6to4 – Transition mechanism for migrating from IPv4 to IPv6. It allows systems to use IPv6 to communicate if their traffic has to transverse an IPv4 network.

A Checklist Test – Copies of the plan are handed out to each functional area for examination to ensure the plan properly deals with the area's needs and vulnerabilities.

A Cold Site – Is just a building with power, raised floors, and utilities. No devices are available. This is the cheapest of the three options, but can take weeks to get up and operational.

A Full-Interruption Test – One in which regular operations are stopped and processing is moved to the alternate site.

A Hot Site – Fully configured with hardware, software, and environmental needs. It can usually be up and running in a matter of hours. It is the most expensive option, but some companies cannot be out of business longer than a day without very detrimental results.

A Parallel Test – One in which some systems are actually run at the alternate site.

A Reciprocal Agreement – One in which a company promises another company it can move in and share space if it experiences a disaster, and vice versa. Reciprocal agreements are very tricky to implement and are unenforceable.

A Simulation Test – A practice execution of the plan takes place. A specific

scenario is established, and the simulation continues up to the point of actual relocation to the alternate site.

A Structured Walk-Through Test – Representatives from each functional area or department get together and walk through the plan from beginning to end.

A Warm Site – Does not have computers, but it does have some peripheral devices, such as disk drives, controllers, and tape drives. This option is less expensive than a hot site, but takes more effort and time to become operational.

Absolute Addresses – Hardware addresses used by the CPU.

Abstraction – The capability to suppress unnecessary details so the important, inherent properties can be examined and reviewed.

Accepted Ways for Handling Risk – Accept, transfer, mitigate, avoid.

Access – The flow of information between a subject and an object.

Access Control Matrix – A table of subjects and objects indicating what actions individual subjects can take upon individual objects.

Access Control Model – An access control model is a framework that dictates how subjects access objects.

Access Controls – Are security features that control how users and systems communicate and interact with other systems and resources.

Accreditation – Formal acceptance of the adequacy of a system's overall security by management.

Active Attack – Attack where the attacker does interact with processing or communication activities.

ActiveX – A Microsoft technology composed of a set of OOP technologies and tools based on COM and DCOM. It is a framework for defining reusable software components in a programming language–independent manner.

Address Bus – Physical connections between processing components and memory segments used to communicate the physical memory addresses being used during processing procedures.

Address Resolution Protocol (ARP) – A networking protocol used for resolution of network layer IP addresses into link layer MAC addresses.

Address Space Layout Randomization (ASLR) – Memory protection mechanism used by some operating systems. The addresses used by components of a process are randomized so that it is harder for an attacker to exploit specific

memory vulnerabilities.

Algebraic Attack – Cryptanalysis attack that exploits vulnerabilities within the intrinsic algebraic structure of mathematical functions.

Algorithm – Set of mathematical and logic rules used in cryptographic functions.

Analog Signals – Continuously varying electromagnetic wave that represents and transmits data.

Analytic Attack – Cryptanalysis attack that exploits vulnerabilities within the algorithm structure.

Annualized Loss Expectancy (ALE) – Annual expected loss if a specific vulnerability is exploited and how it affects a single asset. SLE × ARO = ALE.

Application Programming Interface (API) – Software interface that enables process-to-process interaction. Common way to provide access to standard routines to a set of software programs.

Arithmetic Logic Unit (ALU) – A component of the computer’s processing unit, in which arithmetic and matching operations are performed.

AS/NZS 4360 – Australia and New Zealand business risk management assessment approach.

Assemblers – Tools that convert assembly code into the necessary machine- compatible binary language for processing activities to take place.

Assembly Language – A low-level programming language that is the mnemonic representation of machine-level instructions.

Assurance Evaluation Criteria – Check-list and process of examining the security-relevant parts of a system (TCB, reference monitor, security kernel) and assigning the system an assurance rating.

Asymmetric Algorithm – Encryption method that uses two different key types, public and private. Also called public key cryptography.

Asymmetric Mode Multiprocessing – When a computer has two or more CPUs and one CPU is dedicated to a specific program while the other CPUs carry out general processing procedures.

Asynchronous Communication – Transmission sequencing technology that uses start and stop bits or similar encoding mechanism. Used in environments that transmit a variable amount of data in a periodic fashion.

Asynchronous Token Generating Method – Employs a challenge/response

scheme to authenticate the user.

Attack Surface – Components available to be used by an attacker against the product itself.

Attenuation – Gradual loss in intensity of any kind of flux through a medium. As an electrical signal travels down a cable, the signal can degrade and distort or corrupt the data it is carrying.

Attribute – A column in a two-dimensional database.

Authentication Header (AH) Protocol – Protocol within the IPSec suite used for integrity and authentication.

Authenticode – A type of code signing, which is the process of digitally signing software components and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was digitally signed. Authenticode is Microsoft's implementation of code signing.

Availability – Reliable and timely access to data and resources is provided to authorized individuals.

Avalanche effect – Algorithm design requirement so that slight changes to the input result in drastic changes to the output.

Base registers – Beginning of address space assigned to a process. Used to ensure a process does not make a request outside its assigned memory boundaries.

Baseband transmission – Uses the full bandwidth for only one communication channel and has a low data transfer rate compared to broadband.

Bastion host – A highly exposed device that will most likely be targeted for attacks, and thus should be hardened.

Behavior blocking – Allowing the suspicious code to execute within the operating system and watches its interactions with the operating system, looking for suspicious activities.

Birthday attack – Cryptographic attack that exploits the mathematics behind the birthday problem in the probability theory forces collisions within hashing functions.

Block cipher – Symmetric algorithm type that encrypts chunks (blocks) of data at a time.

Blowfish – Block symmetric cipher that uses 64-bit block sizes and variable-length keys.

Border Gateway Protocol (BGP) – The protocol that carries out core routing

decisions on the Internet. It maintains a table of IP networks, or "prefixes," which designate network reachability among autonomous systems.

Bots – Software applications that run automated tasks over the Internet, which perform tasks that are both simple and structurally repetitive. Malicious use of bots is the coordination and operation of an automated attack by a botnet (centrally controlled collection of bots).

Broadband transmission – Divides the bandwidth of a communication channel into many channels, enabling different types of data to be transmitted at one time.

Buffer overflow – Too much data is put into the buffers that make up a stack. Common attack vector used by attackers to run malicious code on a target system.

Bus topology – Systems are connected to a single transmission channel (i.e., network cable), forming a linear construct.

Business Continuity Management (BCM) – is the overarching approach to managing all aspects of BCP and DRP.

Business Continuity Plan (BCP) – A business continuity action plan is a document or set of documents that contains the critical information a business needs to stay running in spite of adverse events. A business continuity plan is also called an emergency plan.

Business Impact Analysis (BIA) – An exercise that determines the impact of losing the support of any resource to an organization, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting systems.

Cable Modem – A device that provides bidirectional data communication via radio frequency channels on cable TV infrastructures. Cable modems are primarily used to deliver broadband Internet access to homes.

Cache memory – Fast memory type that is used by a CPU to increase read and write operations.

Caesar Cipher – Simple substitution algorithm created by Julius Caesar that shifts alphabetic values three positions during its encryption and decryption processes

Capability Maturity Model Integration (CMMI) – A process improvement methodology that provides guidance for quality improvement and point of reference for appraising existing processes developed by Carnegie Mellon.

Capability Maturity Model Integration (CMMI) model – A process improvement approach that provides organizations with the essential elements of

effective processes, which will improve their performance.

Capability Table – A capability table specifies the access rights a certain subject possesses pertaining to specific objects. A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) – LANs using carrier sense multiple access with collision avoidance require devices to announce their intention to transmit by broadcasting a jamming signal.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) – Devices on a LAN using carrier sense multiple access with collision detection listen for a carrier before transmitting data.

CBC-MAC – Cipher block chaining message authentication code uses encryption for data integrity and data origin authentication.

Cell – An intersection of a row and a column.

Cell suppression – A technique used to hide specific cells that contain sensitive information.

Central Processing Unit (CPU) – The part of a computer that performs the logic, computation, and decision-making functions. It interprets and executes instructions as it receives them.

Certificate – Digital identity used within a PKI. Generated and maintained by a certificate authority and used for authentication.

Certificate Revocation List (CRL) – List that is maintained by the certificate authority of a PKI that contains information on all of the digital certificates that have been revoked.

Certification – Technical evaluation of the security components and their compliance to a predefined security policy for the purpose of accreditation.

Certification Authority – Component of a PKI that creates and maintains digital certificates throughout their life cycles.

Change control – The process of controlling the changes that take place during the life cycle of a system and documenting the necessary change control activities.

Channel Service Unit (CSU) – A line bridging device for use with T-carriers, and that is required by PSTN providers at digital interfaces that terminate in a Data Service Unit (DSU) on the customer side. The DSU is a piece of telecommunications circuit terminating equipment that transforms digital data between telephone

company lines and local equipment.

Chosen-ciphertext attack – Cryptanalysis attack where the attacker chooses a ciphertext and obtains its decryption under an unknown key.

Chosen-plaintext attack – Cryptanalysis attack where the attacker can choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts.

Cipher – Another name for algorithm.

Ciphertext-only attack – Cryptanalysis attack where the attacker is assumed to have access only to a set of ciphertexts.

Classless Interdomain Routing (CIDR) – A method for using the existing 32-bit Internet Address Space efficiently.

Client-side validation – Input validation is done at the client before it is even sent back to the server to process.

Clipping Level – A threshold.

Closed system – Designs are built upon proprietary procedures, which inhibit interoperability capabilities.

Cloud computing – The delivery of computer processing capabilities as a service rather than as a product, whereby shared resources, software, and information are provided to end users as a utility. Offerings are usually bundled as an infrastructure, platform, or software.

CMAC – Cipher message authentication code that is based upon and provides more security compared to CBC-MAC.

CMM – Block cipher mode that combines the CTR encryption mode and CBC-MAC. One encryption key is used for both authentication and encryption purposes.

CobiT – Set of control objectives used as a framework for IT governance developed by Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI).

Cognitive passwords – Fact or opinion based information used to verify an individual's identity.

Cohesion – A measurement that indicates how many different types of tasks a module needs to carry out.

Collision – (1) A condition that is present when two or more terminals are in contention during simultaneous network access attempts. (2) In cryptography, an instance when a hash function generates the same output for different inputs.

Collusion – Two or more people working together to carry out fraudulent activities.

Common Criteria – International standard used to assess the effectiveness of the security controls built into a system from functional and assurance perspectives.

Compilers – Tools that convert high-level language statements into the necessary machine-level format (.exe, .dll, etc.) for specific processors to understand.

Compression viruses – Another type of virus that appends itself to executables on the system and compresses them by using the user's permissions.

Concealment Cipher – Encryption method that hides a secret message within an open message.

Confidentiality – A security concept that assures the necessary level of secrecy is enforced and unauthorized disclosure is prevented.

Confusion – Substitution processes used in encryption functions to increase randomness.

Content-based access – Bases access decisions on the sensitivity of the data, not solely on subject identity.

Context-based access – Bases access decisions on the state of the situation, not solely on identity or content sensitivity.

Control – Safeguard that is put in place to reduce a risk, also called a countermeasure.

Control functions –

Deterrent: Discourage a potential attacker Preventive: Stop an incident from occurring Corrective: Fix items after an incident has occurred Recovery: Restore necessary components to return to normal operations Detective: Identify an incident's activities after it took place Compensating: Alternative control that provides similar protection as the original control"

Control types – Administrative, technical (logical), and physical

Control unit – Part of the CPU that oversees the collection of instructions and data from memory and how they are passed to the processing components of the CPU.

Cookies – Data files used by web browsers and servers to keep browser state information and browsing preferences.

Cooperative multitasking – Multitasking scheduling scheme used by older operating systems to allow for computer resource time slicing.

Copyright – A form of protection granted by law for original works of authorship fixed in a tangible medium of expression.

COSO – Internal control model used for corporate governance to help prevent fraud developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

Cost/benefit analysis – An estimate of the equivalent monetary value of proposed benefits and the estimated costs associated with a control in order to establish whether the control is feasible.

Coupling – A measurement that indicates how much interaction one module requires for carrying out its tasks.

CRAMM – Central Computing and Telecommunications Agency Risk Analysis and Management Method.

Cross-Site Scripting (XSS) attack – An attack where a vulnerability is found on a web site that allows an attacker to inject malicious code into a web application.

Crosstalk – A signal on one channel of a transmission creates an undesired effect in another channel by interacting with it. The signal from one cable “spills over” into another cable.

Cryptanalysis – Practice of uncovering flaws within cryptosystems.

Cryptography – Science of secret writing that enables an entity to store and transmit data in a form that is available only to the intended individuals.

Cryptology – The study of both cryptography and cryptanalysis.

Cryptosystem – Hardware or software implementation of cryptography that contains all the necessary software, protocols, algorithms, and keys.

Data bus – Physical connections between processing components and memory segments used to transmit data being used during processing procedures.

Data custodian – Individual responsible for implementing and maintaining security controls to meet security requirements outlined by data owner.

Data dictionary – Central repository of data elements and their relationships.

Data diddling – The act of willfully modifying information, programs, or documentation in an effort to commit fraud or disrupt production.

Data Execution Prevention (DEP) – Memory protection mechanism used by

some operating systems. Memory segments may be marked as non-executable so that they cannot be misused by malicious software.

Data hiding – Use of segregation in design decisions to protect software components from negatively interacting with each other. Commonly enforced through strict interfaces.

Data mining – A methodology used by organizations to better understand their customers, products, markets, or any other phase of the business.

Data modeling – Considers data independently of the way the data are processed and of the components that process the data. A process used to define and analyze data requirements needed to support the business processes.

Data owner – Individual responsible for the protection and classification of a specific data set.

Data structure – A representation of the logical relationship between elements of data.

Data warehousing – Combines data from multiple databases or data sources into a large database for the purpose of providing more extensive information retrieval and data analysis.

Database – A cross-referenced collection of data.

Database Management System (DBMS) – Manages and controls the database.

Decipher – Act of transforming data into a readable format.

Defense-in-depth – Implementation of multiple controls so that successful penetration and compromise is more difficult to attain.

Delphi method – Data collection method that happens in an anonymous fashion.

Differential cryptanalysis – Cryptanalysis method that uses the study of how differences in an input can affect the resultant difference at the output.

Diffie-Hellman algorithm – First asymmetric algorithm created and is used to exchange symmetric key values. Based upon logarithms in finite fields.

Diffusion – Transposition processes used in encryption functions to increase randomness.

Digital Rights Management (DRM) – Access control technologies commonly used to protect copyright material.

Digital signals – Binary digits are represented and transmitted as discrete electrical pulses.

Digital signature – Ensuring the authenticity and integrity of a message through the use of hashing algorithms and asymmetric algorithms. The message digest is encrypted with the sender's private key.

Digital Subscriber Line (DSL) – A set of technologies that provide Internet access by transmitting digital data over the wires of a local telephone network. DSL is used to digitize the "last mile" and provide fast Internet connectivity.

Distance-Vector routing protocol – A routing protocol that calculates paths based on the distance (or number of hops) and a vector (a direction).

DNS zone transfer – The process of replicating the databases containing the DNS data across a set of DNS servers.

DNSSEC – A set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attack types.

DoDAF – U.S. Department of Defense architecture framework that ensures interoperability of systems to meet military mission goals.

Domain Name System (DNS) – A hierarchical distributed naming system for computers, services, or any resource connected to an IP based network. It associates various pieces of information with domain names assigned to each of the participating entities.

Dual-homed firewall – This device has two interfaces and sits between an untrusted network and trusted network to provide secure access.

Dumpster diving – Refers to going through someone’s trash to find confidential or useful information. It is legal, unless it involves trespassing, but in all cases it is considered unethical.

Dynamic Host Configuration Protocol (DHCP) – DHCP is an industry standard protocol used to dynamically assign IP addresses to network devices.

Dynamic link libraries (DLLs) – A set of subroutines that are shared by different applications and operating system processes.

El Gamal algorithm – Asymmetric algorithm based upon the Diffie-Hellman algorithm used for digital signatures, encryption, and key exchange.

Elliptic curve cryptosystem algorithm – Asymmetric algorithm based upon the algebraic structure of elliptic curves over finite fields. Used for digital signatures, encryption, and key exchange.

E-mail spoofing – Activity in which the sender address and other arts of the e-

mail header are altered to appear as though the e-mail originated from a different source. Since SMTP does not provide any authentication, it is easy to impersonate and forge e-mails.

Encapsulating Security Payload Protocol (ESP) – Protocol within the IPSec suite used for integrity, authentication, and encryption.

EncipherK – Act of transforming data into an unreadable format.

End-to-End encryption – The encryption of information at the point of origin within the communications network and postponing of decryption to the final destination point.

Ethernet – Common LAN media access technology standardized by IEEE 802.3. Uses 48-bit MAC addressing, works in contention-based networks, and has extended outside of just LAN environments.

Exposure – Presence of a vulnerability, which exposes the organization to a threat.

Facilitated Risk Analysis Process (FRAP) – A focused, qualitative approach that carries out pre-screening to save time and money.

Failure Modes and Effect Analysis (FMEA) – Approach that dissects a component into its basic functions to identify flaws and those flaw’s effects.

Fault tree analysis – Approach to map specific flaws to root causes in complex systems.

Federated identity – A portable identity, and its associated entitlements, that can be used across business boundaries.

Fiber Distributed Data Interface (FDDI) – Ring-based token network protocol that was derived from the IEEE 802.4 token bus timed token protocol. It can work in LAN or MAN environments and provides fault tolerance through dual-ring architecture.

File – A basic unit of data records organized on a storage medium for convenient location, access, and updating.

Foreign key – An attribute of one table that is related to the primary key of another table.

Fraggle attack – A DDoS attack type on a computer that floods the target system with a large amount of UDP echo traffic to IP broadcast addresses.

Frequency analysis – Cryptanalysis process used to identify weaknesses within cryptosystems by locating patterns in resulting ciphertext.

Frequency-Division Multiplexing (FDM) – An older technique in which the available transmission bandwidth of a circuit is divided by frequency into narrow bands, each used for a separate voice or data transmission channel, which many conversations can be carried on one circuit.

Functionality versus Effectiveness of Control – Functionality is what a control does, and its effectiveness is how well the control does it.

Fuzzing – A technique used to discover flaws and vulnerabilities in software.

Garbage collector – Tool that marks unused memory segments as usable to ensure that an operating system does not run out of memory.

General registers – Temporary memory location the CPU uses during its processes of executing instructions. The ALU’s “scratch pad” it uses while carrying out logic and math functions.

Guideline – Suggestions and best practices.

H.323 – A standard that addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multipoint conferences.

Hardware segmentation – Physically mapping software to individual memory segments.

Hashed Message Authentication Code (HMAC) – Cryptographic hash function that uses a symmetric key value and is used for data integrity and data origin authentication.

Hierarchical data model – Combines records and fields that are related in a logical tree structure.

High Availability – Refers to a system, component, or environment that is continuously operational.

High-Level languages – Otherwise known as third-generation programming languages, due to their refined programming structures, using abstract statements.

Honeypots – Systems that entice with the goal of protecting critical production systems. If two or more honeypots are used together, this is considered a honeynet.

HTTPS – A combination of HTTP and SSL\TLS that is commonly used for secure Internet connections and e-commerce transactions.

Hybrid cryptography – Combined use of symmetric and asymmetric algorithms where the symmetric key encrypts data and an asymmetric key encrypts the symmetric key.

Hybrid Microkernel architecture – Combination of monolithic and microkernel architectures. The microkernel carries out critical operating system functionality, and the remaining functionality is carried out in a client\server model within kernel mode.

Hypervisor – Central program used to manage virtual machines (guests) within a simulated environment (host).

IEEE 802.1AE (MACSec) – Standard that specifies a set of protocols to meet the security requirements for protecting data traversing Ethernet LANs.

IEEE 802.1AR – Standard that specifies unique per-device identifiers (DevID) and the management and cryptographic binding of a device (router, switch, access point) to its identifiers.

Immunizer – Attaches code to the file or application, which would fool a virus into “thinking” it was already infected.

Information gathering – Usually the first step in an attacker’s methodology, in which the information gathered may allow an attacker to infer additional information that can be used to compromise systems.

Information Technology Security Evaluation Criteria (ITSEC) – European standard used to assess the effectiveness of the security controls built into a system.

Initialization vectors (IVs) – Values that are used with algorithms to increase randomness for cryptographic functions.

Instruction set – Set of operations and commands that can be implemented by a particular processor (CPU).

Integrated Services Digital Network (ISDN) – A circuit-switched telephone network system technology designed to allow digital transmission of voice and data over ordinary telephone copper wires.

Integrity – Accuracy and reliability of the information and systems are provided and any unauthorized modification is prevented.

International Data Encryption Algorithm (IDEA) – Block symmetric cipher that uses a 128-bit key and 64-bit block size.

Internet Control Message Protocol (ICMP) – A core protocol of the IP suite used to send status and error messages.

Internet Group Management Protocol (IGMP) – Used by systems and adjacent routers on IP networks to establish and maintain multicast group memberships.

Internet Message Access Protocol (IMAP) – A method of accessing electronic mail or bulletin board messages that are kept on a (possibly shared) mail server. IMAP permits a client e-mail program to access remote message stores as if they were local. For example, e-mail stored on an IMAP server can be manipulated from a desktop computer at home, a workstation at the office, and a notebook computer while traveling, without the need to transfer messages of files back and forth between these computers. IMAP can be regarded as the next-generation POP.

Internet Protocol (IP) – Core protocol of the TCP/IP suite. Provides packet construction, addressing, and routing functionality.

Internet Security Association and Key Management Protocol (ISAKMP) – Used to establish security associates and an authentication framework in Internet connections. Commonly used by IKE for key exchange.

Interpreters – Tools that convert code written in interpreted languages to the machine-level format for processing.

Interrupt – Software or hardware signal that indicates that system resources (i.e., CPU) are needed for instruction processing.

Interrupts – Values assigned to computer components (hardware and software) to allow for efficient computer resource time slicing.

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) – An IPv6 transition mechanism meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network.

IPSec – Protocol suite used to protect IP traffic through encryption and authentication. De facto standard VPN protocol.

IPv6 – IP version 6 is the successor to IP version 4 and provides 128-bit addressing, integrated IPSec security protocol, simplified header formats, and some automated configuration.

ISO/IEC 27000 series – Industry-recognized best practices for the development and management of an information security management system.

ISO/IEC 27005 – International standard for the implementation of a risk management program that integrates into an information security management system (ISMS).

ITIL – Best practices for information technology services management processes developed by the United Kingdom's Office of Government Commerce.

Java applets – Small components (applets) that provide various functionalities and are delivered to users in the form of Java bytecode. Java applets can run in a web browser using a Java Virtual Machine (JVM). Java is platform independent; thus, Java applets can be executed by browsers for many platforms.

Kerckhoffs' Principle – Concept that an algorithm should be known and only the keys should be kept secret.

Kernel mode (supervisory state, privilege mode) – Mode that a CPU works within when carrying out more trusted process instructions. The process has access to more computer resources when working in kernel versus user mode.

Key – Sequence of bits that are used as instructions that govern the acts of cryptographic functions within an algorithm.

Key clustering – A weakness that would exist in a cryptosystem if two different keys would generate the same ciphertext from the same plaintext.

Key Derivation Functions (KDFs) – Generation of secret keys (subkeys) from an initial value (master key).

Keyspace – A range of possible values used to construct keys.

Keystream generator – Component of a stream algorithm that creates random values for encryption purposes.

Known-plaintext attack – Cryptanalysis attack where the attacker is assumed to have access to sets of corresponding plaintext and ciphertext.

Layered operating system architecture – Architecture that separates system functionality into hierarchical layers.

Limit registers – Ending of address space assigned to a process. Used to ensure a process does not make a request outside its assigned memory boundaries.

Linear cryptanalysis – Cryptanalysis method that uses the study of affine transformation approximation in encryption processes.

Link encryption – Technology that encrypts full packets (all headers and data payload) and is carried out without the sender's interaction.

Link-state routing protocol – A routing protocol used in packet-switching networks where each router constructs a map of the connectivity within the network and calculates the best logical paths, which form its routing table.

Logic bomb – Executes a program, or string of code, when a certain event happens or a date and time arrives.

Logical addresses – Indirect addressing used by processes within an operating system. The memory manager carries out logical-to-absolute address mapping.

Machine language – A set of instructions in binary format that the computer's processor can understand and work with directly.

Macro virus – A computer virus that spreads by binding itself to software such as Word or Excel.

Maintenance hooks – Code within software that provides a back door entry capability.

Mandatory vacation – Detective administrative control used to uncover potential fraudulent activities by requiring a person to be away from the organization for a period of time.

Maskable interrupt – Interrupt value assigned to a non-critical operating system activity.

Mean Time Between Failures (MTBF) – The predicted amount of time between inherent failures of a system during operation.

Mean Time To Repair (MTTR) – A measurement of the maintainability by representing the average time required to repair a failed component or device.

Media access control (MAC) – Data communication protocol sub-layer of the data link layer specified in the OSI model. It provides hardware addressing and channel access control mechanisms that make it possible for several nodes to communicate within a multiple-access network that incorporates a shared medium.

Meet-in-the-middle attack – Cryptanalysis attack that tries to uncover a mathematical problem from two different ends.

Meme viruses – These are not actual computer viruses, but types of e-mail messages that are continually forwarded around the Internet.

Memory card – Holds information but cannot process information.

Mesh topology – Network where each system must not only capture and disseminate its own data, but also serve as a relay for other systems; that is, it must collaborate to propagate the data in the network.

Message authentication code (MAC) – Keyed cryptographic hash function used for data integrity and data origin authentication.

Metro Ethernet – A data link technology that is used as a metropolitan area network to connect customer networks to larger service networks or the Internet.

Metropolitan area network (MAN) – A data network intended to serve an area approximating that of a large city or college campus. Such networks are being implemented by innovative techniques, such as running fiber cables through subway tunnels.

Microarchitecture – Specific design of a microprocessor, which includes physical components (registers, logic gates, ALU, cache, etc.) that support a specific instruction set.

Microkernel architecture – Reduced amount of code running in kernel mode carrying out critical operating system functionality. Only the absolutely necessary code runs in kernel mode, and the remaining operating system code runs in user mode.

Mobile code – Code that can be transmitted across a network, to be executed by a system or device on the other end.

MODAF – Architecture framework used mainly in military support missions developed by the British Ministry of Defence.

Mode transition – When the CPU has to change from processing code in user mode to kernel mode.

Monolithic operating system architecture – All of the code of the operating system working in kernel mode in an ad-hoc and non-modularized manner.

Multilevel security policies – Outlines how a system can simultaneously process information at different classifications for users with different clearance levels.

Multipart virus – Also called a multipartite virus, this has several components to it and can be distributed to different parts of the system. It infects and spreads in multiple ways, which makes it harder to eradicate when identified.

Multiplexing – A method of combining multiple channels of data over a single transmission line.

Multiprogramming – Interleaved execution of more than one program (process) or task by a single operating system.

Multi-protocol Label Switching (MPLS) – A networking technology that directs data from one network node to the next based on short path labels rather than long network addresses, avoiding complex lookups in a routing table.

Multipurpose Internet Mail Extension (MIME) – The standard for multimedia

mail contents in the Internet suite of protocols.

Multitasking – Simultaneous execution of more than one program (process) or task by a single operating system.

Multi-threading – Applications that can carry out multiple activities simultaneously by generating different instruction sets (threads).

Natural languages – Otherwise known as fifth-generation programming languages, which have the goal to create software that can solve problems by themselves. Used in systems that provide artificial intelligence.

Network address translation (NAT) – The process of modifying IP address information in packet headers while in transit across a traffic routing device, with the goal of reducing the demand for public IP addresses.

Network convergence – The combining of server, storage, and network capabilities into a single framework, which decreases the costs and complexity of data centers. Converged infrastructures provide the ability to pool resources, automate resource provisioning, and increase and decrease processing capacity quickly to meet the needs of dynamic computing workloads.

NIST SP 800-30 – Risk Management Guide for Information Technology Systems A U.S. federal standard that is focused on IT risks.

NIST SP 800-53 – Set of controls that are used to secure U.S. federal systems developed by NIST.

Noise and perturbation – A technique of inserting bogus information in the hopes of misdirecting an attacker or confusing the matter enough that the actual attack will not be fruitful.

Non-Maskable interrupt – Interrupt value assigned to a critical operating system activity.

Object – Can be a computer, database, file, computer program, directory, or field contained in a table within a database.

Object-Oriented database – Designed to handle a variety of data (images, audio, documents, video), which is more dynamic in nature than a relational database.

Object-Relational Database (ORD) – Uses object-relational database management system (ORDBMS) and is a relational database with a software front end that is written in an object-oriented programming language.

One-Time Pad – A system that randomly generates a private key, and is used only

once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key. One-time pads have the advantage that there is theoretically no way to break the code by analyzing a succession of messages.

One-Way Hash – Cryptographic process that takes an arbitrary amount of data and generates a fixed-length value. Used for integrity protection.

Online Certificate Status Protocol (OCSP) – Automated method of maintaining revoked certificates within a PKI.

Open Mail relay – An SMTP server configured in such a way that it allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users.

Open system – Designs are built upon accepted standards to allow for interoperability.

Open Systems Interconnection (OSI) model – International standardization of system-based network communication through a modular seven-layer architecture.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) – Team-oriented approach that assesses organizational and IT risks through facilitated workshops.

Out-of-band method – Sending data through an alternate communication channel.

Packages—EALs – Functional and assurance requirements are bundled into packages for reuse. This component describes what must be met to achieve specific EAL ratings.

Parameter validation – The values that are being received by the application are validated to be within defined limits before the server application processes them within the system.

Passive attack – Attack where the attacker does not interact with processing or communication activities, but only carries out observation and data collection, as in network sniffing.

Patent – Grants ownership and enables that owner to legally enforce his rights to exclude others from using the invention covered by the patent.

Personally Identifiable Information (PII) – Data that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

Phishing – Phishing is a scam in which the perpetrator sends out legitimate-

looking e-mails, in an effort to phish (pronounced fish) for personal and financial information from the recipient.

Ping of Death – A DoS attack type on a computer that involves sending malformed or oversized ICMP packets to a target.

Plaintext – A message before it has been encrypted or after it has been decrypted using a specific algorithm and key; also referred to as cleartext. (Contrast with ciphertext.)

Plenum cables – Cable is jacketed with a fire-retardant plastic cover that does not release toxic chemicals when burned.

Policy – High-level document that outlines senior management's security directives.

Polymorphic virus – Produces varied but operational copies of itself. A polymorphic virus may have no parts that remain identical between infections, making it very difficult to detect directly using signatures.

Polymorphism – Two objects can receive the same input and have different outputs.

Ports – Software construct that allows for application- or service-specific communication between systems on a network. Ports are broken down into categories; well known (0–1023), registered (1024–49151), and dynamic (49152– 65535).

Post Office Protocol (POP) – An Internet standard protocol used by e-mail clients to retrieve e-mail from a remote server and supports simple download-and-delete requirements for access to remote mailboxes.

Preemptive multitasking – Multitasking scheduling scheme used by operating systems to allow for computer resource time slicing. Used in newer, more stable operating systems.

Pretty Good Privacy (PGP) Cryptosystem – used to integrate public key cryptography with e-mail functionality and data encryption, which was developed by Phil Zimmerman.

Primary key – Columns that make each row unique. (Every row of a table must include a primary key.)

Private Branch Exchange (PBX) – A small version of the phone company's central switching office. Also known as a private automatic branch exchange. A central telecommunications switching station that an organization uses for its own

purposes.

Private key – Value used in public key cryptography that is used for decryption and signature creation and known to only key owner.

Procedures – Step-by-step implementation instructions.

Process – Program loaded in memory within an operating system.

Process isolation – Protection mechanism provided by operating systems that can be implemented as encapsulation, time multiplexing of shared resources, naming distinctions, and virtual memory mapping.

Process states (ready, running, blocked) – Processes can be in various activity levels. Ready = waiting for input. Running = instructions being executed by CPU. Blocked = process is "suspended."

Program counter – Holds the memory address for the following instructions the CPU needs to act upon.

Program Status Word (PSW) – Condition variable that indicates to the CPU what mode (kernel or user) instructions need to be carried out in.

Protection profile – Description of a needed security solution.

Proxy server – A system that acts as an intermediary for requests from clients seeking resources from other sources. A client connects to the proxy server, requesting some service, and the proxy server evaluates the request according to its filtering rules and makes the connection on behalf of the client. Proxies can be open or carry out forwarding or reverse forwarding capabilities.

Public key – Value used in public key cryptography that is used for encryption and signature validation that can be known by all parties.

Public key cryptography – An asymmetric cryptosystem where the encrypting and decrypting keys are different and it is computationally infeasible to calculate one form the other, given the encrypting algorithm. In public key cryptography, the encrypting key is made public, but the decrypting key is kept secret.

Public-Switched Telephone Network (PSTN) – The public circuit-switched telephone network, which is made up of telephone lines, fiber-optic cables, cellular networks, communications satellites, and undersea telephone cables and allows all phone-to-phone communication. It was a fixed-line analog telephone system, but is now almost entirely digital and includes mobile as well as fixed telephones.

Qualitative risk analysis – Opinion-based method of analyzing risk with the use of scenarios and ratings.

Quantitative risk analysis – Assigning monetary and numeric values to all the data elements of a risk assessment.

Quantum cryptography – Use of quantum mechanical functions to provide strong cryptographic key exchange.

Race condition – Two or more processes attempt to carry out their activity on one resource at the same time. Unexpected behavior can result if the sequence of execution does not take place in the proper order.

RAM – Hardware inside a computer that retains memory on a short-term basis and stores information while the computer is in use.

It is the working memory of the computer into which the operating system, startup applications and drivers are loaded when a computer is turned on, or where a program subsequently started up is loaded, and where thereafter, these applications are executed.

RAM can be read or written in any section with one instruction sequence. It helps to have more of this working space installed when running advanced operating systems and applications. RAM content is erased each time a computer is turned off. RAM is the most common type of memory found in computers and other devices, such as printers. There are two basic types of RAM: dynamic RAM (DRAM) and static RAM (SRAM).

Random Number Generator – Algorithm used to create values that are used in cryptographic functions to add randomness.

RC4 – Stream symmetric cipher that was created by Ron Rivest of RSA. Used in SSL and WEP.

RC5 – Block symmetric cipher that uses variable block sizes (32, 64, 128) and variable-length key sizes (0–2040).

RC6 – Block symmetric cipher that uses a 128-bit block size and variable length key sizes (128, 192, 256). Built upon the RC5 algorithm.

Real-time Transport Protocol (RTP) – Used to transmit audio and video over IP-based networks. It is used in conjunction with the RTCP. RTP transmits the media data, and RTCP is used to monitor transmission statistics and QoS, and aids synchronization of multiple data streams.

Record – A collection of related data items.

Recovery Point Objective (RPO) – A measurement of the point prior to an outage to which data are to be restored.

Recovery Time Objective (RTO) – The earliest time period and a service level within which a business process must be restored after a disaster to avoid unacceptable consequences.

Reference monitor – Concept that defines a set of design requirements of a reference validation mechanism (security kernel), which enforces an access control policy over subject’s (processes, users) ability to perform operations (read, write, execute) on objects (files, resources) on a system.

Register – Small, temporary memory storage units integrated and used by the CPU during its processing functions.

Registration Authority (RA) – The primary purpose of an RA is to verify an end entity’s identity and determine whether it is entitled to have a public key Certificate issued.

Relational database model – In a relational database, data is organized in two- dimensional tables or relations.

Remote Access Trojans (RATs) – Malicious programs that run on systems and allow intruders to access and use a system remotely.

Remote Authentication Dial-In User Service (RADIUS) – A network protocol that provides client/server authentication and authorization, and audits remote users.

Remote Journaling – Involves transmitting the journal or transaction log offsite to a backup facility.

Replay attack – This type of attack occurs when an attacker intercepts authentication information through the use of network monitoring utilities. The attacker then "replays" this information to the security system in an effort to gain access to the system.

Residual risk – Risk that remains after implementing a control. Threats × vulnerabilities × assets × (control gap) = residual risk.

Restricted interface – Limits the user's environment within the system, thus limiting access to objects.

Rijndael – Block symmetric cipher that was chosen to fulfil the Advanced Encryption Standard. It uses a 128-bit block size and various key lengths (128, 192, 256).

Ring topology – Each system connects to two other systems, forming a single, unidirectional network pathway for signals, thus forming a ring.

Risk – The probability of a threat agent exploiting a vulnerability and the associated impact.

Rollback – An operation that ends a current transaction and cancels all the recent changes to the database until the previous checkpoint/ commit point.

ROM – Computer memory chips with preprogrammed circuits for storing such software as word processors and spreadsheets. Information in the computer's ROM is permanently maintained even when the computer is turned off

Rootkit – Set of malicious tools that are loaded on a compromised system through stealthy techniques. The tools are used to carry out more attacks either on the infected systems or surrounding systems.

Rotation of duties – Detective administrative control used to uncover potential fraudulent activities.

Rule-based access – Access is based on a list of rules created or authorized by system owners that specify the privileges granted to users.

Running Key Cipher – Substitution cipher that creates keystream values, commonly from agreed-upon text passages, to be used for encryption purposes.

SABSA – Framework Risk-driven enterprise security architecture that maps to business initiatives, similar to the Zachman framework.

Sandbox – A virtual environment that allows for very fine-grained control over the actions that code within the machine is permitted to take. This is designed to allow safe execution of untrusted code from remote sources.

Schema – Defines the structure of the database.

Screened host – A firewall that communicates directly with a perimeter router and the internal network. The router carries out filtering activities on the traffic before it reaches the firewall.

Screened Subnet architecture – When two filtering devices are used to create a DMZ. The external device screens the traffic entering the DMZ network, and the internal filtering device screens the traffic before it enters the internal network.

Scytale Cipher – A simple transposition cipher system that employs a rod of a certain thickness around which was wrapped a long, thin strip of parchment.

Secure Electronic Transaction (SET) – The SET specification has been developed by Visa and MasterCard to allow for secure credit card and offline debit card (check card) transactions over the World Wide Web.

Secure MIME (S/MIME) – Secure/Multipurpose Internet Mail Extensions, which outlines how public key cryptography can be used to secure MIME data types.

Secure Shell (SSH) – Network protocol that allows for a secure connection to a remote system. Developed to replace Telnet and other insecure remote shell methods.

Security Assertion Markup Language (SAML) – An XML standard that allows the exchange of authentication and authorization data to be shared between security domains.

Security assurance requirements – Measures taken during development and evaluation of the product to assure compliance with the claimed security functionality.

Security domain – Resources within this logical structure (domain) are working under the same security policy and managed by the same group.

Security functional requirements – Individual security functions which must be provided by a product.

Security kernel – The central part of a computer system (hardware, software, or firmware) that implements the fundamental security procedures for controlling access to system resources.

Security perimeter – Mechanism used to delineate between the components within and outside of the trusted computing base.

Security policy – Strategic tool used to dictate how sensitive information and resources are to be managed and protected.

Security Target – Vendor’s written explanation of the security functionality and assurance mechanisms that meet the needed security solution.

Security through Obscurity – Relying upon the secrecy or complexity of an item as its security, instead of practicing solid security practices.

Self-Garbling virus – Attempts to hide from anti-virus software by modifying its own code so that it does not match predefined signatures.

Sender Policy Framework (SPF) – An e-mail validation system designed to prevent e-mail spam by detecting e-mail spoofing, a common vulnerability, by verifying sender IP addresses.

Separation of Duties – Preventive administrative control used to ensure one person cannot carry out a critical task alone.

Server Side Includes (SSI) – An interpreted server-side scripting language used almost exclusively for web-based communication. It is commonly used to include the contents of one or more files into a web page on a web server. Allows web developers to reuse content by inserting the same content into multiple web documents.

Service Provisioning Markup Language (SPML) – Allows for the automation of user management (account creation, amendments, revocation) and access entitlement configuration related to electronically published services across multiple provisioning systems.

Session hijacking – An intruder takes over a connection after the original source has been authenticated.

Session Initiation Protocol (SIP) – The signaling protocol widely used for controlling communication, as in voice and video calls over IP based networks.

Session keys – Symmetric keys that have a short lifespan, thus providing more protection than static keys with longer lifespans.

Shielded twisted pair (STP) – Twisted-pair cables are often shielded in an attempt to prevent RFI and EMI. This shielding can be applied to individual pairs or to the collection of pairs.

Shoulder surfing – Viewing information in an unauthorized manner by looking over the shoulder of someone else.

Side-channel attack – Non-Intrusive Attack that uses information (timing, power consumption) that has been gathered to uncover sensitive data or processing functions. Often tries to figure out how a component works without trying to compromise any type of flaw or weakness.

Simple Mail Transfer Protocol (SMTP) – An Internet standard protocol for electronic mail (e-mail) transmission across IP-based networks.

Simple Network Management Protocol (SNMP) – Provides remote administration of network device; simple because the agent requires minimal software.

Simple Object Access Protocol (SOAP) – A lightweight protocol for exchange of information in a decentralized, distributed environment.

Single loss expectancy (SLE) – One instance of an expected loss if a specific vulnerability is exploited and how it affects a single asset. Asset Value × Exposure Factor = SLE.

Six Sigma – Business management strategy developed by Motorola with the goal of improving business processes.

Smart card – Plastic cards, typically with an electronic chip embedded, that contain electronic value tokens. Such value is disposable at both physical retail outlets and online shopping locations.

Smurf attack – A DDoS attack type on a computer that floods the target system with spoofed broadcast ICMP packets.

Social Engineering – Gaining unauthorized access by tricking someone into divulging sensitive information.

Social Engineering Attack – Manipulating individuals so that they will divulge confidential information, rather than by breaking in or using technical cracking techniques.

Software Configuration Management (SCM) – Identifies the attributes of software at various points in time, and performs a methodical control of changes for the purpose of maintaining software integrity and traceability throughout the software development life cycle.

Software deadlock – Two processes cannot complete their activities because they are both waiting for system resources to be released.

Software escrow – Storing of the source code of software with a third-party escrow agent. The software source code is released to the licensee if the licensor (software vendor) files for bankruptcy or fails to maintain and update the software product as promised in the software license agreement.

Source Routing – Allows a sender of a packet to specify the route the packet takes through the network versus routers determining the path.

Spanning Tree Protocol (STP) – A network protocol that ensures a loop-free topology for any bridged Ethernet LAN and allows redundant links to be available in case connection links go down.

Special Registers – Temporary memory location that holds critical processing parameters. They hold values as in the program counter, stack pointer, and program status word.

Stack Memory – Construct that is made up of individually addressable buffers. Process-to-process communication takes place through the use of stacks.

Standard – Compulsory rules that support the security policies.

Star topology – Network consists of one central device, which acts as a conduit to

transmit messages. The central device, to which all other nodes are connected, provides a common connection point for all nodes.

Statement of Work (SOW) – Describes the product and customer requirements. A detailed-oriented SOW will help ensure that these requirements are properly understood and assumptions are not made.

Static analysis – A debugging technique that is carried out by examining the code without executing the program, and therefore is carried out before the program is compiled.

Statistical attack – Cryptanalysis attack that uses identified statistical patterns.

Statistical Time-Division Multiplexing (STDM) – This form of multiplexing uses all available time slots to send significant information and handles inbound data on a first-come, first-served basis.

Stealth virus – A virus that hides the modifications it has made. The virus tries to trick anti-virus software by intercepting its requests to the operating system and providing false and bogus information.

Steganography – (1) The method of concealing the existence of a message or data within seemingly innocent covers. (2) A technology used to embed information in for example, audio and graphical material. The audio and graphical materials appear unaltered until a steganography tool is used to reveal the hidden message.

Stream cipher – An encryption method in which a cryptographic key and an algorithm are applied to each bit in a datastream, one bit at a time.

Subject – An active entity that requests access to an object or the data within an object.

Subnet – Logical subdivision of a network that improves network administration and helps reduce network traffic congestion. Process of segmenting a network into smaller networks through the use of an addressing scheme made up of network and host portions.

Substitution Cipher – Encryption method that uses an algorithm that changes out (substitutes) one value for another value.

Symmetric algorithm – Encryption method where the sender and receiver use an instance of the same key for encryption and decryption purposes.

Symmetric Mode Multiprocessing – When a computer has two or more CPUs and each CPU is being used in a load-balancing method.

SYN flood – DoS attack where an attacker sends a succession of SYN packets with

the goal of overwhelming the victim system so that it is unresponsive to legitimate traffic.

Synchronous communication – Transmission sequencing technology that uses a clocking pulse or timing scheme for data transfer synchronization.

Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) – Standardized multiplexing protocols that transfer multiple digital bit streams over optical fiber and allow for simultaneous transportation of many different circuits of differing origin within a single framing protocol.

Synchronous Token Device – Synchronizes with the authentication service by using time or a counter as the core piece of the authentication process. If the synchronization is time-based, the token device and the authentication service must hold the same time within their internal clocks.

System Development Life Cycle (SDLC) – The scope of activities associated with a system, encompassing the system’s initiation, development and acquisition, implementation, operation and maintenance, and, ultimately, its disposal, which instigates another system initiation.

Target of Evaluation (TOE) – Product proposed to provide a needed security solution.

T-carriers – Dedicated lines that can carry voice and data information over trunk lines.

TCP/IP model – Standardization of device-based network communication through a modular four-layer architecture. Specific to the IP suite, created in 1970 by an agency of the U.S. Department of Defense (DoD).

Teredo – Transition mechanism for migrating from IPv4 to IPv6. It allows systems to use IPv6 to communicate if their traffic has to transverse an IPv4 network, but also performs its function behind NAT devices.

Thread – Instruction set generated by a process when it has a specific activity that needs to be carried out by an operating system. When the activity is finished, the thread is destroyed.

Threat – The danger of a threat agent exploiting a vulnerability.

Threat agent – Entity that can exploit a vulnerability.

Threat modeling – A systematic approach used to understand how different threats could be realized and how a successful compromise could take place.

Time Multiplexing – Technology that allows processes to use the same resources.

Time-Division Multiplexing (TDM) – A type of multiplexing in which two or more bit streams or signals are transferred apparently simultaneously as sub- channels in one communication channel, but are physically taking turns on the single channel.

Time-of-Check/Time-of-Use (TOC/TOU) attack – Attacker manipulates the “condition check” step and the “use” step within software to allow for unauthorized activity.

TOGAF – Enterprise architecture framework used to define and understand a business environment developed by The Open Group.

Token ring – LAN medium access technology that controls network communication traffic through the use of token frames. This technology has been mostly replaced by Ethernet.

Total risk – Full risk amount before a control is put into place. Threats × vulnerabilities × assets = total risk.

Trade secrets – Proprietary business or technical information, processes, designs, practices, etc. that are confidential and critical to the business.

Trademark – Protect words, names, product shapes, symbols, colors, or a combination of these used to identify products or a company. These items are used to distinguish products from the competitors’ products.

Transmission Control Protocol (TCP) – The major transport protocol in the Internet suite of protocols providing reliable, connection-oriented, full-duplex streams.

Transport mode – Mode that IPSec protocols can work in that provides protection for packet data payload.

Transposition – Encryption method that shifts (permutation) values.

Triple DES (3-DES) – Symmetric cipher that applies DES three times to each block of data during the encryption process.

Trojan Horse – A program that is disguised as another program with the goal of carrying out malicious activities in the background without the user knowing.

Trusted Computer System Evaluation Criteria (TCSEC) – U.S. DoD standard used to assess the effectiveness of the security controls built into a system. Replaced by the Common Criteria. Also known as the Orange Book.

Trusted Computing Base (TCB) – A collection of all the hardware, software, and firmware components within a system that provide security and enforce the

system’s security policy.

Trusted path – Trustworthy software channel that is used for communication between two processes that cannot be circumvented.

Tunnel mode – Mode that IPSec protocols can work in that provides protection for packet headers and data payload.

Tuple – A row in a two-dimensional database.

Two-Phase Commit – A mechanism that is another control used in databases to ensure the integrity of the data held within the database.

Type I error – When a biometric system rejects an authorized individual (false rejection rate).

Type II error – When the system accepts impostors who should be rejected (false acceptance rate).

Uncertainty Analysis – Assigning confidence level values to data elements.

Unshielded Twisted Pair (UTP) – Cabling in which copper wires are twisted together for the purposes of canceling out EMI from external sources. UTP cables are found in many Ethernet networks and telephone systems.

User Datagram Protocol (UDP) – Connectionless, unreliable transport layer protocol, which is considered a “best effort” protocol.

User mode (problem state) – Protection mode that a CPU works within when carrying out less trusted process instructions.

User provisioning – The creation, maintenance, and deactivation of user objects and attributes as they exist in one or more systems, directories, or applications, in response to business processes.

Validation – Determines if the product provides the necessary solution for the intended real-world problem.

Verification – Determines if the product accurately represents and meets the specifications.

Very high-level languages – Otherwise known as fourth-generation programming languages and are meant to take natural language-based statements one step ahead.

View – A virtual relation defined by the database administrator in order to keep subjects from viewing certain data.

Virtual Local Area Network (VLAN) – A group of hosts that communicate as if

they were attached to the same broadcast domain, regardless of their physical location. VLAN membership can be configured through software instead of physically relocating devices or connections, which allows for easier centralized management.

Virtual memory – Combination of main memory (RAM) and secondary memory within an operating system.

Virtualization – Creation of a simulated environment (hardware platform, operating system, storage, etc.) that allows for central control and scalability.

Virus – A small application, or string of code, that infects host applications. It is a programming code that can replicate itself and spread from one system to another.

Vishing (Voice and Phishing) – Social engineering activity over the telephone system, most often using features facilitated by VoIP, to gain unauthorized access to sensitive data.

VLAN hopping – An exploit that allows an attacker on a VLAN to gain access to traffic on other VLANs that would normally not be accessible.

Voice over IP (VoIP) – The set of protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice data and multimedia sessions over IP-based networks.

Vulnerability – Weakness or a lack of a countermeasure.

War dialing – When a specialized program is used to automatically scan a list of telephone numbers to search for computers for the purposes of exploitation and hacking.

Wave-Division Multiplexing (WDM) – Multiplying the available capacity of optical fibers through use of parallel channels, with each channel on a dedicated wavelength of light. The bandwidth of an optical fiber can be divided into as many as 160 channels.

Web proxy – A piece of software installed on a system that is designed to intercept all traffic between the local web browser and the web server.

Wide Area Network (WAN) – A telecommunication network that covers a broad area and allows a business to effectively carry out its daily function, regardless of location.

Wiretapping – A passive attack that eavesdrops on communications. It is only legal with prior consent or a warrant.

Work Breakdown Dtructure (WBS) – A project management tool used to

define and group a project’s individual work elements in an organized manner.

Wormhole attack – This takes place when an attacker captures packets at one location in the network and tunnels them to another location in the network for a second attacker to use against a target system.

Worms – These are different from viruses in that they can reproduce on their own without a host application and are self-contained programs.

Zachman framework – Enterprise architecture framework used to define and understand a business environment developed by John Zachman.

Zero Knowledge Proof – One entity can prove something to be true without providing a secret value.