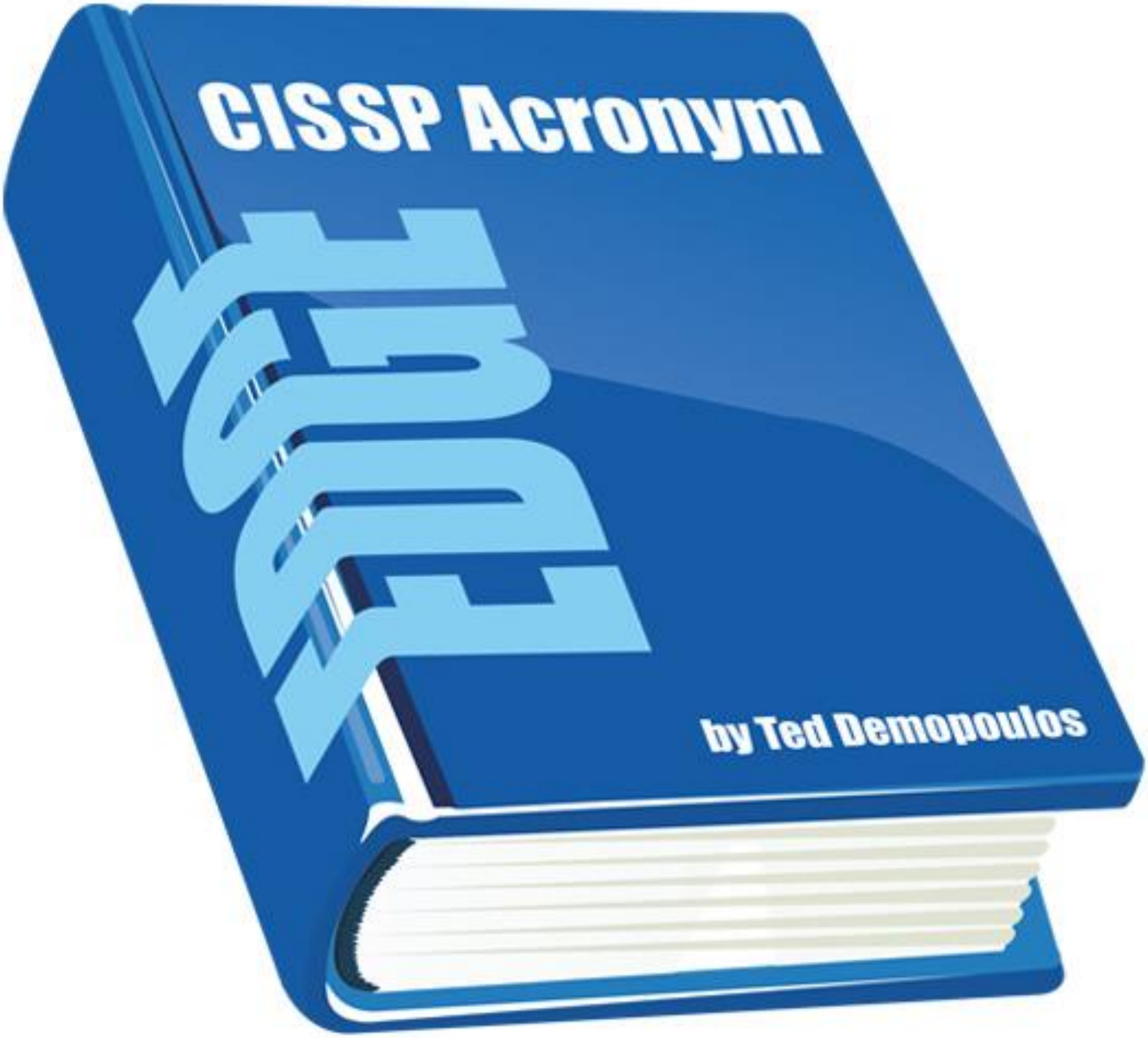
This may be the difference between passing and failing . . .



This may be the difference between passing and failing . . .

# My one line advice:

## "Study; relax; remember you just need to pass, not excel"

Most of my students by far pass the CISSP exam, but those who fail the first time fail usually by 1 to 3 questions. Many other befall the same fate . . .

Almost zero of my students fail the second time, but you do not want to take the exam twice, never mind more than twice if you can avoid it! Yet many people do.

It's not fun, you have better things to do with your life, and it costs money.

Anything that gives you an edge ethical, however slight, is great.

Remember – what seems obvious and trivial now, may not 4 or 5 hours into the exam.

- Read every question and EVERY answer. If when tired you just start picking answers that sound good, they own you – you've already failed.
- Do not just get a good night's sleep – get two good nights sleep before the exam.
- Stay at or damn near the exam location – that mere 5 minute drive may become 25 if there is an accident or road construction begins on exam day (like it did for me). Or you may get a flat tire or have a dead car battery (oh yeah, I hear stories all the time).
- Stay in the night before. Celebrate after the exam.
- If you have done your homework, do not worry about being unprepared. **You can never be 100% prepared.** The CBK is bigger than your head (metaphorically speaking) and memorizing the entire thing is probably impossible and trying is a waste of time.
- Smile – it's only 6 hours and it doesn't suck that big time. It's actually fun in a perverse Jeopardy kind of way! Yes, attitude can make THE difference.

# Domain 1: Security and Risk Management

Of course you need to study and be prepared, but you will never feel 100% prepared. That is OK! Whether you barely pass, or pass with a 99%, you will still be a CISSP. And if you pass with a 99%, you've wasted a lot of your life preparing, memorizing things you'd look up in the real world, and that's time you'll never get back.

Ethics are covered in this domain, and on ethics questions pick the most conservative approach or answer.

CIA – Confidentiality, Integrity, and Availability, the three tenets of security. For every organization one of these will be most important, but they will all be important.

DAD – Disclosure, Alteration, and Destruction. The opposite of CIA. CIA is often expressed as DAD, its opposite. Confidentiality and (unauthorized) Disclosure as well as Integrity and (unauthorized) Alteration are fairly obvious opposites. By Availability and Destruction being opposites we mean any "Destruction of Access."

Confidentiality – Only authorized access by authorized entities for authorized purposes. Authorized entities accessing data they are authorized to access for unauthorized purposes is a breach of confidentiality. For example an authorized hospital employee accessing a medical record they are authorized to access because the patient is famous and they are curious is a breach of confidentiality.

Integrity – Only authorized alterations by authorized entities for authorized purposes.

Availability – Data and services are available when needed for authorized business purposes.

This may be the difference between passing and failing . . .

**Least Privilege** – The concept that a user has the least privileges needed to fulfill their role. Least privilege is probably impossible to implement perfectly. In dynamic organizations without well defined roles it is harder to implement than in more static organizations with well defined roles, but a little least privilege goes a long way and it must always be implemented even if far from perfect.

**Need to Know** – Need to Know is a related concept to Least Privilege and is more granular and hence may further restrict access. A user only has access to a specific piece of data when they have a need to know it.

**Separation of Duties** – If an operation is too sensitive for one user to be able to do it, it can be separated so that two or more users are required. For example, think of bank safe deposit boxes, and launching nuclear weapons. No one individual has the privilege alone to do these operations.

**Rotation of Duties** – Rotation of duties is often added in addition to Separation of Duties to lessen the likelihood of collusion, two or more individuals cooperating to defeat Separation of Duties.

**Quantitative Risk Assessment** – Risk Assessment using "quantities" or metric, commonly expressed as dollars. For example, "If XYZ happens, it will cost the organization 7750 dollars."

**Qualitative Risk Assessment** – Risk Assessment using banded values, for example very low risk, low risk, medium risk, high risk, and very high risk, instead of quantities/metrics.

**EF** – Exposure Factor. The amount of an asset that is lost when a threat is manifested. For example, if you sell vintage wedding dresses, and the threat is theft, the EF is 100% - if a dress is stolen it is 100% gone!

**SLE** – Single Loss Expectancy. The asset value times the Exposure Factor. If each vintage wedding dress is worth $20,000, the SLE is $20,000.

**ARO** – Annualized Rate of Occurrence. How many times a year a threat is manifest. If 5 of your vintage wedding dresses are stolen each year, your ARO is 5.

This may be the difference between passing and failing . . .

**ALE** – Annualized Loss Expectancy. Your SLE times your ARO. If your SLE is $20,000 per wedding dress stolen, and your ARO is 5, your ALE is $100,000. Knowing this value helps you make intelligent business decisions including those pertaining to security controls.

**TCO** – Total Cost of Ownership. A financial estimate of the direct and indirect costs of a product or system. For example, an Intrusion Detection System (IDS) might cost $25,000, but if there are expenses involved with setup, training of personnel, and personnel time or maybe even dedicated personnel are required, the TCO will be much higher. For an IDS it will typically be significantly higher.

**ROI** – Return on Investment. If the ROI is positive, it is "worth" doing. If it is negative, it is not.

**RFI** – Request For Information. A business process used to collect information from potential suppliers. Often used to identify suppliers to be included in an RFP/RFQ.

**RFQ** – Request For Quote. A document sent to potential suppliers asking for pricing information, i.e. a "quote."

**RFP** – Request For Proposal. A request to potential suppliers, often via a bidding process, for proposals. Even for non security related proposals/projects, security is very often important and unfortunately the inclusion of appropriate security is often falsely assumed. A RFP may include a RFI and RFQ or they may be separate requests.

**BPA** – Business Partnership Agreement. A legal agreement between partners detailing the relationship and individual contributions and obligations. Often a complex document as it attempts to cover all possible business situations. Certainly security breaches and other security situations are one possible situation which could cause stress in a partnership.

**MOU** – Memorandum Of Understanding. A document detailing an agreement between two entities. Often seen in government, as government agencies typically cannot have contracts with each other.

**MOA** – Memorandum Of Agreement. See MOU above.

**ISA** – Interconnection Security Agreement. An agreement specifying technical requirements between organizations connecting systems and networks designed to support the MOU/MOA. Most commonly seen in governments like the MOU/MOA.

**ELA** – Enterprise License Agreement. An enterprise level software licensing agreement.

**SLA** – Service Level Agreements. A service level agreement is a contract stipulating a certain level of performance with financial penalties for not meeting that performance. For example an SLA with a service provider might stipulate 99% uptime for full payment, with payment prorated or otherwise reduced for not maintaining 99% uptime or greater.

**OLA** – An internal document specifying agreements between internal departments designed to support the SLA.

**COTS** –Commercial Off The Self (or sometimes Common Off The Shelf), as in COTS software. Microsoft Office is COTS software. Custom applications are not. The term COTS originated from and is used by the USA government.

**STRIDE/DREAD** – Microsoft's threat modeling approach is known as STRIDE. Their previous approach was known as DREAD.

(STRIDE - Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege.
DREAD - Damage, Reproducibility, Exploitability, Affected users, Discoverability).
No need to memorize these.

**OCTAVE** – Operationally Critical Threat, Asset, and Vulnerability Evaluation. A threat modeling approach from Carnegie Mellon University.

**OWASP** – Open Web Application Security Project, a non-profit focused on software security.

**CVSS** – Common Vulnerability Scoring System. An open standard metric for comparing the severity of IT vulnerabilities.

**MITM** – Man In The Middle attack. In a MITM attack, two parties believe they are directly communicating but a third party is in the middle secretly reading, possibly modifying, and relaying the messages.

**DOS** – Denial of Service.

**DDOS** – Distributed Denial of Service. An example of DDOS would be a 100,000 computer strong botnet where each computer sends a few packets to one IP address. Good chance that whatever sits at that IP address will be overwhelmed.

**EMI –** Electronic Magnetic Interference or Electromagnetic Interference. Especially with older systems, for example ones using Cathode Ray Tube based monitors, there is a substantial amount of EMI. It is possible to remotely receive this EMI and recreate what is on the screen. Although perhaps beyond the capability of your competitors, this is well within the capability of many nation-states.

**TEMPEST** – The codename for NSA specifications and a NATO certification to prevent spying via EMI. TEMPEST includes both methods for spying and shielding requirements to prevent such spying.

**MLAT** – Mutual Legal Assistance Treaty. An agreement between countries covering gathering and sharing information for the purpose of enforcing laws.

**CAPEX** – CAPital EXpenditure. A business expense which is an investment in the future of the organization. Examples include investments in software, hardware, and buildings.

**OPEX** – OPerational EXpenditure. A business expense which is required for the day to day operation of an organization, but which is NOT an investment in the future. Examples include taxes, maintenance, salaries, and depreciation.

**NDA** – Non Disclosure Agreement. A short legal document between two or more parties usually doing business together which states that confidential information may be shared but cannot be disclosed to other parties. For example I have an NDA with The SANS Institute that allows them to share confidential information with me such as new class dates and new course information that is not yet public, and I cannot disclose that information to anyone else.

BSA – Business Software Alliance, an industry group whose primary purpose is to prevent copyright infringement of software produced by its members. Software piracy is a big issue, but they are controversial because of some of their tactics, including their “Bust Your Boss!” campaign and others which pay disgruntled employees up to $200,000 to report alleged software piracy.

OECD – European Organization for Economic Cooperation and Development. Primarily European countries but also including Australia, Canada, the USA, Japan and others.

FISMA – Federal Information Security Management Act. A USA government framework designed to strengthen information security.

PCI – See PCI DSS below.

PCI DSS – Payment Card Industry Data Security Standard, usually abbreviated to PCI. Originally started by Visa but now controlled by an industry consortium. A set of best practices for organizations that handle payment cards such as credit and debit cards.

SOX – Sarbanes–Oxley Act of 2002. USA regulatory law covering financial information for publically traded companies which states that top management must personally certify accuracy of financial information. Some parts of SOX also apply to privately held companies.

GLBA – Gramm–Leach–Bliley Act, also known as the Financial Services Modernization Act of 1999, is USA regulatory law covering financial services companies such as brokerages, banks, and insurance companies.

HIPAA – Health Insurance Portability and Accountability Act of 1996, is USA regulatory law covering health care organizations.

# Domain 2: Asset Security

**"Study; relax; remember you just need to pass, not excel."**

PII – Personally Identifiable Information. Any data that could potentially be used to identify, contact, or locate a specific individual either alone or in conjunction with other data.

PHI – Personal Health Information. Any information about health, health care, or health care payments that can be connected to a specific individual. Regulatory law tends to define PHI very broadly.

CHD – Card Holder Data. Credit Card related information such as credit card numbers, cardholders names, card verification values (CVV), expiration dates, etc.

SBU – Sensitive But Unclassified. A US government classification between Confidential and Unclassified. Disclosure of SBU information will not cause damage to national security.

Think for example of the Veterans Administration laptop that went missing with lots of veteran's personal information such as dates of birth, social security numbers, etc. Clearly this was sensitive information, but no damage to national security could result.

FOIA – Freedom of Information Act. Data that would otherwise be classified can be made public through the FOIA. With the emphasis on internationalizing the exam, you probably won't see FOIA, but it still may be lingering in some questions in the question bank.

ESI – Electronically Stored Information.

Data Controller – The entity that creates and manages sensitive data. A commonly given example is a company that collects and manages their employee data for payroll purposes.

**Data Processor** – A 3rd party entity that processes data on behalf of the Data Controller. A commonly given example is a company that processes payroll data on behalf of the Data Controller.

**Memory:** The basic rule with memory is: the faster it is, the more expensive it is, and the less of it you have! Hence most systems have far less SRAM than DRAM for example.

**RAM** – Random Access Memory.

**DRAM** – Dynamic Random Access Memory. A type of RAM usually used for main memory, for example the laptop I'm typing on now has 8 Gig of memory/DRAM. DRAM must be refreshed many times a second as it depends on small capacitance charges that decay with time.

**SRAM** – Static Random Access Memory. A very fast and expensive form of RAM that is typically used for cache.

**WORM** – Write Once Read Many. Sometimes called Write Once Read Memory. A data storage device that once written cannot be rewritten.

**ROM** – Read Only Memory. Memory that is directly addressable from the CPU and contains critical startup code such as that to start the bootup sequence. This critical code is often called "firmware." For example, think BIOS (Basic Input/Output System) on PCs. ROM is non-volatile – it doesn't go away when power is removed.

**PROM** – Programmable Read Only Memory. This is ROM but is blank when manufactured, and programmed by the system developer/designer. Standard PROM can only be programmed once. Thousands or millions of tiny traces on the chip actually burn out when it is programmed. This makes PROMs not so cool for firmware, as the firmware can never be updated.

**EPROM** – A type of PROM that can be erased and reprogrammed. It is erased by "flashing" it with ultraviolet light. EPROMs are uncommon today.

**EEPROM** – Electrically Erasable PROM. A type of ROM that can be rewritten. Most computers use EEPROM for their BIOS today. This is sometimes called "Flash Memory" even though it is the far less common EPROMs that are erased by flashing them with UV light.

**PLD** – Programmable Logic Device. PROMs, EPROMs, and EEPROMs are examples of a more general technology and type of chip called a Programmable Logic Device. This term seems to show up fairly often on the exam.

**GAL** – Generic Array Logic or Gate Array Logic. A type of PLD which is reprogrammable.

**CPU** – Central Processing Unit.

**SSD** – Solid State Drive. Also called a Solid State Disk. Very fast drives which have no moving parts and use integrated circuit assemblies to store data.

**ATA Secure Erase** – Used to securely erase SSDs. More secure than an OS disk format, however not all data may be erased in case of physical damage; physical blocks marked as "bad" may still contain data.

**CIS** – The Center for Internet Security. A non profit organization whose goal is to foster cyber security through collaborative best practices. They make a wide variety of benchmarks, assessment tools, and much more available.

**NIST** – National Institute of Standards and Technology, a US Governmental body formerly known as the National Bureau of Standards (NBS), and responsible for a number of standards pertaining to security, such a DES and AES among many others.

**DISA** – The USA Defense Information Systems Agency, a United States Department of Defense (DoD) support agency that provides information technology and communications support.

**STIGS** – Secure Technical Implementation Guides from DISA. Secure configuration standards to lockdown software and hardware.

This may be the difference between passing and failing . . .

**ISO** – The International Organization for Standardization.

**IETF** – Internet Engineering task Force. Very simply the group that develops and promotes Internet standards.

**RFC** – Internet standards are known as RFCs, Requests For Comments.

**Scoping** – Determining which parts of a standard are applicable and will be followed.

**Tailoring** – Customizing a standard for a particular organization. Tailoring consists of Scoping then supplementing with additional controls and/or control enhancements as appropriate.

This may be the difference between passing and failing . . .

# Domain 3: Security Engineering

This is a massive domain!

BLP – Bell-LaPadula. A theoretical security model focused solely on protecting confidentiality, and used in DoD classified systems. Requires data classification. There are two main rules:

▪ No Read Up (Simple Security Property). A subject cannot read an object at a higher classification level. For example a secret user cannot read top secret data.

▪ No Write Down (* Security Property, pronounced "Star Security Property"). A subject at a higher classification level cannot write to a lower classification level. For example a secret user cannot email to unclassified systems.

BIBA – The Biba Security Model, named after Ken Biba, is a theoretical security model focused solely on integrity, and the opposite of Bell-LaPadula. Requires data classification. There are two main rules:

▪ No Read Down (Simple Security Axiom). A subject cannot read an object at a lower classification level. For example a top secret user cannot read secret data. This is to prevent bad information from moving up. Think about a document that has been declassified for example. It is often less integral as parts of it have been removed (or blacked out for physical documents).

▪ No Write Up (* Integrity Axiom). A subject at a lower classification level cannot write to a higher classification level. For example a secret user cannot write to a top secret file.

Clark-Wilson – A theoretical security model focused on integrity, both internal and external. Does not require data classification. Integrity is enforced through separation of duties and well formed transactions.

**Chinese Wall Model** (also called **Brewer and Nash**) – A model designed to help prevent Conflicts of Interest. Different Conflict of Interest groups are defined and users may not access data across groups where a conflict of interest may occur. For example, Conflict of Interest groups could be set up in a consulting organization that do not allow an employee to access confidential data about a client and their other clients who are competitors.

**COI** – Conflict of Interest.

**ACL** – Access Control List.

**ACM** – Access Control Matrix. An ACM is a matrix where the X-axis specifies resources or objects, and the Y-axis specifies subjects such as users (or maybe roles/groups). Each cell specifies what access a specific subject (or role/group) has to a specific object. In a typical computer environment, where you may have thousands of users, groups, and other subjects like running processes, and who knows how many files and other objects, a full blown ACM is going to be absurdly large meaning it's basically a theoretical concept in this case. A limited ACM, one for example showing which roles have what access to certain functionality, can be useful in designing and understanding systems.

**TCB** – Trusted Computing Base. The low level hardware, software like the OS kernel and firmware, that must be trusted or nothing secure can be built on the system. TCSEC and ITSEC (below) are concerned with defining and qualifying the TCB.

**TCSEC** – Trusted Computer Systems Evaluation Criteria, also known as the Orange Book. A US centric (Department of Defense) standard. Ranges from "D" – minimal protection, to "A" – verified design. Not actively used today, but other models are built using its concepts (like ITSEC).

**ITSEC** – Information Technology Security Evaluation Criteria. The first European attempt at an evaluation criteria (similar to the Orange Book or TCSEC). Despite being European, it's considered "International."

ITSEC has two parts, Functionally (F) and Assurance (E). It is quite complex and essentially superseded by the much simpler EAL below.

**EAL** – Evaluation Assurance Level, also known as the **Common Criteria**, a follow on to ITSEC and much simpler and more reasonable. Each product or system gets an EAL level, ranging from EAL1 (functionally tested) to EAL7 (formally verified, designed, and tested).

The second European attempt at an evaluation criteria. Once again, despite being European, it's considered "International."

**ToE** – Target of Evaluation, what is being evaluated by the Common Criteria (EAL).

**OS** – Operating System. The basic software that controls the hardware and allows the execution of application software efficiently. Examples of common operating systems include Windows 10, MacOS, and the various types of Linux and Unix.

**IPL** – Initial Program Load. The operating system on a mainframe computer is sometimes called the IPL.

**TPM** – Trusted Platform Module. A chip on the motherboard that stores encryption keys. Think of it as an on-motherboard smart card. Included in many motherboards and mobile devices. Apple stopped including the TPM in their hardware in 2009.

**GUI** – Graphical User Interface. Many programs and operating systems have a GUI (pronounced "gooey") while others may only have a command line interface.

**ALU** – Arithmetic Logic Unit. The part of the CPU that performs arithmetic and logic operations.

**CISC** – Complex Instruction Set Computer. A CPU which has a rich instruction set. This makes life easy for low level programmers as they have lots of instructions they can call, instead of needing to rely on just a very basic instruction set. Most personal computers are CISC based.

**RISC** – Reduced Instruction Set Computer. As CPUs became more complex and got a more complex instruction set, some manufacturers started to make RISC CPU based computers. A RISC based CPU has only a few instructions, but can execute them all very quickly. Low level programming is more difficult on a RISC based computer.

**ASLR** – Address Space Layout Randomization. ASLR arranges the address space of a process differently each time it executes to make buffer overflow vulnerabilities more difficult to exploit.

**DEP** – Data Execution Protection. An operating system security feature that marks areas of memory as either executable or non-executable. It helps prevent against buffer overflow exploits as well as some other exploits and some program errors.

**NX Stack** – Non eXecutable Stack. A technique used to make buffer overflow vulnerabilities more difficult to exploit. DEP is often implemented at the hardware level by processor architectures that support the NX (No eXecute) bit.

**Canary** – Canaries are another technique to help prevent buffer overflows. A canary is a known value that is put between a buffer and control data on the stack. If the canary value changes, it is likely that the buffer has overflowed and overwritten the canary, and appropriate action can be taken such as terminating the program.

**VM** – Virtual memory. VM allows each process to believe it has its own dedicated physical memory and the Virtual Memory Manager (VMM) maps between virtual memory and the underlying physical memory.

**VMM** – Virtual Memory Manager. The part of the operating system that handles virtual memory. Today often implemented in part by hardware support (a MMU or memory management unit) that is part of the same chip that holds the CPU, such as on the Intel x86 microprocessors.

**TOC/TOU** – Time of Check/Time of Use. A timing attack. Imagine an application that creates a file, and then applies appropriate permissions to it (hey, that's how they taught me to do it in school). There is a vulnerability for a fraction of second between when the file is created and when the file has appropriate security permissions applied that might be exploitable. Also known as a race condition.

**VDI** – Virtual Desktop Interface. With VDI, hosts run a virtual desktop client which loads a virtual machine image from a centralized location.

**VPS** – Virtual Private Server. A Virtual Machine hosted by a third party hosting provider. Full access to the Virtual Machine is typically allowed by the provider.

**VMEscape** – Escaping from a virtual machine to the host operating system or to another virtual machine. Although VMEscape has not been seen in the wild, this attack has been demonstrated before.

**P2V** - Physical to Virtual. Converting a physical machine to a virtual machine. This can be done manual, semi-automatically, or automatically.

**TPM** – Trusted Platform Module. Essentially a chip on the motherboard. Many PCs and laptops have TPMs built in, although Apple hasn't included TPMs in years. The TPM is similar to a built in smart card, and performs cryptographic functions. Originally designed for Digital Rights Management. As one example of its use, Windows systems implementing Bitlocker can use the TPM to do bootup file integrity checking to detect infection by kernel level rootkits.

**DBMS** – Database Management System. Some well known DBMSs include MySQL, Microsoft SQL Server, and Oracle. Most DBMSs support a relational data model (think tables, rows, columns) but there are other data models such as hierarchical, mesh, object oriented, and more.

**DML** – Data Manipulation Language. A database term. Structured Query Language (SQL), pronounced "Sequel," is the most popular and is used to retrieve and manipulate data in relational databases.

**DDL** – Data Definition Language. A database term. A language for defining data structures such as database schemas. Commonly this is Structured Query Language (SQL), or more specifically a subset of SQL.

**XSS** – Cross Site Scripting. A vulnerability where client side code, for example Javascript, HTML, or SQL, can be injected into and executed on the server side. A prime defense is sanitizing all input on the server side (assuming "all input is evil").

**SQL Injection** – An injection attack where SQL code is placed into an input field and passed to the backend database, modifying how it operates. For example a SQL injection attack might be used to dump a database's contents, destroy data, or acquire administrator privileges. SQL Injection is a common attack vector for Web Sites.

**IOT** – Internet of Things. A term used to describe all the various Internet connected embedded devices such as baby monitors, fitness monitors, refrigerators, light bulbs and more.

**SCADA –** Supervisory Control and Data Acquisition systems. Think Industrial Control Systems, for example to control oil refineries.

**RTU** – Remote Terminal Units. RTUs connect to physical sensors in SCADA systems and convert data to digital signals. Sometimes called a Remote Telecontrol Unit.

**HMI** – Human Machine Interface. HMIs present data to human operators in SCADA systems.

**DDP** – Distributed Data Processing. An ancient term ISC2 still uses (Wikipedia doesn't even have a reference) that means we are not still all on a mainframe from very dumb terminals nearby.

## Cryptography:

Basic Crypto, now part of Domain 3, is nothing to be afraid of nor nothing complicated. If you do not know crypto at all though, there are plenty of simple concepts AND acronyms you need to know.

Most of my students do VERY well on the crypto questions, despite this being a difficult area for most others.

**Cryptography** – The art and science of hidden writing, or as Wikipedia says, "The practice and study of techniques for secure communication." Often shortened to "crypto." Crypto has been used by humans for thousands of years (Egyptian

Hieroglyphics are an example) and today crypto is primary based on mathematics and done by computers.

**Cryptanalysis** – Attacking crypto. Reasons to attack crypto include to see if it is any good. There are rarely mathematical proofs showing that a specific cryptosystem is "secure" but if cryptanalysts have been attacking a cryptosystem for years without much progress that is a very positive sign!

**Cryptology** – The overarching field which includes cryptography and cryptanalysis.

**Plaintext** – Unencrypted data, whether it is text, audio, video, smellovision, or something else.

**Ciphertext** – Encrypted data.

**COCOM** – Coordinating Committee for Multilateral Export Controls. An attempt by Western Block countries to prevent the export of advanced technologies including encryption technologies to "dangerous" countries. Formerly dissolved in 1994, it was followed up by Wassenaar Agreement which has similar goals. Of course the definition of dangerous countries depends on who you are.

Both focused on the export of technologies, and allowed symmetric key technology to be exported.

**XOR** – eXclusive OR. A simple and blazingly fast way to add two binary numbers and used extensively in encryption especially because it is so fast. It is binary addition without carry.

**Diffusion** – Dispersing (or "diffusing") the plaintext within the ciphertext.

**Confusion** – The relationship between the plaintext and the ciphertext. The more confusion, the more randomness, and the better.

**SKC** – Secret Key Cryptography. The original type of crypto where the same keys are used to encrypt and decrypt. Examples include ROT n, DES, AES, IDEA, SAFER, RC4, RC5, and RC6.

**ROT n** – A symmetric substitution algorithm where each letter of the alphabet is replaced by the letter which comes “n” characters later in the alphabet.

**Caesar Cipher** – ROT 3. Yes, Julius Caesar used it. “a” is replaced by “d”, “b” is replaced by “e”, “c” is replaced by “f” etc. This is very easy to break using character frequency analysis.

**DES** – Data Encryption Standard. A very widespread symmetric encryption algorithm that is very fast. It was first developed in 1975 and not considered secure today because of its small key size, 56 bits. Triple DES is still widely used, for example by Web browsers.

**ECB** – Electronic Code Book, the default way (or “mode”) that the DES encryption algorithm is used.

**CBC** – Cipher Block Chaining, a mode of DES that utilizes an initialization vector to introduce randomness. This initialization vector is simply a random number that is combined (via the XOR operation) with the first block of plaintext before it is encrypted. Each subsequent block of plaintext is XORed with the previous ciphertext block before being encrypted.

**CFB** – Cipher FeedBack, a mode of DES similar to CBC. This is a streaming cipher, as opposed to ECB and CBC which are block ciphers, and suitable for use with streaming data such as streaming audio and streaming video.

**OFB** – Output FeedBack, a streaming mode of DES like CFB. OFB has the property that flipping a bit in the ciphertext flips the same bit in the plaintext, so many error correcting codes still function even when applied before encryption.

**CTR** – CounTeR Mode, a streaming mode of DES that uses an initialization vector (also called a “nonce” – which is simply a random number) which is combined with the first block of plaintext as in CBC, however this initialization vector is incremented and reused with each subsequent block. Used by IPSec.

**IDEA –** International Data Encryption Algorithm. A symmetric encryption algorithm. Used by PGP, Pretty Good Privacy, but not in widespread use otherwise.

**SAFER** – Secure And Fast Encryption Routine. A family of symmetric key algorithms. Bluetooth optionally uses a variant of SAFER.

**AES** – Advanced Encryption Standard. A symmetric key encryption algorithm chosen by the US government as a replacement for DES. It was chosen as the result of a contest by The Nation Institute of Standards and Technologies, NIST, in 2000, and was formerly known as Rijndael (pronounced "Rain Doll" unless you are Dutch, in which case you'd probably laugh at this pronunciation). It has variable block length and variable key length.

**Rijndael** – The algorithm used by AES.

**RC4, RC5, RC6** – A family of symmetric key ciphers by Ron Rivest. Sometimes called "Ron's Cipher" or Rivest's Cipher."

**PKC** – Public Key Cryptography. Also known as Asymmetric Cryptography. In public key cryptography, as opposed to secret key cryptography, keys come in pairs. If one key in the pair is used to encrypt something, only the other key in the key pair will decrypt it. Examples include RSA, El Gamal, and ECC.

In common usage, each party has a key pair, and the keys are referred to as the private key and the public key. The private key is kept private; no one else knows it. For example, it may live on a smart card and be further protected by a PIN. The public key is publicly available, often as part of a data structure called a Digital Certificate.

**RSA** – Rivest, Shamir, and Adelman, named after the three inventers of this very popular asymmetric key encryption algorithm. It is based on the mathematical fact that large prime integers are easy to multiply together, but the result is difficult to factor into the original factors, meaning the original large prime numbers. Or to put it even more simply: multiplication is easier than division.

**ECC** – Ecliptic Curve Cryptosystems. ECCs are public key cryptosystems and are ideal for small devices such as smart cards as ECC does NOT use a lot of resources such as power, CPU, and memory. The reason for this is that ECC provides a high level of security with relatively short key lengths, so the underlying mathematics are simpler and hence the resources required are minimal.

**MD2, MD4, MD5** – Message Digest. These are hashing algorithms, used primarily for integrity. MD5 is used quite a bit and has a 128 bit hash value. MD5 is considered end of life.

**SHA-1, SHA-2** – Secure Hashing Algorithm.

**HMAC** – Hashed Message Authentication Code, a cryptographic checksum.

**PKI** – Public Key Infrastructure. An infrastructure to distribute the public key of public-private key pairs (used in asymmetric cryptography). PKIs create Digital Certificates, which are data structures containing a name and associated public key, which are digitally signed by a central authority called a Certificate Authority.

**CA** – Certificate Authority, the part of a PKI which creates and digitally signs Digital Certificates, data structures containing a name and associated public key.

The best known CA on the Internet is Verisign, and many organizations have their own internal CAs.

**Digital Certificate** - A data structure that contains, at a minimum, a name and a public key, and that is digitally signed, most commonly by a Certificate Authority.

**X.509** - X.509 is the standard for Public Key Infrastructure, which includes a standard format for Digital Certificates.

**ORA** – Organizational Registration Authority. A registration authority vets an entity before a CA will issue a Digital Certificate for it.

**CRL** – Certificate Revocation List. A list of Digital Certificates that have not expired (the expiration date in the certificate has not past) but that are not to be trusted. CRLs are typically stored in LDAP databases along with Digital Certificates.

A Digital Certificate may be added to a CRL for a multitude or reasons, such as suspected compromise of the associated private key, a name change perhaps due to marriage or religious conversion, retirement, death, etc.

**OCSP** – Online Certificate Status Protocol. An alternative and perhaps eventual replacement for CRLs. OCSP involves real time certificate status checks, as opposed to CRLs which are updated periodically.

**Certification Practice Statement** – A policy document from a Certificate Authority that defines their practices for issuing and managing Digital Certificates.

**PGP** – Pretty Good Privacy, a program used primarily for email encryption but which also supports file, directory, and partition encryption. Provides confidentiality (data encryption) and authentication (via digital signature). Based on a "Web of Trust" model instead of central authority like PKI (although later versions can work with a PKI).

**Escrowed Encryption** – A brain dead scheme proposed by the US government which allowed communication encryption but had a back door key that could be used for legitimate purposes by law enforcement. The key was split into two pieces and escrowed by two different government entities, and these key pieces could only be retrieved by court order. Escrowed Encryption was implemented by the Clipper Chip and used the Skipjack algorithm. Stupid idea that never took off due to public outcry.

**SSL** – Secure Sockets Layer, a cryptographic protocol that allows secure communications over the Internet and other untrusted networks. It supports digital certificates both on both the client and server side, but in practice most commonly only the server has a certificate and the client is authenticated "out of band" (for example by verification of a credit card or other information). TLS (see below) is a standards based replacement of SSL, and considered a later version, for example TLS 1.0 is often referred to as SSL 3.1.

**TLS** – Transport Layer Security, a standards based version and successor to SSL. Modern browsers and Web servers support TLS 1.0 or greater.

**IPSec** – IP Security. IPSec is best known as a VPN protocol used in IPv4 and IPv6. It is complex and provides much more than merely traditional VPN functionality.

This may be the difference between passing and failing . . .

**AH** – Authentication Header. An IPSec protocol that provides for integrity, origin authentication, but no confidentiality.

**ESP** – Encapsulating Security Payload. An IPSec protocol that provides for integrity, origin authentication, and confidentiality.

**PFC** – Perfect Forward Secrecy. PFS encrypts new session (secret) keys with previous keys.

**SSH** – Secure Shell. A protocol for making secure connections between machines. Often used for administering Unix and Linux machines remotely.

**Steganography** – Data hiding. Steganography gives you secrecy but not confidentiality. Cryptography gives you confidentially but not secrecy. For example if someone finds the data, commonly hidden in a file, it is plain text. Steganography and Cryptography are often combined.

## Site and Facility Design and Physical Security:

The simplest question on physical security counts as much as the most complicated question on crypto.

Remember, safety is always #1 on the exam. There are a few things to memorize here, like heights of fences, types of fire extinguishers, classes of gates, etc.

**CCTV** – Closed Circuit TeleVision. A primarily detective physical control. Although wireless and IP based cameras are more common these days, there are still a lot of CCTV systems in use.

**CRT** – Cathode Ray Tube. Old style monitors, which are heavy, relatively fragile, and deep, and made of a vacuum tube with three electron beams, one for red, green, and blue, producing an image. Older cameras were also CRT based.

**CCD** – Charge Coupled Discharge. The technology used by newer cameras, and in fact most cameras today.

This may be the difference between passing and failing . . .

**Heights of Fences** - Seriously, just memorize this (feet and meters). It shows up often enough on the exam.

- A 1 meter or 3 to 4 foot fence will deter casual trespassers.
- A 2 meter or 6 to 7 foot fence are difficult to climb and will deter general intruders.
- A 2.4 meter or 8 foot fence with 3 strands of barbed wire will deter a determined intruder.

**HVAC** – Heating, Ventilation, and Air Conditioning. HVAC is an issue in physical and environmental security. With joint tenancy, HVAC can be a major concern as others may have access to your HVAC controls.

**EPO** – Emergency Power Off. Sometimes called the "big red button" which can shut off power to the entire data center when an emergency occurs (or when it's pressed by mistake).

**EMI** – ElectroMagnetic Interference. High frequency EMI is called RFI.

**RFI** – Radio Frequency Interference. RFI can be caused by devices like neon lights and electric motors and RFI can modulate electric power, called "noise" on the electric power. Normally electric cables are routed away from other cables, grounded, and shielded to help prevent noise from RFI and from EMI (ElectroMagnetic Interference).

**IP** – Intellectual Property. Physical security, at least in large part for most organizations, should be focused on protecting IP. Yeah, yeah, I know it stands for something else too!

# Domain 4: Communications and Network Security

This is a very large domain. Even if you are a “networking person,” do not blow this domain off.

I know networking gurus who have failed the exam because of this domain!

**OSI Model** – Open Systems Interconnection model, a networking model that breaks networking into 7 layers. Essentially theoretical today but often referred to. You must know the layers for the exam!

**NIC** – Network Interface Card.

**MAC address** – Media Access Control address, a unique hardware address assigned to a network interface, commonly burnt into a NIC at manufacture time.

**LLC** – Logical Link Control. LLC is the upper part of Layer 2 in the OSI model and acts as the interface between Media Access Control (MAC) and Layer 3, the Network Layer. It handles flow control, error checking, and the multiplexing of protocols over the MAC Layer, allowing multiple disparate network protocols to be used simultaneously, for example IP and AppleTalk.

**IP** – Internet Protocol. The main protocol of the Internet. A layer 3 protocol. There are two versions of IP, IPv4 and IPv6. IPv4 is currently dominant.

**Private Networking Addressing** – An Internet standard (RFC1918) that allows the network address ranges 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, and 192.168.0.0-92.168.255.255 to be used in private Internets and does not allow them to be routed over the public Internet. A host with a private network address typically is allowed to access the public Internet using Network Address Translation (NAT).

**NAT** – Network Address Translation.

**CIDR** – Classless Inter-Domain Routing. A method for allocating (and routing) IP addresses that extends IP addresses beyond classful addressing (e.g. Class A, B, and C).

**DNS** – Domain Name System, a hierarchical distributed naming system for converting names like securitycerts.org to IP addresses and vice-versa.

**UDP** – User Datagram Protocol. A layer 4 protocol.

**TCP** – Transmission Control Protocol. A layer 4 protocol.

**ICMP** – Internet Control Message Protocol. A layer 3 protocol like IP, but carried in an IP packet like UDP and TCP.

**MIME** – Multipurpose Internet Mail Extensions. An Internet standard for the format of email that allows non-ASCII character sets, non text attachments, and more. Essentially all Internet email is in MIME format.

**S/MIME** – Secure/Multipurpose Internet Mail Extensions, a standard for email encryption and digital signature based on digital certificates. Supported by most modern email clients like Thunderbird and Microsoft Outlook.

**HTTP** – Hypertext Transfer Protocol. An application protocol that is the foundation of the web.

**S-HTTP** – Secure Hypertext Transfer Protocol. A protocol for encrypting web communications that is considered legacy and was never much used. HTTPS is used instead.

**HTTPS** – HTTP over SSL/TLS. Widely used.

**SET** – Secure Electronic Transaction. A protocol for transferring credit card information over insecure networks like the Internet. A legacy protocol that never took off.

**PEM** – Privacy Enhanced Mail. A standard for securing email that never became popular. S/MIME is used instead.

**FTP** – File Transfer Protocol, a clear text protocol that is widely used but that passes passwords and usernames in clear text over the network.

**TFTP** –Trivial File Transfer Protocol. A simplified version if FTP most commonly used for transferring configuration or boot files over LANs.

**SMTP –** Simple Mail Transfer Protocol, the Internet standard for email transmission over IP.

**SNMP** – Simple Network Management Protocol.

**DNP3** – Distributed Network Protocol. Mainly used in SCADA systems by electric and water companies. An example of a multi-layer protocol. DNP3 is layer 2 and layer 7 and arguably layer 4 as well.

**DASD** – Direct Access Storage Device. Secondary storage directly attached to a host computer. Examples include internal and external device drives connected via IDE, SATA and other interfaces. Allows direct block level access.

**NAS** – Network Attached Storage. File and directory access, usually over Ethernet. Direct block level access is not possible.

**SAN** – Storage Area Network. The network equivalent to directly attached storage. Allows direct block level access.

**IDE** – Integrated Drive Electronics. Western Digital's original interface specification for the attachment of storage devices. Used for directly attached storage.

**SATA** – Serial AT Attachment, A more modern interface specification for the attachment of storage devices than IDE. Used for directly attached storage.

**SCSI** – Small Computer System Interface. SCSI consists of a set of standards for connecting and transferring data between computers and hard drives, tape drives, and other peripheral devices. Used for directly attached storage.

**iSCSI** – Internet Small Computer System Interface. SCSI over IP networks. A Storage Area Network (SAN) protocol. Uses normal network cabling.

**Fibre Channel** – A high speed network technology used primarily as a Storage Area Network (SAN) protocol.

**FCoE** – Fibre Channel over Ethernet. A Storage Area Network (SAN) protocol. Runs directly on Ethernet, not IP, hence not IP routable.

**FCIP** - Fibre Channel over IP. FCIP encapsulate Fibre Channel frames and forwards them over IP.

**VOIP** – Voice Over IP, which interestingly is considered a WAN protocol by ISC2.

**PSTN** – Public Switched Telephone Network. The legacy phone network.

**PBX** – Private Branch Exchange. A phone switch. Many legacy PBXs are so large you can actually walk into them.

**FXS Adaptor**– Foreign eXchange Subscriber (or Service or System) Adaptor, also known as an **ATA** (Analog Telephone Adaptor). Used to connect an analog phone or FAX to VOIP.

**SIP** – Session Initialization Protocol. A VOIP signaling protocol for setting up and tearing down VOIP calls, locating users, and negotiating common protocols. The other VOIP signaling protocol is the much more complex H.323.

**RTP** – Real Time Protocol. The VOIP protocol that carries digitized voice. Can also carry digitized video.

**SRTP** – Secure Real Time Protocol. Currently in draft (Dec 2015), SRTP adds encryption, authentication, message integrity and replay protection to RTP.

**RTCP** – Real Time Control Protocol, used in conjunction with the RTP to carry statistics, quality of service information, and more.

**VTC** – Video Teleconferencing. Commonly uses VOIP protocols.

**IM** – Instant Messaging.

**RDP** – Remote Desktop Protocol. A Microsoft protocol for Remote Assistance/troubleshooting and Remote Desktop Services which lets admins control remote servers. Allows a user to connect to a remote computer via a GUI.

**VNC** – Virtual Network Computing. Similar conceptually to RDP above but platform independent.

**NFC** – Near Field Communications. Wireless protocol that allows smart phones and other devices to communicate when very close to each other, commonly touching or within very few inches apart.

**WEP** – Wired Equivalent Privacy. The original Wi-Fi (IEEE 802.11 wireless networks) security protocol. Depreciated as it is very weak and has numerous flaws.

**WPA** – Wi-Fi Protected Access, and **WPA2**, Wi-Fi Protected Access II, replacements for WEP.

**TKIP** –Temporal Key Integrity Protocol. WPA, but NOT WPA2, uses TKIP.

**LAN** – Local Area Network. A bunch of computers electronically close to each other, typically used to mean within one broadcast domain, i.e. they can broadcast to each other. From the security standpoint, the LAN is also a security demarcation perimeter as if you are in a LAN you are fundamentally more trusted than if you are not in the LAN.

**WAN** – Wide Area Network. A bunch of LANs connected together via a (usually high speed) backbone.

**MAN** – Metropolitan Area Network. As in "What's bigger than a LAN but smaller than a WAN? A MAN." Term is not used that often anymore.

**GAN** – Global Area Network. A big WAN. The biggest GAN is obviously the Internet. At least on this planet.

**PAN** – Personal Area Network. A small number of personal devices connected via a network, for example your phone, tablet, and your dorky ear piece via Bluetooth.

**DMZ** – DeMilitarized Zone, the Internet accessible part of an organization's network.

**ATM** – Asynchronous Transfer Mode. An older protocol which is typically used as a high speed backbone connecting LANs together, although it also can be used as a LAN protocol. Frames are 53 bytes, 48 of data and 5 of header. Elegant design based on the technologies and limitations of the day or an odd bastard designed by committee? Perhaps a bit of both.

**FDDI** – Fiber Distributed Data Interface. A token ring based network. It contains two fiber based rings, one as a backup for the other. Considered legacy as fast Ethernet and other technologies have eclipsed it.

**SDLC** – Synchronous Data Link Control. An old mainframe protocol. Think IBM's SNA, System Network Architecture. A layer 2 protocol. Pretty rare these days as IP has taken over the world.

**HDLC** – High-Level Data Link Control. A bit-oriented synchronous data link layer protocol based on SDLC (above). I think of it as the protocol that moves data over an X.25 or Frame Relay cloud.

**ISDN** – Integrated Services Digital Network, or perhaps "It Still Does Nothing." A "faster than modem" technology that works over standard copper telephone lines. Never really took off at least in North America, since DSL and Cable Modem came around the same time and are much faster, but still used for some purposes including video teleconferencing and popular in parts of Europe and India as well.

**X.25** – A WAN technology popular in the 1980s and still in use. Primarily legacy.

**Frame Relay** – A WAN technology similar to X.25 but without extensive error checking as modern networks are reliable. Primarily legacy.

**CSMA** – Carrier Sense Multiple Access.

**CSMA/CD** – Carrier Sense Multiple Access with Collision Detection, used for example by Ethernet.

**CSMA/CA** – Carrier Sense Multiple Access with Collision Avoidance, used for example by Wi-Fi.

**DSL** – Digital Subscriber Line.

**ASDL** – Asymmetric Digital Subscriber Line. Faster download speeds than upload speeds.

**SDSL** – Single Line Digital Subscriber Line – Symmetrical download and upload rates of 1.544 mbps. An operating range of 10,000 feet from the phone company's central switching equipment.

**HDSL** – High Rate Digital Subscriber Line. Like SDSL but uses two pairs of twisted copper lines instead of one to give a 12,000 feet operating range at 1.544mps symmetric. Sometimes used to implement a T1 line.

**VDSL** – Very high rate Digital Subscriber Line. Asymmetric, downstream rates of 13 to 52 mbps and upstream rates of 1.5 to 2.3 mbps, Short range, only 1000 to 4,500 feet from the phone company's central switching equipment.

**QoS** – Quality of Service. The concept that network bandwidth can be reserved, for example by an application. In reality, QoS encompasses far more than just bandwidth, including response time, loss, signal-to-noise ratio, echo, interrupts, frequency response, and more.

**Circuit Switching** – A circuit switched network establishes a dedicated communications channel, called a circuit, between two network nodes before they can communicate. The legacy phone network (PSTN) is an example of a circuit switched network.

**Packet Switching** – In a packet switched network, data is separated into little pieces called "packets" which are transmitted independently though the network. Each packet may take a different route. Also, there are no dedicated communication channels, and different connections may compete for bandwidth on a given communication channel. IP is an example of a packet switched networking technology.

**VC** – Virtual Circuit. A virtual circuit simulates a circuit over a packet switched network.

**SVC** – Switched Virtual Circuit.

**PVC** – Permanent Virtual Circuit.

**DTE** – Data Terminal Equipment, any device connected to a network like a workstation, server, router, bridge, etc.

**DCE** – Data Communication Equipment or Data Circuit-Terminating Equipment, a hardware device that sits between a DTE and the data transmission circuit. One example of a DCE is a modem.

**DSU/CSU** – Data Service Unit/Channel Service Unit. A modem sized hardware device that connects a DTE (like a router) to a digital circuit like a T1 or T3 line. A DSU/CSU is an example of a DCE.

**VLAN** – Virtual Local Area Network.

**ARP** – Address Resolution Protocol, resolves between network addresses and link layer addresses, for example between IP addresses and MAC addresses.

**RARP** – Reverse Address Resolution Protocol, resolves between link layer addresses and network addresses.

**RIP –** Routing Information Protocol, a simple routing protocol that solely uses hop count as the distance metric. The fewer hops, the closer something is, and it ignores any other factors such as network speeds etc.

**OSPF** – Open Shortest Path First, a common routing protocol that is more advanced and complex than RIP.

**EGP** – Exterior Gateway Protocol. A routing protocol used to exchange information between autonomous systems, for example BGP below.

**BGP** – Border Gateway Protocol, a very commonly used routing protocol between autonomous systems on the Internet. Basically the "glue" that holds the Internet together.

**MPLS** – Multiprotocol Label Switching. A common way of providing WAN access between networks.

**SDN** – Software Defined Networking. The concept of controlling a router's control plane (which includes routing updates, time synchronization, logging and more) remotely/centrally instead of on a granular per router basis.

**CDN** – Content Distribution Network. Examples include CloudFlare and Akamai.

**VPN** – Virtual Private Network.

**RADIUS** – Remote Authentication Dial In User Service.

**Diameter** – A draft specification for a replacement for RADIUS servers that overcomes many limitations of RADIUS. I've never seen a Diameter server. Do they actually exist?

**TACACS** – Terminal Access Controller Access Control System.

**PAP** – Password Authentication Protocol, an early protocol that sends the username and password over the network in clear text. For example, some (legacy) RADIUS servers use PAP.

**CHAP** – Challenge Handshake Authentication Protocol, a protocol that does not send the password over the network. Some RADIUS servers use CHAP.

**EAP** – Extensible Authentication Protocol, an authentication framework used with PPP, wireless, and more. There are many EAP protocols, over 100. Some RADIUS Servers use EAP.

**802.1x** – An IEEE standard which separates physical access to a network from logical access. Physically connecting to a network, i.e. OSI Layer 1, for example by physically plugging into a network switch or connecting to a 802.11 Wi-Fi network, does not guarantee logical access. Numerous checks can be done before allowing logical access.

**NAC** – Network Access Control. At its simplest, NAC is 802.1x. Most people however agree that NAC goes above and beyond simple 802.1x (although you may hear the terms used interchangeably at times). NAC adds more control to 802.1x, and allows defining granular policies. These can include pre admission controls and post admission controls such as where users/devices are allowed on the network and what they are authorized to do.

**SLIP** – Serial Line Internet Protocol . A protocol for relaying IP packets over dialup lines. Mostly replaced by PPP.

**PPP** – Point to Point Protocol, used for dialup connections to the Internet, including ISDN and cellular modems.

**NTP** – Network Time Protocol.

# Domain 5: Identity and Access Management

**Identity** – Who an entity claims they are. “I am Ted Demopoulos.”

**Authentication** – Proving an identity, for example by showing a government issued ID or entering a correct password or biometrics.

**AAA** – Authentication, Authorization, and Accountability.

**OTP**  – One Time Passwords, for example created by a hardware device like RSA SecurID or software like S/KEY.

**FRR** – False Reject Rate. In biometric systems, the FRR is the percentage of authentic users who are denied access. It is also known as Type I Error (pronounced as “type one error”). I remember it as Type I as it is not as bad as Type II, below.

**FAR** – False Accept Rate. In biometric systems, Type II Error (pronounced as “type two error”) is the percentage of fake or unenrolled users allowed access. I remember it as Type II as it is worse than Type I (of course the requirements of the system are an issue, but in general it is worse).

**CER** – Crossover Error Rate. A biometric system can be tuned to minimize FAR or FRR. The CER is when a system is tuned so that the FAR and FRR are the same, and is used as a metric to indicate the overall accuracy of the biometric system.

**Enrollment Time** –In biometric systems, how long it takes to initially enter a user into the system. In enrollment, information about the user is captured and entered into the system. **An enrollment time of 2 minutes is considered acceptable.**

**Throughput Time** – After enrollment, how long it takes it takes to identify or authenticate a user. **6 to 10 seconds per user**, which is 10 to 6 users per minute, is considered standard and acceptable.

**SSO** – Single Sign On.

KDC – Key Distribution Server. In the Kerberos Authentication System, the KDC is essentially a login server that knows everyone's password (or "secret key") and issues login credentials, known as TGTs.

TGT – Ticket Granting Ticket. Kerberos issues a TGT when a user first logs in. It is sent to the user encrypted by a secret key derived from their password, and if they got their password correct, the TGT is decrypted and their login succeeds.

SESAME – Secure European System for Applications in a Multi-Vendor Environment. Kerberos is seen by ISC2 as USA centric, as it was developed at MIT in Massachusetts. SESAME is the same idea, but considered international by ISC2 (European somehow equals international). Kerberos uses tickets and symmetric encryption, SESAME uses Privilege Attribute Certificates or PACs and both symmetric and asymmetric encryption. This conveniently avoids the issue that SESAME never took off or was widely implemented at all, and essentially doesn't exist anymore (yes, I'm aware there is a smidgen of legacy use at Master Card, but really, who cares?).

PAC – Privilege Attribute Certificate. Again, SESAME uses PACs, while Kerberos uses tickets.

LDAP – Lightweight Directory Access Protocol. Although a protocol, LDAP is commonly used to refer to directory services/databases that support this protocol.

Federated IdM – Federated Identity Management. Single Sign On (SSO) usually refers to identity management across an enterprise. Federated Identity Management refers to identity management across enterprises. Two main Federated Identity Management standards are OpenID and SAML.

OpenID – An "open and decentralized identity system" which is considered consumer oriented (but which doesn't have to be). For example, Google, Yahoo!, Facebook, and Wordpress use OpenID.

IdP – Identity Provider. An OpenID and SAML term that refers to an online service such as a Web site that provides identity information and authenticates users.

**RP** – Relying Party. An OpenID term. Sites that can use identity information from Identity Providers.

**SAML** – Security Assertions Markup Language.  A standards based approach that allows leveraging authentication across multiple disparate identity providers. Can also be used for authorization.

**SP** – Service Provider. A SAML term that refers to applications that can use identity and authentication information from Identity Providers.

**IDaaS** – Identity as a Service (IaaS, Infrastructure as a Service, was already taken).

**DAC** – Discretionary Access Control. A system where access controls are under the discretion of the owner of a resource as well as the administrators. For example, Windows is a DAC system and if you own a file, you can give rights to other users. Also an administrator can give rights to users. When you think DAC, think consumer and most commercial systems.

**MAC** – Mandatory Access Control. A MAC system is one where access control is based on labels (such as security classifications and clearances), enforced by the system, and cannot be overridden. If you think government systems with classified data on them you have the right idea. Ordinary operating systems like Windows, Unix, and Linux are not MAC. There are MAC versions of Unix and Linux.

**RBAC** - Role Based Access Control. A system where access is based on what roles you have. In reality, these roles are usually mapped to operating systems groups, so the access or rights you have are determined by what groups you belong to.

# Domain 6: Security Assessment and Testing

**Security Assessment** – A "Holistic Big Picture" review of security, though technical security testing, security process review, and security audits.

**Server Side Attacks** – An attack initiated against a listening service by an attacker.

**Client Side Attacks** – An attack initiated by the victim/client, often by clicking on a link on the web or in an email.

**Host Discovery** – Determining which IP addresses in the network have live system. Techniques include ARP scans, passive listening, ICMP Sweeps, IPv6 neighbor discovery and many more.

**Port Scanning** – Scanning TCP and UDP ports on one or more hosts to determine which are open. Nmap is a common port scanning tool.

**Service Fingerprinting** – Determining which services are running on specific ports, as opposed to determining the service by the port number, which may be wrong. For example, a user may attempt to "hide" an unauthorized service by placing it on the HTTP port, port 80. Service fingerprinting will figure out what that service is.

**OS Fingerprinting** – Determining what OS exists at an IP address. Accomplished by sending a variety of packets and examining the replies. Nmap and Xprobe3 are common tools.

**Vulnerability Scanners** – Tools which scan over the network looking for known vulnerabilities. These go way beyond simple port scans. Examples include Nessus, Qualys, SAINT, and many more.

**Penetration Testing –** A proactive detective measure whose goals are to find exploitable vulnerabilities before an adversary can. Penetration testers attempt to "break in" within a carefully defined scope.

**Fuzzing** – Automated stress testing, commonly used to find potential vulnerabilities.

# Domain 7: Security Operations

Domain 7 has grown and now includes Business Continuity Planning/Disaster Recovery Planning, some legal issues and more.

When it comes to legal issues, the goal is not to turn you into legal or law enforcement, but to help you effectively interface with them. Remember, you have no legal training (even if you actually do, pretend you do not for the exam).

If there is a legal related question and one of the answers is similar to “I have no legal training," "consult consul,” or “consult someone with the appropriate expertise,” seriously consider that answer.

Decommissioning/Deprovisioning – Removing a resource from active production. Possible resources include systems, applications, users, and data. Decommissioning/Deprovisioning must be done securely.

IaaS – Infrastructure as a Service. A cloud term. An example is a Virtual Private Server (VPS), a Virtual Machine (VM) you have complete control over. It may be automatically provisioned by your cloud provider on demand or you may supply the VM.

PaaS – Platform as a Service.  A cloud term. An example is one of the many hosting providers which provide you with a Web Server, for example Apache, to host your Web site(s).

SaaS – Software as a Service.  A cloud term. Gmail is one example, providing email services.

Multi Tenant Cloud – A cloud where data and services for different organizations share the same hardware.  Similar to different organizations sharing the same physical building. Sometimes this is appropriate, sometimes it is not!

CCB – Change Control Board.

CMDB – Change Management Database, or Configuration Management Database.

NGFW – Next Generation FireWall. Originating as a marketing term from Palo Alto Networks, NGFW means a very smart firewall that understands Application Layer (layer 7) protocols.

IDS – Intrusion Detection System. An IDS is an alarm system. It watches and raises “alerts” when something occurs that needs human investigation. Just like physical alarm systems, IDSs have false alarms or alerts as well. The primary (or at least one of the primary) technical detection controls.

NIDS – Network Intrusion Detection System. An IDS that functions by watching the packets on a network. A NIDS will commonly be placed at a network aggregation point, for example before the firewall, after the firewall, or on a spanning/mirroring port on a network switch. Snort is a popular open source NIDS.

HIDS – Host Intrusion Detection System. An IDS that sits on one specific host and watches it. HIDS is commonly used to refer to anything that protects a host, and there are also HIDS specific products available. OSSEC is a popular open source HIDS.

IPS – Intrusion Prevention System. An IPS, unlike an IDS, is an inline device that can stop attacks.

An IPS can be implemented in many ways. For example it can be implemented as part of a firewall (for example as an option with CheckPoint’s firewall), as a separate physical network device (for example HP’s TippingPoint), or as a part of an endpoint protection suite (typically combined with AntiVirus/AntiMalware etc.).

SIEM – Security Information and Event Management. “Provides real-time analysis of security alerts generated by network hardware and applications” – Wikipedia. The terms SEM (Security Event Management) and SIM (Security Information Management) are often used interchangeably.

PICERL – Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned. The 6 steps in incident handling. Yes, you need to know these, including the order.

RAID – Redundant Array of Inexpensive Disks or Redundant Array of Independent Disks . There are several RAID levels defined by the RAID advisory board. Note that RAID 0, striping, does NOT provide any redundancy, and RAID 2 is the only level which has a required number of disks, 39. 39 might seem like a strange number unless you are mainframe person as traditionally IBM mainframes had 39 disks. I have no idea what they do today on mainframes. If you care, feel free to google it!

FRDS– Failure Resistant Disk Systems. RAID, except for RAID 0, are examples of Failure Resistant Disk Systems.

## Business Continuity Planning/Disaster Recovery Planning

Once upon a time this was its own domain.

There are not too many terms here. I also suggest reading or at least being familiar with NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, as part of preparing for the CISSP Exam.

BCP – Business Continuity Plan. An overarching plan to minimize interruption to a business after a disruptive event like a disaster occurs. The BCP is a long term and strategic plan. The BCP deals with risks that have not been handled by other controls.

There is always a default BCP, which is you die or go out of business when a large disruptive event occurs.

DRP – Disaster Recovery Plan. The subcomponent of the Business Continuity plan that deals with the recovery of IT systems. Short term and tactical.

COOP – Continuity Of Operations Plan. A term commonly used in the US Government and other governments similar to the term BCP. Although in practice the terms COOP and BCP are sometimes used interchangeably, for the exam at least, the COOP is part of the BCP dealing with sustaining or continuing operations.

BIA – Business Impact Analysis. The BIA comes after the (limited to critical systems) risk analysis and determines tolerable impact levels to systems.

This may be the difference between passing and failing . . .

**MTD** – Maximum Tolerable Downtime, also sometimes called Maximum Allowable Downtime. How long critical systems can be down until the point of no return, until irreparable damage to the organization is done. The MTD is the primary output of the Business Impact Analysis. For some reason the acronym MAD is never used.

**RTO –** Recovery Time Objective. The targeted duration of how long a system or process will be down. The RTO had better be no more than the MTD!

**RPO** – Recovery Point Objective. The targeted duration of how long data can be unavailable. The RPO had better be no more than the MTD!

# Domain 8: Software Development Security

We don’t just sit down and start writing code anymore! We follow a Software Development Life Cycle (SDLC) which begins with planning.

CMM – Capability Maturity Model. A model aimed at improving process and quality. CMM assigns one of 5 levels.

- Level One, Initial: uses terms like “chaotic.”
- Level Two, Repeatable: Some repeatable processes have been defined. Basic project management.
- Level Three, Defined: A standard software process for both engineering and management is defined and all projects use an approved tailored version.
- Level Four, Quantitatively Managed: Adds detailed metrics.
- Level Five, Optimizing: Focused on continual process improvement.

CMMI – Capability Maturity Model Integration. A recent version of CMM with the same 5 levels as the original CMM.

SDLC – Software Development Life Cycle. Instead of simply sitting down and starting to write code, unfortunately a common technique used in software development historically and still somewhat today, software development should follow a lifecycle, beginning with planning and eventually ending in retirement of the system. It also stands for Synchronous Data Link Control, an old IBM mainframe technology.

RAD – Rapid Application Development.

XP – eXtreme Programming, an Agile development method.

CASE tools – Computer Aided Software Engineering tools.

IDE – Integrated Development Environment. A development environment that provides an integrated workspace which commonly includes source code control, debugging, and compiling.

**DevOps** – The concept, practice, and philosophy that development and operations are integrated; code is developed with the operational environment in mind.

**SDL** – Security Development Lifecycle

**MS SDL** – Microsoft Security Development Lifecycle. Microsoft is the name most closely associated with SDL. Their approach has 16 SDL practices.

**SD3+C** – Secure by Design, by Default, by Deployment and Communications. A centerpiece of MS SDL.

**RPC** – Remote Procedure Call.

**ORB** – Object Request Broker. A middleware service, commonly implemented as a server process per machine, which takes object references and resolves them regardless of where the object may reside in the network.

**CORBA** – Common Object Request Broker Architecture. An industry standard for ORBs from the OMG (below) that was a good first attempt but was so vague that CORBA compliant ORB implementations from different vendors like IBM, Sun, and HP, simply did not interoperate.

**OMG** – Object Management Consortium. A bunch of smart folks from Framingham Mass that had the "Object Religion" a bit too intensely and developed CORBA. Apparently they still exist but no one really cares.

**COM/DCOM** – Component Object Model/Distributed Component Object Model. A Microsoft proprietary technology similar to CORBA. Good stuff, and they let out the source code and people started implementing on other platforms like Unix/Linux but the WWW protocols took over.

**QA** – Quality Assurance. A type of dynamic application testing.

**UAT** – User Acceptance Testing. A type of dynamic application testing.

### *CISSP Bootcamps and other Classes*

Ted Demopoulos regularly delivers CISSP Bootcamps as well as other classes at conferences, in hotels, online, as well as onsite. Contact us via demop.com or ted@demop.com.

### ***The Infosec Rock Star Project and Guide***

Technical Knowledge ("Geek") and for some, Managerial Knowledge, is critical for success but is not enough alone for maximum influence and results.

The Infosec Rock Star project gathers advice from true "Infosec Rock Stars" on how to achieve extraordinary results in our field.

Download the latest guide: Infosec Rockstar: Extraordinary Results, Geek will only get you so far . . .

### *About The Author:*

Ted Demopoulos' professional background includes over 25 years of experience including 20+ years as an independent consultant. His clients have included Cisco, Hewlett Packard, IBM, The SANS Institute, The US Department of Defense, The Royal Hong Kong Jockey Club, Motorola, The Singapore Ministry of Education, The UK Post Office, T Rowe Price, TRW, and The Hong Kong Post.

His first professional computer work was in 1984, and in 1990 he founded Demopoulos Associates. He has been very fortunate since then to be able to work on a number of exciting projects worldwide. Along the way, Ted has also helped start a successful information security company, was the CTO at a "textbook failure" of a software startup, has advised several other startups, and has received a DoD Award of Excellence.

Ted is a frequent speaker at conferences, conventions, and other business events, quoted often by the press, and a published author.

Ted conducts Leadership and Information Security Bootcamps and is the principal of Demopoulos Associates. He holds a BA from Dartmouth College and an MS from the University of New Hampshire. More information about Ted is available at www.demop.com.

This may be the difference between passing and failing . . .

## *Disclaimer – The Small Print:*

We make neither representation nor warranties with respect to the accuracy or completeness of this material and specifically disclaim any and all warranties of fitness or applicability of this material for any purpose.

This is not intended as advice and may or may not be suitable for any purposes, including printing out and wrapping fish.

This material may be fattening, unhealthy, cause sudden onset baldness, or otherwise be undesirable.

We are not liable for anything.