive trust is the concept that if A trusts B and B trusts C, then A inherits trust of C through the transitive property— which works like it would in a mathematical equation: if a = b, and b = c, then a = c. A transitive trust extends the trust relationship between the two security domains to all of their subdomains. Within the context of least privilege, it's important to examine these trust relationships.
Nontransitive trust - exists between two security domains, which could be within the same organization or between different organizations. It allows subjects in one domain to access objects in the other domain. A nontransitive trust enforces the principle of least privilege and grants the trust to a single domain at a time.

Electrical Power (319)

Interference
Clean=no interference
Line noise: can be EMI or RFI
Transient: short duration of noise
Counter: voltage regulators, grounding/shielding and line conditioners
EMI
COMMON mode noise: difference between hot and ground
Traverse mode noise: difference between hot and neutral
HINT: common--grounds
Excesses
SPIKE: short high voltage
SURGE: long high voltage
Counter: surge protector
Losses
FAULT: short outage
BLACKOUT: long outage
Counter: Backup power
Long term: Backup Power generator
Short term: UPS
-Online uses ac line voltage to charge batteries, power always though UPS
-Standby UPS, inactive till power down
Degradation
SAG/DIP: short low voltage
BROWNOUT: long low voltage
Counter: constant voltage transformers
Other
Inrush Surge: surge of current required to power on devices
Common-mode noise: radiation from hot and ground wires
Traverse-mode noise: radiation from hot and neutral wires.
Static charge
40 volts sensitive circuits
1000 scramble monitor display
1500 disk drive data loss
2000 system shutdown
4000 Printer Jam
17000 Permanent chip damage

Humidity (326)

<40% static electricity up to 20.000 volts
NORMAL 40-60% up to 4000 volts
>60% corrosion

Tempest

shielding and other emanations-reducing mechanism, a technology that allows the electronic emanations that every monitor produces (known as Van Eck radiation) to be read from a distance (this process is known as Van Eck phreaking)

White noise - broadcasting false traffic at all times to mask and hide the presence of real emanations.
Faraday cage - a box, mobile room, or entire building designed with an external metal skin, often a wire mesh that fully surrounds an area on all sides (in other words, front, back, left, right, top, and bottom). This metal skin acts as an EMI absorbing capacitor
control zone - the implementation of either a Faraday cage or white noise generation or both to protect a specific area in an environment

Fire (328)

Prevention
Training construction, supplies, reach ability
Detection
Manual: pull boxes
Automatic dial- up: Fire department, aka Auxiliary station alarm
Detectors:
- Smoke activated,
- Heat activated,
- Flame activated(infrared)

Classes
A Common WATER, SODA ACID (take away temp)
B Liquids----GAS/CO2, SODA ACID (takes away fuel)
C Electrical-----GAS/CO2 (displace O2)
D Metals----DRY POWDER

WATER suppress temperature
SODA ACID reduces fuel supply
CO2 reduces oxygen
HALON chemical reaction
Fire distinguishers should be 50 feet from equipment and toward the door
Heat
Computer hardware 175F (80c)
Magnetic storage 100F (37c)
Paper 350F (176c)
Sprinklers Wet pipe always contains water, fuse nozzle melts at 165F
Dry pipe water in tank until clapper valve releases it – only begins to fill when triggered by excessive heat
Douches, large amounts of water/foam Pre-action (MOST RECOMMENDED)
water in tanks, first water in pipes when air is lost when heat is detected, then thermal link in nozzle melts to release water

HALON
1211 = portable
1301 = flooding
FM-200 most common replacement (others: CEA, NAF, FE-13 Argon INERGEN Low Pressure Water)

RESISTANCE
Walls: 1 hour fire rating and adjacent room with paper 2 hours

Security Capabilities of Information Systems

TPM - Trusted Platform Module is both a specification for a cryptoprocessor chip on a mainboard and the general name for implementation of the specification. A TPM chip is used to store and process cryptographic keys for the purposes of a hardware supported/ implemented hard drive encryption system. Generally, a hardware implementation, rather than a software-only implementation of hard drive encryption, is considered to be more secure.
Constrained or restricted interface - is implemented within an application to restrict what users can do or see based on their privileges.

Domain 4 – Communications and Network Security

Network Layers OSI MODEL (347)

(later succeeded by TCP/IP)

HINT: All People Seems to Need Data Processing

It encapsulates data when going through the layers

Application – layer 7 – C, AU, I, NR

FTP, SNMP, TELNET, TFTP, SMTP, HTTP, NNTP, CDP, GOPHER, SMB, NDS, AFP, SAP, NCP, SET, LDAP. Technology: Gateways. **User data**

Secure HTTP, S-HTTP - encrypting HTTP documents. Also overtaken by SSL

SSL, Secure Socket Layer - encryption technology to provide secure transactions like credit card numbers exchange. Two layered: SSL record protocol and handshake protocol. Same as SSH it uses symmetric encryption for private connections and asymmetric or public key cryptography for peer authentication.

Secure Electronic Transaction (SET) - authentication for credit card transactions. Overtaken by SSL

Also uses message authentication code for integrity checking.

Telnet - terminal emulation enables user to access resources on another machine. Port 23

FTP, File Transfer Protocol - for file transfers. Cannot execute remote files as programs. Authentication. Port 20 and 21

TFTP, Trivial File Transfer Protocol - stripped down, can only send/receive but not browse directories. No authentication thus insecure. Port 69

SMTP, Simple Mail Transfer protocol - email queuing. Port 25

SNMP, Simple Networking Management Protocol collection of network information by polling the devices from a management station. Sends out alerts –called traps- to an database called Management Information Bases (MIBs)

Presentation – layer 6 – C, AU, Encryption

Translations like EBCDIC/ANSI; compression/decompression and encryption/decryption. Uses a common format to represent data, Standards like JPEG, TIFF, MID, HTML; Technology: Gateway. **Messages**

Session -layer 5 -- None

Inter-host communication, logical persistent connection between peer hosts, a conversation, simplex, half duplex, full duplex. Protocols as NSF, SQL, RADIUS, and RPC. Protocols: PAP, PPTP, RPC Technology: Gateway

PAP – Password Authentication Protocol

PPTP – Point-to-Point Tunneling Protocol

RPC – Remote Procedure Call Protocol

NFS, Network File System - protocol that supports file sharing between two different file systems

NetBIOS –

SSL/TLS -

Network Layers OSI MODEL (cont.) (347)

Transport – layer 4 – C, AU, I

End-to-end data transfer services and reliability. Technology: Gateways. Segmentation, sequencing, and error checking at this layer. **Datagrams**

TCP Three-way Handshake – SYN, SYN-/ACK, ACK

Protocols: TCP, UDP, SSL, SSH-2, SPX, NetBIOS, **ATP**

Secure Shell (SSH-2) - Authentication, compression, confidentiality and integrity.

Uses RSA certificates for authentication and triple DES for encryption

TCP, Transmission control protocol – reliable, sequences and works with acknowledgements. Provides a manageable data flow to avoid congestions overloading and data loss. (Like having a telephone conversation with someone). Connection Oriented. **User**

UDP, Datagram protocol – unreliable, scaled down version of TCP, no error correction, no sequencing. Less overhead. (Like sending a letter to someone). Connectionless.

Network – layer 3 – C, AU, I

Path selection and logical/network addressing.

Technology: Virtual circuits (ATM), routers. **Packets**

Addressing – IP uses the destination IP to transmit packets thru networks until delivered

Fragmentation – IP will subdivide a packet if its size is greater than the maximum allowed on a local network

Message routing, error detection and control of node data are managed. IP, IPSEC, ICMP, BGP, OSPF, RIP, BOOTP, DHCP, ZIP, DDP, X.25, NAT and IGMP

OSPF Open Shortest Path First – routing protocol short path

SKIP, Simple Key Management for Internet Protocols - provides high availability in encrypted sessions to protect against crashes. Exchanges keys on a session by session basis.

ARP, Address resolution protocol - Used to match an IP address to a hardware MAC address**.** ARP sends out broadcast to a network node to reply with its hardware address. It stores the address in a dynamic table for the duration of the session, so ARP requests are only sent the first time

ICMP, Internet control message protocol - sends messages between network nodes regarding the health of the network. Also informs about rerouting in case of errors. Utility PING uses ICMP messages to check physical connectivity of the network machines IPX, Appletalk, and NetBEUI are non-IP protocols.

IP, Internet protocol - all hosts have an IP address. Each data packet has an IP address of sender and recipient. Routing in network is based upon these addresses. Datagram service is considered unreliable because there's no guarantee that the packet will be delivered, not even that its delivered only once and no guarantee that its delivered in the same sequence that its sent 32 bits long, IPv6 is 128 bits long

DHCP: Dynamic Host Configuration Protocol

BootP, Bootstrap Protocol when wireless workstation is on-lined it sends out a BootP request with its MAC address to get an IP address and the file from which it should boot. Replaced by DHCP

Network Layers OSI MODEL (cont.) (347)

Data Link – layer 2 - C

This layer deals with addressing physical hardware. FRAMES Translates data into bits and formats them into **data frames** with destination header and source address. Error detection via checksums.

LLC, the Logical Link Control Sub layer - Flow control and error notification

MAC: the Media Access Control layer - Physical addressing. Concerns frames, logical topologies and MAC-addresses

Protocols: L2F, PPTP, L2TP, PPP, SLIP, ARP, RARP, SLARP, IARP, SNAP, BAP, CHAP, LCP, LZS, MLP, Frame Relay, Annex A, Annex D, HDLC, BPDU, LAPD, ISL, MAC,

Ethernet, Token Ring, FDDI

RARP, Reverse address resolution protocol - When a hardware address is known but the IP address has to be found. (like an diskless machine)

Switches, bridges, hardware addressing

Physical – layer 1 - C

Physical signaling. Coverts **bits** into voltages or light impulses. Electrical, Hardware and software drivers are on this level. It sends and receives bits.

Repeaters, hubs, cables, USB, DSL, ISDN, ATM

Physical topologies: BUS, MESH, STAR, TREE, RING

Network layers TCP/IP Model (353)

Developed by Department of Defense in the 1970s to support the construction of the internet

HINT: AHIN

Application – layer 4 (Application/Presentation/Session)

Applications and processes that uses the network

Host-to-Host – Layer 3 (Transport)

End-to-end data delivery

Protocols: TCP and UDP

Internet – Layer 2 (corresponds to OSI network layer) Defines the IP datagram and handles routing of data across networks

Protocols: IP, ARP, RARP, ICMP

Network access – Layer 1 (Data link, Physical)

Routines for accessing physical networks and the electrical connection

LPD, Line printer daemon for printing and spooling

X Windows graphical user interface

Domain 4 – Communications and Network Security

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols		DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent. Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP	GATEWAY	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed). Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT		
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports). Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names		
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control. Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP		Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address). Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP	Can be used on all layers	Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) (NIC card — Switch — NIC card) (end to end). Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch Bridge WAP** PPP/SLIP	Land Based Layers	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**		

Security Modes (used in MAC)

Dedicated security mode :

- **All users** can access all data.
- Clearance for all information.
- Need to know for **ALL** data system high security mode:
- **All users** can access **some data**, based on need to know
- Clearance for all information
- Need to know for **SOME** data compartmented security mode:
- **All users** can access **some data**, based on their need to know and approval.
- Clearance for all information they access
- Need to know for **SOME data**
- Use of information labels

Multi-level:

- **All users** can access **some data**, based on their need to know, approval and clearance.
- Clearance for all information they access
- Need to know for **SOME data** Others:

controlled type of multilevel security where a limited amount of trust is placed in the system's hardware/software along with classification

limited access: minimum user clearance is not cleared and the maximum data classification is unclassified but sensitive

Firewalls

A method of guarding a private network by analyzing the data leaving and entering. Firewalls can also provide network address translation, so the IP addresses of computers inside the firewall stay hidden from view.

Packet-filtering firewalls (layer 3/4) - use rules based on a packet's source, destination, port or other basic information to determine whether or not to allow it into the network.

Stateful packet filtering firewalls **(layer 7)** - have access to information such as; conversation, look at state table and context of packets; from which to make their decisions.

Application Proxy firewalls (layer 7) **(3-7 actually)-** which look at content and can involve authentication and encryption, can be more flexible and secure but also tend to be far slower.

Circuit level **proxy (layer 5)-** looks at header of packet only, protects wide range of protocols and services than app-level proxy, but as detailed a level of control. Basically once the circuit is allowed all info is tunneled between the parties. Although firewalls are difficult to configure correctly, they are a critical component of network security.

SPF, Static Packet Firewall (layer 3) -

Wireless (364)

IEEE 802.15 is the standard for Bluetooth. IEEE 802.3 defines Ethernet, 802.11 defines wireless networking, and 802.20 defines LTE.

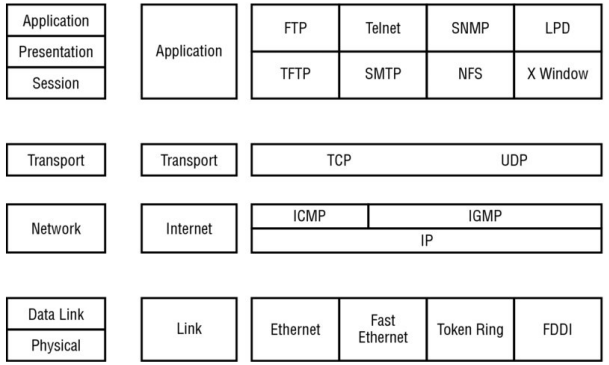
Amendment	Speed	Freq.	Range	Comp.
802.11	2 Mbps	2.4 GHz	FHSS/DSSS	
802.11a	54 Mbps	5 GHz	150 - OFD	A
802.11b	11 Mbps	2.4 GHz	300 - DSSSS	b/g/n
802.11g	54 Mbps	2.4 GHz	300	b/g/n
802.11n	200+ Mbps	2.4 or 5 GHz	300	a/b/g
802.11ac	1 Gbps	5 GHz	300	a/b/g
802.16	IEEE 802	WBA		
802.11i	AES	CCMP	WPA2	

Security Enhancement Protocols

TELNET: Remote terminal access and Secure Telnet

REMOTE PROCEDURE CALL: Secure remote procedure call (SRA)

SSH – Secure Shell over Telnet for remote server administration via the command line



Domain 4 – Communications and Network Security

Netwok IPV4 (354)

TCPIP Classes
Class A network number values begin at 1 and end at 127
Class B network number values begin at 128 and end at 191
Class C network number values begin at 192 and end at 223

ISDN
BRI B-channel 64Kbps, D-channel 16Kbps
PRI B- and D-channels are 64Kbps

80211 has CSMA/CA as protocol. Can use DSSS and FHSS (ss stands for spread spectrum)
802.11b uses only DSSS

Before a computer can communicate with the internet, it needs an IP-address, a default gateway and a subnet mask

To connect multiple LAN segments you can use Bridges, Switches and Routers
Fast Ethernet 100Base-TX has as characteristics: 100Mbps data transmission, 1 pairs Cat5 UTP and max segment of 100 meters (328 feet)
Unsubnetted netmask is shown as /24

Other word for DMZ is screened subnet

FTP, RLOGIN and TELNET never uses UDP but TCP

Attenuation - is a decrease in amplitude as a signal propagates along a transmission medium

SSL session key length is from 40bit to 256 bit

The bridge connects multiple networks at the data link layer, while router connects multiple networks at the network layer.

Data backups addresses availability, integrity and recovery but not confidentiality

IP headers contain 32-bit addresses (in IPv4) and 128 in IPv6. In an Ethernet LAN, however, addresses for attached devices are 48 bits long.

Subnet Masks
Class A 255.0.0.0
Class B 255.255.0.0
Class C 255.255.255.0

Types of Wireless Networks (364)

Uses the 802.11x specification to create a wireless LAN
Ad hoc Mode – directly connect two+ clients, no access point
Infrastructure Mode – connects endpoints to a central network, not directly to each other**,** need access point and wireless clients for IM mode wireless
Stand-alone Mode – isolated system
WEP – don't use can be cracked in seconds, predecessor to WPA and WPA2, confidentiality, uses RC4 for encryption, weakened by use of RC4 use of common key and a limited number of initialization vectors
WPA – uses TKIP for data encryption
WPA2 – based on 802.11i, uses AES, key management, reply attack protection, and data integrity, most secure, CCMP included, WPA2 ENTERPRISE Mode - uses RADIUS account lockout if a password-cracker is used
TKIP – Temporal Key Integrity Protocol, uses RC4
LEAP – Lightweight Extensible Authentication Protocol, Cisco proprietary protocol to handle problems with TKIP, security issues don't use. Provides reauthentication but was designed for WEP

TCP Ports

- TCP 20 & 21; TCP
- UDP 21; not used for any common file transfer protocol
- TCP 21 & UDP 21;
- TCP 22; SSH (SFTP operates oevr SSH)
- TCP 23; telnet: TCP 515; LPD - print
- TCP 25; SMTP (Simple Mail Transfer Protocol)
- TCP 53; DNS; TCP 110; POP3
- TCP 80; HTTP – no confidentiality
- TCP 143; IMAP (Internet Message Access Protocol)
- TCP 389; unsecure LDAP
- TCP 636; LDAP-S over SSL or TLS
- TCP 9100; network printers
- UDP 69; TFTP (Trivial FTP)
- 6000-6063; X Windows, Linux
- TCP 443; HTTPS – Nikto to scan
- TCP 445; Active Directory
- TCP; 1433; Microsoft SQL, Db
- TCP 1521; Oracle: TCP 3389; RDP
- TCP 3268/3269; global catalog (unsecure/secure)
- TCP/UDP; 137-139; NetBIOS services

Switched Networks (378)

Coaxial - many workstations, length. 1000Base-T – 100 M Twisted pair to long. Cat 5 better than cat3 for interference Fiber optics immune to EMI, can be broken and high cost/expertise **Topology failures**
Ethernet twisted pair - more resistant than coaxial Token Ring because a token is passed by every station, a NIC that's is set to wrong speed or error can take all network down
Fiber Distributed Data Interface - form of token ring that has second ring that activates on error
Leased lines use multiple lines and/or multiple vendors
Frame Relay WAN - over a public switched network. High Fault tolerance by relaying fault segments to working.

Speeds; T-1 – 1.544 Mbps, T-3 – 44,736 Mbps (45)

ATM – 155 Mbps, ISDN – 64 or 128 Mbps

CAT 3 UTP; 10 Mbps, CAT 5;100 Mbps CAT 5e/6 – 1,000 Mb

Email Security Solutions & Certs (368)

LDAP – Lightweight Directory Access Protocol, client/server based directory query protocol loosely based upon X.500, commonly manages user information, for accessing directory services and manage certificates Ex. Active Directory, cn=ben+ou=sales
Zero or more, comma separated, no semi-colon, + to join
SASL – provides secure LDAP authentication
OpenLDAP – default, stores user PW in the clear
Client SSL Certificates – used to identify clients to servers via SSL (client authentication)
S/MIME Certificates – used for signed and encrypted emails, can form sign, and use as part of a SSO solution
MOSS – MIME Object Security Services, provides authentication, confidentiality, integrity, and nonrepudiation
PEM – provides authentication, confidentiality, integrity, and nonrepudiation
DKIM – Domain Keys Identified Mail, domain validation tool
OAuth – ability to access resources from another service
OpenID – paired with OAuth is a RESTful, JSON-based authentication protocol can provide identity verification and basic profile information, phishing attack possible by sending fake data

Security Perimeter (370)

The first line of protection between trusted and untrusted networks. Generally includes a firewall and router that help filter traffic. May also include proxies, IDSs, and IPSs.
Zero Day – application white list

Operations of Hardware (374)

Multiplexors- device that enables more than one signal to be send out of one physical circuit
WAN switches - multi-port networking devices that are used in carrier networks. Connect private data over public data by using digital signals. Data link layer.
Access servers - server that provides dial-in and dial-out connections to the network
Modems - transmits data over telephone lines
Channel Service Unit (CSU)/Data service unit (DSU) - digital interface device used to terminate the physical interface on a DTE device. They connect to the closest telephone company switch in a central office (CO)

LAN Devices (374)

Repeaters - amplify data signals to extend range (physical)
HUBS - connect multiple LAN devices into a concentrator. Is actually a multi-port repeater (physical)
Bridges - Forwards data to all other network segments if it's not on the local segment. Operates at level 2 (thus no IP-addressing)
Switches - Will only send data to the specific destination address. It's actually a multi-port bridge. (Data link)
Routers - opens up data packet, reads hardware or network address and then forwards it to the correct network
Gateway - software that acts as access point to another network or device that translates between different protocols
LAN extenders - remote access, multi layer switch that connects LANs over a WAN

Domain 4 – Communications and Network Security

Terms

Broadband Technologies – ISDN, cable modems, DSL, and T1/T3 lines that can support multiple simultaneous signals. They are analog and not broadcast technologies**.**
Broadcast Domain – set of systems that can receive a broadcast from each other
CHAP – Challenge-Handshake Authentication Protocol, used by PPP servers to authenticate remote clients. Encrypts username and PW and performs periodic re authentication while connected using techniques to prevent replay attacks.
CIR – (committed Information Rate) minimum bandwidth guarantee provided by service provider to customers
Collision Domain – set of systems that could cause a collision if they transmitted at the same time, more number of systems in domain increases likelihood of network congestion due to more collisions
Data Streams – occur at Application, Presentation, and Session layers.
EAP, Extensible Authentication Protocol - an authentication framework. Effectively, EAP allows for new authentication technologies to be compatible with existing wireless or point-to-point connection technologies, extensible was used for PPP connections
FCoE – Fiber Channel Over Ethernet, allows existing high-speed networks to be used to carry storage traffic
FDDI – Fiber Distributed Data Interface, token-passing network uses a pair of rings with traffic flowing in opposite directions, uses tokens
FTP – File Transfer Protocol
Gateway – translates between protocols
ICMP – Internet Control Message Protocol, means to send error messages for non-transient error conditions and provides a way to probe the network in order to determine general characteristics about the network, ping
iSCI – Internet Small Computer Interface, Converged protocol that allows location-independent file services over traditional network technologies. Cost less than Fiber. Standard for linking data storage sites
ISDN – PRI (Primary Rate Interface) bandwidth of 1.544 Mbps, faster than BRI's 144 Kbps
MAC – Machine Access Control, hardware address of machine, can tell manufacturer,
Multilayer Protocols – allow encryption at various layers, support a range of protocols at higher levels. Bad – conceal covert channels, filters can be bypassed, sometimes logical boundaries can be bypassed
MPLS – Multiprotocol Label Switching, high performance networking, uses path labels instead of network addresses, wide area networking protocol, label switching, finds final destination and then labels route for others to follow
PAP – Password Authentication Protocol, sends PW unencrypted
PEAP – provides encryption for EAP methods and can provide authentication, does not implement CCMP, encapsulates EAS in a TLS tunnel
Port Based Authentication – 802.1x, can be used with EAP

Terms (Cont)

PPP – Point-to-Point Protocol, most common, used for dial up connections, replaced SLIP
Proxy – form of gateway that provide clients with a filtering, caching, or other service that protects their information from remote systems
PVCs – Private Virtual Circuits,
RST flag – used to reset or disconnect a session, resumed by restarting the connection via a new three-way handshake
Converged Network – carries multiple types of traffic like voice, video, and data
SDN – Software designed networking, defined and configured as code or software, quickly change the network based on organizational requirements
Hypervisor-based Network – may be software defined, but it could also use traditional network devices running as virtual machines
SSID – normally disabled for secure networks
Site Survey – identify areas where wireless network may be accessible
SONET – protocol for sending multiple optical streams over fiber
SUBNET – logical division of a network
Supernet – made up of two or more networks
UDP – User Datagram Protocol, lightweight service for connectionless data transfer without error detection and correction
WAF – Web Application Firewall
Wired Extension Mode – uses WAP to link wireless clients to a wired network
AMP - Asymmetric multiprocessing - used in applications that are dedicated, such as embedded systems, when individual processors can be dedicated to specific tasks at design time.
SMP – Symmetric Multiprocessors, hardware and software architecture where two or more identical processors are connected to a single, shared main memory, have full access to all I/O devices, and are controlled by a single operating system instance that treats all processors equally, reserving none for special purposes.

Attacks, Malware, and Bad Stuff

ARP Spoofing –
Bluejacking – when attackers send unsolicited messages via Bluetooth
Bluesnarfing – targets the data or information on Bluetooth-enabled devices
CAIN Attack -
DNS Spoofing – when an attacker sends false replies to a requesting system, beating valid replies from the real DNS server
DNS Poisoning – when an attacker changes the domain name to IP address mappings of a system to redirect traffic to alternative systems
RDP – provides terminal sessions w/out
Screenscraper – copy actual screen, subset of remote control
SPIT attacks – Spam over Internet Telephony and targets VoIP systems

Things to Know

Nikto, Burp Suite, Wapiti – web application vulnerability scanners

Network Attacks – Denial of Service

Used to overwhelm a targets resources

- Filling up hard drive by using huge email attachments or file transfers
- Sends messages to reset targets host subnets masks
- Using up all system resources

DOS - performed by sending malformed packets to a system; can interrupt service or completely deny legitimate users of system resources, an attack that attempts to prevent authorized use of a resource. This can be done through flaw exploitation, connection overloading, or traffic flooding.

DDOS – botnet, zombie, massive dos attack using multiple computers
SMURF – ICMP requires three players (attacker, victim and amplifying network); attacker spoofs packet header to make it appear that it originated on the victim system with amplifying network broadcasting the message.
Countermeasures – disable broadcast at border routers; border routers should not accept packets that originate within network; restrict ICMP traffic (Hint IC = Its Smurf though spelled wrong)
FRAGGLE – similar to Smurf but uses UDP
Countermeasures – disable broadcast at border routers; border routers should not accept packets that originate within network; restrict UDP traffic; employ IDS; apply appropriate patches, block UDP port 7 & 9 from entering network
Land Attack - The attack involves sending a spoofed TCP SYN packet (connection initiation) with the target host's IP address and an open port as both source and destination.
The reason a LAND attack works is because it causes the machine to reply to itself continuously.
SYN FLOOD - TCP packets requesting a connection (SYN bit set) are sent to the target network with a spoofed source address. The target responds with a SYN-ACK packet, but the spoofed source never replies. This can quickly overwhelm a system's resources while waiting for the half-open connections to time out. This causes the system to crash or otherwise become unusable. Counter: sync cookies/proxies, where connections are created later
Teardrop - The length and fragmentation offset fields of sequential IP packets are modified, causing the target system to become confused and crash. Uses fragmented packets to target a TCP flaw in how the TCP stack reassembles them. DOS
Common Session Hijacking Attacks:
Session hijacking (Spoofing) - IP spoofing involves altering a TCP packet so that it appears to be coming from a known, trusted source, thus giving the attacker access to the network. Intercept cookies from a request header
TCP sequence number attack – intruder tricks target to believe it is connected to a trusted host and then hijacks the session by predicting the targets choice of an initial TCP sequence number

Domain 4 – Communications and Network Security

Packet switching technologies

X25 defines point-to-point communication between Data terminal Equipment (DTE) and Data Circuit Terminating Equipment (DCE)

Link Access Procedure-Balanced (LAPB) created for use with X25, LAPB defines frame types and is capable of retransmitting, exchanging and acknowledging frames as detecting out of sequence or missing frames

Frame Relay High performance WAN protocol designed for use across ISDN interfaces. Is fast but has no error correction, supports multiple PVCs, unlike X.25, packet switched technology that provides CIR, requires DTE/DCE at each connection point

Switched Multimegabit DATA Service (SMDS) high speed communication over public switches networks for exchanging 'bursts of data' between enterprises

Asynchronous Transfer mode (ATM) very high bandwidth. It uses 53-byte fixed size cells instead of frames like Ethernet. It can allocate bandwidth up on demand making it a solution for Busty applications. Requires fiber optics.

Voice over IP (VOIP) combines many types of data into a single IP packet. Cost, interoperability and performance wise it's a major benefit.

Other important WLAN protocols

Synchronous Data Link Control (SDLC) - created by IBM for mainframes to connect to their remote offices. Uses a polling media access method. Works with dedicated leased lines permanent up.
Data link layer of OSI model

High-level Data Link Control (HDLC) - extension to SDLC also for mainframes. Uses data encapsulation on synchronous serial links using frame characters and checksums. Also data link layer

High Speed Serial Interface (HSSI) - Defines electrical and physical interfaces to use for DTE/DCE communications. Physical layer of OSI

LAN Cables (378)

Twisted pair
Shielded (STP) or unshielded (UTP) Cat 3=10BaseT, Cat5=100BaseT

Coaxial
More EMI resistant. Baseband: only one single channel, Broadband: multiple signal types like data, video, audio **Fiber Optic**
Most expensive, but hard to tap and resistant to EMI

Firewalls (376)

TYPES

First generation – (**static) Packet filtering firewall AKA screening router** Examines source/destination address, protocol and ports of the incoming package. Based on ACL's access can be denied or accepted. Is considered a firewall and operates at Network or Transport layer of OSI

Second generation - **Application level firewall AKA proxy server** While transferring data stream to another network, it masks the data origin. operating at Application layer of OSI

Third generation - **Stateful inspection firewall** (also known as Dynamic) All packages are inspected at the Networking layer so it's faster. By examining the state and context of the data packages it helps to track connectionless protocols like UDP and RPC. Analyzed at all OSI Layers.

Fourth generation - Dynamic Packet Filtering firewall Enables modification of the firewall rule. It provides limited support for UDP by remembering UDP packages across the network.

Fifth generation - **Kernel Proxy Firewall / Application level Firewall** Runs in windows NT, modular, kernel based, multiplayer session evaluation. Uses dynamic TCP/IP stacks to inspect network packages and enforce security policies.

Firewall architecture (377)

Packet filtering routers
Sits between trusted and un-trusted network, sometimes used as boundary router. Uses ACL's. Protects against standard generic external attacks. Has no user authentication, has minimal auditing.

Screened-Host firewall system
Has both a packet-filter router and a bastion host. Provides both network layer (package filtering) as application layer (proxy) server.

Dual homed host firewall
Consists of a host with 2 NIC's. One connected to trusted, one to un-trusted. Can thus be used as translator between 2 network types like Ethernet/token ring. Internal routing capabilities must not be enabled to make it impossible to circumvent inspection of data.

Screened-subnet firewalls
Has also defined a De-Militarized Zone (DMZ) : a small network between trusted an untrusted.

Socks firewall

Every workstation gets some Socks software to reduce overhead

Tiers – design separates distinct protected zones and can be protected by a single firewall that has multiple interfaces

Access Control Methodologies Remote Access Authentication Systems (390)

Centralized access control
CALLBACK; system calls back to specific location (danger in user forwarding number) somewhere you are
CHAP (part of PPP) supports encryption
XTACACS separates authentication, authorization and accounting processes
TACACS+: stronger through use of tokens

Terminal Access Controller Access Control System TACACS
User passwords are administrated in a central database instead of individual routers. A network device prompts user for a username and static password then the device queries a TACACS server to verify the password. TACACSs **does not** support prompting for password change or use of dynamic password tokens. Port 49
TACACS: user-id and static password for network access via TCP

TACACS+ Enhanced version with use of two factor authentication, ability to change user password, ability of security tokens to be resynchronized and better audit trails and session accounting

Remote Authentication Dial-In User Service RADIUS
Client/server protocol, often leads to TACACS+. Clients sends their authentication request to a central radius server that contains all of the user authentication and network ACL's RADIUS does not provide two way authentication, therefore it's not used for router-to-router authentication. Port 1812. Contains dynamic password and network service access information (Network ACLs) NOT a SSO solution, TLS over TCP – to encrypt, Default UDP, PW encrypted, supports TCP and TLD if set, Remote connectivity via dial in (user dials in to access server, access server prompt for credentials, user enters credentials and forwards to radius server, radius server accepts or rejects). USES UDP. Incorporates an AS and dynamic/static password user can connect to any network access server, which then passes on the user's credentials to the RADIUS server to verify authentication and authorization and to track accounting. In this context, the network access server is the RADIUS **client** and a RADIUS server acts as an authentication server. The RADIUS server also provides AAA services for multiple remote access servers.

DIAMETER - remote connectivity using phone **wireless** etc, more secure than radius, cordless phone signal is rarely encrypted and easily monitored

Remote Access Technologies (390)

Asynchronous Dial-Up Access This is how everyone connects to the internet. Using a public switched telephone network to access an ISP

Integrated Serviced Digital Network (ISDN) communication protocol that permits telephone line to carry data, voice and other source traffic. Two types: BRI Basic rate interface and Primary Rate Interface (PRI) **xDSL** uses regular telephone lines for high speed digital access **Cable Modems** Via single shared coaxial cable, insecure because of not being filtered or firewalled

Domain 4 – Communications and Network Security

Remote Access Security Technologies

Restricted Address - incoming calls are only allowed from specific addresses on an approval list. This authenticates the node, not the user!

Callback - User initiates a connection, supplies identifying code, and then the system will call back a predetermined telephone number. Also less useful for travelling users

Caller ID - checks incoming telephone number against an approval list and then uses Callback. Less useful for travelling users.

Remote Node Security Protocols

Password Authenticate Protocol PAP

Provides identification and authentication of the user using static replayable passwords. No encryption of user-id or password during communication

Challenge Handshake Authenticate Protocol (CHAP) non-replayable challenge/response dialog

LAN Topologies (394)

BUS - all transmissions have to travel the full length of the cable
RING - Workstations are connected to form a closed loop
STAR - nodes are connected to a central LAN device
TREE - bus type with multiple branches
MESH - all nodes interconnected

LAN Transmission Methods (396)

Unicast - Packet is sent from single source to single destination
Multicast - source packet is copied and sent to multiple destinations
Broadcast - source packet is copied and sent to all nodes

DATA NETWORK SIGNALS

Analog signal - Infinite wave form, continuous signal, varied by amplification
Digital signal - Saw-tooth form, pulses, on-off only, digital signals are a means of transmission that involves the use of a discontinuous electrical signal and a state change or on-off pulses.
Asynchronous - sends bits of data sequentially. Same speed on both sides. Modems and dial-up remote access systems
Synchronous very high speed governed by electronic clock timing signals
Asynchronous communications, broadband connections, and half-duplex links can be digital or analog.

LAN Media Access (398)

Ethernet IEEE 802.3 using CSMA with an BUS-topology
Thinnet: 10base2 with coax cables up to 185 meters
Thicknet: 10Base5, coax up to 500 meters
UTP: 10BaseT=10MBps
100baseT=Fast Ethernet =100MBps
1000BaseT=Gigabit Ethernet=1GBps
Ethernet networks were originally designed to work with more sporadic traffic than token ring networks

ARCnet - uses token passing in a star technology on coax

Token Ring IEEE 802.5 - IBM created. All end stations are connected to a MAU Multi Access Unit. CAU: Controlled Access Units – for filtering allowed MAC (Extended Unique Identifier) addresses.

FDDI, Fiber Distributed Data Interface - token-passing dual token ring with fiber optic. Long distances, minimal EMI interference permits several tokens at the time active

LAN Transmission Protocols (398)

Carrier Sense Multiple Access CSMA - for Ethernet. Workstations send out packet. If it doesn't get an acknowledgement, it resends
CSMA with Collision Avoidance workstations - are attached by 2 coax cables. In one direction only. Wireless 802.11
CSMA with Collision Detection - Only one host can send at the time, using jamming signals for the rest.
Polling - Host can only transmit when he polls a secondary to see if its free
Token-passing - Used in token rings, Hosts can only transit when they receive a clear to send token.

DATA NETWORK TYPES

Local Area Network LAN

Limited geographically to e.g. a building. Devices are sharing resources like printers, email and files. Connected through copper wire or fiber optics.
CAN: campus area network, multiple building connected to fast backbone on a campus
MAN: metropolitan network extends over cities

Wide Area network WAN

Connects LANS over a large geographical area

Internet intranet and extranet

Internet is global, intranet local for use within companies and extranet can be used e.g. by your customers and clients but is not public.

Virtual Private Networks VPN (388)

A VPN is created by dynamically building a secure communications link between two nodes, using a secret encapsulation method via network address translation (NAT) where internal IP addresses are translated to external IP addresses. Cannot double NAT with the same IP range, same IP address cannot appear inside and outside of a NAT router.

VPN Protocols

Hint: TP at end for Tunneling Protocols

PPTP, Point to Point tunneling protocol

- Works at data link layer of OSI
- Only one single point-to-point connection per session
- Point To Point protocol (PPP) for authentication and tunneling
- Dial-up network use
- Does not support EAP
- Sends initial packets in plaintext

L2F, Layer 2 Forwarding

- Cisco developed its own VPN protocol called which is a mutual authentication tunneling mechanism.
- L2F does not offer encryption. L2F was not widely deployed and was soon replaced by L2TP.
- both operate at layer 2. Both can encapsulate any LAN protocol.

L2TP, Layer 2 tunneling protocol

- Also in data-link layer of OSI
- Single point-to-point connection per session
- Dial-up network use
- Port 115
- Uses IPsec

IPSEC

- Operates at Network Layer of OSI
- Enables multiple and simultaneous tunnels
- Encrypt and authenticate
- Build into IPv6
- Network-to-network use
- Creates a private, encrypted network via a public network
- Encryption for confidentiality and integrity

2 protocols: AH Authentication header and ESP Encapsulated Security Payload
works with Security Associations (SA's)
works with IKE protocols IKE IS FOR MANAGING SECURITY ASSOCIATIONS 2 modes:
transport, data is encrypted header is not tunneled: new uses rc6; IP header is added, old IP header and data is encrypted
cipher types: block (padding to blocks of fixed size) like DES 3DES AES or stream (bit/byte one by one o padding) like RC4, Sober

TLS – Transport Layer Security

- encrypt and protect transactions to prevent sniffing while data is in transit along with VPN and IPsec
- most effective control against session hijacking
- ephemeral session key is used to encrypt the actual content of communications between a web server and client
- TLS - **MOST CURRENT not SSL!!!**

PVC - Permanent virtual circuits, is like a dedicated leased line; the logical circuit always exists and is waiting for the customer to send data. Like a walkie-tealie

SVC – switched virtual circuit, is more like a shortwave or ham radio. You must tune the transmitter and receiver to a new frequency every time you want to communicate with someone.

Domain 4 – Communications and Network Security

VPN Devices

Is hardware or software to create secure tunnels

IP-sec compatible

- Encryption via Tunnel mode (entire data package encrypted) or Transport mode (only datagram encrypted)
- Only works with IP at Network layer of OSI **NON IP-sec compatible**

Socks-based proxy servers Used to reach the internal network from the outside. Also contains strong encryption and authentication methods

PTP used in windows machines. Multiprotocol, uses PAP or CHAP

Dial-up VPN's remote access servers using PPTP commonly used by ISP's

Secure Shell SSH2 not strictly a VPN product but opens a secure encrypted shell session from the internet through a firewall to a SSH server

Encapsulating Security Payload (389)

Encrypts IP packets and ensured integrity.

- ESP Header – contains information showing which security association to use and the packet sequence number. Like the AH, the ESP sequences every packet to thwart replay attacks.
- ESP Payload

Spread Spectrum

FHSS – Frequency Hopping Spread Spectrum**,** The entire range of available frequencies is employed, but only one frequency at a time is used.

DSSS – Direct Sequence Spread Spectrum, employs all the available frequencies simultaneously in parallel. This provides a higher rate of data throughput than FHSS. DSSS also uses a special encoding mechanism known as chipping code to allow a receiver to reconstruct data even if parts of the signal were distorted because of interference.

OFDM – Orthogonal Frequency-Division Multiplexing, employs a digital multicarrier modulation scheme that allows for a more tightly compacted transmission. The modulated signals are perpendicular and thus do not cause interference with each other.

5

All use spread spectrum techniques to transmit on more than one frequency at the same time**.** Neither FHSS nor DHSS uses orthogonal modulation, while multiplexing describes combining multiple signals over a shared medium of any sort. Wi-Fi may receive interference from FHSS systems but doesn't use it.

WAN Protocols (404)

Private Circuit technologies

Dedicated line reserved communication, always available **Leased line** can be reserved for communications. Type of dedicated line.

- **T1** 1,5 Mbps through telephone line
- **T3** 44,7 Mbps through telephone line
- **E1** European 2048 Mbps digital transmission
- **Serial Line IP (SLIP)** TCP/IP over slow interfaces to communicate with external hosts (Berkley UNIX, windows NT RAS), no authentication, supports only half-duplex communications, no error detection, manual link establishment and teardown

Point to Point protocol (PPP) improvement on slip, adds login, password and error (by CHAP and PAP) and error correction. Data link.

Integrated Services Digital Network (ISDN) combination of digital telephony and data transports. Overtaken by xDSL, not all useable due to "D Channel" used for call management not data

xDSL Digital subscriber Line uses telephone to transport high bandwidth data to remote subscribers

- **ADSL -** Asymmetric. More downstream bandwidth up to 18,000 feet over single copper cable pair
- **SDSL -** Symmetric up to 10,000 feet over single copper cable pair
- **HDSL -** High Rate T1 speed over two copper cable pairs up to 12,000 feet
- **VDSL -** Very High speed 13-52MBps down, 1,5-2,3 Mbps upstream over a single copper pair over 1,00 to 4500 feet

Circuit-switched networks

There must be a dedicated physical circuit path exist during transmission. The right choice for networks that have to communicate constantly. Typically for a telephone company network Voice oriented. Sensitive to loss of connection

Message switching networks

Involves the transmission of messages from node-to-node. Messages are stored on the network until a forwarding path is available.

Packet-switched networks (PSN or PSDN)

Nodes share bandwidth with each other by sending small data units called packets. Packets will be send to the other network and reassembled. Data oriented. Sensitive to loss of data. More cost effective than circuit switching because it creates virtual circuits only when they are needed.

Converged Protocols (406)

Converged Protocols - are the merging of specialty or proprietary protocols with standard protocols, such as those from the TCP/ IP suite. The primary benefit of converged protocols is the ability to use existing TCP/ IP supporting network infrastructure to host special or proprietary services without the need for unique deployments of alternate networking hardware.

Fibre Channel over Ethernet (FCoE) - a form of network data-storage solution (SAN or NAS) that allows for high-speed file transfers at upward of 16 GBps. It was designed to be operated over fiber-optic cables; support for copper cables was added later to offer less-expensive options. Fibre Channel over Ethernet (FCoE) can be used to support it over the existing network infrastructure. FCoE is used to encapsulate Fibre Channel communications over Ethernet networks. Fibre Channel operates as a Network layer or OSI layer 3 protocol, replacing IP as the payload of a standard Ethernet network.

MPLS - (Multiprotocol Label Switching) is a high-throughput high-performance network technology that directs data across a network based on short path labels rather than longer network addresses. MPLS is designed to handle a wide range of protocols through encapsulation.

iSCSI - Internet Small Computer System Interface (iSCSI) is a networking storage standard based on IP. This technology can be used to enable location-independent file storage, transmission, and retrieval over LAN, WAN, or public Internet connections.

It is often viewed as a low-cost alternative to Fibre Channel.

VoIP - Voice over IP - a tunneling mechanism used to transport voice and/ or data over a TCP/ IP network. VoIP has the potential to replace or supplant PSTN because it's often less expensive and offers a wider variety of options and features.

SDN - a unique approach to network operation, design, and management. SDN aims at separating the infrastructure layer (i.e., hardware and hardware-based settings) from the control layer (i.e., network services of data transmission management). Furthermore, this also removes the traditional networking concepts of IP addressing, subnets, routing, and so on from needing to be programmed into or be deciphered by hosted applications. SDN offers a new network design that is directly programmable from a central location, is flexible, is vendor neutral, and is open-standards based.

Domain 5 – Identity and Access Management

Access Control (440)

ACCESS - is flow of information between a subject and an object
CONTROL - security features that control how users and systems communicate and interact with other systems and resources
Subject - active entity that requests access to an object or data within the object (user, program)
Object - is a passive entity that contains information (computer, database, file, program) access control techniques support the access control models

Approaches to Administration (441)

Centralized administration – one element responsible for configuring access controls. Only modified through central administration, very strict control,
Decentralized administration – access to information is controlled by owners or creators of information, may not be consistency with regards to procedures, difficult to form system wide view of all user access at any given time
Hybrid – centralized control is exercised for some information and decentralized for other information

Identity Management (448)

IAAA - Four key principles upon which access control relies
- **Identification/Assertion -**
  - **Registration –** verify an individual's identity and adds a unique identifier to an identity system
  - ensuring that a subject is who he says he is
  - bind a user to the appropriate controls based on the unique user instance
  - Unique user name, account number etc. OR an issuance (keycard)
- **Authentication -**
  - Process of Verifying the user
  - User provides private data
  - Establish trust between the user and the system for the allocation of privileges
- **Authorization –**
  - resources user is allowed to access must be defined and monitored
  - First piece of credentials Authorization
- **Accountability –** who was responsible for an action?
  - **Logging –** best way to provide accountability, change log for approved changes and change management process

Relationship between Identity, Authentication, and Authorization
- Identification provides uniqueness
- Authentication provides validity
- Authorization provides control

Logical Access Controls: tools used for IAAA
MAC Address – 48 bit number, supposed to be globally unique, but now can be changed by software, not a strong ID or auth. Tool

Single Sign On (SSO) (462)

SSO referred to as reduced sign-on or federated ID management
Advantage - ability to use stronger passwords, easier administration, less time to access resources.
Disadvantage - once a key is compromised all resources can be accessed, if Db compromised all PWs compromised
Thin client is also a single sign on approach

KERBEROS (463)

Guards a network with three elements: authentication, authorization, & auditing. **SYMMETRIC KEYS**
Kerberos addresses Confidentiality and integrity and authentication, not availability, can be combined with other SSO solutions
Kerberos Is based on symmetric key cryptology (and is not a propriety control)
Time synchronization is critical, 5 minutes is bad
MIT project Athena
AES from user to KDC, encrypted key, time stamped TGT and hash of PW, install TGT and decrypt key
Kerberos is included in windows now (replaced NTLM=NT-LAN Manager)
Passwords are never exchanged only hashes of passwords
Benefits: inexpensive, loads of OS's, mature protocol
Disadvantage: takes time to administer, can be bottleneck or single point of failure
Realm - indicates an authentication administrative domain. Its intention is to establish the boundaries within which an authentication server has the authority to authenticate a user, host or service.
Uses symmetric Key cryptography
- **KDC -** Key Distribution Center, grants tickets to client for specific servers. Knows all secret keys of all clients and servers from the network, TGS and AS, single point of failure
- **AS** (Authentication server)
- **TGS -** Ticket granting server

The Kerberos logon process works as follows:
- The user types a username and password into the client.
- The client encrypts the username with AES for trans. to the KDC.
- The KDC verifies the username against a database of known credentials.
- The KDC generates a symmetric key that will be used by the client and the Kerberos server. It encrypts this with a hash of the user's password. The KDC also generates an encrypted time-stamped TGT. The KDC then transmits the encrypted symmetric key and the encrypted time-stamped TGT to the client.
- The client installs the TGT for use until it expires. The client also decrypts the symmetric key using a hash of the user's password.
- Then the user can use this ticket to service to use the service as an application service

SESAME
- Public Key Cryptology
- European
- Needham-Schroeder protocol

Weakness: only authenticates the first block and not the complete message
Two tickets:
- One authentication, like Kerberos
- Other defines the access privileges a user has
- Works with PACS (Privileged Attribute Certificates)
- sesame uses both symmetric as asymmetric encryption (thus improvement upon Kerberos)

KRYPTOKNIGHT - IBM – thus RACF
Peer-to-peer relationship between KDC and parties
SCRIPTING - scripts contain logon information that auths. users
DIRECTORY SERVICE - a centralized database that includes information about subjects and objects, .Hierarchical naming schema, active directory has sophisticated security resources (group policy, user rights accounts, DNS services)

Single/Multiple Factor Authentication (467)

Type 1 - authentication factor is something you know. Examples include a password, PIN, or passphrase.
Type 2 - authentication factor is something you have. Physical devices that a user possesses can help them provide authentication. Examples include a smartcard (CAC), hardware token, smartcard, memory card, or USB drive.
Type 3 - authentication factor is something you are or something you do. It is a physical characteristic of a person identified with different types of biometrics.

Something a user knows TYPE 1

PASSWORDS
cheap and commonly used
password generators
user chooses own (do triviality and policy checking)
Longer PW more effective than all else
PWs never stored for web applications in a well-designed environment. Salted hashes are stored and compared
62 choices (upper, lower, 10 numbers), add single character to PW and complexity goes up 62X
One-time password aka dynamic password used only once
Static password Same for each logon
Passphrase easiest to remember. Converted to a virtual password by the system.
Cognitive password: easy to remember like your mother's maiden name
Hacking - access password file
brute force attack - (try many different characters) aka exhaustive
dictionary attack - (try many different words)
Social engineering - convince an individual to give access
Rainbow Tables - (tables with passwords that are already in hash format, pre-hashed PW paired with high-speed look up functions
Implementation Attack - This is a type of attack that exploits weaknesses in the implementation of a cryptography system. It focuses on exploiting the software code, not just errors and flaws but the methodology employed to program the encryption system
Statistical Attack - exploits statistical weaknesses in a cryptosystem, such as floating-point errors and inability to produce truly random numbers. Statistical attacks attempt to find a vulnerability in the hardware or operating system hosting the cryptography application.
password checker and password hacker - both programs that can find passwords (checker to see if its compliant, hacker to use it by the hacker)
hashing and encryption
- On windows system with utility SYSKEY. The hashed passwords will be encrypted in their store LM hash and NT Hash
- some OS's use Seed SALT or NONCE, random values added to the encryption process to add more complexity
- **HAVAL -** Hash of Variable Length (HAVAL) is a modification of MD5. HAVAL uses 1,024-bit blocks and produces hash values of 128, 160, 192, 224, and 256 bits. Not a encryption algorithm

Domain 5 – Identity and Access Management

Something a user has TYPE 2

Key, swipe card, access card, badge, tokens

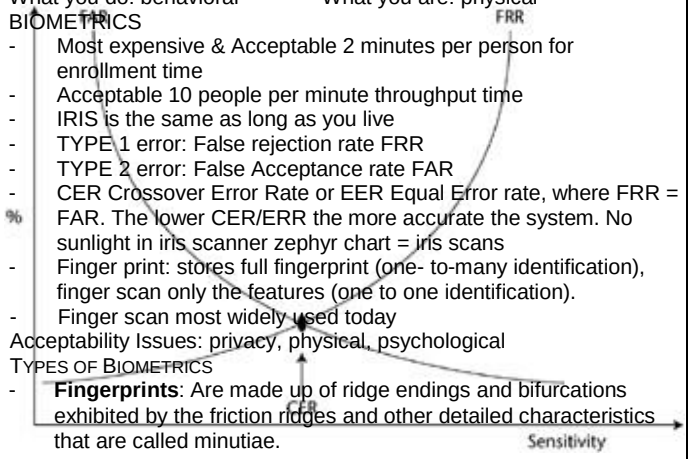
Static password token - owner authenticates to token, token authenticates to the information system
Synchronous (TIME BASED) dynamic - uses time or a counter between the token and the authentication server, secure-ID is an example
Asynchronous (NOT TIME BASED) - server sends a nonce (random value) This goes into token device, encrypts and delivers a one-time password, with an added PIN its strong authentication
Challenge/response token - generates response on a system/workstation provided challenge; synchronous – timing, asynchronous - challenge

Something a user is TYPE 3

What you do: behavioral What you are: physical
BIOMETRICS

- Most expensive & Acceptable 2 minutes per person for enrollment time
- Acceptable 10 people per minute throughput time
- IRIS is the same as long as you live
- TYPE 1 error: False rejection rate FRR
- TYPE 2 error: False Acceptance rate FAR
- CER Crossover Error Rate or EER Equal Error rate, where FRR = FAR. The lower CER/ERR the more accurate the system. No sunlight in iris scanner zephyr chart = iris scans
- Finger print: stores full fingerprint (one- to-many identification), finger scan only the features (one to one identification).
- Finger scan most widely used today

Acceptability Issues: privacy, physical, psychological



TYPES OF BIOMETRICS

- **Fingerprints**: Are made up of ridge endings and bifurcations exhibited by the friction ridges and other detailed characteristics that are called minutiae.
- **Retina Scans:** Scans the blood-vessel pattern of the retina on the backside of the eyeball. Can show medical conditions MOST ACCURATE
- **Iris Scans:** Scan the colored portion of the eye that surrounds the pupil.
- **Facial Scans:** Takes attributes and characteristics like bone structures, nose ridges, eye widths, forehead sizes and chin shapes into account.
- **Palm Scans:** The palm has creases, ridges and grooves throughout it that are unique to a specific person. Appropriate by itself as a Type 3 authenticator
- **Hand Geometry:** The shape of a person's hand (the length and width of the hand and fingers) measures hand geometry.
- **Voice Print:** Distinguishing differences in people's speech sounds and patterns.
- **Signature Dynamics:** Electrical signals of speed and time that can be captured when a person writes a signature.
- **Keyboard Dynamics:** Captures the electrical signals when a person types a certain phrase.
- **Hand Topology:** Looks at the size and width of an individual's hand and fingers.

SAML (478) (SOAP/XML)

To exchange authentication and authorization data between security domains.
SAML 2.0 enables web-based to include SSO
Roles

- Principal (user)
- Identity provider (IdP)
- Service provider (SP)

Most used federated SSO
XML Signature – use digital signatures for authentication and message integrity based on XML signature standard.
Relies on XML Schema

Identity as a Service (IDaaS) (486)

IDaaS - Identity as a Service, or Identity and Access as a Service is a third-party service that provides identity and access management, Effectively provides SSO for the cloud and is especially useful when internal clients access cloud-based Software as a Service (SaaS) applications.

- Ability to provision identities held by the service to target applications
- Access includes user authentication, SSO, authorization enforcement
- Log events , auditing
- **Federation -** sharing identity and authentication behind the scenes (like booking flight --> booking hotel without re authenticating) by using a federate identity so used across business boundaries
- SSO
- Access Management enforces RULES!

Manage User Accounts within a Cloud (492)

Cloud Identity – users are created and managed in Office 365
Directory Synchronization – users are created and managed in an on premises identity provider
Federated Identity – on-premises identity provider handles login request. Usually used to implement SSO

- MS AD using MS AD Federation Services
- Third Party based identity
- Shibboleth SAML 2.0

Authorization Mechanisms (496)

The method of authorizing subjects to access objects varies depending on the access control method used by the IT system.
A subject is an active entity that accesses a passive object and an object is a passive entity that provides information to active subjects.
There are several categories for access control techniques and the CISSP CIB specifically mentions four: discretionary access control (DAC), mandatory access control (MAC), role-based access control (role-BAC), and rule-based access control (rule-BAC).

Windows uses Kerberos for authentication. RADIUS is typically used for wireless networks, modems, and network devices, while OAuth is primarily used for web applications. TACACS+ is used for network devices.

Authorization Mechanisms (496)

Role-BAC (RBAC) - task-based access controls define a subject's ability to access an object based on the subject's role or assigned tasks, is often implemented using groups, form of nondiscretionary. OFF BUSINESS DESIGN
Hybrid RBAC
Limited RBAC
CAN MODEL ALL GROUPS OFF ORGANIZATION #! USED
Rule-BAC – based on rules within an ACL, uses a set of rules, restrictions, or filters to determine what can and cannot occur on a system. It includes granting a subject access to an object, or granting the subject the ability to perform an action. A distinctive characteristic about rule-BAC models is that they have global rules that apply to all subjects. One common example of a rule-BAC model is a **firewall**. Firewalls include a set of rules or filters within an ACL, defined by an administrator. The firewall examines all the traffic going through it and only allows traffic that meets one of the rules. Government #1
Mandatory Access Control BELL Model!
Lattice based, **Label** – all **objects and subjects** have a label
Authorization depended on security labels which indicate **clearance** and classification of objects (**M**ilitary). Restriction: need to know can apply. Lattice based is part of it! (A as in mAndatory!). Rule based access control. Objects are: files, directories and devices;
Non-discretionary access control / Mandatory
A central authority determines what subjects have access based on policies. Role based/task based. Also lattice based can be applied (greatest lower, least upper bounds apply)
Discretionary Access Control – Graham Denning
Access through ACL's. Discretionary can also mean: Controlled access protection (object reuse, protect audit trail). User directed
Performs all of IAAA, identity based access control model

- hierarchical x500 standard protocol like LDAP for allowing subjects to interact with the directory
- Organized through name spaces (Through Distinguished names)
- Needs client software to interact
- META directory gathers information from multiple sources and stores them into once central directory and synchronizes
- VIRTUAL directory only points where the data resides

DACs allows the owner, creator, or data custodian of an object to control and define access to that object. All objects have owners, and access control is based on the discretion or decision of the owner. As the owner, the user can modify the permissions of the file to grant or deny access to other users. Identity-based access control is a subset of DAC because systems identify users based on their identity and assign resource ownership to identities. A DAC model is implemented using access control lists (ACLs) on objects. Each ACL defines the types of access granted or denied to subjects. It does not offer a centrally controlled management system because owners can alter the ACLs on their objects at will. Access to objects is easy to change, especially when compared to the static nature of mandatory access controls.

Domain 5 – Identity and Access Management

Access Control Models () ?

Access control models use many different types of authorization mechanisms, or methods, to control who can access specific objects.
Implicit Deny - basic principle that most authorization mechanisms use it. The implicit deny principle ensures that access to an object is denied unless access has been explicitly granted to a subject.
Access Control Matrix - An access control matrix is a table that includes subjects, objects, and assigned privileges. When a subject attempts an action, the system checks the access control matrix to determine if the subject has the appropriate privileges to perform the action
Capability Tables - They are different from ACLs in that a capability table is focused on subjects (such as users, groups, or roles). For example, a capability table created for the accounting role will include a list of all objects that the accounting role can access and will include the specific privileges assigned to the accounting role for these objects.
The difference between an ACL and a capability table is the focus. ACLs are object focused and identify access granted to subjects for any specific object. Capability tables are subject focused and identify the objects that subjects can access.
Comparing Permissions, Rights, and Privileges When studying access control topics, you'll often come across the terms permissions, rights, and privileges. Some people use these terms interchangeably, but they don't always mean the same thing.
Permissions - refer to the access granted for an object and determine what you can do with it. If you have read permission for a file, you'll be able to open it and read it. You can grant user permissions to create, read, edit, or delete a file on a file server. Similarly, you can grant user access rights to a file, so in this context, access rights and permissions are synonymous
Rights - refers to the ability to take an action on an object. For example, a user might have the right to modify the system time on a computer or the right to restore backed-up data. This is a subtle distinction and not always stressed. You'll rarely see the right to take action on a system referred to as a permission.
Privileges - are the combination of rights and permissions. For example, an administrator for a computer will have full privileges, granting the administrator full rights and permissions on the computer. The administrator will be able to perform any actions and access any data on the computer.

Understanding Authorization Mechanisms

Access control models use many different types of authorization mechanisms, or methods, to control who can access specific objects.
Constrained Interface Applications – (restricted interfaces) to restrict what users can do or see based on their privileges. Applications constrain the interface using different methods. A common method is to hide the capability if the user doesn't have permissions to use it. Other times, the application displays the menu item but shows it dimmed or disabled.
Content-Dependent – internal data of each field, data stored by a field, restrict access to data based on the content within an object. A database view is a content-dependent control. A view retrieves specific columns from one or more tables, creating a virtual table.
Context-Dependent - require specific activity before granting users access. For example, it's possible to restrict access to computers and applications based on the current day and/ or time. If users attempt to access the resource outside of the allowed time, the system denies them access.
Work Hours – context-dependent control
Need to Know - ensures that subjects are granted access only to what they need to know for their work tasks and job functions. Subjects may have clearance to access classified or restricted data but are not granted authorization to the data unless they actually need it to perform a job.
Least Privilege - ensures that subjects are granted only the privileges they need to perform their work tasks and job functions. This is sometimes lumped together with need to know. The only difference is that least privilege will also include rights to take action on a system.
Separation of Duties and Responsibilities - ensures that sensitive functions are split into tasks performed by two or more employees. It helps to prevent fraud and errors by creating a system of checks and balances.

Service Provisioning Markup Language, or SPML is an XML-based language designed to allow platforms to generate and respond to provisioning requests. SAML is used to make authorization and authentication data, while XACML is used to describe access controls. SOAP, or Simple Object Access Protocol, is a messaging protocol and could be used for any XML messaging, but is not a markup language itself.

Reconnaissance Attacks (506)

While malicious code often relies on tricking users into opening or accessing malware, other attacks directly target machines. Performing reconnaissance can allow an attacker to find weak points to target directly with their attack code. To assist with this targeting, attacker-tool developers have created a number of automated tools that perform network reconnaissance.
IP Probes - (also called IP sweeps or ping sweeps) are often the first type of network reconnaissance carried out against a targeted network. With this technique, automated tools simply attempt to ping each address in a range. Systems that respond to the ping request are logged for further analysis. Addresses that do not produce a response are assumed to be unused and are ignored.
Nmap tool - one of the most common tools used to perform both IP probes and port scans. IP probes are extremely prevalent on the Internet today. Indeed, if you configure a system with a public IP address and connect it to the Internet, you'll probably receive at least one IP probe within hours of booting up. The widespread use of this technique makes a strong case for disabling ping functionality, at least for users external to a network. Default settings miss @64 K ports
When nmap scans a system, it identifies the current state of each network port on the system. For ports where nmap detects a result, it provides the current status of that port:

- **Open -** The port is open on the remote system and there is an application that is actively accepting connections on that port.
- **Closed -** The port is accessible on the remote system, meaning that the firewall is allowing access, but there is no application accepting connections on that port.

Filtered Nmap - is unable to determine whether a port is open or closed because a firewall is interfering with the connection attempt
Port Scans - After an attacker performs an IP probe, they are left with a list of active systems on a given network. The next task is to select one or more systems to target with additional attacks. Often, attackers have a type of target in mind; web servers, file servers, and other servers supporting critical operations are prime targets. To narrow down their search, attackers use port scan software to probe all the active systems on a network and determine what public services are running on each machine. For example, if the attacker wants to target a web server, they might run a port scan to locate any systems with a service running on port 80, the default port for HTTP services.
Vulnerability Scans - The third technique is the vulnerability scan. Once the attacker determines a specific system to target, they need to discover a specific vulnerability in that system that can be exploited to gain the desired access permissions. A variety of tools available on the Internet assist with this task. Some of the more popular tools for this purpose include Nessus, OpenVAS, Qualys, Core Impact, and Nexpose. These packages contain a database of known vulnerabilities and probe targeted systems to locate security flaws. They then produce very attractive reports that detail every vulnerability detected. From that point, it's simply a matter of locating a script that exploits a specific vulnerability and launching an attack against the victim.

Domain 6 - Security Assessment and Testing

Security Testing (522)

Security Testing - verifies that a control is functioning properly. These tests include automated scans, tool-assisted penetration tests and manual attempts to undermine security. When scheduling security controls for review, information security managers should consider the following factors:

- Availability of security testing resources
- Criticality of the systems and applications protected by the tested controls Sensitivity of information contained on tested systems and applications
- Likelihood of a technical failure of the mechanism implementing the control
- Likelihood of a misconfiguration of the control that would jeopardize security
- Risk that the system will come under attack
- Rate of change of the control configuration
- Other changes in the technical environment that may affect the control performance
- Difficulty and time required to perform a control test
- Impact of the test on normal business operations

After assessing each of these factors, security teams design and validate a comprehensive assessment and testing strategy.

Verification & Validation (523)

Verification – objective evidence that the design outputs of a phase of the SDLC meet requirements. 3rd party sometimes
Validation – develop "level of confidence" that the software meets all requirements and expectations, software improve over time
Find back doors thru structured walk through

Logs (530)

Network Flow – captured to provide insight into network traffic for security, troubleshooting, and performance management

Audit logging – provides information about events on the routers

NTP - Network Time Protocol, One important consideration is ensuring that logs have accurate time stamps and that these time stamps remain consistent throughout the environment. A common method is to set up an internal NTP server that is synchronized to a trusted time source such as a public NTP server. Other systems can then synchronize with this internal NTP server.

Syslog – message logging standard commonly used by network devices, Linux and Unix systems and other devices (firewalls)
Reboot – generates an information log entry

- Errors – significant problem
- Warnings – future problem
- Information – successful operations
- Success Audits – successful security accesses
- Failure Audits – failed security access attempts

Inconsistent Time Stamps – often caused by improperly set time zones or due to differences in how system clocks are set

Modified logs – often a sign of intrusion or malicious intent
NetFlow is a feature that was introduced on Cisco routers that provides the ability to collect IP network traffic as it enters or exits an interface. a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion.

Security Software (534)

Antimalware and Antivirus – records instances of detected malware,
IDS/IPS = security testing, NIST 800-4
War driving - driving a car with notebook to find open access points
IDS intrusion detection system
NETWORK BASED

- Detects intrusions on the LAN behind a firewall.
- Is passive while it acquires data.
- Reviews packets and headers
- Problem with network based is that it will not detect attacks by users logged into hosts

HOST BASED

- monitoring servers through EVENT LOGS AND SYSTEM LOGS
- as good as the completeness of the host logging

easier to discover and disable
Signature based method (AKA Knowledge based) - compared with signature attack database (aka misuse detector)
Statistical anomaly based - defines a 'normal' behavior and detects abnormal behaviors.
Response box - is a part of an IDS that initiates alarm or activity
Components: Information source/sensor, centralized monitor software, data and even report analysis, database components and response to an event or intrusion
IPS Intrusion prevention system - detect attack and PREVENT that attack being successful
Remote Access Software – granted and secured through VPNs
Web Proxies – intermediate hosts, restrict access
Vulnerability Management Software – patching
Authentication Servers – SSO servers
Routers – permit or block traffic based on policy
Firewalls – more sophisticated than routers to examine traffic

Monitoring and auditing (537)

Companies can set predefined thresholds for the number of certain types of errors that will be allowed before the activity is considered suspicious. This baseline is referred to as **clipping level**

Audit trails

- Transaction date/time
- Who processed the transaction
- At which terminal

Protecting Logs (538)

Breaches – protect from breaches of confidentiality and integrity.
Availability – archival process to prevent loss by overwritten logs
Log Analysis – study logs for events of interest
Set maximum size. If too small, attacker can make little changes and push them out of window

Synthetic Transactions (540)

Real User Monitoring – aims to capture and analyze every transaction of a user
Synthetic Performance Monitoring – uses scripted or recorded data. Traffic capture, Db performance monitoring, website performance monitoring can be used. NOT User Session Monitoring
Types

- Proactive monitoring involves having external agents run scripted transactions against a web application
- Db monitoring; availability of Db
- TCP port monitoring; availability of website, service, or application

Code Review and Testing (542)

Code review is the foundation of software assessment programs. During a code review, also known as a "peer review," developers other than the one who wrote the code review it for defects.
The most formal code review processes, known as Fagan inspections, follow a rigorous review and testing process with six steps:

- Planning
- Overview
- Preparation
- Inspection
- Rework
- Follow-up

Code Coverage Report – information on the functions, statements, branches, and conditions covered in testing.
Use cases – used as part of test coverage calculation that divides the tested use case by total use cases

Code Review Report – generated if the organization was manually reviewing the application's source code

- **Black-box testing** observes the system external behavior, no internal details known
- **Dynamic Testing –** does not require access to source code, evaluates code in a runtime environment
- **White-box testing** (crystal) is a detailed exam of a logical path, checking the possible conditions. Requires access to source code
- **Static Testing –** requires access to source code, performs code analysis
- **CSV –** Comma Separated Values
- **CVE -** Common Vulnerability and Exposures dictionary. The CVE dictionary provides a standard convention used to identify vulnerabilities, list by MITRE
- **CVSS –** Common Vulnerability Scoring System, metrics and calculation tools for exploitability, impact, how mature exploit code is, and how vulnerabilities can be remediated, also to score vulnerabilities against unique requirements.
- **NVD –** National Vulnerability Db
- **Compiled code** poses more risk than interpreted code because malicious code can be embedded in the compiled code and can be difficult to detect.
- **Regression testing** is the verification that what is being installed does not affect any portion of the application system already installed. It generally requires the support of automated process to repeat tests previously undertaken. Known inputs against an application then compares results to earlier version results
- **nonRegression testing –** code works as planned
- **Code comparison** is normally used to identify the parts of the source code that have changed.
- **Integration testing** is aimed at finding bugs in the relationship and interfaces between pairs of components. It does not normally test all functions.
- **Attack surface -** exposure

Domain 6 – Security Assessment and Testing

Threat Assessment Modeling (544)?

STRIDE - is often used in relation to assessing threats against applications or operating systems, threat categorization scheme, spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

Spoofing - An attack with the goal of gaining access to a target system through the use of a falsified identity. Spoofing can be used against IP addresses, MAC address, usernames, system names, wireless network SSIDs, and other types of logical identification.

Tampering - Any action resulting in the unauthorized changes or manipulation of data, whether in transit or in storage. Tampering is used to falsify communications or alter static information. Such attacks are a violation of integrity as well as availability.

Repudiation -The ability for a user or attacker to deny having performed an action or activity.

Information disclosure - The revelation or distribution of private, confidential, or controlled information to external or unauthorized entities.

Elevation of privilege - An attack where a limited user account is transformed into an account with greater privileges/powers/ access

Key Performance and Risk Indicators (562)

Security managers should also monitor key performance and risk indicators on an ongoing basis. The exact metrics they monitor will vary by organization but may include the following:

- Number of open vulnerabilities
- Time to resolve vulnerabilities
- Number of compromised accounts
- Number of software flaws detected in preproduction scanning & Repeat audit findings
- User attempts to visit known malicious sites

Performing Vulnerability Assessments

Vulnerability scans - automatically probe systems, applications, and networks, looking for weaknesses that may be exploited
Network discovery scanning - uses a variety of techniques to scan a range of IP addresses, searching for systems with open ports.

TCP SYN Scanning - Sends a single packet to each scanned port with the SYN flag set. This indicates a request to open a new connection. If the scanner receives a response that has the SYN and ACK flags set, this indicates that the system is moving to the second phase in the three-way TCP handshake and that the port is open. TCP SYN scanning is also known as "half-open" scanning.

TCP Connect Scanning - Opens a full connection to the remote system on the specified port. This scan type is used when the user running the scan does not have the necessary permissions to run a half-open scan.

TCP ACK Scanning - Sends a packet with the ACK flag set, indicating that it is part of an open connection.

Xmas Scanning - Sends a packet with the FIN, PSH, and URG flags set. A packet with so many flags set is said to be "lit up like a Christmas tree," leading to the scan's name.

Passive Scanning – user scan wireless to look for rogue devices in addition to IDS

Bluetooth Scans – time consuming, many personal devices

- Active; strength of PIN, security mode
- Passive; only active connections, multiple visits

Authenticated scans – read-only account to access config files

Testing Software (549)

Static Testing - evaluates the security of software without running it by analyzing either the source code or the compiled application. Static analysis usually involves the use of automated tools designed to detect common software flaws, such as buffer overflows.

Dynamic Testing - evaluates the security of software in a runtime environment and is often the only option for organizations deploying applications written by someone else. In those cases, testers often do not have access to the underlying source code. One common example of dynamic software testing is the use of web application scanning tools to detect the presence of cross-site scripting, SQL injection, or other flaws in web applications. Testing may include the use of synthetic transactions to verify system performance.

Fuzz Testing - is a specialized dynamic testing technique that provides many different types of input to software to stress its limits and find previously undetected flaws. Fuzz testing software supplies invalid input to the software, either randomly generated or specially crafted to trigger known software vulnerabilities. Often limited to simple errors, does find important, exploitable issues, don't fully cover code

Mutation (Dumb) Fuzzing - Takes previous input values from actual operation of the software and manipulates (or mutates) it to create fuzzed input. It might alter the characters of the content, append strings to the end of the content, or perform other data manipulation techniques.

Generational (Intelligent) Fuzzing - develops inputs based on models of expected inputs to perform the same task. The zzuf tool automates the process of mutation fuzzing by manipulating input according to user specifications.

Misuse Case testing - Software testers use this process or abuse case testing to evaluate the vulnerability of their software to known risks.

Misuse Case diagrams – threats and mitigate

Test Coverage Analysis - method used to assess how well software testing covered the potential use of an application

Interface testing - is an important part of the development of complex software systems. In many cases, multiple teams of developers work on different parts of a complex application that must function together to meet business objectives. The handoffs between these separately developed modules use well-defined interfaces so that the teams may work independently. Interface testing assesses the performance of modules against the interface specifications to ensure that they will work together properly when all of the development efforts are complete.

- **Application Programming Interfaces (APIs) -** Offer a standardized way for code modules to interact and may be exposed to the outside world through web services. Developers must test APIs to ensure that they enforce all security requirements.
- **User Interfaces (UIs) -** Examples include graphic user interfaces (GUIs) and command-line interfaces. UIs provide end users with the ability to interact with the software. Interface tests should include reviews of all user interfaces to verify that they function properly.

Physical Interfaces - Exist in some applications that manipulate machinery, logic controllers, or other objects in the physical world. Software testers should pay careful attention to physical interfaces because of the potential consequences if they fail.

Levels of Development Testing (550)

Unit testing - testing small piece of software during a development stage by developers and quality assurance, ensures quality units are furnished for integration into final product

Integration level testing – focus on transfer of data and control across a programs interfaces

Integration level testing – focus on transfer of data and control across a programs interfaces

System level testing – demonstrates that all specified functionality exists and that the software product is trustworthy

Things to Know

SAS 70 – outdated 2011, based on ISAE 3402

SOC Reports - service organization control report. (569)

- SOC-1 report, covers only internal controls over financial reporting. SSAE 16 is the same most common synonym
  SOC 1 - Finances
- SOC-2 (design and operational effectiveness) If you want to verify the security, integrity, privacy, and availability controls, in detail for business partners, auditors @security
- SOC-3 report; shared with broad community, website seal, support organizations claims about their ability to provide CIA
  Type 1 – point in time covering design
  Type 2 – period of time covering design and operating effectiveness

Passive monitoring only works after issues have occurred because it requires actual traffic

Log Management System – volume of log data, network bandwidth, security of data, and amount of effort to analyze. NOT enough log sources

OPSEC process - Understanding your day-to-day operations from the viewpoint of a competitor, enemy, or hacker and then developing and applying countermeasures.

Pen-test – testing of network security as would a hacker do to find vulnerabilities. Always get management approval first

Port scanner - program that attempts to determine whether any of a range of ports is open on a particular computer or device

Ring zero - inner code of the operating system. Reserved for privileged instructions by the OS itself

War dialer - dials a range of phone numbers as in the movie wargames

Superzapping - system utility or application that bypasses all access controls and audit/logging functions to make updates to code or data

Operational assurance – Verification that a system is operating according to its security requirements

- Design & development reviews
- Formal modeling
- Security architecture
- ISO 9000 quality techniques
- Assurance – degree of confidence that the implemented security measures work as intended

Piggybacking - when an unauthorized person goes through a door behind an authorized person.

Tailgating – authorized person circumventing controls

Supervisor mode - processes running in inner protected ring

Domain 7 – Security Operations

Incident Scene (581)

- ID the Scene
- Protect the environment
- ID evidence and potential sources of evidence
- Collect evidence – hash +
- Minimize the degree of contamination

Locard's Exchange Principle – perps leave something behind

Evidence (581)

Sufficient –persuasive enough to convince one of its validity
Reliable –consistent with fact, evidence has not been tampered with or modified
Relevant –relationship to the findings must be reasonable and sensible, Proof of crime, documentation of events, proof of acts and methods used, motive proof, identification of acts
Permissible – lawful obtaining of evidence, avoid: unlawful search and seizure, secret recording, privacy violations, forced confessions, unlawful obtaining of evidence
Preserved and identifiable – collection, reconstruction
Identification labeling, recording serial number etc**.**
Evidence must be preserved and identifiable
•Collection, documentation, classification, comparison, reconstruction
EVIDENCE LIFECYCLE

1. *Discovery*
2. *Protection*
3. *Recording*
4. *Collection and identification*
5. *Analysis*
6. *Storage, preservation, transportation*
7. *Present in court*
8. *Return to owner*

Witnesses that evidence is trustworthy, description of procedures, normal business methods collections, error precaution and correction

Live evidence (582)

Best Evidence:
–Primary Evidence–is used at the trial because it is the most reliable.
–Original documents–are used to document things such as contracts – NOTE: no copies!
–Note: Oral is not best evidence though it may provide interpretation of documents, etc.
Secondary Evidence
–Not as strong as best evidence.
–A copy, Secondary Evidence, is not permitted if the original, Best Evidence, is available –Copies of documents.
–Oral evidence like Witness testimony
Direct Evidence:
–Can prove fact by itself and does not need any type of backup.
–Testimony from a witness –one of their 5 senses:
•Oral Evidence is a type of Secondary Evidence so the case can't simply stand on it alone
But it is Direct Evidence and does not need other evidence to substantiate

Live evidence (582) (cont)

Conclusive evidence
–Irrefutable and cannot be contradicted
–Requires no other corroboration
Circumstantial evidence
–Used to help assume another fact
–Cannot stand on its own to directly prove a fact
Corroborative Evidence:
–Supports or substantiates other evidence presented in a case
Hearsay Evidence something a witness hears another one say. Also business records are hearsay and all that's printed or displayed. One exception to business records: audit trails and business records are not considered hearsay when the documents are created in the normal course of business.

Interviewing and Interrogation (584)

Interviewing – gather facts and determine the substance of the case.
Interrogation–Evidence retrieval method, ultimately obtain a confession
The Process - Due Process
–Prepare questions and topics, put witness at ease, summarize information –interview/interrogation plan
–Have one person as lead and 1-2 others involved as well
–never interrogate or interview alone

Witnesses

Opinion Rule
–Requires witnesses to testify only about the facts of the case, cannot be used as evidence in the case.
Expert Witnesses
–Used to educate the jury, can be used as evidence**.**

Digital Evidence (584)

Six principles to guide digital evidence technicians as they perform media analysis, network analysis, and software analysis in the pursuit of forensically recovered evidence:

- When dealing with digital evidence, all of the general forensic and procedural principles must be applied.
- Upon seizing digital evidence, actions taken should not change that evidence.
- When it is necessary for a person to access original digital evidence, that person should be trained for the purpose.
- All activity relating to the seizure, access, storage, or transfer of digital evidence must be fully documented, preserved, and available for review.
- An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession.
- Any agency that is responsible for seizing, accessing, storing, or transferring digital evidence is responsible for compliance with these principles.

Media analysis - a branch of computer forensic analysis, involves the identification and extraction of information from storage media. This may include the following: Magnetic media (e.g., hard disks, tapes) Optical media (e.g., CDs, DVDs, Blu-ray discs) Memory (e.g., RAM, solid state storage) Techniques used for media analysis may include the recovery of deleted files from unallocated sectors of the physical disk, the live analysis of storage media connected to a computer system (especially useful when examining encrypted media), and the static analysis of forensic images of storage media.
Network Analysis - Forensic investigators are also often interested in the activity that took place over the network during a security incident. Network forensic analysis, therefore, often depends on either prior knowledge that an incident is underway or the use of preexisting security controls that log network activity. These include: Intrusion detection and prevention system logs Network flow data captured by a flow monitoring system Packet captures deliberately collected during an incident Logs from firewalls and other network security devices The task of the network forensic analyst is to collect and correlate information from these disparate sources and produce as comprehensive a picture of network activity as possible.
Software Analysis - Forensic analysts may also be called on to conduct forensic reviews of applications or the activity that takes place within a running application. In some cases, when malicious insiders are suspected, the forensic analyst may be asked to conduct a review of software code, looking for back doors, logic bombs, or other security vulnerabilities. In other cases, forensic analysis may be asked to review and interpret the log files from application or database servers, seeking other signs of malicious activity, such as SQL injection attacks, privilege escalations, or other application attacks.
Hardware/ Embedded Device Analysis - Forensic analysts often must review the contents of hardware and embedded devices. This may include a review of Personal computers & Smartphones

Domain 7 – Security Operations

Evidence (584)

Admissible Evidence

- The evidence must be relevant to determining a fact.
- The fact that the evidence seeks to determine must be material (that is, related) to the case.
- The evidence must be competent, meaning it must have been obtained legally. Evidence that results from an illegal search would be inadmissible because it is not competent.

Digital Forensics (585)

Five rules of evidence:

- Be authentic; evidence tied back to scene
- Be accurate; maintain authenticity and veracity
- Be complete; all evidence collected, for & against view
- Be convincing; clear & easy to understand for jury
- Be admissible; be able to be used in court

Forensic Disk Controller – intercepting and modifying or discarding commands sent to the storage device

- Write Blocking, intercepts write commands sent to the device and prevents them from modifying data on the device
- Return data requested by a read operation
- Returning access-significant information from device
- Reporting errors from device to forensic host

LOGS TAKEN IN THE NORMAL COURSE OF BUSINESS

Investigation (590)

MOM means, opportunity and motive
Determine suspects
Victimology –why certain people are victims of crime and how lifestyle affects the chances that a certain person will fall victim to a crime Investigation
Types

- Operational
- Criminal
- Civil
- eDiscovery

When investigating a hard drive, don't use message digest because it will change the timestamps of the files when the file-system is not set to Read-Only
Slack space on a disk should be inspected for hidden data and should be included in a disk image

Law

Common law - USA, UK Australia Canada (judges)
Civil law - Europe, South America
Islamite and other Religious laws – ME, Africa, Indonesia
USA
3 branches for laws:
Legislative: writing laws (statutory laws).
Executive: enforces laws (administrative laws)
Juridical: Interprets laws (makes common laws out of court decisions)
3 categories
Criminal law – individuals that violate government laws. Punishment mostly imprisonment
Civil law – wrongs against individual or organization that result in a damage or loss. Punishment can include financial penalties. AKA tort law (I'll Sue You!) Jury decides liability
Administrative/Regulatory law – how the industries, organizations and officers have to act. Wrongs can be penalized with imprisonment or financial penalties
Uniform Computer Information Transactions Act (UCITA) - is a federal law that provides a common framework for the conduct of computer-related business transactions. UCITA contains provisions that address software licensing. The terms of UCITA give legal backing to the previously questionable practices of shrink-wrap licensing and click-wrap licensing by giving them status as legally binding contracts.
Computer Crime Laws -3 types of harm

- unauthorized intrusion,
- unauthorized alteration or destruction
- malicious code

Admissible evidence relevant, sufficient, reliable, does not have to be tangible
Hearsay second-hand data not admissible in court
Enticement is the legal action of luring an intruder, like in a honeypot
Entrapment is the illegal act of inducing a crime, the individual had no intent of committing the crime at first
Federal Sentencing Guidelines provides judges and courts procedures on the prevention, detection and reporting

Security incident and event management (SIEM) (595)

- Automating much of the routine work of log review.

Provide real-time analysis of events occurring on systems throughout an organization but don't necessarily scan outgoing traffic.

Intrusion Detection and Prevention (594)

An intrusion occurs when an attacker is able to bypass or thwart security mechanisms and gain access to an organization's resources. Intrusion detection is a specific form of monitoring that monitors recorded information and real-time events to detect abnormal activity indicating a potential incident or intrusion.
IDS - intrusion detection system automates the inspection of logs and real-time system events to detect intrusion attempts and system failures. IDSs are an effective method of detecting many DoS and DDoS attacks. They can recognize attacks that come from external connections, such as an attack from the Internet, and attacks that spread internally such as a malicious worm. Once they detect a suspicious event, they respond by sending alerts or raising alarms. In some cases, they can modify the environment to stop an attack. A primary goal of an IDS is to provide a means for a timely and accurate response to intrusions. An IDS is intended as part of a defense-in-depth security plan. It will work with, and complement, other security mechanisms such as firewalls, but it does not replace them.
IPS - intrusion prevention system includes all the capabilities of an IDS but can also take additional steps to stop or prevent intrusions. If desired, administrators can disable these extra features of an IPS, essentially causing it to function as an IDS.

DLP (597) Data Loss Prevention

PROTECT SENSITIVE INFORMATION

Data loss prevention systems attempt to detect and block data exfiltration attempts. These systems have the capability of scanning data looking for keywords and data patterns.
Network-based DLP - scans all outgoing data looking for specific data. Administrators would place it on the edge of the negative to scan all data leaving the organization. If a user sends out a file containing restricted data, the DLP system will detect it and prevent it from leaving the organization. The DLP system will send an alert, such as an email to an administrator.
Endpoint-based DLP - can scan files stored on a system as well as files sent to external devices, such as printers. For example, an organization endpoint-based DLP can prevent users from copying sensitive data to USB flash drives or sending sensitive data to a printer.

3 states of information

- data at rest (storage)
- data in transit (the network)
- data being processed (must be decrypted) / in use / end-point

Can look for sensitive information stored on hard drives

Domain 7 – Security Operations

Configuration Management (603)

Configuration item (CI) - component whose state is recorded
Version: recorded state of the CI
Configuration - collection of component CI's that make another CI
Building - assembling a version of a CI using component **CI's**
Build list - set of versions of component CI's used to build a
CI Software Library - controlled area only accessible for approved users
ARTIFACTS – CONFIGURATION MANAGEMENT

Recovery procedures (606)

Recovery procedures: system should restart in **secure mode**
Startup should occur in **maintenance mode** that permits access only by privileged users from privileged terminals
Fault-tolerant continues to function despite failure
Fail safe system, program execution is terminated and system protected from compromise when hardware or software failure occurs DOORS usually
Fail Closed/secure – most conservative from a security perspective
Fail Open
Fail Hard – BSOD, human to see why it failed
Fail soft or resilient system, reboot, selected, non-critical processing is terminated when failure occurs
Failover, switches to hot backup.
FAIL SAFE: doors UNLOCK
FAIL SECURE: doors LOCK

Trusted Path (606)

Protect data between users and a security component. Channel established with strict standards to allow necessary communication to occur without exposing the TCB to security vulnerabilities. A trusted path also protects system users (sometimes known as subjects) from compromise as a result of a TCB interchange.
ONLY WAY TO CROSS SECURITY BOUNDARY RIGHT WAY

Incident Response (624)

Events: anything that happens. Can be documented verified and analyzed
Security Incident - event or series of events that adversely impact the ability of an organization to do business
Security incident – suspected attack
Security intrusion – evidence attacker attempted or gained access
Lifecycle - **Response Capability** (policy, procedures, a team), **Incident response and handling** (Triage, investigation, containment, and analysis & tracking), **Recovery** (Recovery / Repair), **Debriefing / Feedback** (External Communications)
Mitigation – limit the effect or scope of an incident

RCA, Root Cause Analysis (632)

Tree / Boolean -FAULT TREE ANALYSIS
- 5Ways
- Failure Mode and Effects analysis
- Pareto Analysis
- Fault Tree Analysis
- Cause Mapping

Firewalls (636)

HIDS - Host-based IDS, monitors activity on a single computer, including process calls and information recorded in firewall logs. It can often examine events in more detail than an NIDS can, and it can pinpoint specific files compromised in an attack. It can also track processes employed by the attacker. A benefit of HIDSs over NIDSs is that HIDSs can detect anomalies on the host system that NIDSs cannot detect.
NIDS - Network-based IDS, monitors and evaluates network activity to detect attacks or event anomalies. It cannot monitor the content of encrypted traffic but can monitor other packet details. A single NIDS can monitor a large network by using remote sensors to collect data at key network locations that send data to a central management console.

Backup types (658)

Full - All files, archive bit and modify bit are cleared. Advantage: only previous day needed for full restore, disadvantage: time consuming
Incremental - only modified files, archive bit cleared, Advantage: least time and space, Disadvantage: first restore full then all incremental backups, thus less reliable because it depends on more components
Differential - only modified files, doesn't clear archive bit. Advantage: full and only last diff needed, Intermediate time between full and diff.
Redundant servers – applies raid 1 mirroring concept to servers. On error servers can do a fail-over. This AKA server fault tolerance
Server clustering – group of independent servers which are managed as a single system. All servers are online and take part in processing service requests.
Individual computing devices on a cluster vs. a grid system – cluster devices all share the same OS and application software but grid devices can have different OSs while still working on same problem

Tape Rotation Schemes – GF/Father/Son, Tower of Hanoi, Six Cartridge Weekly

RAIT – robotic mechanisms to transfer tapes between storage and drive mechanisms

Disaster Processing Continuity plan (659)

Mutual aid agreements (aka reciprocal agreement)
Arrangement with another similar corporation to take over processes. Advantage: cheap. Disadvantage: must be exact the same, is there enough capability, only for short term and what if disaster affects both corporations. Is not enforceable.

Subscription services
Third party, commercial services provide alternate backups and processing facilities. Most common of implementations!
Redundant – Mirrored site, potential 0 down time
HOT SITE – Internal/External, Fully configured computer facility. All applications are installed, up-to-date mirror of the production system. For extremely urgent critical transaction processing. Advantage: 24/7 availability and exclusive use are assured. Short and long term. Disadvantage: extra administrative overhead, costly, security controls needs to be installed at the remote facility too. Exclusive to one company **hours to be up**
WARM SITE - Cross between hot and cold site. The computer facility is available but the applications may not be installed or need to be configured. External connections and other data elements that take long time to order are present. Workstations have to be delivered and data has to be restored. Advantage: Less costly, more choices of location, less administrative resources. Disadvantage: it will take some time to start production processing. Nonexclusive. 12 hours to be up
COLD SITE - Least ready but most commonly used. Has no hardware installed only power and HVAC.
Disadvantage: Very lengthy time of restoration, false sense of security but better than nothing. Advantage: Cost, ease of location choice. Nonexclusive. week
SERVICE BUREAU - Contract with a service bureau to fully provide alternate backup processing services. Advantage: quick response and availability, testing is possible. Disadvantage: expense and it is more of a short time option.

Multiple centers (aka dual sites)
Processing is spread over several computer centers. Can be managed by same corporation (in-house) or with another organization (reciprocal agreement). Advantage: costs, multiple sites will share resources and support. Disadvantage: a major disaster could affect both sites; multiple configurations have to be administered.
Other data center backup alternatives
- **Rolling/mobile sites -** Mobile homes or HVAC trucks. Could be considered a cold site
- **In-house or external -** supply of hardware replacements. Stock of hardware either onsite or with a vendor. May be acceptable for warm site but not for hot site.

Prefabricated buildings - A very cold site.

RTO: recovery time objectives. Refers to business processes not hardware.
RTO 5 minutes or hours⇗ Hot site; RTO 1-2 days ⇗ warm site
RTO 3-5 days ⇗ mobile site; RTO 1tgt-2 weeks ⇗cold site

Domain 7 – Security Operations

Raid Levels (665)

RAID 0 Striped, one large disk out of several –Improved performance but no fault tolerance
RAID 1 Mirrored drives –fault tolerance from disk errors and single disk failure, expensive; **redundancy only, not speed**
RAID 2 not used commercially. Hammering Code Parity/error
RAID 3 Striped on byte level with extra parity drive –Improved performance and fault tolerance, but parity drive is a single point of failure and write intensive. 3 or more drives
RAID4 Same as Raid 3 but striped on block level; 3 or more drives
RAID 5 Striped on block level, parity distributed over all drives – requires all drives but one to be present to operate hot-swappable. Interleave parity, recovery control; 3 or more drives
RAID 6 Dual Parity, parity distributed over all drives –requires all drives but two to be present to operate hot- swappable
RAID 7 is same as raid5 but all drives act as one single virtual disk

Backup storage media

Tape: sequential, slow read, fast write 200GB an hour, historically cheaper than disk (now changing), robotic libraries
Disk fast read/write, less robust than tape
Optical drive: CD/DVD. Inexpensive
Solid state: USB drive, security issues, protected by AES
MTTF (mean time to failure)
MTTR (mean time to repair)
MTBF Mean time between failures (Useful Life) = MTTF + MTTR
JBOD – MOST BASIC TYPE OF STORAGE

Transaction Redundancy Implementations (667)

Electronic vaulting - transfer of backup data to an offsite storage location via communication lines
Remote Journaling - parallel processing of transactions to an alternative site via communication lines
Database shadowing - live processing of remote journaling and creating duplicates of the database sets to multiple servers

Data destruction and reuse (143)

Object reuse - use after initial use
Data remanence - remaining data after erasure
Format magnetic media 7 times (orange book)
Clearing - overwriting media to be reused
Purging - degaussing or overwriting to be removed
Destruction - complete destroy preferably by burning

Disaster Recovery Planning (672)

End Goal - Restore normal business operations.
Statement of actions that have to be taken before, during and after a disruptive event that causes a significant loss of information Goal: provide organized way for decision making, reduce confusion and deal with the crisis. Planning and development must occur before the disaster

BIA has already been done, now were going to protect!

Disaster – any event, natural or manmade, that can disrupt normal IT operations
The disaster is not over until all operations have been returned to their normal location and function
It will be officially over when the data has been verified at the primary site, as accurate

Disaster recovery process (673)

TEAMS
Recovery team mandated to implement recovery after the declaration of the disaster
Salvage team goes back to the primary site to normal processing environmental conditions. Clean, repair, Salvage. Can declare when primary site is available again
Normal Operations Resume plan has all procedures on how the company will return processing from the alternate site
Other recovery issues
Interfacing with other groups: everyone outside the corporation
Employee relations: responsibility towards employees and families
Fraud and Crime: like vandalism, looting and people grabbing the opportunity
Financial disbursement, Media relations
1. Find someone to run it

Documenting the Plan
Activation and recovery procedures
Plan management
HR involvement
Costs
Required documentation
Internal /external communications
Detailed plans by team members

GET COMMUNICATIONS UP FIRST THEN MOST CRITCAL BUSINESS FUNCTIONS

Disaster Recovery Test (679)

Desk Check – review plan contents
Table-top exercise -members of the disaster recovery team gather in a large conference room and role-play a disaster scenario.
Simulation tests - are more comprehensive and may impact one or more noncritical business units of the organization, all support personnel meet in a practice room
Parallel tests - involve relocating personnel to the alternate site and commencing operations there. Critical systems are run at an alternate site, main site open also
Full-interruption tests - involve relocating personnel to the alternate site and shutting down operations at the primary site.

BCP (685)

Plan for emergency response, backup operations and post disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation

BCP (pro) & DRP (reactive)Goals

Business continuity- Ensuring the business can continue in an emergency, 1st business organization analysis

Focus on business processes

1. **Scope and plan initiation** - Consider amount of work required, resources required, management practice
2. **BIA** – helps to understand impact of disruptive processes
3. **Business Continuity Plan development**
    a. Use BIA to develop BCP (strategy development phase bridges the gap between the business impact assessment and the continuity planning phases of BCP development)
    b. Testing
4. **Plan approval and implementation**
    - Management approval
    - Create awareness

Update plan as needed, At least once a year testing

Disaster Recovery – Recover as quickly as possible

- Heavy IT focus
- Allows the execution of the BCP
- Needs Planning
- Needs Testing

CRITICA, URGENT, IMPORTANT

Domain 7 – Security Operations

Business Continuity plans development

- Defining the continuity strategy
- Computing: strategy to preserve the elements of hardware/software/ communication lines/ applications/ data
- Facilities: use of main buildings or any remote facilities
- People: operators, management, technical support persons
- Supplies and equipment: paper, forms HVAC -

Documenting the continuity strategy

Roles and responsibilities

BCP committee

- Senior staff (ultimate responsibility, due care/diligence)
- Various business units (identify and prioritize time critical systems)
- Information Systems
- Security Administrator
- People who will carry out the plan (execute)

representatives from all departments

CCTV (692)

Multiplexer allows multiple camera screens shown over one cable on a monitor
Via coax cables (hence closed)
Attacks: replayed (video images)
Fixed mounting versus PTZ Pan Tilt Zoom
accunicator system (detects movements on screen and alerts guards)
Recording (for later review) = detective control
CCTV enables you to compare the audit trails and access logs with a visual recording

Lightning (694)

Glare protection - against blinding by lights
Continuous lightning - evenly distributed lightning
Controlled lightning - no bleeding over no blinding
Standby Lightning - timers
Responsive areas illumination - IDS detects activities and turns on lightning
NIST: for critical areas the area should be illuminated 8 feet in height with 2-foot candle power

Fences

Small mesh and high gauge is most secure
3-4 feet deters casual trespasser
6-7 feet too hard to climb easily
8 feet + wires deters intruders, difficult to climb
no one STOPS a determined intruder

ALARMS (697)

Local alarms - audible alarm for at least 4000 feet far
Central stations - less than 10mins travel time for e.g. an private security firm
Proprietary systems - owned and operated by the customer. System provides many of the features in-**house**
Auxiliary Station systems - on alarm ring out to local fire or police
Line supervision check - if no tampering is done with the alarm wires
Power supplies - alarm systems needs separate circuitry and backup power

Intrusion detection (698)

PHYSICAL PARAMETER DETECTION
Electromechanical - detect a break or change in a circuit magnets pulled lose, wires door, pressure pads
Photoelectric - light beams interrupted (as in an store entrance)
Passive infrared - detects changes in temperature
Acoustical detection - microphones, vibrations sensors
MOTION
wave pattern motion detectors - detects motions
proximity or capacitance detector - magnetic field detects presence around an object

Locks (702)

Warded lock - hanging lock with a key
Tumbler lock - cylinder slot
Combination lock - 3 digits with wheels
Cipher Lock - Electrical
Device lock - bolt down hardware
Preset - ordinary door lock
Programmable - combination or electrical lock

Raking - circumvent a pin tumbler lock

Audit trails

Date and time stamps
Successful or not attempt
Where the access was granted
Who attempted access
Who modified access privileges at supervisor level

Security access cards

Photo id card: dumb cards Digital-coded cards:

- Swipe cards
- Smartcards

Wireless proximity cards

- User activated
- System sensing
  - Passive device, no battery, uses power of the field
    - Field Powered device: active electronics, transmitter but gets power from the surrounding field from the reader

Transponders: both card and receiver holds power, transmitter and electronics

Trusted recovery ()

Ensures that the security is not breached when a system crash or failure occurs. *Only required for a B3 and A1 level systems*.

Failure preparation Backup critical information thus enabling data recovery

System recovery after a system crash

1. Rebooting system in single user mode or recovery console, so no user access is enabled
2. Recovering all file systems that were active during failure
3. Restoring missing or damaged files
4. Recovering the required security characteristic, such as file security labels
5. Checking security-critical files such as system password file

Common criteria hierarchical recovery types

1. **Manual** System administrator intervention is required to return the system to a secure state
2. **Automatic** Recovery to an secure state is automatic when resolving a single failure (though system administrators are needed to resolve additional failures)
3. **Automatic without Undo Loss** Higher level of recovery defining prevention against the undue loss of protected objects
4. **Function** system can restore functional processes automatically

Types of system failure

System reboot System shuts itself down in a controlled manner after detecting inconsistent data structures or runs out of resources
Emergency restart when a system restarts after a failure happens in an uncontrolled manner. E.g. when a low privileged user tries to access restricted memory segments
System cold start when an unexpected kernel or media failure happens and the regular recovery procedure cannot recover the system in a more consistent state.

Domain 7 – Security Operations

Things to know

Hackers and crackers - want to verify their skills as intruders
Entitlement - refers to the amount of privileges granted to users, typically when first provisioning an account. A user entitlement audit can detect when employees have excessive privileges
Aggregation - Privilege Creep, accumulate privileges
Hypervisor - software component that manages the virtual components. The hypervisor adds an additional attack surface, so it's important to ensure it is deployed in a secure state and kept up-to-date with patches, controls access to physical resources
Notebook - most preferred in the legal investigation is a bound notebook, pages are attached to a binding.
Exigent circumstances allows officials to seize evidence before its destroyed (police team fall in)
Data haven is a country or location that has no laws or poorly enforced laws
Chain of custody = collection, analysis and preservation of data
Forensics uses bit-level copy of the disk
Darknet – unused network space that may detect unauthorized activity
Pseudo flaw – false vulnerability in a system that may attract an attacker
FAIR INFORMATION PRACTICES

- Openness
- Collection Limitation
- Purpose Specification
- Use Limitation
- Data Quality
- Individual Participation
- Security Safeguards
- Accountability

Noise and perturbation: inserting bogus information to hope to mislead an attacker
First step by change process = management approval.
NB: when a question is about processes, there must always be management's approval as First step.
PROTOTYPING: customer view taken into account
SQL –SUDIGR, 6 basic SQL commands
Select, Update, Delete, Insert, Grant, Revoke
Bind variables are placeholders for literal values in SQL query being sent to the database on a server
Bind variables in SQL used to enhance performance of a database
Monitor progress and planning of projects through
GANTT and PERT charts
Piggybacking: looking over someone's shoulder to see how someone gets access.
Data center should have:

- Walls from floor to ceiling
- Floor: Concrete slab: 150 pounds square foot
- No windows in a datacenter
- Air-conditioning should have own Emergency Power Off (EPO)

Electronic Access Control (EAC): proximity readers, programmable locks or biometric systems

Location

CPTED Crime Prevention Through Environmental design

- Natural Access control: guidance of people by doors fences bollards lightning. Security zones defined
- Natural surveillance: cameras and guards
- Territorial Reinforcements: walls fences flags Target Hardening: focus on locks, cameras guards

Facility site: CORE OF BUILDING (thus with 6 stores, on 3rd floor)

Attacks ()

Hacktivists - combination of hacker and activist), often combine political motivations with the thrill of hacking.
Thrill attacks - are the attacks launched only for the fun of it. Pride, bragging rights
Script kiddies - Attackers who lack the ability to devise their own attacks will often download programs that do their work for them. The main motivation behind these attacks is the "high" of successfully breaking into a system. Service interruption. An attacker may destroy data, the main motivation is to compromise a system and perhaps use it to launch an attack against another victim. Common to do website defacements,
Business Attacks - focus on illegally obtaining an organization's confidential information. The use of the information gathered during the attack usually causes more damage than the attack itself.
Financial Attacks - carried out to unlawfully obtain money or services.
Terrorist Attacks - purpose of a terrorist attack is to disrupt normal life and instill fear
Military or intelligence attack - designed to extract secret information.
Grudge Attacks - are attacks that are carried out to damage an organization or a person. The damage could be in the loss of information or information processing capabilities or harm to the organization or a person's reputation.
Sabotage - is a criminal act of destruction or disruption committed against an organization by an employee. It can become a risk if an employee is knowledgeable enough about the assets of an organization, has sufficient access to manipulate critical aspects of the environment, and has become disgruntled.
Espionage - is the malicious act of gathering proprietary, secret, private, sensitive, or confidential information about an organization. Attackers often commit espionage with the intent of disclosing or selling the information to a competitor or other interested organization (such as a foreign government). Attackers can be dissatisfied employees, and in some cases, employees who are being blackmailed from someone outside the organization. Countermeasures against espionage are to strictly control access to all nonpublic data, thoroughly screen new employee candidates, and efficiently track all employee activities.
Integrity breaches - unauthorized modification of information, violations are not limited to intentional attacks. Human error, oversight, or ineptitude accounts for many instances
Confidentiality breaches – theft of sensitive information

Domain 8 – Software Development Security

System Development Life Cycle (SDLC) (720)

Project initiation - Feasibility, cost, risk analysis, Management approval, basic security objectives

Functional analysis and planning - Define need, requirements, review proposed security controls

System design specifications - Develop detailed design specs, Review support documentation, Examine security controls

Software development - Programmers develop code. Unit testing Check modules. *Prototyping, Verification, Validation*

Acceptance testing and implementation - Separation of duties, security testing, data validation, bounds checking, certification, accreditation , part of release control

System Life Cycle (SLC) (extends beyond SDLC)

Operations and maintenance - release into production. Certification/accreditation

Revisions/ Disposal - remove. Sanitation and destruction of unneeded data

The has three basic components:

Change Management Process

Together, change and configuration management techniques form an important part of the software engineer's arsenal and protect the organization from development-related security issues.

The change management process has three basic components:

Request Control - provides an organized framework within which users can request modifications, managers can conduct cost/ benefit analysis, and developers can prioritize tasks.

Change Control - provides an organized framework within which multiple developers can create and test a solution prior to rolling it out into a production environment. Change control includes conforming to quality control restrictions, developing tools for update or change deployment, properly documenting any coded changes, and restricting the effects of new code to minimize diminishment of security.

Release Control - Once the changes are finalized, they must be approved for release through the release control procedure.

Configuration Management Process

This process is used to control the version(s) of software used throughout an organization and formally track and control changes

Configuration Identification - administrators document the configuration of covered software products throughout the organization.

Configuration Control - ensures that changes to software versions are made in accordance with the change control and configuration management policies. Updates can be made only from authorized distributions in accordance with those policies.

Configuration Status Accounting - Formalized procedures are used to keep track of all authorized changes that take place.

Configuration Audit - periodic configuration audit should be conducted to ensure that the actual production environment is consistent with the accounting records and that no unauthorized configuration changes have taken place.

SDLC

- Conceptual definition
- Functional requirements definition
- Control specifications development
- Design review
- Code review
- System test review
- Maintenance and change management

Software Capability Maturity model (CMM) (725)

Quality of software is a direct function of quality of development and maintenance

Defined by Carnegie Mellon University SEI (Software Engineering Institute)

Describes procedures, principles, and practices that underlie software development process maturity

1-2 REACTIVE, 3-5 PROACTIVE

5 levels

1. **initiating –** competent people, informal processes, ad-hoc, absence of formal process
2. **repeatable –** project management processes, basic life-cycle management processes
3. **defined –** engineering processes, presence of basic life-cycle management processes and reuse of code, use of requirements management, software project planning, quality assurance, configuration management practices
4. **managed –** product and process improvement, quantitatively controlled
5. **Optimizing –** continuous process improvement Works with an IDEAL model.

Initiate begin effort, Diagnose perform assessment, Establish an action plan, Action implement improvements, Leverage reassesses and continuously improve

Project Management Tools

Gantt Chart - a type of bar chart that shows the interrelationships over time between projects and schedules. It provides a graphical illustration of a schedule that helps to plan, coordinate, and track specific tasks in a project. WBS a subpart

PERT - Program Evaluation Review Technique is a project-scheduling tool used to judge the size of a software product in development and calculate the standard deviation (SD) for risk assessment. PERT relates the estimated lowest possible size, the most likely size, and the highest possible size of each component. PERT is used to direct improvements to project management and software coding in order to produce more efficient software.

DevOps (728)

The DevOps approach seeks to resolve issues by bringing the three functions together in a single operational model. The word DevOps is a combination of Development and Operations, symbolizing that these functions must merge and cooperate to meet business requirements.

Integrates:

- Software Development,
- Quality Assurance
- IT Operations

NOT SECURITY

Software Development Methods (732)

MODELS

Simplistic model

This model was simplistic in that it assumed that each step could be completed and finalized without any effect from the later stages that may require rework.

Waterfall model

Can be managed if developers are limited going back only one step. If rework may be done at any stage it's not manageable.

Problem: it assumes that a phase or stage ends at a specific time.

System Requirements-> Software Requirements -> Analysis -> Program Design -> Coding -> Testing -> Operations & Maintenance

Waterfall including Validation and Verification (V&V)

Reinterpretation of the waterfall model where verification evaluates the product during development against specification and validation refers to the work product satisfying the real-world requirements and concepts.

Verification=doing the job right Validation:= doing the right job

Spiral model

Angular = progress made

Radial = cost

Lower left = development plans

Upper left = objectives of the plans, alternatives checked

Upper right = assessing alternatives, risk analysis

Lower right = final development

Left horizontal axis = includes the major review required to complete each full cycle

Cleanroom – write code correctly first time, quality thru design

Cleanroom design – prove original design

Agile Software Development (733)

Developers increasingly embraced approaches that placed an emphasis on the needs of the customer and on quickly developing new functionality that meets those needs in an iterative fashion.

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan

WORKING SOFTWARE PRIMARY MEASURE OF SUCCESS

Domain 8 – Software Development Security

Database Systems (736)

Database - general mechanism for defining, storing and manipulating data without writing specific programs
DBMS - refers to a suite of software programs that maintains and provides controlled access to data components store in rows and columns of a table
Types

- Hierarchical= tree (sons with only one parent), one to many relationship
- Network = tree (all interconnected)
- Mesh
- Object-orientated
- Relational – one-to-one relationships, has DDL and DML, has TUPLES and ATTRIBUTES (rows and columns)
- Key-Value Store - key-value database, is a data storage paradigm designed for storing, retrieving, and managing associative arrays, a data structure more commonly known today as a *dictionary* or *hash*.

DDL – Data definition language defines structure and schema
DML – Data manipulation language view, manipulate and use the database via VIEW, ADD, MODIFY, SORT and DELETE commands.
Degree of Db –number of attributes (columns) in table
Tuple – row or record
DDE – Dynamic data exchange enables applications to work in a client/server model by providing the inter-process communications mechanism (IPC)
DCL – Data control language subset of SQL used to control access to data in a database, using GRANT and REVOKE statements
Semantic integrity - make sure that the structural and semantic rules are enforced on all data types, logical values that could adversely affect the structure of the database
Referential integrity - all foreign keys reference existing primary keys,
Candidate Key – an attribute that is a unique identifier within a given table, one of the candidate keys is chosen to be the primary key and the others are alternate keys, A candidate key is a subset of attributes that can be used to uniquely identify any record in a table. No two records in the same table will ever contain the same values for all attributes composing a candidate key. Each table may have one or more candidate keys, which are chosen from column headings.
Primary Key – provide the sole tuple-level addressing mechanism within the relational model. Cannot contain a null value and cannot change or become null during the life of each entity. When the primary key of one relation is used as an attribute in another relation, it is the foreign key in that relation. Uniquely identify a record in a database
Foreign Key – represents a reference to an entry in some other table that is a primary key there. Link between the foreign and primary keys represents the relationship between the tuples. Enforces referential integrity
Main Components of a Db using Db

- Schemas; blueprints
- tables
- views

Database Systems (736) (cont.)

Incorrect Summaries – when one transaction is using an aggregate function to summarize data stored in a Db while a second transaction is making modifications to a Db, causing summary to include incorrect information
Dirty Reads – when one transaction reads a value from a Db that was written by another transaction that did not commit, Db concurrency issue
Lost Updates – when one transaction writes a value to the Db that overwrites a value needed by transactions that have earlier precedence
Dynamic Lifetime Objects: Objects created on the fly by software in an Object Oriented Programming environment. An object is preassembled code that is a **self-contained** module
ODBC - Open Database Connectivity is a database feature that allows applications to communicate with different types of databases without having to be directly programmed for interaction with each type. ODBC acts as a proxy.
Multilevel security - it's essential that admins and developers strive to keep data with different security requirements separate.
Database contamination - Mixing data with different classification levels and/ or need-to-know requirements and is a significant security challenge. Often, administrators will deploy a trusted front end to add multilevel security to a legacy or insecure DBMS.
Database partitioning - is the process of splitting a single database into multiple parts, each with a unique and distinct security level or type of content.
Polyinstantiation - occurs when two or more rows in the same relational database table appear to have identical primary key elements but contain different data for use at differing classification levels. It is often used as a defense against inference attacks

Database transactions

Four required characteristics: atomicity, consistency, isolation, and durability. Together, these attributes are known as the ACID model, which is a critical concept in the development of database management systems.
Atomicity - Database transactions must be atomic— that is, they must be an "all-or-nothing" affair. If any part of the transaction fails, the entire transaction must be rolled back as if it never occurred.
Consistency - All transactions must begin operating in an environment that is consistent with all of the database's rules (for example, all records have a unique primary key). When the transaction is complete, the database must again be consistent with the rules, regardless of whether those rules were violated during the processing of the transaction itself. No other transaction should ever be able to use any inconsistent data that might be generated during the execution of another transaction.
Isolation - principle requires that transactions operate separately from each other. If a database receives two SQL transactions that modify the same data, one transaction must be completed in its entirety before the other transaction is allowed to modify the same data. This prevents one transaction from working with invalid data generated as an intermediate step by another transaction.
Durability - Database transactions must be durable. That is, once they are committed to the database, they must be preserved. Databases ensure durability through the use of backup mechanisms, such as transaction logs.

Knowledge Management (755)

Expert Systems

Expert systems seek to embody the accumulated knowledge of experts on a particular subject and apply it in a consistent fashion to future decisions.
Every expert system has two main components: the knowledge base and the inference engine.

- Based on human reasoning
- Knowledge base of the domain in the form of rules
- ***If-then statements***=called forward chaining
- Priority in rules are called salience
- Interference system = decision program
- Expert system = inference engine + knowledge base - Degree of uncertainty handled by approaches as Bayesian networks(probability of events), certainty factors(probability an event is true) or fuzzy logic(to develop conclusions)
- Two modes:
  - Forward chaining: acquires info and comes to a conclusion
  - Backward chaining: backtracks to determine IF a hypothesis is correct

Neural Networks

- Use complex computations to replace partial functions of the human mind
- Based on function of biologic neurons
- Works with weighted inputs
- If a threshold is exceeded there will be output
- Single-layer : only one level of summoning codes
- Multi-level: more levels of summoning codes
- Training period needed to determine input vectors - adaptability (learning process)

Programming Language Generations (762)

First-generation languages (1GL) include all machine languages.
Second-generation languages (2GL) include all assembly languages.
Third-generation languages (3GL) include all compiled languages.
Fourth-generation languages (4GL) attempt to approximate natural languages and include SQL, which is used by databases.
Fifth-generation languages (5GL) allow programmers to create code using visual interfaces.

Programs

Compiler Translates higher level program into an executable file
Interpreter reads higher level code, one line at the time to produce machine instructions
Assembler converts machine-code into binary machine instructions. Translate assembly language into machine language.

Domain 8 – Software Development Security

Object Orientated Technology (769)

Objects behave as a black box; they are encapsulated to perform an action. Can be substituted if they have compatible operations. It can store objects like video and pictures

Encapsulation (Data Hiding) – only data it needs, no accidental access to data

Message - communication to object to perform an action

Method - code that defines an action an object performs in response to a message

Behavior - results exhibited by an object in response to a msg.

Class - collection of methods that defines the behavior of objects

Instance - objects are instances of classes that contain their methods

Inheritance - allows a subclass to access methods belonging to a superclass

Multiple Inheritance - class inherits characteristics from more than one parent class

Delegation - forwarding a request to another object

Polymorphism: objects of many different classes that are related by some common super class. When different subclasses may have different methods using the same interfaces that respond differently

Poly-instantiation - occurs when two or more rows in the same relational database table appear to have identical primary key elements but contain different data for use at differing classification levels. It is often used as a defense against some types of inference attacks

5 phases of object orientation

OORA, Requirements Analysis - defines classes of objects and their interactions

OOA, Analysis - understanding and modeling a particular problem Domain Analysis (DA) seeks to identify classes and objects that are common to all applications in a domain

OOD, Design - Objects are the basic units, and instances of classes

OOP, Programming - employment of objects and methods If class = airplane, objects like fighter plane, cargo plane, passenger plane can be created. Method would be what a plane would do with a message like: climb, dive, and roll.

ORBs, Object Request Brokers - middleware that acts as locators and distributors of the objects across networks.

Standards

CORBA, Common object request - broker architecture enables programs written in different languages and using different platforms and OS's through IDL (Interface Definition Language)

COM, **Common Object Model** - support exchange of objects amongst programs. This used to be called OLE. DCOM is the network variant (distributed)

Conclusion - Object orientation (e.g. with C++ and Smalltalk) supports reuse of objects and reduces development risk, natural in its representation of real world entities.

Cohesion: ability to perform without use of other programs, strength of the relationship between the purposes of methods within the same class

High cohesion - without use of other modules

Low cohesion - must interact with other modules

Coupling - effect on other modules. Level of interaction between objects

High coupling - module largely affects many more modules

Low coupling - it doesn't affect many other modules

Technical Security Protection Mechanisms

Abstraction - one of the fundamental principles behind object-oriented programming. It is the "black-box" doctrine that says that users of an object (or operating system component) don't necessarily need to know the details of how the object works; they need to know just the proper syntax for using the object and the type of data that will be returned as a result

Separation of privilege - builds on the principle of least privilege. It requires the use of granular access permissions; that is, different permissions for each type of privileged operation. This allows designers to assign some processes rights to perform certain supervisory functions without granting them unrestricted access to the system.

Process isolation - requires that the operating system provide separate memory spaces for each process's instructions and data. It also requires that the operating system enforce those boundaries, preventing one process from reading or writing data that belongs to another process.

- It prevents unauthorized data access. Process isolation is one of the fundamental requirements in a multilevel security mode system.
- It protects the integrity of processes.

Layering processes - you implement a structure similar to the ring model used for operating modes and apply it to each operating system process.

Hardware segmentation - is similar to process isolation in purpose. Difference is that hardware segmentation enforces these requirements through the use of physical hardware controls rather than the logical process isolation controls imposed by an operating system.

Covert channels (778)

Is a way to receive information in an unauthorized manner, information flood that is not protected by a security mechanism

2 types

Storage covert channel - processes communicate via storage space on the system

Covert timing channel - one process relays to another by modulating its use of system resources. Typing rhythm of Morse Code is an example

Countermeasures: eal6 systems have less than eal3 systems because covert channels are normally a flaw in design.

Mobile code

Java – sandboxes, no warnings, programs are compiled to bytecode

ActiveX – Authenticode, relies on digital signatures, annoying dialogs people click away

Malicious code threats (787)

Virus - reproduces using a host application. It inserts or attaches itself to the file, spread thru infected media

Worm - reproduces on its own without host application

Logic Bomb/Code Bomb - executes when a certain event happens (like accessing a bank account or employee being fired) or a data/time occurs

Trojan Horse - program disguised as a useful program/tool

HOAXES – False warnings like: DON'T OPEN X SEND TO ALL YOUR COLLEGUES

RAT, Remote Access Trojan - remote control programs that have the malicious code and allow for unauthorized remote access Back orifice, sub seven, net bus)

Buffer Overflow - Excessive information provided to a memory buffer without appropriate bounds checking which can result in an elevation of privilege. If executable code is loaded into the overflow, it will be run as if it were the program.

Buffer overflows can be detected by disassembling programs and looking at their operations.

Buffer overflows must be corrected by the programmer or by directly patching system memory.

Trap Door - An undocumented access path through a system. This typically bypasses the normal security mechanisms and is to plant any of the malicious code forms.

Backdoor - program installed by an attacker to enable him to come back on a later date without going through the proper authorization channels , maintenance hook for developers sometimes

Covert Channel - a way to receive information in an unauthorized manner. Information flood that is not protected by a security mechanism.

Covert Storage Channel - Writing to storage by one process and reading by another of lower security level.

Covert Timing Channel - One process relays to another by modulating its use of system resources.

Countermeasures - EAL6 systems have less than EAL3 systems because covert channels are normally a flaw in design.

LOKI - is a tool used for covert channel that writes data directly after the ICMP header

Botnet - compromise thousands of systems with zombie codes can be used in DDOS attacks or spammers, send spam messages, conduct brute force attacks, scan for vulnerable systems

Directory Traversal Attack – attacker attempts to force the web application to navigate up the file hierarchy and retrieve a file that should not normally be provided to a web user.

Macro Virus – Most common in office productivity documents .doc/.docx

Trojans – pretends to do one thing while performing another

Worms – reproduces and spreads, capacity to propagate independent of user action

MDM, Mobile device management - a software solution to manage the myriad mobile devices that employees use to access company resources. The goals of MDM are to improve security, provide monitoring, enable remote management, and support troubleshooting.

Collisions – two different files produce the same result from a hashing operation

Domain 8 – Software Development Security

Virus (784)

Boot sector – moves or overwrites the boot sector with the virus code.
System infector – infects BIOS command other system files. It is often a memory resident virus.
Phlashing - a malicious variation of official BIOS or firmware is installed that introduces remote control or other malicious features into a device. UEFI – **replacement for BIOS**
Compression – appended to executables
Companion virus - A specific type of virus where the infected code is stored not in the host program, but in a separate 'companion' files. For example, the virus might rename the standard NOTEPAD.EXE file to NOTEPAD.EXD and create a new NOTEPAD.EXE containing the virus code. When the user subsequently runs the Notepad application, the virus will run first and then pass control to the original program, so the user doesn't see anything suspicious. Takes advantage of search order of an OS
Stealth virus – hides modifications to files or boot records and itself
Multipart virus - infects both the boot sector and executable files; becomes resident first in memory and then infects the boot sector and finally the entire system, uses two or more propagation mechanisms
Self-garbling virus – attempts to hide by garbling its code; as it spreads, it changes the way its code is encoded
Polymorphic virus – this is also a self-garbling virus where the virus changes the "garble" pattern each time is spreads. As a result, it is also difficult to detect.
Macro virus – usually written in Word Basic, Visual Basic or VBScript and used with MS Office
Resident virus – Virus that loads when a program loads in memory
Master boot record /boot sector - (MBR) virus attack the MBR—the portion of bootable media (such as a hard disk, USB drive, or CD/ DVD) that the computer uses to load the operating system during the boot process. Because the MBR is extremely small (usually 512 bytes), it can't contain all the code required to implement the virus's propagation and destructive functions. To bypass this space limitation, MBR viruses store the majority of their code on another portion of the storage media. When the system reads the infected MBR, the virus instructs it to read and execute the code stored in this alternate location, thereby loading the entire virus into memory and potentially triggering the delivery of the virus's payload.
Non-resident virus - attached to .exe

ANTI-Virus

Signature based cannot detect new malware
Heuristic behavioral can detect new malware

Threats

Natural (Fires, explosions water, storm)
Man-made (bombing, strikes, toxin spills)

Protection mechanisms (795)

Protection domain
Execution and memory space assigned to each process
TRUSTED COMPUTER BASE
Combination of protection systems within a computer system, which include the hardware, software and firmware that are trusted to enforce the security policy.
Security Kernel - hardware, software, firmware, elements of TCB that implement the reference monitor concept — must be isolated from reference monitor (reference monitor: isolation, completeness and verifiability, that compares the security labels of subjects and objects)
Multistate systems - capable of implementing a much higher level of security. These systems are certified to handle multiple security levels simultaneously by using specialized mechanisms
Protection rings - (MIT's MULTICS design)
Ring 0 - Operating system kernel. The OS' core. The kernel manages the HW (for example, processor cycles and memory) and supplies fundamental services that the HW does not provide.
Ring 1 - Remaining parts of the operating system
Ring 2 - I/O drivers and utilities
Ring 3 - Applications and programs
Layers 1 and 2 contain device drivers but are not normally implemented in practice. Layer 3 contains user applications. Layer 4 does not exist.

Terms

CSRF (XSRF) – Cross site request forgery, attacks exploit the trust that sites have in a user's browser by attempting to force the submission of authenticated request to third-party sites.
Cross-site Scripting – uses reflected input to trick a user's browser into executing untrusted code from a trusted site
Session Hijacking – attempt to steal previously authenticated sessions but do not force the browser to submit request.
SQL Injection – directly attacks a database through a web app,, CARROT'1=1;-- quotation mark to escape out of input field
Blue Screen of Death – when a Windows system experiences a dangerous failure and enters a full secure state (reboot)
Hotfix, update, Security fix – single patch, patches provide updates to operating systems and applications.
Service Pack – collection of unrelated patches released in a large collection
Patch management system - prevents outages from known attacks by ensuring systems are patched. Patches aren't available for new attacks. However, the patch management system doesn't provide the updates. Ensuring systems are patched reduces vulnerabilities but it does not eliminate them

Nice to Know

Code Review - peer-driven process that includes multiple developers, may be automated, may review several hundred lines of code an hour, done after code developed
Strong Passwords – social engineering best attack method to beat
Threat Modeling – reduce the number of security-related design and coding flaws, reduce severity of non-security related files, not to reduce number of threat vectors
Aggregate – summarize large amounts of data and provide only summary information as a result
Port Scan – attacking system sends connection attempts to the targets system against a series of commonly used ports

Account [name of class]
Balance: currency = 0 [attributes of class] Owner: string [attributes of class]
AddFunds(deposit: currency) [method of class] RemoveFunds (withdrawal: currency) [method of class]

JavaScript – is an interpreted language that does not make use of a complier to transform code into an executable state. Java, C, and C++ are all compiled languages.
Directory Traversal Attack - %252E%252Fetc/passwd, %252E = . & %252F = /
Open system - is one with published APIs that allow third parties to develop products to interact with it.
Closed system - is one that is proprietary with no third-party product support, does not define if it's code can be viewed
Open source - is a coding stance that allows others to view the source code of a program, distributed free or for a fee
Closed source - is an opposing coding stance that keeps source code confidential. can be reverse engineered or decompiled
API Keys - like passwords and should be treated as very sensitive information. They should always be stored in secure locations and transmitted only over encrypted communications channels. If someone gains access to your API key, they can interact with a web service as if they were you! Limit access to API
Nessus - is a popular vulnerability scanner managed by Tenable Network Security, and it combines multiple techniques to detect a wide range of vulnerabilities. It uses port scans to detect open ports and identify the services and protocols that are likely running on these systems. Once Nessus discovers basic details about systems, it can then follow up with queries to test the systems for known vulnerabilities, such as if the system is up-to-date with current patches. Attacker can use to best identify vulnerabilities in a targeted system
CASE - tool for development, if concerned about security
OWASP – Open Web Application Security Project, most authoritative source on web application security issues
Shadow Password File - , /etc./ shadow. This file contains the true encrypted PWs of each user, but it is not accessible to anyone but the administrator. The publicly accessible /etc./ passwd file then simply contains a list of usernames without the data necessary to mount a dictionary attack. "x"
User Mode – processor mode used to run the system tools used by admins to make configuration changes to a machine
Kernel Mode – used by processor to execute instructions from OS