Domain 1—(Security and Risk Management)

IT Governance Committee:

Responsible for recruiting and maintaining the governance board. Responsible for determining missing qualifications and characteristics of board members.

Board of directors responsibilities:

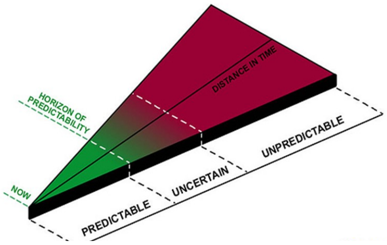
Be informed about information security. Set direction to drive policy and strategy. Provide resources to security efforts. Assign management responsibilities. Set priorities . Support changes required. Define cultural values related to risk assessment. Obtain assurance from internal or external auditors. Insist that security investments are made measurable and reported on for program effectiveness.

Management responsibilities:

Write security policies with business input. Ensure that roles and responsibilities are defined and clearly understood. Identify threats and vulnerabilities. Implement security infrastructures and control frameworks (standards, guidelines, baselines, and procedures). Ensure that policy is approved by the governing body. Establish priorities and implement security projects in a timely manner. Monitor breaches. Conduct periodic reviews and tests. Reinforce awareness education as critical. Build security into the systems development life cycle.

Security Planning:

Strategic Plan:
Long term & stable
Period of 5 years
Tactical Plan:
Midterm & detailed
Period of 1 year
Operational Plan:
Short-term & highly detailed
Updated regularly



Security Council:

Vision statement: Draws upon the security concepts of CIA to support the business objective. Nontechnical, brief, to the point and achievable
Mission statement: Objectives that support the overall vision. Goals, initiatives, objectives to achieve vision

European Union (EU) Privacy:

EU Data Protection Directive (also known as Directive 95/46/EC) is a regulation adopted by the European Union to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using or exchanging such data. The EU Data Protection Directive is based on recommendations first proposed by the Organization for Economic Co-operation and Development's (OECD). The Data Protection Directive is superseded by the General Data Protection Regulation (GDPR), which was adopted by the European Parliament and European Council in April 2016 and has become enforceable in May 2018. The new regulation expands upon previous requirements for collecting, storing and sharing personal data and requires the subject's consent to be given explicitly and not checked off by default.

EU-US Safe Harbor: EU citizen personal data can not be transmitted, even with permission of the individual, outside of the EU. Safe Harbor allows US companies to pass data. American companies doing business in Europe can obtain protection under a treaty between the European Union and the United States that allows the Department of Commerce to certify businesses that comply with regulations and offer them “Safe Harbor” from prosecution. US Organization are Data Processors when they classify and handle data. EU companies would be Business/Mission owners. US Organization would also be Data Administrators. Data processors have responsibility to protect privacy of data. Department. of Commerce holds list of participants. US Organization can transfer to non-Safe Harbor entities with permission. Federal Trade Commission (FTC) overseas the compliance framework for organizations wishing to use personal data of EU citizens.

Import and Export Restrictions:

Import/export laws were created because of concerns about new information technologies and products with military applications being transferred outside of the USA.
International Traffic In Arms Regulation (ITAR): Controls the import/export of items considered defense articles and defense services.
Export Administration Regulations (EAR): Allows the President to regulate the export of civilian goods and technologies that have military applications.
Wassenaar Arrangement (post cold war): Standard for export controls. Restricts access to countries not included in arrangement.

Data Breaches:

Incident: Security event that compromises the integrity, confidentiality or availability of an information asset.
Breach: Incident that results in disclosure or potential exposure of data.
Data Disclosure: Breach for which it was confirmed that data was actually disclosed to an unauthorized party.
US Breach Notification Laws are at the state level.
Purpose: to notify an individual that his personal information has been compromised.

Threat Sources:

Hacker gaining access to confidential information.
Processing errors / buffer overflows.
Coding / programming errors.
User errors causing a system malfunction.
Privilege abuse.
Virus infection.
Energy anomalies.
Theft.
Natural disasters that cause damage or injury.
Terrorism that causes injury or destroys systems.

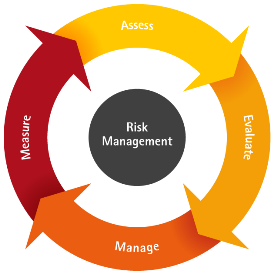
Ten Commandments of Computer Ethics:

Thou shalt not use a computer to harm other peoples.
Thou shalt not interfere with other people's computer work.
Thou shalt not snoop around in other people's computer files.
Thou shalt not use a computer to steal.
Thou shalt not use a computer to bear false witness.
Thou shalt not copy or use proprietary software for which you have not paid (without permission).
Thou shalt not use other people's computer resources without authorization or proper compensation.
Thou shalt not appropriate other people's intellectual output.
Thou shalt think about the social consequences of the program you are writing or the system you are designing.
Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Risk Terminology:

Asset: A resource (physical or logical) that is valued by the organization.
Asset Valuation: Goal is to assign a specific dollar value to an asset based on purchase, replacement, development, etc. costs.
Threat: Any potential violation of security, particular to information or an Information System (IS) such as unauthorized access, HW failure, utility failure, loss of key personnel, human errors, disgruntled employees; could be man-made, natural or technical.
Threat Agent: The source that has the potential of causing a threat.
Vulnerability: An IS weakness that could be exploited; could be a weakness in a Configuration Management (CM) or complete lack of CM.
Exposure: Instance of being exposed to losses from a threat (damage factor – something that can be measured).
Safeguard (Countermeasure): Mitigates potential risk; something we use for protection against the threat, also designed to detect, prevent or recover from an attack.
Attack: An action intending harm by exploiting a vulnerability – we'll talk much more about attack methodologies later.
Breach: Occurrence of a security mechanism being bypassed or thwarted by a threat agent.
To have risk, a threat must connect to a vulnerability.
Risk=Threat x Vulnerability x Impact (Cost).

Risk Lifecycle:



Audit Frameworks for Compliance:

Committee of Sponsoring Organizations of the Treadway Commission (COSO): Is a joint initiative to combat corporate fraud. It was established in the United States by five private sector organizations, dedicated to guide executive management and governance entities on relevant aspects of organizational governance, business ethics, internal control, enterprise risk management, fraud, and financial reporting. COSO has established a common internal control model against which companies and organizations may assess their control systems. COSO is supported by five supporting organizations, including the Institute of Management Accountants (IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA), and Financial Executives International (FEI).
Information Technology Infrastructure Library (ITIL): Is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. ITIL is published as a series of five core volumes:

- ITIL Service Strategy: understands organizational objectives and customer needs.
- ITIL Service Design: turns the service strategy into a plan for delivering the business objectives.
- ITIL Service Transition: develops and improves capabilities for introducing new services into supported environments.
- ITIL Service Operation: manages services in supported environments.
- ITIL Continual Service Improvement: achieves services incremental and large-scale improvements.

Control Objectives for Information and Related Technology (COBIT): is a good-practice framework created by international professional association ISACA for information technology (IT) management and IT governance. COBIT provides an implementable "set of controls over information technology and organizes them around a logical framework of IT-related processes and enablers."
ISO 27002 aka ISO 17799/BS7799-2 (ISO 27001): Provides best practice recommendations on information security controls for use by those responsible for initiating, implementing or maintaining information security management systems (ISMS). Information security is defined within the standard in the context of the C-I-A triad: "the preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required)."

Candidate screening and hiring

Position description: a well written job description defines the job duties and responsibilities, identifies the qualifications necessary to perform the role, identifies the supervisory relationships, identifies the salary or rate of pay, and sets the baseline expectations for performance.

Screening and interviewing: Conduct it legally. Never interview a candidate alone. Ask all candidates the same questions.

Background investigation: must be done based on local laws and jurisdiction. Can not discriminate based on race, color, national origin, sex, religion, disabilith, generic information, or age.

Financial information: The fair credit reporting act sets a national standard for employers to follow when conducting background checks.

Social media: during a background investigation social media accounts are often reviewed. Organizations should have clear policies in place prior to using the Internet for social media research.

Criminal history: Depending on jurisdiction, it may or may not be legal to use criminal history to discriminate.

Driving records: Hiring someone that would be driving as part of their job makes this an acceptable practice and way to avoid risk.

Medical records: Prior to a job offer an employer can not ask any disability related questions or require a medical examination.

Drug testing: No restrictions and many businesses have mandatory screening programs.

Prior employment: generally accepted practice prior to employment. Serves as one of the most valuable indicators for job success.

Other tests: personality, integrity, cognitive, and emotional intelligence.

Reasonable Expectation of Privacy

Privacy expectations are higher when the employee has a dedicated space. Privacy expectations are lessened in common areas such as open cubicles. Privacy expectations are different for public and private employers. Private employers have a greater latitude in monitoring employees.

ISO 31000:2018

It is based on 8 principles for the development of a risk framework which in turn structures the processes of risk management. The principles are: proportionate, aligned, comprehensive, embedded, dynamic, best available information, inclusive, continual improvement.

STRIDE

Standard for identifying threats. It is a mnemonic for spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege.

Payment Card Industry Data Security Standard (PCI-DSS)

As of this writing, the current version is 3.2. It identifies 12 high-level requirements that merchangts are contractually obligated to meet. It also identifies 6 goals. The level of compliance is dependent on the volume of transactions processed by the merchant. Failure to meet requirements can result in fines levied by the credit card processor.

Service Provider Levels:

Service provider level 1: more than 6 million annual transactions
Service provider level 2: 1-6 million annual transactions
Service provider level 3: 20,000—1 million annual transactions
Service provider level 4: fewer than 20,000 annual transactions

PCI-DSS Goals

Goal 1: build and maintain a secure network
Goal 2: protect cardholder data
Goal 3: maintain a vulnerability management program
Goal 4: implement strong access control measures
Goal 5: regularly monitor and test networks
Goal 6: maintain an information security policy

PCI-DSS Requirements

1. install a firewall
2. Do not use vendor supplied defaults
3. Protect stored cardholder data
4. Encrypt transmission of card holder data
5. Regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by need to know
8. Assign unique IDs for access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

Supply Chain Operational Reference (SCOR)

The SCOR model integrates business process improvement, performance benchmarking, best practices, and organizational design into a framework. The six management processes are:

Plan: processes that balance supply and demand to meet the best sourcing, production, and delivery requirements.

Source: processes that procure goods and services to meet demand

Make: processes that transform a product into a state that meets demand.

Deliver: processes that provide finished goods or services to the planned or actual demand.

Return: processes for the return or receiving goods that are returned for any reason.

Enable: processes that prepare, support, or handle information or relations dependent on planning and execution.

Domain 2—(Asset Security)

Data Stewards

Different than a data custodian. They implement data governance policies. SME for categorization of data, data definitions for its use, and implementing data governance

Data Controller

Determines the purpose and the means of processing personal data.

Domain 3—(Security Architecture and Engineering)

SP 800-27 Rev A IT Security Principles:

Engineering Principles for Information Technology Security is a list of system-level security principles to be considered in the design, development, and operation of an information system.

Categories:

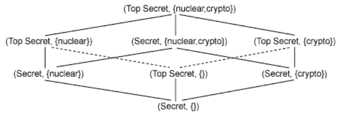
Security Foundation (principles 1-4); Risk Based (principles 5-11) Ease of Use (principles 12-15); Increase Resilience (principles 16-23); Reduce Vulnerabilities (principles 14-29); Design with Network in Mind (principles 30-33)

State Machine Models:

Based on Finite State Model (FSM). A finite-state machine (FSM) is a mathematical model of computation. It is an abstract machine that can be in exactly one of a finite number of states at any given time. The FSM can change from one state to another in response to some external inputs; the change from one state to another is called a transition. An FSM is defined by a list of its states, its initial state, and the conditions for each transition. Simple examples are vending machines, which dispense products when the proper combination of coins is deposited. Always in a secure state. In current states and in transitions. Implemented through the security policy. Basis for other models

Multi-Level Lattice Models:

Zones of security (compartmentalization). One way information flow. Subjects are assigned security clearances. Objects are assigned security labels. The lattice model essentially puts all possible combinations of entity access on each privilege level. As such, an individual can only possibly be at one point in the lattice.



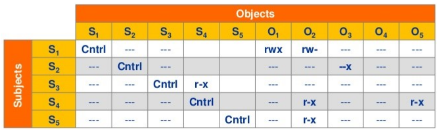
Non-interference Models:

Preventing high-level actions from being examined by low-level users. Information leakage concerns through: Inference attack (indirect covert channel). Requires complete separation between security levels. In simple terms, a computer is modeled as a machine with inputs and outputs. Inputs and outputs are classified as either low (low sensitivity, not highly classified) or high (sensitive, not to be viewed by uncleared individuals). A computer has the non-interference property if and only if any sequence of low inputs will produce the same low outputs, regardless of what the high level inputs are. That is, if a low (uncleared) user is working on the machine, it will respond in exactly the same manner (on the low outputs) whether or not a high (cleared) user is working with sensitive data. The low user will not be able to acquire any information about the activities (if any) of the high user.

Matrix Based Models:

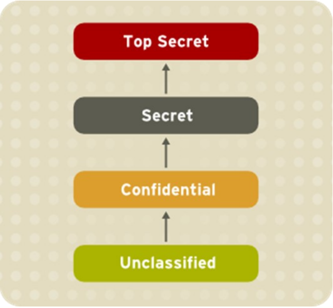
Focus on one to one relationship between subject and object.

Access control matrix. Typical access methods: Read / Write / Edit / Delete



		Objects									
		S_1	S_2	S_3	S_4	S_5	O_1	O_2	O_3	O_4	O_5
Subjects	S_1	Cntrl	---	---			rwx	rw-	---	---	---
	S_2	---	Cntrl	---			---	---	--x	---	---
	S_3	---	---	Cntrl	r-x		---	---	---	---	---
	S_4	---	---	---	Cntrl		---	r-x	---	---	r-x
	S_5	---	---	---		Cntrl	---	r-x	---	---	---

Information Flow Model:



Primary focus is controlling the flow of information whether up/down or within its own compartment . Prevent covert channels that would bypass the designed flow of information. Each piece of information must have unique properties. It evaluates writing low level data to high levels. Illegal operations are prevented. Example: Biba, Bell LaPadula

Common Criteria:

TCSEC	ITSEC	CC	Designation
A1	F6+E6	EAL 7	Verified Security
B3	F5+E5	EAL 6	Security Domains
B2	F4+E4	EAL 5	Structured Security
B1	F3+E3	EAL 4	Security Labels
C2	F2+E2	EAL 3	Controlled Access
C1	F1+E1	EAL 2	Discretionary Security
D	E0	EAL 1	Minimal Security

Vulnerabilities:

Client-Side Attacks

Caused by the user downloading malicious content. Attack initiates from victim

Server-Side Attacks

A listening service is attacked directly by an attacker Defense: Firewalls / Patching / System hardening / Defense in depth

Design Principles:

Diskless workstations: Computer without a hard drive (sometimes also no CDROM or floppy).

Thin clients: Replacement for desktop PCs. Similar to mainframes where there is a centralized server supplying applications to the clients.

Thin processing: Very little processing is performed by the client. Only performs keyboard input and screen output. All application processing is done on the server.

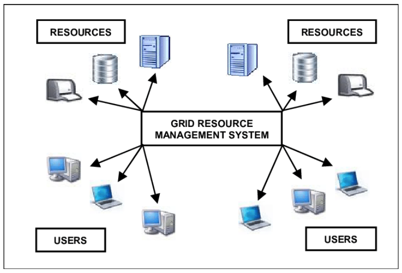
Thin storage: shared, centralized storage (NAS/SAN).

Design Principles (cont.):

Thick clients: also called heavy clients, are full-featured computers that are connected to a network. Client systems should minimally include: A supported and licensed OS. Updated, verified and supported anti-malware and anti-virus capabilities are installed. HIDS are installed. Whole drive encryption or file level encryption capabilities. User access should be based on the principle of least privilege. The ability to actively monitor for vulnerabilities and patches.

Grid Computing:

Harness the power of computer cycles not being utilized. Load balance processing among multiple computers.



Cryptography Concepts and Definitions:

Cryptography: Science of protecting information by encoding it into an unreadable form.

Cryptanalysis: The science of breaking the secrecy of encryption algorithms.

Cryptology: The study of both cryptography and cryptanalysis.

Algorithm: The set of mathematical rules used in encryption and decryption,

Plaintext/Cleartext: Data in readable format, also referred to as cleartext.

Ciphertext/Cryptogram: Data that has been encrypted.

Encipher/encode: Act of transforming data into an unreadable format.

Decipher/decode: Act of transforming data into a readable format.

Avalanche Effect: A minor change in either the key or plaintext will have a significant change in the resulting cipher text.

S-Box: Substitution box.

Key space: The total number of possible values of keys.

Key Zeroization: The process of properly destroying keys at the end of their useful life.

Work Factor: Estimated time, effort, and resources necessary to break a cryptosystem.

Collision: When a hash function generates the same output from different inputs.

Initialization Vector/Salt: Numeric seeding value that is used with a symmetric key to provide more randomness.

Confusion: Provided by mixing key values during repeated rounds of encryption (random placement).

Diffusion: Provided by mixing up the location of the plaintext throughout the cipher (dispersed).

Zero Knowledge Proof: Prove knowledge of a fact to a third party without revealing the fact itself.

Steganography: Attempts to conceal data by hiding it. Used by placing information in objects such as graphics, sound files, or document headers.

Rounds: Mathematical operation performed several times on the same message block.

Encryption System:

Substitution Cipher (confusion): Characters are substituted or shifted. Caesar Cipher shifted up 3 (ROT3) characters. ROT13 came from Unix.

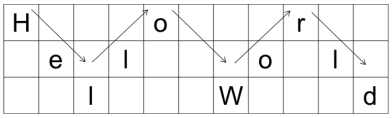
Transposition Cipher (diffusion): Rearranges bits or bytes

Null Cipher: Used in cases where encryption is not necessary Used for low security needs. Plain text is mixed with non cipher material (similar to steganography). a.k.a concealment cipher Protection similar to that of invisible ink.

Playfair Cipher: Used in WWII. Sender and receiver agree on a key word which is used in the table first, followed by the remainder of the alphabet skipping the key word letters and using I and J as the same letter.

Rail Fence Cipher: Simple transposition cipher. Susceptible to frequency analysis write across two lines diagonally and then list them a line at a time.

Original Message: Hello World



H				o				r		
	e		l				o		l	
		l				W				d

Encrypted Message: Horel ollWd

Vigenere Cipher: Polyalphabetic cipher. Ciphertext created by intersecting Plain text and a key.

Modular Math:

Letters represented by their numerical place in the alphabet.

A B C D E F G H I J … Z

0 1 2 3 4 5 6 7 8 9 10 …25

Ciphertext = plaintext + key (C = P + K)

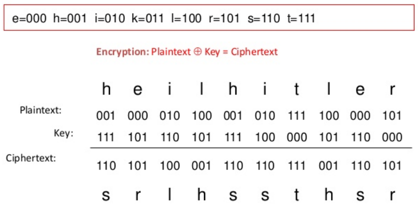
> Modulo function: result is the remainder. Running key ciphers use modular math. Often referred to as "clock math". 4 hours past 10 pm = 2am. (4 + 10) /12 remainder of 2.

A book cipher: Uses whole words from a well known text. Benedict Arnold used this to talk to the British. Agree on text source, page number, line, and word offset.

A running key cipher: Uses modulus math to add letters to message. Uses a line of text from a book.

One-Time Pad: Considered unbreakable. Each pad in the scheme must meet the following requirements: Made up of truly random values. Used once. Duplicate pad securely distributed to destination. Protected at sender's and receiver's sites. Must be at least as long as the message.

One-time Pad: Encryption



e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Encryption: Plaintext ⊕ Key = Ciphertext

	h	e	i	l	h	i	t	l	e	r
Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

Symmetric Encryption System:

International Data Encryption Algorithm (IDEA): Uses a block cipher and operates on 64-bit blocks of data. Uses 128 bit key and is faster than DES, 8 rounds. Used in PGP and other encryption software Patented (ends 2010) and licensing fees stopped Currently; no successful practical attacks.

Carlisle Adams and Stafford Tavares (CAST): Developed by Carlisle Adams and Stafford Tavares. Cast-128—64-bit block cipher. Uses keys between 40 and 128-bit lengths. Performs 12 to 16 rounds of operations. Cast-256—128-bit block cipher. Uses keys of 128,192,160, 224, and 256-bit lengths. Performs 48 rounds of operations.

Blowfish: Block cipher: 64-bit blocks of data, Variable key length from 32 bits up to 448 bits (128 bit is default). Performs 16 rounds of operations.

Twofish: Block cipher: 128-bit blocks of data. Variable key length from 128, 192, to 256 bits. Performs 16 rounds of operations.

SAFER (Secure And Fast Encryption Routine): 64 bit input block (SAFER-SK64) or 128 bit input block (SAFER-SK128). Used in Bluetooth for key derivation (block cipher).

RC4, 5, 6: Developed by Ron Rivest. Supports SSL and WEP protocol standards. RC4 most widely used software stream cipher RC5 and RC6 are block ciphers. RC6 lost out as replacement for DES.

Mobile Targets:

SMS: Short Message Service (SMS) SMS messages may be forwarded to the attacker.

Email: Email messages may be forwarded or searched for by an attacker.

Telephone: Attacker may be able to listen or record voice conversations.

Video/photo: Attacker may be able to activate the internal camera and record videos or take photos.

Social networking: May propagate malware; impersonation attacks may reveal personal information.

Location information: Attacker may be able to query location information.

Voice recording: Attacker may be able to activate the internal microphone to record sound or voice as well as phone calls.

Documents: Attacker may be able to retrieve documents stored on device.

Credentials: Cached credentials may be insecurely stored on device or in 3rd party applications.

Certificates & Authentication (PKI):

Certificate Policy

Set of rules dictating the circumstances under which a certificate can be used. Certificate policy used to protect CAs from claims of loss if the certificate is misused

Certificate Practice Statement

Published document describing:
How the CA is structured
Which standards and protocols are used. How certificates are managed.

Encrypting Keys Standards for Financial Institutions:

American National Standards Institute (ANSI) X9.17: Addresses the need to transmit securities and funds security over a electronic medium. Base on the hierarchy of keys. Data keys (DK) Used to encrypt and decrypt messages with normally a single connection or message life span.

Master Key Encrypting Keys (KKM): Must be distributed manually (Longer lifespan). Two tier model (they encrypt the data keys) Three tier model (they encrypt other key encrypting keys (KK) which are exchanged electronically and used to encrypt the data keys).

Key Wrapping and Key Encrypting Keys (KEK): Special purpose long term use key for key distribution or key exchange. The process of using a KEK to protect a session key is called “key wrapping”. Key wrapping can use either symmetric or asymmetric ciphers. Used by SSL, PGP, S/MIME to provide session key confidentiality, integrity and sometimes authentication.

Key Management:

Key Storage: Placement of a copy of secret keys in a secure location. There are two types of methods of key storage:

Software-based: Subject to access violations/intrusions. Easily destroyed. Subject to the security of the OS.

Hardware-based: The most secure form of digital certificate storage. More expensive than SW solutions. Relies on physical security. Smart cards or flash drives.

Key Escrow: Keys needed to decrypt cyphertext are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. Third parties may include; businesses, who may want access to employees' private communications. Governments, who may wish to be able to view the contents of encrypted communications. The third party should be permitted access only under carefully controlled conditions, as for instance, a court order.

Recovery Agent: Has authority to remove keys from escrow. Key removal can be protected by implementing an access mechanism called M of N control. Requires two or more recovery agents. There must be multiple key escrow recovery agents (N) in any given environment. A minimum number of agents (M) must work together to recover a key. Agents share a PIN or password. When N of them get together and split this PIN the key may be recovered.

Key Archival: Storage of keys and certificates for an extended period of time. Essential element of business continuity and disaster recovery planning.

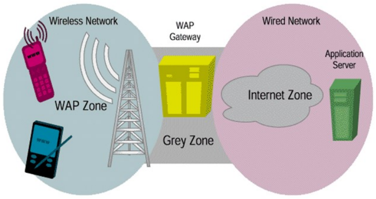
Multiple Key Pairs: Best reason to use multiple key pairs is to keep one key pair fully private and not use an escrow service. Eliminates the possibility of the escrow being compromised and your key pairs used in impersonation attacks.

ISO/IEC 19249

Information Technology-Security Techniques. **5 architectural principles:** domain separation, layering, encapsulation, redundancy, virtualization. **5 design principles:** least privilege, attack surface minimization, centralized parameter validation, centralized general security services, error and exception handling.

Domain 4—(Communications and Network Security)

Wireless Network – Wireless Application Protocol (WAP):



Wireless Markup Language (WML) is wireless markup language. Because of limited memory and processing power, the WAP Gateway modifies the HTML and makes it easier for the micro-browser to interpret by converting it into WML. Discusses on the “WAP Gap”, where the encrypted connection from your phone to the WAP gateway is decrypted to be re-encrypted over a common TLS/SSL link. This occurs in WAP 1.X versions only. WAP 2.X corrected the problem.

Secure Network Components – Hardware:

Modem (modulator-demodulator): Is a device that modulates analog carrier signals to encode digital information and then demodulates carrier signals to decode information. Commonly use Point to Point Protocol (PPP) encapsulation. Still use today.
Concentrators: Multiplexes connected devices into 1 signal to be transmitted on a network. A type of multiplexor that combines multiple channels onto a single transmission medium in such a way that all the individual channels can be simultaneously active.
Hubs: Are used to implement a physical star topology. Are inefficient and insecure because they forward all traffic to all hosts & allow anyone with physical access to intercept all of the traffic.
Repeaters: Are used to re-amplify signals. Increases the length of an Ethernet bus to accommodate a physically larger network.
Bridges: Filters traffic between segments based on MAC addresses. Amplify signals to facilitate physically larger networks. Used to connect LANs. Does not reformat frames. Does not prevent an intruder from intercepting traffic on the local segment.
Switches: Is a multiport device to which LAN hosts connect. Forward frames only to the device specified in the frame’s destination MAC address. Can perform more sophisticated functions to increase network bandwidth.
Routers: Forward packets to other networks. Read destination Layer 3 (IPv4 or IPv6) addresses to determine the route (next hop) to send the packet. Interconnect different technologies (i.e. Token Ring to Ethernet).
LAN extender: Is a remote access, multilayer switch used to connect distant networks over WAN links.
Brouters: Are combination devices comprising a router and a bridge. A brouter attempts to route first, but if that fails, it defaults to bridging. A brouter operates primarily at layer 3 but can operate at layer 2 when necessary.
Repeaters, Concentrators, and Amplifiers: Are used to strengthen the communication signal over a cable segment as well as connect network segments that use the same protocol. These devices can be used to extend the maximum length of a specific cable type by deploying one or more repeaters along a lengthy cable run. Repeaters, concentrators, and amplifiers operate at OSI layer 1. Systems on either side of a repeater, concentrator, or amplifier are part of the same collision domain and broadcast domain.

Secure Voice Communication – Phone System Abuse:

POTS/PSTN; Old school Phreaking (free phone calls).
Black – box (Home Phone Abuse). Voltage Manipulator.
Red –box (Pay Phone Abuse). Coin tone generator.
Beige/White - box. Telco Handset, Frequency generator, DTMF, what phone techs carry.
Blue – box. Hack the Phone Switch. Trunk system tone generator.

Remote Connectivity Technology:

Integrated Services Digital Network (ISDN)
Basic Rate Interface (BRI) (One 16Kbps D channel, Two 64Kbps B channels).
Primary Rate Interface (PRI) (One 64Kbps D channel, Twenty Three 64Kbps B channels).
In Europe, One D channel, Thirty B channels.
Commonly used in PBXs.
D-Channels: Call setup/maintenance.
B-Channels: Carry network payload.

Switching Technologies:

Circuit Switched: Dedicated physical circuit path is established, maintained, and terminated, Extensively used in telephone company’s networks. Uses a fixed bandwidth and fixed path, Constant packet queues.
Packet Switched: Splits data into packets. Static or variable sized, Each packet may take a different route (path) over a shared network. Emulates a circuit switched network by using virtual links. Devices share bandwidth (by using statistical multiplexing) on communications links. Network is more resilient to error and congestion.

Switching Technologies Examples:

Circuit Switching Network: Digital Subscriber Line (xDSL), Data Over Cable Service Interface Specification (DOCSIS), Integrated Services Digital Network (ISDN).
Packet Switching Network: Asynchronous Transfer Mode (ATM), Frame Relay, Multi-Protocol Label Switching (MPLS), Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH), X.25.

Switching Technologies:

Switched Virtual Circuit (SVC): Temporary connection established on demand (like a dial-up connection). Maintains constant packet queues. Actual bit rate and latency are dependent on packet switched traffic load.

Permanent Virtual Circuit (PVC): Dedicated circuit link (seldom disconnected). Doesn't require the bandwidth overhead associated with circuit establishment and termination. More expensive option than SVCs.

Switching Technologies —Wide Area Network (WAN) Technologies:

T = Copper Carrier

T1 = 1.544 Mbit/s   T3 = 44.736 Mbit/s

E = Copper Carrier

E1 = 2.048 Mbit/s   E3 = 34.368 Mbit/s

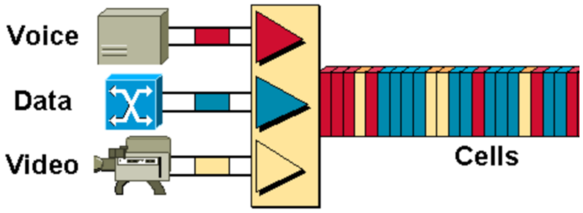
J = Copper Carrier

J1 = 1.544 Mbit/s   J3 = 32.064 Mbit/s

O = Optical Carrier

OC-n = n x 51.8 Mbit/s

Asynchronous Transfer Mode (ATM): Cell switching, Broadband ISDN. Provides both SVC and PVC. Fixed size frame, 53-byte cells Reduces jitter, good for voice. Initially designed for T3+ carriers.



Domain 5—(Identity and Access Management (IAM))

Identification - Security Identifier (SID) Breakdown:

S-1-5-21-4035617097-1094650281-2406268287-1981

S - identifies string as a SID

1 – revision level or version

5 – authority value

21-4035617097-1094650281-2406268287 – local computer identifier (48 bit).

1981 – Relative ID (RID) "greater than 1000 for all non-system users.

Identity Management Implementation – Directory Technologies:

X.400 guidelines for the exchange of e-mail. Known as the "Message Handling System". Supports two basic functions; message transfer and message storage. Addresses consist of a series of name/value pairs separated by semicolons. Largely replaced by SMTP based e-mail systems.

X.400 address specifications:

O-organization name

OU-organizational unit name

S-surname

G-given name

I-initials

C-country name

Identity Management Implementation – Kerberos Elements:

Key Distribution Center (KDC): The foundation of Kerberos is the client and server's trust in the KDC. Consists of a ticket granting service and authentication server. Holds user's and services' keys.

Authentication service (AS): Provides the service of authentication of principals. Supports mutual authentication for workstation and servers.

Ticket-Granting Service (TGS): A network service that supplies temporary session keys and tickets to authorized users or services. Gives the user the ability to request access to a resource.

Realm: Is the set of components and principles that the KDC provides services for (Kerberos domain). Knowledge of that secret key equals proof of identity.

Principals: Entities requiring KDC services – users, apps or services. The KDC and each principal share a secret key.

Ticket: Tickets are created by the KDC and given to a principle when that principle needs to authenticate to another principle Data that authenticates a principle's identity.

Credentials: Ticket + a service key.

Ticket contents: Principle; intended service principle, Internet Protocol (IP) of requester; time stamp, ticket lifetime (10 hours - <24 hours); and session key.

KDC database: Encrypted with a master key. All subsequent dumps and backups encrypted with same master key.

KDC database contents: Principle, encryption key and key version number, maximum ticket validity, maximum time for ticket renewal, attributes or flags, password expiration date, and expiration date of principle (no tickets after this time).

Identity Management Implementation – Accountability:

Strong Identification: An action must be attributable to a single individual/process/device/object. An individual can repudiate any action if it cannot be directly associated with them (i.e. shared accts).

Strong Authentication: Helps ensure non-repudiation by strongly associating something only 1 individual has to an account. Increases accountability when used with strong identification.

User Training & Awareness: Informed users are less likely to intentionally/unintentionally abuse accts/access/information if they're aware of the consequences.

Monitoring: Visibility into an information system will help identify when accountability issues arise. Also must ensure that visibility is created with regards to internal activities/information flows.

Audit Logs: Are necessary to track an action back to a user. Very useful in ensuring accountability.

Identity Management Implementation – Accountability (cont.):

Independent Audits: Provides an unbiased 3rd party review of accts/actions/impacts. Is required to establish accountability when collusion may have occurred between several parties.

Policy: Provides expectations of behavior and defines sanctions/ rewards for accountability related behaviors. Accountability cannot be enforced consistently/fairly without a policy.

Organizational Behavior: Expectations must come from senior management (i.e. top down approach) to ensure that accountability is the culture of the organization. Requires that violations of accountability be met with in a timely/consistent manner.

Additional measures:

Control Physical Access

Control Electronic Access to Password Files

Encrypt Password Files

Use Password Masking

Deploy Multifactor Authentication

Use Account Lockout Controls

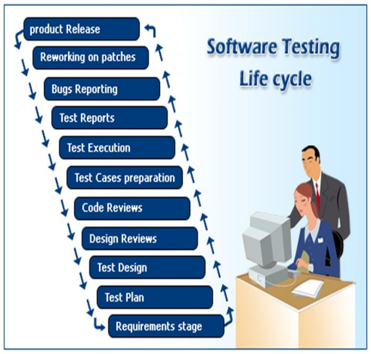
Use Last Logon Notification

Actively Manage Accounts

Use Vulnerability Scanners

Domain 6—(Asset Security)

Software Testing Levels:



Interface testing – very important test to test quality. Checks data passage between systems

Alpha testing – conducted by a team of highly skilled testers at development site

Beta testing – conducted in real-time environment by customers or end users

Pilot testing – evaluation functionality

Installation testing – installation and first operation

Integration testing – testing multiple components as they function together (big bang integration testing tests all components)

Regression testing – test after update or modification

Acceptance testing – testing directly with the customer

Function testing – validate against checklist of requirements

Parallel testing – test between and unchanged system

Sociability testing – validate system can operate in target environment

Unit testing – low level software components

Combinatorial Software Testing:

Black box testing method

Seeks to test all unique combinations of software inputs

Example: pairwise testing; 8 steps could be tested in 4 steps by pairing up requirements.

Software Testing Tenets:

Expected test outcome is predefined

Good testing has a high probability of finding an error

Successful testing finds errors

Testing is independent from coding

Employ both user and programmer expertise

Use different programs than those of the programmer

Test documentation is reusable

Examining only the usual case is insufficient

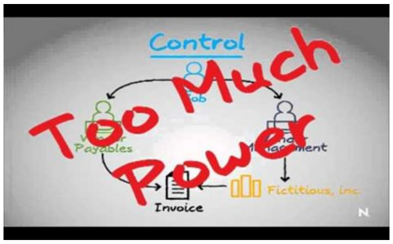
Domain 7—(Security Operations)

Types of Attacks Requiring Incident Response:

Threat Agents
Password Guessing and Cracking
Session Hijacking and MITM
Threat Vectors
Malware
DoS/DDoS

Administrative Control Methods:

Separation of Duties (separation of powers): Prevents a single individual from performing necessary steps requires to compromise security. Load balance functionality - requires two or more people to perform a specific function. The goal is to make it difficult to perform and/or hide fraudulent activities. Organizations should have a complete list of roles with associated responsibilities. KEEPS A COMPANY FROM PLACING DANGEROUSLY HIGH TRUST NI A SINGLE INDIVIDUAL



Least Privilege: The principle of least privilege will ensure that individuals know only that information required to do their assigned tasks. Users are given the minimum access necessary to perform their jobs. The greater number of privileges that operate in privileged mode the more attack vectors available in that mode. Assign no other privileges than those needed to accomplish the task.

Need to Know: Can prevent unauthorized disclosure or espionage. Access determination is based on clearance level of the subject and classification level of the object. Insufficient. Compartmentalization enforces need to know. Not everyone at a certain level needs to know everything at that level.

Job Rotation/Rotation of Duties: Rotation of responsibilities. Builds skill redundancy. Can mitigate fraud. Can relieve worker burnout. Some companies find the cost of job rotation not worthy of the practice. Can be implemented through mandatory vacations.

Mandatory Vacations: Reducing or detecting personnel single points of failure. Detecting or deterring fraud. Good for all key billets. Should be at least 2 weeks in length.

Security Audits and Reviews: Typically performed by a third party, sometimes penetration tests. Internal, performed by someone without management responsibility for the system. External, outside entities perform the review. Clipping levels, baselines/thresholds. Record Retention, example where HR records may be kept on file for 7 years.

Supervision: can involve audit logs, screenshots, network activity.

Input/Output Controls: input involve time stamps, authentication, and logging for accountability and validation. Output involves things like coversheets, etc.

Antivirus Management: Requires continual updates and scheduled scanning.

Statistical Inference: Reporting based on statistical and nonstatisitical (random) sampling.

THESE MITIGATE FRAUD

Controlling Privileged Accounts - Privileged Accounts:

System Administrators: Ensure that a system or systems functions properly for users. Perform maintenance and monitoring tasks. Require the ability to affect critical operations such as boot sequence, log files, and passwords. Manage hardware and software for workstations and servers.

Operators: Have elevated privileged, but less than administrators. Can usually perform the following:
Start the operating system
Mount / Dismount volumes
Control jobs.
Monitor process execution
Bypass / Rename labels

Security Administrators: Provide oversight for the security operations of a system. Usually have fewer rights than system administrators. Ensure separation of duties is enforced. Provide a check and balance of power to system administrators. Ensure security policies are enforced.

Ordinary Users: Only have access to applications and systems necessary for them to perform a given task. Should not be able to monitor processes. Must operate within security labels. Should be prevented from altering the boot process.

Service Account: Dedicated to providing a system service. Usually run background services/daemons. Often assigned elevated privileges upon install of an operating system. Many are created by database installations.

Functional Security Operations Concepts – Monitoring Special Privileges:

Those with the most access require the most watching:
Job functions that require greater scrutiny:
Account creation/modification/deletion
System reboots
Data restoration
Audit log access
Data backup
Source code access
Security configuration capabilities.

Preventative Measures Against Attack – Intrusion Detection System (IDS) – Alarms and Signals:

Meant to notify people and systems of adverse events.
Three fundamental components:
Sensor: Detection mechanism.
Control and Communication: Handling the alert information.
Enunciator: Relay system.

Whitelisting, Blacklisting, Greylisting:

Whitelist - Known good. Whitelisting is the practice of identifying entities that are provided a particular privilege, service, mobility, access or recognition. Entities on the list will be accepted, approved and/or recognized.

Blacklist - Known bad. In computing, a blacklist or block list is a basic access control mechanism that allows through all elements (email addresses, users, passwords, URLs, IP addresses, domain names, file hashes, etc.), except those explicitly mentioned. Those items on the list are denied access.

Greylist - Not fully trusted. Greylisting is a method of defending e-mail users against spam. A mail transfer agent (MTA) using greylisting will "temporarily reject" any email from a sender it does not recognize. If the mail is legitimate, the originating server will try again after a delay, and if sufficient time has elapsed, the email will be accepted.

Change and Configuration Management – Recovery Site Strategies:

Dual data center: employed for applications which cannot be down without impacting business. Application is split between two geographically dispersed data centers and either load balanced or hot swapped between the two businesses.

Hot Site: Office space appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and personnel. Typically staffed 24/7. Hot site personnel prepare the site the moment they are notified. Maximum Tolerable Downtime (MTD) measured in hours.

Internal Hot Site: Site on standby. Must keep hot site identical to working environment to eliminate delaying recovery.

External Hot Site: Equipment is on site but site must be built. Service is through a contracted service/recovery provider. Site ran by a hot site vendor. It should mimic the site it is recovering

Warm site: leased or rented facility that is partially configured where the rest of the configuration happens after the disaster has occurred; includes some or all of the system hardware, software, and power sources. Maintained in an operational status ready to receive the relocated system. May serve as a normal operational location for another system or function. MTD is 1-3 days (usually 48 hours). Warm Mobile: Self contained, transportable shells, custom fitted with specific IT and telephone equipment. Available for lease through commercial vendors. Data center on wheels.

Cold Site: An empty data center space with no technology on the floor with adequate space and infrastructure to support IT systems (no IT or ADP equipment) MTD is in weeks. All equipment will have to be purchased or acquired at the time of the disaster.

Recovery Time:

Cold sites (1-2 weeks)   Warm sites (5+ days)
Hot sites (few minutes/hours)   Mobile sites (3-5 days)
Multiple processing sites (minutes - hours)
Workspace and facilities (hours - days)
Virtual business partners (days - weeks)

Other sites: Rolling, service bureaus, redundant

Virtual business partners: Create a Mutual Assistance Agreement (MAA)

Processing Agreement: Similar to a reciprocal or outsourced agreement to create different processing agreements with other organizations.

Outsourcing: allowing another organization to provide contingency operations and disaster recovery services.

Multiple Processing Sites: A distributed implementation that requires each processing site to be capable of processing, storing and transmitting another site's data.

Mirrored: fully redundant with full real time information mirroring. Highest degree of availability. Most expensive choice.

Tertiary site: A second backup site (backup to the backup). IT full production backup: if the workload can not be identified in terms of hardware resources and data storage requirements, then the alternative is to recover the entire IT production workload.

Distances of Sites: Minimum site distance is 5 miles. Low to medium critical site minimum distance is 15 miles. Maximum protection of critical components distance is 50 – 200 miles.

Drives and Data Storage – Redundant Array of Independent Disk (RAID) Levels:

RAID 0: writes files across multiple drives at once (striping). Provides no fault tolerance, but does provide increased performance for data read and writes.

RAID 1: mirroring – duplicates all data from one disk to another. Provides redundancy for data and, optionally, for RAID controllers. Disk reads can also be improved with RAID 1 arrays.

RAID 3 and 4: require 3 or more drives; stripes data; uses a dedicated parity drive; RAID 3 stripes at the byte level (more efficient) while RAID 4 stripes at the block level (faster)

RAID 5: stripes data and parity information across multiple drives, offering both performance and redundancy. Block level, OS can do it (same as dynamic disks) (same as Linux MDADM distributed parity)

RAID 6: extends the capabilities of RAID 5 by computing 2 sets of parity information (it accommodates the failure of 2 drives)

RAID Level 7: enables the drive array to continue to operate if any disk or any path to any disk fails, because it adds caching. RAID 7 is based on concepts used in RAID levels 3 and 4, but adds caching. RAID 7 isn't an open industry standard; it is really a trademarked marketing term of Storage Computer Corporation used to describe their proprietary RAID design.

RAID 10: a combination of RAID 0 and RAID 1, sometimes called RAID 1+0 or RAID 0+1 .

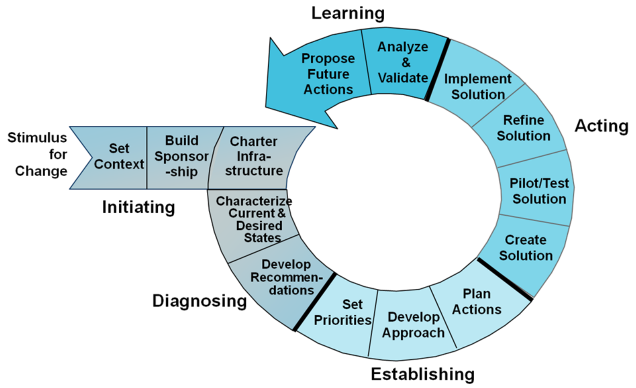
Nested RAID/Multi-RAID: RAID 1+0 (10); RAID 5+0 (50); RAID 6+0(60); RAID (1+0)+0 (100).

Striping increases read/write efficiency. Parity provides data redundancy. All of the RAID levels from RAID 3 to RAID 7 use parity. The most popular of these today is RAID 5. RAID usually has 2 out of 3 of these qualities: CHEAP, FAST, RELIABLE.

Domain 8—(Software Development Security)

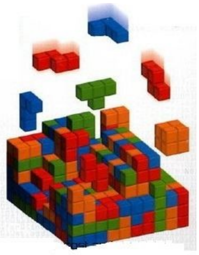
IDEAL Model:

Initiating (business reasons behind the change are outlined).
Diagnosing (current state and recommendations for change)
Establishing (plan of action to achieve changes)
Acting (develop solutions, test, refine, implement)
Learning (analyze efforts to determine if goals are achieved)
Roadmap for initiating , planning, and implementing improvements. Initiating: stimulus for improvement, set context and establish sponsorship; establish improvement infrastructure. Diagnosing: appraise and characterize current practice; develop recommendations and document phase results. Establishing: set strategy and priorities; plan actions; establish process action teams.



Structured Programming Model:

Non-iterative. Widely known model taught in almost all academic systems development courses. Promotes discipline, allowing introspection, and provides controlled flexibility. Requires refined processes and modular development. Each phase subject to review and approval. Allows for security to be added in a formalized, structured approach. Widely known; flexible; taught in school. Incremental model: divide project into builds; sections created and tested separately; find errors in user requirements quickly; user feedback solicited after each stage.

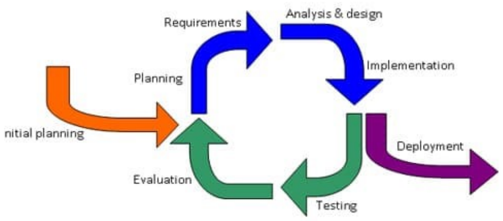


The Pieces Fall Into Place

Structured Programming

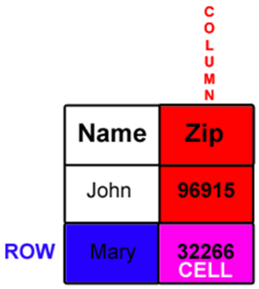
Iterative Development Model:

Allow for successive refinements, requirements, design, and coding. Change control mechanism implemented. Makes security more difficult. Project scope may be exceeded by requirement changes.



Database Terminology:

Cell: Intersection of a row and column.
Element: Data within the cell. Any unit of data defined for processing, for example: "Name", "Address", "City“. Defined by size (in characters) and type (alphanumeric, numeric only, date, etc.).
Degree: Number of columns.
Candidate Key: Attributes identifying a record.
Primary Key: Unique identifier. Each table has only 1 primary key from the set of candidate keys.
Foreign Key: Attribute related to another table.


COLUMN
ROW
CELL

Name	Zip
John	96915
Mary	32266

View: Virtual table.
Schema: DB structure. The description of the tables and views with the relationship between them.

Structured Query Language (SQL):

SQL gives the user a high level view of the data.
Data Manipulation Language (DML) Contains all the commands that enable a user to view, manipulate, and use the database, (add, modify, delete).
Data Definition Language (DDL): Defines the structure and the schema of the database (table size, key placement, views, and data element relationships). Create / Alter / Drop databases, tables, views.
Data Control Language (DCL): Defines the internal organization of the database. You can grant or revoke rights to connect, select, insert, update, delete, usage. Provides security aspects of SQL: commit, save point, rollback, and set transaction.
Data Query Language (DQL): Allows users to make requests of the database.
Dynamic Data Exchange (DDE): When MSWord (client) requests data from an Access data base (server), a DDE channel is opened to transfer the data.
Types: MySQL, PostgressSQL, PL/SQL (procedural language/SQL (oracle)), T-SQL, ANSI-SQL>MSSQL
Common SQL commands: create, select, delete, insert, update.

Database Interface Languages:

Open Database Connectivity (ODBC): An application programming interface (API) that allows an application to communicate with a database locally or remotely.
Java Database Connectivity (JDBC): An Application Programming Interface (API) that allows a Java application to communicate with a database. Same as ODBC but for Java. Allows Java programs to execute SQL commands. Allows Java apps to communicate to DB directly or through ODBC (API).
Extensible Markup Language (XML): A standard for structuring data so it can be easily shared by applications that use web technologies. Standard for structuring data on the web in a neutral format.

Database Interface Languages (cont.):

Object Linking and Embedding (OLE): It allows access to data no matter where it is located or how it is formatted. (such as viewing Excel data via MS Access). Uses the component object model (COM) to function. Allows the linking of data across various DBMSs.

Active-X Data Objects (ADO): A set of ODBC interfaces that exposes the functionality of a database through accessible objects. SQL (structured query language) commands are not required when using ADO. Developers can write programs that access data, without knowing how the database is implemented. Non SQL API.

Metadata Controls:

Can manage restricted access to information. Serves as a gatekeeper to filter access. Metadata should be tightly bound to the data (do not move the data without the metadata). Metadata can be disclosed via documents such as word (in the properties); ensure information is removed from the properties of the document. Metadata: used to permit communication about the data to take place between programs that do not otherwise know about each other.

Data Contamination Controls:

Input controls: Transaction counts, dollar counts, hash totals, error detection, error correction, resubmission, self-checking digits, control totals, and label processing.

Output controls: Reconciliation, physical handling procedures, authorization controls, verification, and audit trails.

Open Source:

Code is freely available to those that chose to use it. The more eyes on the code, the more likely the bugs will be discovered (Full Disclosure). There is no security through obscurity. "Security through obscurity" – idea that if a system is little known, there is less likelihood that someone will find out how to break it; Does not work!

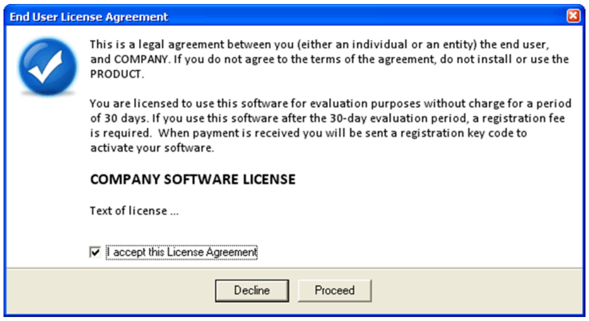
Issues: Does not ensure that all security bugs will be found; leads to false sense of security. Dishonest programmers may not disclose problems (at least until it has been exploited). Blackhats have blackmailed vendors when they have found problems.

Software Licensing:

What does "FREE" really mean? In the context of software licensing, free doesn't refer to price. It means free in the sense of "free speech" and refers to the rights and restrictions imposed on using software. In everyday conversation, there's not much difference between "free software" and "free and open-source software" (FOSS). However, the official definitions and underlying philosophies do differ. End User Licensing Agreement (EULA), spells out what you can and can't do with software. It covers everything from how many copies you can install to what the software company can do with your data and what additional software the company can install on your computer.

Open Source Licenses:
GNU Public License (GPLv2, GPLv3)
Berkley Software Distribution License (BSD)
Apache Software Foundation License

The GNU General Public License (GPL) is one of the most commonly used licenses for open-source projects. The GPL grants and guarantees a wide range of rights to developers who work on open-source projects. Basically, it allows users to legally copy, distribute and modify software.



This is a legal agreement between you (either an individual or an entity) the end user, and COMPANY. If you do not agree to the terms of the agreement, do not install or use the PRODUCT.

You are licensed to use this software for evaluation purposes without charge for a period of 30 days. If you use this software after the 30-day evaluation period, a registration fee is required. When payment is received you will be sent a registration key code to activate your software.

COMPANY SOFTWARE LICENSE

Text of license ...

☑ I accept this License Agreement

Software Licensing—Copyleft verses Copyright:

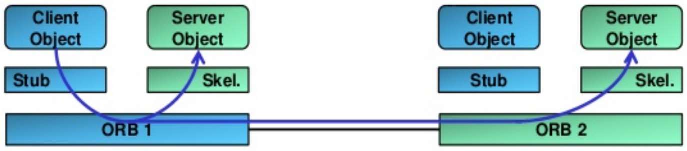
Copyleft: A general method for making a program (or other work) free, and requiring all modified and extended versions of the program to be free as well. Copyleft guarantees that every user has freedom. To copyleft a program, we first state that it is copyrighted; then we add distribution terms, which are a legal instrument that gives everyone the rights to use, modify, and redistribute the program's code, or any program derived from it, but only if the distribution terms are unchanged. Thus, the code and the freedoms become legally inseparable.

Copyright: Source code is a work much like a book, written by one or more people. The source code is copyrighted by the authors (whether or not they register this copyright, it's automatic). An author can thus decide to distribute source code if he/she wants to. This distribution does not give the recipients of the source code any rights other than to make use of it. They can not create derivative works and redistribute it.

Distributed Object Oriented Systems:

Applications are broken into components. Components can exist in different locations and communicate in a way that is seamless to the user. Today's applications are designed on distributed objects such as (examples):
Java Remote Method Invocation (JRMI)
Enterprise JavaBean (EJB)
Common Object Request Broker (CORBA)
Distributed Component Object Model (DCOM)

Common Object Request Broker Architecture (CORBA):



Inter-ORB communication uses the GIOP (General Inter-ORB Protocol)

Object Request Brokers (ORB)::

Mechanisms that enable objects to communicate locally or remotely.

Object Request Brokers (ORB): Enables different components throughout a network to communicate with each other. The middleware that establishes client/server relationships between objects. ORBs perform language mapping and operate similar to a .DLL file. Connect programs to programs

Object Management Group (OMG): An international open membership nonprofit computer industry consortium Develops enterprise integration standards.

Object Management Architecture (OMA): Set of standard interfaces for objects that support CORBA applications. Defines the behavior of objects in a distributed environment. Provides guidance on how standardization of component interfaces penetrate through applications in order to create a plug and play component software environment based on object technology

Interface Definition Language (IDL): A generic term for a language that lets a program or object written in one language communicate with another program written in an unknown language.

Middleware: Computer software that connects software components or applications.

Pipes: Objects communicate with each other using pipes Examples are RPCs (remote procedure calls) and ORBs If an object on a workstation needs an object on a server to process data, it makes the request through an ORB OOA (Object Oriented Analysis) – analyze a problem (problem domain). OOD (Object Oriented Design) – develops the solution OOAD (Object Oriented Analysis and design) when the two are used as one.

Component Object Model (COM) / Distributed Component Object Model (DCOM):

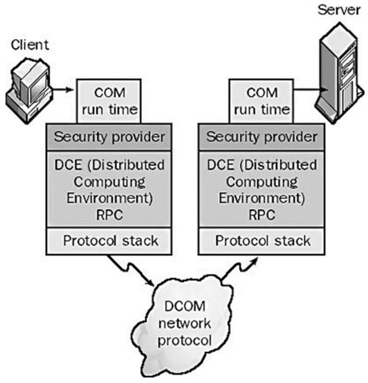
Component Object Model (COM): Microsoft's framework for developing and supporting components. COM objects allows other applications or components to access their features. Binary standard language agnostic similar to CORBA and JAVA Beans. Uses a class factory, component whose main function is to create other components by implementing a standard interface.

Distributed Component Object Model (DCOM): Allows for applications to access objects on different parts of the network. Provides ORB like services as it operates as middleware to enable distributed processing. Supports Object Linking and Embedding (OLE)

Application Programming Interface, interface between an application process and the TCP/IP protocol stack

Globally Unique Identifier (GUID), application identifier which provides a unique reference number. Used in the registry to identify COM DLLs

Object Linking and Embedding (OLE), allows embedding and linking to objects developed by Microsoft.



Inter-Process Communication (IPC) / Distributed Inter-Process Communication (DIPC):

Inter-Process Communication (IPC): Mechanisms that facilitate communication and data exchange between processes or threads (child processes). IPC is a Windows and Linux process; DIPC is used within Linux/UNIX.

Distributed Inter-Process Communication (DIPC): Software-only solution for distributed data exchange and programming under Linux. Enables programmers to write distributed software without the need to know about network programming.

Object Oriented Analysis (OOA):

Seeks to understand the problem. Identifies all objects and their interaction. Uses Unified Modeling Language (UML) . UML is a standard language for specifying, visualizing, constructing, and documenting the artifacts of software systems. Created by the Object Management Group (OMG).

Object Oriented Design (OOD):

Sometimes combined with Object Oriented Analysis Design (OOAD). Develops the solution based on the analysis. Uses Unified Modeling Language (UML)

Threats in the Software Environment – Software Vulnerabilities:

Hard-coded Credentials (backdoors)
Buffer Overflow
SQL Injection, manipulate data base via front end web server,
Directory Path Traversal, escape from root of web server by referencing directories such as ../..
PHP Remote File Inclusion, Alter Hypertext Preprocessor (PHP) urls to include and execute remote content.
Cross-site Scripting & Cross-site Request Forgery, 3rd party execution of web scripting languages.
Privilege Escalation, (vertical escalation) become a administrator (horizontal escalation) become a different user.

Threats in the Software Environment – Malicious Software:

Virus: A small application, or string of code, that infects applications; replicates itself to other disks; requires a host to reproduce. Viruses has 3 parts; replicator, concealer, and payload. Must have a technology that allows them to spread from system to system. 1st priority is to replicate. Require a host to reproduce. Viruses have 2 main functions; propagation and destruction.

> Stealth: Hides by tampering with the OS to fool antivirus software. Encryption/Compression will help hide the virus
> Polymorphic: Mutates by modifying its own code as it travels from system to system, while still keeping the original algorithm intact. Pads code but keeps original code intact; sometimes encrypted. Makes pattern recognition hard.
> Oligomorphic: common, code similar to polymorphic, but has a decryptor that does not show up on signature list.
> Metamorphic: reprograms itself; carries various versions of itself. Avoids pattern recognition, more effective than polymorphic, and requires code emulation to detect. Translates itself into temporary representations and then back to normal code. Capable of infecting more than one OS.
> Zoo Viruses: laboratory viruses not found in the wild.
> Retro virus: turn off anti-virus
> Multipartite: dual infector; (original term) boot sector and program files; (now) infect more than one type of object.
> Macro: visual basic mostly, targeting word or power point; attack templates like normal.dot to stay resident.

Trojan Horse: a program that is disguised as another program; performs its malicious activity in the background. Conceals itself by renaming itself to normal files. Can corrupt the antimalware programs. Can be polymorphic.
Logic Bomb: executes a program, or string of code, when a certain event happens or a date and time arrives.
Worm: Different from a virus as it can self reproduce without a host application and are a self-contained program. Worms can propagate by using mail, website downloads, etc. Worm has 5 parts; penetration tool, installer, discovery tool, scanner, and payload.
Adware: Software which generates adds that installs itself on your computer. Some types of adware are also spyware or malware. Companies sometimes track user browser habits through cookies. Some cookies cause popup windows that advertise a product or service.
Spyware: Secretly installed on a computer to intercept or take partial control over the user's interaction with the computer, without the user's consent. Could capture surfing habits, keystrokes, passwords, system information, or install a backdoor.
Drive by Download: ZERO CLICK ATTACK, once you visit a website, malware is downloaded to your system.
A lot of well known sites have been infected by trojans: USA Today; Wal-Mart; Target; zdnet; cdnet, ABC News; Bank of India; china.com; nature.com; redmonmag.com; Google; barakobama.com.

Threats in the Software Environment – Malformed Input Attacks:

Attacks employing specially crafted user input. Examples: Unicode format for a browser URL that bypasses firewall rule sets. Structured Query Language (SQL) queries in the browser. URL box (cross-site scripting). Firewalls may not recognize a Unicode format (as opposed to ASCII format). Unicode recognizes other languages, ASCII does not (only English). Unicode (32-bit characters); ASCII (8-bit Characters). ASCII is the primary format for storing text (in DOS, Win95; NOT NT/2000 series). Web browser could be redirected to another site. The largest attack vectors are:
Cross-site scripting SQL injection Privilege escalation
XSS example:
<script src=http://hackers.org/xss.js></script>
<img src=javascript:alert (‘xss’)>

Threats in the Software Environment – Trapdoor / Backdoor:

a.k.a. Maintenance or Programming Hook. Software entry point that is inserted by the programmer. Allows developers to bypass normal access restrictions. There are sometimes “unknown backdoors” especially with older software.
Malware backdoor programs: subseven, back orifice, netbus, bionet, deep throat.
Find the backdoors with programs such as Mbam, GMER, and unhack me.

Threats in the Software Environment – Ransomware:

A type of malicious software designed to block access to a computer system until a sum of money is paid (Bitcoin). Ransomware can be spread through malicious email attachments, infected software apps, infected external storage devices and compromised websites. A growing number of attacks have used remote desktop protocol and other approaches that don't rely on any form of user interaction. In a lockscreen variant of a ransomware attack, the malware may change the victim's login credentials for a computing device. In a data kidnapping attack, the malware may encrypt files on the infected device, as well as other connected network devices. In May 2017, an attack called WannaCry was able to infect and encrypt more than a quarter million systems globally. The malware uses asymmetric encryption so that the victim cannot reasonably be expected to recover the (private and undistributed) key needed to decrypt the ransomed files.
2016: 1,419 ransomware variants reported.
2017: 2,855 ransomware variants reported.

Threats in the Software Environment – Rootkits:

4 generations of root kits (Trojans, kernel based, hardware based, memory based). An undetected assembly or collection of programs and code that allows constant presence on a computer or automated information system. A collection of tools, binaries, scripts, configuration files that allow intruders to conceal their activity on a computer so that they can covertly monitor and control the system for an extended period. Exist to provide sustained covert access to a machine so that the machine can be remotely controlled and monitored in a manner that is extremely difficult to detect.
1st Generation: Rootkits have historically demonstrated a co-evolutionary adaptation and response to the development of defensive technologies designed to apprehend their subversive agenda. If we trace the evolution of rootkit technology, this pattern is evident. First generation rootkits were primitive. They simply replaced / modified key system files on the victim's system. The UNIX login program was a common target and involved an attacker replacing the original binary with a maliciously enhanced version that logged user passwords. Because these early rootkit modifications were limited to system files on disk, they motivated the development of file system integrity checkers such as Tripwire.
2nd Generation: In response, rootkit developers moved their modifications off disk to the memory images of the loaded programs and, again, evaded detection. These 'second' generation rootkits were primarily based upon hooking techniques that altered the execution path by making memory patches to loaded applications and some operating system components such as the system call table. Although much stealthier, such modifications remained detectable by searching for heuristic abnormalities. For example, it is suspicious for the system service table to contain pointers that do not point to the operating system kernel. This is the technique used by VICE.
3rd Generation: Third generation kernel rootkit techniques like Direct Kernel Object Manipulation (DKOM), which was implemented in the FU rootkit, capitalize on the weaknesses of current detection software by modifying dynamically changing kernel data structures for which it is impossible to establish a static trusted baseline.
4th Generation: Shadow Walker – memory hooking/hiding 4th generation Rootkit. Used in collusion with FUTo.

Acronyms

3DES	Triple Data Encryption Standard
802.1X	Extensible Authentication Protocol
A	
AAA	Authentication, Authorization, and Accounting
ABAC	Attribute-Based Access Control
ABM	Asynchronous Balanced Mode
ABR	Available Bit Rate
AC	Alternating Current
ACE	Access Control Entry
ACID	Atomicity, Consistency, Isolation, Durability
ACK	Acknowledge - TCP
ACL	Access Control List
ACS	Annual Cost of Safeguard
ACSE	Association Control Service Element
AD	Active Directory
ADDS	Active Directory Domain Service or Active Directory
AD-IDS	Anomaly Detection Intrusion Detection System
ADM	Architecture Development Method
ADO	Active-X Data Objects
ADS	Alternate Data Streams
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AES-CCMP	AES-Counter Mode CBC-MAC Protocol
AFP	Apple Filing Protocol
AFS	Apple File Sharing
AH	Authentication Header
ALE	Annualized Loss Expectancy
AMTSO	Anti-Malware Testing Standards Organization
ANAC	Automatic Number Announcement Circuit
AP	Access Point
API	Application Programming Interface
APIPA	Automatic Private IP Addressing
APT	Advanced Persistent Threat
ARM	Asynchronous Response Mode
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
AS	Authentication Server / Service
AS	Autonomous System
ASA	Adaptive Security Appliances
ASCII	American Standard Code for Information Interchange
ASIC	Application Specific Integrated Circuits
ASLR	Address Space Layout Randomization
ASR	Automated System Recovery
ATM	Automated Teller Machine
ATM	Asynchronous Transfer Mode
AUI	Attachment Unit Interface
AUP	Acceptable Use Policy
AV	Asset Value
AV	Antivirus
AVP	Attribute Value Pairs

B	
BBP	Best Business Practice
BBP	Best Business Practices
BCDR	Business Continuity and Disaster Recovery
BCI	Business Continuity Institute
BCM	Business Continuity Management
BCNF	Boyce Code Normalization Form
BCP	Business Continuity Plan
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BIOS	Basic Input / Output System
BMS	Balanced Magnetic Switch
BNC	Bayonet Neill–Concelman
BOOTP	Bootstrap Protocol
Botnet	Bot (Robot) Network
Bots	Robot
BPA	Business Partnership Agreement
BPA	Blanket Purchase Agreement
BPDU	Bridge Protocol Data Unit
BPL	Broadband over Power Line
BPO	Blanket Purchase Order
BRI	Basic Rate Interface
BRP	Business Recovery Plan
BS	British Standard
BSA	Business Software Alliance
BSD	Berkley Software Distribution License
BSS	Basic Service Set
BSSID	Basic Service Set Identification
BT	Bluetooth
BYOD	Bring Your Own Device
C	
C&C	Command and Control
CA	Certificate Authority
CA	Continuous Availability
CAA	Computer-Aided Assessment or Computer - Assisted Assessment
CaaS	Connectivity-as-a-Service
CAC	Common Access Card
CAN	Campus Area Network
CARP	Common Address Redundancy Protocol
CASE	Common Application Service Element
CASE	Computer-Aided Software Engineering
CAST	Carlisle Adams and Stafford Tavares
CAT	Category
CB	Configuration Baseline
CBC	Cipher Black Chaining
CBF	Critical Business Functions
CBR	Constant Bit Rate
CC	Common Criteria
CC	Country Code
CCB	Configuration (Change) Control Board
CCD	Charged Coupled Device
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

Acronyms

CCP	Crisis Communication Plan
CCR	Commitment Concurrency and Recovery
CCTV	Closed Circuit Television
CD	Compact Disk
CDI	Constrained Data Items
CDM	Continuous Diagnostics and Mitigation
CDMA	Code Division Multiple Access
CDN	Content Distribution Networks
CDPI	Control to Data-Plane Interface
CD-R	Compact Disk Recordable
CDROM	Compact Disk Read Only Memory
CE	Customer Edge
CEI	Computer Ethics Institute
CEO	Chief Executive Officer
CER	Crossover Error Rate
CESA	Cyberspace Electronic Security Act
CFB	Cipher Feedback
CFR	Code of Federal Regulations
CGI	Common Gateway Interface
CHAP	Challenge Handshake Authentication Protocol
CIA	Confidentiality, Integrity, and Availability
CIDR	Classless Inter-Domain Routing
CIFS	Common Internet File System
CIP	Cyber Incident Plan
CIR	Committed Information Rate
CIS	Center for Internet Security
CLNS	Connectionless Network Service
CM	Countermeasure
CMIP	Common Management Information Protocol
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CMP	Crisis Management Planning
CMP	Certificate Management Protocols
CMTS	Cable Modem Termination System
CN	Common Name
CO	Central Office
CobIT	Control Objectives for Information and related Technology
COBO	Corporate Owned, Business Only
COC	Chain of Custody
COCOM	Coordinating Committee for Multilateral Export Controls
COE	Council of Europe
COM	Component Object Model
COOP	Continuity Of Operation Plan
COPE	Corporate Owned, Personally Enabled
CORBA	Common Object Request Broker Architecture
COSO	Committee of Sponsoring Organizations of the Treadway Commission
CPPT	Continuity Planning Project Team
CPS	Characters Per Second
CPS	Certificate Practice Statement
CPS	Cyber Physical Systems
CPSR	Computer Professionals of Social Responsibility
CPTED	Crime Prevention Through Environmental Design
CPU	Central Processing Unit
CRAC	Computer Room Air Conditioners
CRAH	Computer Room Air Handlers
CRAMM	Central Computer and Telecommunications Agency Risk Analysis and Management Method
CRL	Certificate Revocation List
CSF	Critical Success Factors
CSIRT	Computer Security Incident Response Team
CSMA	Carrier-Sense Multiple Access
CSMA/CA	Carrier-Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSP	Continuity of Support
CSR	Certificate Signing Request
CSS	Cascading Style Sheets
CSS	Central Security Service
CSU	Channel Service Unit
CTM	Community Trade Mark
CTR	Counter
CTS	Clear to Send
CYOD	Choose Your Own Device
D	
DAC	Discretionary Access Control
DACL	Dynamic Access Control List
DAP	Directory Access Protocol
DARPA	Defense Advanced Research Projects Agency
DAS	Direct Attached Storage
DB	Database
DBMS	Database Management System
DC	Domain Controllers
DC	Direct Current
DC	Domain Component
DCBX	Data Center Bridging Exchange Protocol
DCE	Data Communication Equipment
DCL	Data Control Language
DCOM	Distributed Component Object Model
DCS	Distributed Control Systems
DDL	Data Definition Language
DDoS	Distributed Denial of Service
DEA	Data Encryption Algorithm
Demarc	Demarcation
DEP	Data Execution Prevention
DES	Data Encryption Standard
DevOps	Development Operations
DFS	Distributed File System
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DHE	Diffie-Hellman Exchange
DISP	Directory Information Shadowing Protocol

Acronyms

DIT	Directory Information Tree
DK	Data keys
DLCI	Data Link Connection Identifiers
DLP	Data Loss Prevention
DMCA	Digital Millennium Copyright Act of 1998
DML	Data Manipulation Language
DMZ	Demilitarized Zone
DN	Distinguished Names
DNA	Deoxyribonucleic acid
DNAT	Dynamic Network Address Translation
DNS	Domain Name Services / System
DNSSEC	Domain Name System Security
DOCSIS	Data Over Cable Service Interface Specification
DoD	Department of Defense
DOM	Document Object Model
DOP	Directory Operational Bindings Management Protocol
DoS	Denial of Service
DOS	Disk Operating System
DQL	Data Query Language
DRAM	Dynamic Random Access Memory
DRDoS	Distributed Reflective Denial of Service
DRM	Digital Rights Management
DRP	Disaster Recovery Plan
DRP	Disaster Recovery Planning
DSA	Digital Signature Algorithm
DSA	Directory System Agent
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSP	Directory system protocol
DSS	Digital Signature Standard
DSSS	Direct-Sequence Spread Spectrum
DSU	Data Service Unit
DTE	Data Terminal Equipment
DTP	Distributed Transaction Processing
DTP	Dynamic Trunking Protocol
DVD	Digital Video Disc
DVR	Digital Video Recorder
DWDW	Dense Wavelength Division Multiplexing
E	
EAC	Electronic Access Control
EAL	Evaluation Assurance Levels
EAP	Extensible Authentication Protocol
EAP-AKA	EAP - Authentication And Key Agreement
EAP-EKE	EAP - Encrypted Key Exchange
EAP-FAST	EAP - Flexible Authentication Via Secure Tunneling
EAP-GTC	EAP - Generic Token Card
EAP-IKEv2	EAP - Internet Key Exchange V. 2
EAP-MD5	EAP - Message Digest V5
EAP-POTP	EAP - Protected One-Time Password
EAP-PSK	EAP - Pre-Shared Key
EAP-PWD	EAP - Password
EAP-SIM	EAP - Subscriber Identity Module

EAP-TLS	EAP - Transport Layer Security
EAP-TTLS	EAP - Tunneled Transport Layer Security
EBCDIC	Extended Binary Coded Decimal Interchange Code
ECB	Electronic Code Book
ECC	Elliptical Curve Cryptography
ECDHE	Elliptical Curve Diffie-Hellman Ephemeral
ECDSA	Elliptical Curve Digital Signature Algorithm
EDE	Encrypting, Decrypting, Encrypting
EDFA	Erbium-Doped Fiber Amplifiers
EEE	Encrypting, Encrypting, Encrypting
EEPROM	Electrically Erasable Programmable Read-Only Memory
EES	Escrowed Encryption Standard
EF	Exposure Factor
EFS	Encrypted File System
EGP	Exterior Gateway Protocols
EIA	Electronic Industries Alliance
EIGRP	Enhanced Interior Gateway Routing Protocol
EJB	Enterprise JavaBean
EM	Emergency Management
EMI	Electromagnetic Interference
EMO	Emergency Management Organization
EOC	Emergency Operations Center
EPROM	Erasable Programmable Read-Only Memory
ESA	Enterprise Security Architecture
ESD	Electrostatic Discharge
ESP	Encapsulating Security Payload
ESSID	Extended Service Set Identification
ETS	Enhanced Transmission Selection
ETSi	European Telecommunications Standards Institute
EU	European Union
EUI	Extended Unique Identifier
EULA	End User License Agreement
EUM	End-User Experience Monitoring
EV	Extended Validation
F	
FAR	False Accept Rate
FAST	Federation against Software Theft
FAT	File Allocation Table
FCIP	Fibre Channel over Internet Protocol
FCoE	Fibre Channel over Ethernet
FDDI	Fiber Distributed Data Interface
FDE	Full Disk Encryption
FDMA	Frequency Division Multiple Access
FEK	File Encryption Key
FERPA	Family Educational Rights and Privacy Act
FFC	Federal Communications Commission
FFIEC	Federal Financial Institutions Examination Council
FHSS	Frequency Hopping Spread Spectrum
FIdM	Federated Identity Management
FIN	Finish - TCP

Acronyms

FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FIUO	For Internal Use Only
FMEA	Failure Modes and Effects Analysis
FQDN	Fully Qualified Domain Name
FRAP	Facilitated Risk Analysis Process
FRR	False Reject Rate
FTAM	File Transfer, Access and Manager
FTP	File Transfer Protocol
FTPS	File Transfer Protocol Secure
FX	Fiber
G	
GAN	Global Area Network
GCM	Galois Counter Mode
GFS	Grandfather Father Son
GHz	Giga Hertz
GIF	Graphics Interchange Format
GLBA	Gramm-Leach-Bliley Act
GNU	GNU's Not Unix
GPG	GNU Privacy Guard
GPLv2, v3	GNU Public License
GPO	Group Policy Object
GPS	Global Positioning System
GRC	Governance, Risk Management, and Compliance
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications
GUID	Globally Unique Identifier
H	
HA	High Availability
HAIPE	High Assurance Internet Protocol Encryptor
HDLC	High-Level Data Link Control
HDSL	High Bit-Rate Digital Subscriber Line
HIDS	Host-Based Intrusion Detection System
HIPPA	Health Insurance Portability and Accountability Act
HIPS	Host-based Intrusion Prevention
HMAC	Hashed Message Authentication Code
HMS	Hardware Security Model
HOIC	High Orbit Ion Cannon
HOTP	Hashed Message Authentication Code-Based One-Time Password
HPKP	Http Public Key Pinning
HSM	Hardware Security Module
HSPA+	Evolved High Speed Packet Access
HSRP	Hot Standby Router Protocol
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
I	
I/O	Input / Output
IaaS	Infrastructure-as-a-Service
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
IAU	Internet Architecture Board
IAX	Inter-Asterisk eXchange
IB	InfiniBand
IBSS	Independent Basic Service Set
ICA	Independent Computing Architecture
ICMP	Internet Control Message Protocol
ICS	Incident Command System
ICS	Industrial Control Systems
ICV	Integrity Check Value
IDaaS	Identity-as-a-Service
IDC	Insulation Displacement Connector
IDEA	International Data Encryption Algorithm
IDEAL	Initiating, Diagnosing, Establishing, Analyze, Lessons learned
IDF	Intermediate Distribution Frame
IDL	Interface Definition Language
IdP	Identity Provider
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFCP	Internet Fibre Channel Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IIS	Internet Information Server
IKE	Internet Key Exchange
IKMP	Internet Key Management Protocol
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IOCE	International Organization of Computer Evidence
IOS	Internet Operating System
iOS	iPhone OS
IoT	Internet of Things
IP	Internet Protocol
IPC	Inter-Process Communication
Ipconfig	Internet Protocol Configuration
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol v4
IPv6	Internet Protocol v6
IPX	Internetwork Packet Exchange
IR	Infrared
IRC	Internet Relay Chat
IRP	Incident Response Plan
IS	Information System
ISA	Interconnection Security Agreement
ISACA	Information Systems Audit and Control Association
ISAKMP	Internet Security Association and Key Management Protocol

Acronyms

ISC^2	International Information Systems Security Certification Consortium
ISCM	Information Security Continuous Monitoring
ISCP	Information System Contingency Plan
iSCSI	Internet Small Computer System Interface
ISDN	Integrated Systems Digital Network
iSER	iSCSI Extensions for RDMA
IS-IS	Intermediate System to Intermediate System
ISL	Inter-Switch Link Protocol
ISMS	Information Security Management System
ISN	Initial Sequence Number
ISO	International Organization for Standardization
ISOC	Internet Society
ISP	Internet Service Provider
IT	Information Technology
ITGI	Information Technology Governance Institute
ITIL	Information Technology Infrastructure Library
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
IV	Initialization Vector
J	
JAD	Joint Application Development
JDBC	Java Database Connectivity
JFS	Journeyed File System
JON	JavaScript Object Notation
JPEG	Joint Photographic Experts Group
JRMI	Java Remote Method Invocation
JSON	JavaScript Object Notation
JTA	Job Task Analysis
JVM	Java Virtual Machine
K	
KDC	Key Distribution Center
KDD	Knowledge Discovery in Databases
KEA	Key Exchange Algorithm
KEK	Key Encrypting Keys
KKM	Master Key Encrypting Keys
KMIP	Key Management Interoperability Protocol
L	
L2F	Layer 2 Forwarding
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LANMAN	LAN Manager
LAPB	Link Access Procedure, Balanced
LBAC	Label-Based Access Control
LC	Local Connector
LCD	Liquid-Crystal Display
LCP	Link Control Protocol
LDAP	Lightweight Directory Access Protocol
LDAPS	Lightweight Directory Access Protocol Secure
LDP	Label Distribution Protocol
LEAP	Lightweight Extensible Authentication Protocol
LEC	Local Exchange Carrier

LED	Light Emitting Diode
LER	Label Edge Router
LLC	Logical Link Control
LM	Local Area Network Manager
LPD	Line Printer Daemon
LPR	Line Printer
LRA	Local Registration Authority
LSO	Local Shared Objects
LSP	Label Switched Path
LSR	Label Switching Router
LTE	Long Term Evolution
M	
M.O.M.	Motive, Opportunity, Means
MaaS	Monitoring-as-a-Service
MAC	Mandatory Access Control
MAC	Media Access Control
MAC	Message Authentication Code
MAN	Metropolitan Area Network
MAPI	Messaging Application Programming Interface
MD	Message Digest
MD5	Message Digest v5
MDA	Message Digest Algorithm
MDF	Main Distribution Frame
MD-IDS	Misuse Detection Intrusion Detection System
MDM	Mobile Device Management
MFA	Multi-factor Authentication
MGCP	Media Gateway Control Protocol
MIB	Management Information Base
MIC	Message Integrity Code
MIME	Multipurpose Internet Mail Extensions
MIMO	Multiple In / Multiple Out
MitB	Man-in-the-Browser
MitM	Man-in-the-Middle
MMF	Multimode Fiber
MMS	Manufacturing Message Service
MODEM	MOdulate/DEModulate
MOR	Minimum Operation Requirements
MOSS	Multipurpose Internet Mail Extension Object Security Services
MOTIS	Message Oriented Text Interchange Standard
MOU	Memorandum of Understanding
MOV	Metal Oxide Varistor
MPLS	Multi-Protocol Label Switching
MPM	Modified Prototype Model
MPPE	Microsoft Point to Point Encryption
MS-CHAP	Microsoft - Challenge Handshake Authentication Protocol
MSSP	Managed Security Service Provider
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failure
MTBSI	Mean Time Between Service Incidents
MTD	Maximum Tolerable Downtime
MTR	My Traceroute
MT-RJ	Mechanical Transfer - Registered Jack

Acronyms

MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MTU	Maximum Transmission Unit
N	
NaaS	Network-as-a-Service
NAC	Network Access Control
NAP	Network Access Protection
NAS	Network Attached Storage
NASD	National Association of Security Dealers
NAT	Network Address Translation
NBI	Northbound Interface
NBTSTAT	NetBIOS over TCP/IP Statistics
NCP	Network Control Protocol
NDA	Non-Disclosure Agreement
NDS	Netware/Novell Directory Service
NetBEUI	Network Basic Input Output System Extended User Interface
NetBIOS	Network Basic Input / Output System
NETSTAT	Network Statistics
NF	Normalization Form
NFC	Near Field Communications
NFS	Network File System
NIC	Network Interface Card
NID	Network interface Device
NIDS	Network Based Intrusion Detection System
NIPS	Network-based Intrusion Detection Prevention
NIS	Network Information Service
NIST	National Institute of Standards and Technology
NIU	Network Interface Unit
Nmap	Network Mapper
NNTP	Network News Transfer Protocol
NOC	Network Operations Center
NOS	Network Operating System
NRM	Normal Response Mode
NSA	National Security Agency (No Such Agency)
NSP	Network Service Provider
NTFS	New Technology File System
NTLM	New Technology Local Area Network Manager
NTP	Network Time Protocol
NVR	Network Video Recorder
NYSE	New York Stock Exchange
O	
O	Organization
OAuth	Open Standard for Authorization
OC	Optical Carrier
OC	Optical Connector
OCR	Optical Character Recognition
OCSP	Online Certificate Status Protocol
OCTAVE	Operationally Critical Threat Asset & Vulnerability Evaluation
ODBC	Open Database Connectivity
OECD	Organization of Economic Cooperation and Development
OEP	Occupant Emergency
OES	Open Enterprise Server
OFB	Output Feedback
OFDM	Orthogonal Frequency-Division Multiplexing
OHIM	Office for Harmonization in the Internal Market
OID	Object Identifier
OLAP	Online Analytical Processing
OLE	Object Linking and Embedding
OLT	Optical Line Termination
OLTP	Online Transaction Processing
OMA	Object Management Architecture
OMG	Object Management Group
ONU	Optical Network Units
OOA	Object Oriented Analysis
OOAD	Object Oriented Analysis and Design
OOD	Object Oriented Design
OOP	Object Oriented Programming
OpenPGP	Open Pretty Good Privacy
ORB	Object Request Brokers
OS	Operating System
OSA	Open System Authentication
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
OTDR	Optical Time-Domain Reflectometer
OTP	One Time Password
OTP	One-Time Pad
OU	Organizational Unit
OUI	Organizational Unique Identifier
OUIA	Once In Unlimited Access
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
P	
P	Provider
P2P	Peer to Peer
PaaS	Platform-as-a-Service
PAC	Privilege Attribute Certificate
PACS	Physical Access Control Systems
PAN	Personal Area Network
PAP	Password Authentication Protocol
PAT	Port Address Translation
PBKDF2	Password-Based Key Derivation Function 2
PBNAC	Port Based Network Access Control
PBX	Private Branch Exchange
PCI-DSS	Payment Card Industry Data Security Standard
PDA	Personal Digital Assistants
PDCA	Plan, Do, Check, Act
PE	Provider Edge
PEAP	Protected Extensible Authentication Protocol
PEM	Privacy Enhanced Mail
PFC	Priority Based Flow Control

Acronyms

PGP	Pretty Good Privacy
PHI	Protected Health Information
PID	Passive infrared Detector
PIDAS	Perimeter Intrusion Detection and Assessment System
PII	Personally Identifiable Information
PIN	Personal Identification Number
PING	Packet Internet Groper
PIR	Passive Infrared Sensor
PIV	Personal Identity Verification
PKC	Public Key Cryptography
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public-Key Infrastructure X.509
PLC	Packet Loss Concealment
PLC	Power Line Communications
PLC	Programmable Logic Controllers
PoE	Power over Ethernet
POF	Plastic Optical Fiber
POLP	Principle of Least Privilege
PON	Passive Optical Network
POP	Point of Presence
POPv3	Post Office Protocol v3
POTS	Plain Old Telephone System
PP	Protection Profiles
PPP	Point-to-Point Protocol
PPPoE	Point-to-Point over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PR	Public Relations
PRI	Primary Rate Interface
PROM	Programmable Read-Only Memory
PSH	Push – TCP
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network
PTZ	Pan Tilt Zoom
PUSH	Preparation, Universe definition, Scoring, Hitting the Mark
PVC	Permanent Virtual Circuit
PVC	Polyvinyl Chloride
PVLAN	Private Virtual Local Area Network
Q	
QA	Quality Assurance
QC	Quality Control
QCN	Quantized Congestion Notification
QoS	Quality of Service
R	
RA	Registration Authority
RAD	Rapid Application Development
RADIUS	Remote Authentication Dial-in User Service
RADSL	Rate-Adaptive Asymmetric Digital Subscriber Line
RAID	Redundant Array of Independent Disks
RAIT	Redundant Array of Independent Tapes
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol
RAS	Remote Access Service
RBAC	Role-Based Access Control
RC4	Rivet Cipher/Ron's Code
RCA	Root Cause Analysis
RCP	Remote Copy Protocol
RDA	Remote Database Access
RDBMS	Relational Database Management Systems
RDC	Remote Desktop Connection
RDMA	Remote Direct Memory Access
RDN	Relative Distinguished Names
RDP	Remote Desktop Protocol
REST	Representational State Transfer
RF	Radio Frequency
RFC	Request for Comments
RFI	Radio Frequency Interference
RFID	Radio-Frequency Identification
RID	Relative Identifier
RIP	Routing Information Protocol
RIPEMD	RACE Integrity Primitives Evaluation Message Digest
RIPng	Routing Information Protocol Next Generation
RLOGIN	Remote Log-in
RMF	Risk Management Framework
ROI	Return on Investment
ROM	Read-Only Memory
ROSE	Remote Control Service Element
ROT13	Rotation 13
RPC	Remote Procedure Call
RPO	Recovery Point Objective
RPT	Real-time Transport Protocol
RRAS	Routing and Remote Access Server
RSA	Rivest, Shamir, Adleman
RSH	Remote Shell
RSTP	Rapid Spanning Tree Protocol
RSVP-TE	Resource Reservation Protocol with Traffic Engineering
RSYNC	Remote Synchronization
RTCP	Real Time Transport Control Protocol
RTGS	Remote Ticket-Granting Server
RTO	Recovery Time Objective
RTP	Real-time Transport Protocol
RTS	Request to Send
RTSE	Reliable Transfer Service Element
RUM	Real User Monitoring
RX	Receiver
S	
S/Key	Secure Key
S/MIME	Secure Multipurpose Internet Mail Extensions
SA	Security Association
SA	System Administrator
SaaS	Software-as-a-Service
SABSA	Sherwood Applied Business Security Architecture
SAS	Statement on Auditing Standards
SASE	Specific Application Service Element
SASL	Simple Authentication and Security Layer
SAST	Static Source Code Analysis

Acronyms

SATCOM	Satellite Communications
S-Box	Substitute Bytes
SBU	Sensitive but Unclassified
SC	Subscriber (or square) Connector
SCADA	Supervisory Control and Data Acquisition
SCIF	Sensitive Compartmented Information Facility
SCP	Secure Copy Protocol
SCSI	Small Computer System Interface
SCTP	Stream Control Transmission Protocol
SD	Secure Digital
SDDC	Software Defined Data Center
SDH	Synchronous Digital Hierarchy
SDLC	Synchronous Data Link Control
SDLC	Systems Development Life Cycle
SDLC	Software Development Life Cycle
SDN	Software Defined Network
SDP	Session Description Protocol
SDS	Software Defined Storage
SDSL	Symmetric Digital Subscriber Line
SEI	Software Engineering Institute
SEM	Security Event Management
SESAME	Secure European System and Applications in a Multivendor Environment
SET	Secure Electronic Transaction
SFA	Single Factor Authentication
SFTP	Secure File Transfer Protocol
SGID	Set Group ID
SHA	Secure Hashing Algorithm
S-HTTP	Secure Hypertext Transport Protocol
SID	Security Identifier
SIEM	Security Information and Event Management
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SLA	Service Level Agreements
SLD	Systems Life Cycle
SLE	Single Loss Expectancy
SLIP	Serial Line Internet Protocol
SMB	Server Message Block
SMF	Single-mode Fiber
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transport Protocol Secure
SNAT	Static Network Address Translation
SNFS	Secure Network File System
SNMPv3	Simple Network Management Protocol v3
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOC	Service Organizational Control
SOC	Systems Operation Center
SOCKS	Socket Secure
SOHO	Small Office Home Office
SOMAP	Security Officers Management and Analysis
SONET	Synchronous Optical Network
SOP	Standard Operating Procedures
SOX	Sarbanes-Oxley Act of 2002
SP	Service Provider
SPAA	Software Protection Association
SPAN	Switched Port Analyzer
SPAP	Shiva Password Authentication Protocol
SPIM	SPAM over Instant Messaging
SPIT	SPAM over Internet Telephony
SPOF	Single Point of Failure
SPX	Sequenced Packet Exchange.
SQL	Structured Query Language
SRP	SCSI Remote Direct Memory Access Protocol
SRTP	Secure Real Time Transport Protocol
SSD	Solid State Drive
SSDP	Simple Service Discovery Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
SSN	Social Security Number
SSO	Single Sign-On
SSTP	Secure Socket Tunneling Protocol
ST	Security Targets
ST	Service Ticket
ST	Straight Tip
STA	Spanning Tree Algorithm
STP	Shielded Twisted Pair
STP	Spanning Tree Protocol
SUID	Set User ID
SVC	Switched Virtual Circuit
SWA	Software Assurance
SWGDE	Scientific Working Group on Digital Evidence
SYN	Synchronize - TCP
T	
TACACS	Terminal Access Controller Access Control System
TACACS+	Terminal Access Controller Access Control System Plus
TCB	Trusted Computing Base
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCSEC	Trusted Computer Security Evaluation Criteria
TDE	Transparent Data Encryption
TDMA	Time Division Multiple Access
TDR	Time-Domain Reflectometer
TELNET	TCP/IP Terminal Emulation Protocol
TEMPEST	Telecommunications and Electrical Machinery Protected from Emanations Security
TESEC	Trusted Computer System Evaluation Criteria
TFN	Tribal Flood Network
TFN2K	Tribe Flood Network 2000
TFTP	Trivial File Transfer Protocol
TGS	Ticket-Granting Service
TGS	Ticket Granting Server
TGT	Ticket-Granting Ticket

Acronyms

TIA	Television Interface Adaptor
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOC	Time of Check
TOE	Target of Evaluation
TOGAF	The Open Group Architecture Framework
TOTP	Time-Based One-Time Password
TOU	Time of Use
TP	Transformation Procedures
TPM	Trusted Platform Module
TSC	Terminal Services Client
TSC	Time Stamped Counter
TTL	Time to Live
TX	Transmitter
U	
UBE	Unsolicited Bulk E-mail
UBR	Unspecified Bit Rate
UCE	Unsolicited Commercial E-mail
UDDI	Universal Description, Discovery, and Integration
UDP	User Datagram Protocol
UID	Unique Identifier
ULA	Unique Local Addresses
UML	Unified Modeling Language
UMLD	Unified Modeling Language and Design
UPN	User Principal Name
UPnP	Universal Plug and Play
UPS	Uninterruptible Power Supply
URG	Urge - TCP
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTF-8	Universal Coded Character Set +Transformation Format—8-bit
UTM	Unified Threat Management
UTP	Unshielded Twisted Pair
V	
VAR	Value At Risk
VBR	Variable Bit Rate
VCDB	VERIS Community Data Base
VCS	Virtual circuit switching
VDI	Virtual Desktop Infrastructure
VDSL	Variable Digital Subscriber Line
VDSL	Very High Speed Digital Subscriber Line
VERIS	Vocabulary for Recording and Incident Sharing
VLAN	Virtual Local Area Network
VLSM	Variable-length subnet masking
VM	Virtual Machine
VNC	Virtual Network Computing
VOFDM	Vector Orthogonal Frequency-Division Multiplexing
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VSLM	Variable Length Subnet Mask
VT	Virtual Terminal
VTP	Virtual Local Area Network Trunking Protocol
W	
W3C	World Wide Web Consortium
WAE	Wireless Application Environment
WAM	Web Access Management
WAN	Wide Area Network
WAP	Wireless Access Point
WAP	Wireless Application Protocol
WBAN	Wireless Body Area Network
WDM	Wavelength Division Multiplexing
WDP	Wireless Datagram Protocol
WEP	Wired Equivalent Privacy
WIC	Wireless Interface Card
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WINS	Windows Internet Naming Service
WIPO	World Intellectual Property Organization
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WLANA	Wireless Local Area Network Association
WMAN	Wireless Metropolitan Area Network
WML	Wireless Markup Language
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access v2
WPAN	Wireless Personal Area Network
WPS	Wi-Fi Protected Setup
WRT	Work Recovery Time
WSDL	Web Services Description Language
WSP	Wireless Session Protocol
WSS	Web Services Security
WSUS	Windows Server Update Services
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol
WWIC	Wireless Area Network Interface Card
WWW	World Wide Web
X	
X.500	Directory Services
X.509	Digital Certificates Standard
XACML	Extensible Access Control Markup Language
xDSL	Digital Subscriber Line Modem to Multiplexer
X-KISS	XML Key Information Service Specification
XKMS	XML Key Management Specification 2.0
X-KRSS	XML Key Registration Service Specification
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol
XOR	Exclusive OR Operation
XP	Extreme Programming
XSRF	Cross-site Request Forgery
XSS	Cross-Site Scripting
XTACACS	Extended Terminal Access Controller Access Control System