Veritas News Service and CAJI/IS Exclusive
09 May12
Information Assurance and Security
By Samly P. Hall

Times have changed dramatically over the last few decades, especially with today's rapidly changing technologies and the increased risk of attacks, spying, and identity intrusions. I have gathered this working data on some of the newest forms of Information Access in the security world being discussed. Information security, known as InfoSec, is defined as the protection of information and the systems and hardware that use, store, and transmit the information. The need for information security knowledge gets more pressing every year. The FBI teams up with the Computer Security Institute every year to do a survey about computer crimes. A recent survey indicated that quantified losses due to computer crime were up 42% over the year before.

Information assurance (IA) and information security (IS) are often incorrectly used interchangeably, but the two terms are not synonymous. The people who make up the U.S. government define IA as "*Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.*" This definition can be simplified to "*the complete preservation of information confidentiality, integrity and availability in all of the information's various states, otherwise known as the C.I.A. Model*."

Information security is a large subset of IA, which deals primarily with the more glorious tools and tactics for protecting information from threats such as con artists (phishing), hackers (exploits) and malicious code (viruses). IA covers a much broader spectrum of information management and protection such as certification and accreditation (C&A), business continuity planning (BCP), compliance and disaster recovery planning (DRP).

To better understand the management of information assurance and security, one must become familiar with the key characteristics of information that make it valuable. The C.I.A. triangle has been the industry standard for computer security since the development of the main frame. The C.I.A. triangle is founded on three desirable characteristics of information – Confidentiality, Integrity, and Availability – that are as important today as they were when first put forth. However, present day needs have made these three concepts alone inadequate because they are limited in scope and cannot encompass the constantly changing environment of Information Technology and Information Security needs. The C.I.A triangle, therefore, has expanded into a more comprehensive list of critical characteristics of information. This list contains confidentiality, integrity, availability, privacy, identification, authentication, authorization, and accountability. It is critical that computer users of all types, whether at their job or at home understand how to protect themselves and their organizations from attacks. Four distinct areas that a user should be knowledgeable about include Access Controls, Policy, Cryptography, and Forensics. Access Controls, Policy, and Cryptography can be checked against the expanded C.I.A triangle to ensure user security, assurance, and safety. Digital forensics is also an important topic that a computer user should be made aware of. When an unauthorized incident occurs, such as an attacker penetrating network defenses, a response is required. These incident response procedures include forensic science and properly responding to a computer forensics event. Below is a manual I have put together regarding Access Controls, Policy, Cryptography, and Forensics.

-----Access Controls Part 1-----

What is Access Control?

- The process by which resources or services are granted or denied on a computer system or network.
- "Access controls are security features that control how users and systems communicate and interact with other systems and resources."
-"Access controls give organizations the ability to control, restrict, monitor, and protect resource availability, integrity, and confidentiality."

Best Practices for Access Control

-Separation of duties--system is not vulnerable to actions performed by a single person.
-Job rotation--limits amount of time that individuals are in a position to manipulate security configurations.
-Also cross training and mandatory vacations.
-Least privilege
-Implicit deny--if a condition is not explicitly met, then it is to be rejected.

Access Control Methods

-Administrative Control
-Technical Controls
-Physical Controls

Administrative Controls

-Policies and procedures
-Personnel controls-incorporate access into HR, what happens when we hire, fire people, someone Resigns-- do they retain privileges?
-Supervisory structure-a supervisor should be responsible for employee's actions.
-Security awareness training
-Testing

Technical Controls

-Enable policy enforcement where human behavior is difficult to regulate
-User name/password
-Encryption
-System Access Control-use access control technologies and security technologies to enforce rules. There are many different models of this.
-Biometrics
-Remote Access Authentication Protocol
-Network Monitoring and Intrusion Detection

Physical Controls

-Computer security
    -USB ports, DVD drives
    -Locking up server racks
-Perimeter security
    -Badges, closed-circuit TV, fences, lighting, motion detectors, sensors, alarms, location of building, signs.
    -Single point of entry, emergency exits
-Man trap
-Guards and dogs
-Control zones-areas that require higher level of security
    -Located away from public access
    -Unobtrusive
    -Extra rules-no cameras, recording devices, searches
-Logged entry
    -Visitors

Access Control Types

-Administrative, physical, technical controls have different functions
-Deterrent--intended to discourage a potential attacker
-Preventative--intended to avoid an incident from occurring
-Corrective--fixes components or systems after an incident has occurred
-Recovery--intended to bring controls back to regular operations
-Detective--helps identify an incident's activities.
-Compensating--controls that provide for an alternative measure of control. Any control can end up being one.
-Directive--mandatory controls that have been put in place due to regulations or environmental requirements.

Access Control Services

-Identification:
    -A method of ensuring that a subject is the entity it claims to be
    -Non-proven assertion.
-Authentication: user provides password, confirms the identity.
-Authorization: user authorized to login and access certain data or systems.
-Accountability

Identification

-User enters username, account number.
-A person can have many digital identities which can complicate the process of identification.
-Identities should include three aspects:
    -Unique--everyone has a unique ID for accountability.
    -Non-descriptive--do not use ADMIN, the identifier should not indicate the purpose of the account.
    -Issuance--issued by some authority.

Authentication

-Authentication is a two-step process with part one being identification and the second being authentication or verification of the ID. It determines who can log in.
    -Password, passphrase, token, anatomical attribute, cryptographic key, PIN.

-Something you know
-Something you have
-Something you are
-Something you produce
    -Often combined with something you are.

Two-Factor or Strong Authentication

-Two-factor/strong authentication/multifactor--Requires two or more authentication methods.
-Disadvantages:
    -Implementation cost: hardware, software, time/effort, tokens/smart cards
    -Increased support cost
    -Lost devices

Authentication Issues

-Password quality--need a standard-tough, but not too tough
-Forgotten credentials
-Compromised credentials--detect, restrict, reset
-Staff terminations
-Password management approaches:
    -Password synchronization
    -Reduces help-desk call volume
    -Hacker only has to figure out one credential set
        -Same as single sign-on? No, these are two different things.
            -Single sign-on--you log in once and this gives you access to multiple (authorized) systems. Password synchronization--you use the same username and password in multiple systems, have to log in to each of these systems.

-Self-service password reset--By answering secret questions, or perhaps by having a link to reset your password sent to your registered email account.
-Assisted password reset-- you have to call the help desk to get your password reset. The help desk can't tell you your password, they can just reset your password after they verify your identity, perhaps using secret questions. When the help desk resets your password or gives you a temporary password, the user should have to change it the first time they use it. This way the help desk does not have your password.
-Hard to pick good secret question--it may be easy to find the answers to someone's secret question on social media sites or other sources, but it also has to be something a person can remember every time and remember to spell the same way every time.

Something You Know

-This type of authentication mechanism verifies the user's identity by means of a password, passphrase, lock combination, PIN, or other unique code.
-Usually least expensive type of authentication.
-Primary weakness is that someone else might acquire the knowledge
-A password is a private word or combination of characters that only the user should know.
-A passphrase is a plain-language phrase, typically longer than a password, from which a virtual password is derived.

-Whitman-A good rule of thumb is to require that passwords be at least eight characters long (is this enough?) and contain at least one number and one special character.
-Most common authentication method
-Do not share

-Use non-keyboard characters (charmap.exe)

Passphrase Example

-The virtual password MTFBWYA is derived from "May the force be with you always"

-Could also construct virtual password using a set of construction rules:

-1st 3 letters of your last name, a hyphen, first two letters of your first name, an underscore, the first two letters of your mother's maiden name, a hyphen, and the first 4 letters of the city in which you were born.

-Considered easy to use (by whitman) once you know the construction rules.

Problems with Passwords

-Human Nature --Choosing words that are easy to remember or writing them down.

-In one study of 144 users, avg of 16 passwords each

-What is the most popular password? 123456

-Transmission and Storage – easily found in text files or weak hashing algorithms.

-Easily Broken by Brute Force, Dictionary or rainbow Attacks.

-Inconvenient – Users use "remember my password," neglect to log out or lock workstations.

Password Controls – Best Practices

-Length – Longer the Better.

-Older Windows operating systems break password into 2-7 character passwords before hashing.

-Old style of hash is called LM hash. It was also case-insensitive. By limiting the length and complexity of the password, it is much easier to break. This type of hash is considered obsolete, but it is still used in many systems for backward compatibility. If you create a password of 15 characters or more, this type of hash is not stored.

-Complexity – Upper and Lower Case and Special Character

-Does it matter where in the password these are? Yes, password crackers will assume they are most likely to be at beginning and end--most effective to use them in random locations.

-Aging – Change Dates – 30, 60, 90 days.

-Minimum time between changes?

-Yes. If you don't set one, then a person can just change their password again and again multiple times to overcome any history restrictions. For example, if you don't allow people to use one of the last 10 passwords, but they can change their password every 5 minutes, then a person who really likes a certain password could change their password enough times in one hour to cycle back to that first password that they really like.

-History – Keeps users from using same passwords over and over again.

-Should combine aging and history.

-Limited Attempts – 3 is recommended with 30-minute wait.

-Use a password checker to test user-chosen passwords

-Different passwords at different sites

-2005 study: 44% use same password at multiple sites, 37% of online banking customers use same password at less secure sites.

-Prohibit shared accounts

-These passwords rarely get changed
-People give it out freely
-Impossible to know who is responsible if account used inappropriately.
-Passwords should be random

Password Attacks

-Dictionary
-Hybrid dictionary-looks for adding a number at beginning or end, looks for simple replacements like o replaced with 0, a replaced with @, etc.
-Brute force
-Can enter parameters to make it even quicker to crack the password:
-Length
-Character set
-Language -Pattern (if any part of the password is known)
-Rainbow tables
-Considered superior to brute force and dictionary attacks.
-Rainbow tables create a large pre-generated set of hashes from nearly every possible password combination. Rainbow tables contain passwords already in their hashed format.
-Much faster than dictionary attacks.
-Amount of memory needed on the attacking machine greatly reduced. Tradeoff is greatly reduced. Tradeoff is time to create.
-Can salt passwords to make them harder to break.

-----Access Controls Part 2-----

Something You Have

-This authentication mechanism makes use of something (a card, key, or token) that the user or the system possesses.
-One example is a dumb card (such as an ATM card) with magnetic stripes.
-Another example is the smart card containing a processor.

Something You Are

-This authentication mechanism takes advantage of something inherent in the user that is evaluated using biometrics.
-Most of the technologies that scan human characteristics convert these images to obtain some form of minutiae—unique points of reference that are digitized and stored in an encrypted format.
-Physiological

Something You Do/Produce

-This type of authentication makes use of something the user performs or produces.
-It includes technology related to signature recognition and voice recognition, for example.
-Behavioral

Biometrics and Behavior

-Individual presents the particular biometric characteristic and the system matches this against the database.
-More complex and expensive than other types of identity verification processes.
-Accuracy – The uniqueness of the body organ or characteristic, usually fingers or eyes.

Biometrics Ratings Measures

-False Reject Rate (FRR) – Type I Error – Authorized users are incorrectly denied access. Usually stated as a percentage. Also probability that system will reject a person who should be matched to a template.
-False Accept Rate (FAR) – Type II Error – Unauthorized users are incorrectly granted access. Usually stated as a percentage. Also, a match to a template that should not be made.
-Which is worse-false acceptance or false rejection? Door vs. watch list
-Crossover Error Rate (CER) – The point at which the FRR equals the FAR. Usually stated as a percentage. The most important measure of biometric system accuracy. Allows you to compare across systems.

Biometrics and Behavior

-Barriers to acceptance:
-Speed and Throughput – the time required to complete the entire authentication procedure.
-User acceptance
-Enrollment time
    -During enrollment, key features are extracted and saved as the user's template.
    -What percent is considered a match?
-Generally accepted standards are a speed of less than five seconds, a throughput of six to ten per minute, and an enrollment time of less than two minutes.

Common Physiological Biometric Access Control Systems

-Finger Scan Systems – Create an image of ridges, whorls, and minutia of the fingerprint. Save a digitized file of finger characteristics, not the fingerprint.
-Stats – Accuracy = 1-5% CER
-Speed – 1-7 Seconds
-Advantages – Non-Intrusive and Inexpensive
-Disadvantages – Sensor wear and effected by swelling or injury. Can be defeated. Use where little danger of deception.
-Two types: Static and Dynamic
    -Static uses entire finger.
    -Dynamic has a small slit or opening.
-Most commonly used.

Common Physiological Biometric Access Control Systems

-Hand Geometry Systems – Create an image of length, width, height, and other characteristics of a hand. A digitized image records characteristics.
-Stats
-Accuracy – 1-2% CER

-Speed – 3-5 Seconds
-Disadvantages – Sensor wear and swelling, injury, or wearing rings.

Common Physiological Biometric Access Control Systems

-Retina Patterns – Record Unique elements in the blood vessel pattern of the retina on the backside of the eyeball.
-Concerns include eye damage from laser.
-Concerns include that the retina pattern can change with diabetes or heart disease.

Common Physiological Biometric Access Control Systems

-Retina Scans Stats
-Accuracy – 1.5% CER
-Speed – 4-7 Seconds
-Advantages – Overall Accuracy
-Disadvantages – Intrusiveness

Common Physiological Biometric Access Control Systems

-Iris Patterns – Most Accurate of all biometric tests. It offers more reference coordinates than other types of biometrics.
-The iris is the colored portion of the eye surrounding the pupil.
-Iris patterns stay constant through adulthood and are different between two eyes on the same person.
-There is only a chance of one in 1078 that two irises will be identical.

Common Physiological Biometric Access Control Systems

-Iris Pattern Stats
-Accuracy <0.5% CER
-Speed – 2.5-4 Seconds
-Advantages – Best Accuracy
-Disadvantages – Subject must stay still. Optical unit must be placed so sun doesn't shine into equipment.

Common Behavioral Biometric Access Control Systems

-Voice Recognition – captures unique characteristics of a subject's voice and analyze phonetic and linguistic patterns.
-Stats Accuracy - <10% CER
-Speed 10-14 Seconds
-Advantages – Inexpensive and Non-intrusive.
-Disadvantages – Accuracy, speed, and voice changes. Can have high false rejects, frustrates users.

Common Behavioral Biometric Access Control Systems

-Signature Dynamic Systems – Require the subject to sign their name on a tablet.
    -Captures speed of signing, how pen is held, pressure exerted.

-Stats – Accuracy – 1% CER
-Speed – 5-10 seconds
-Advantages – Non-Intrusive
-Disadvantages – Signature Tablet wear, speed, and can be forged. This can also change.

-----Policy-----

Why Policy?

-A quality information security program begins and ends with policy
-Policies are the least expensive means of control and often the most difficult to implement.
-Some basic rules must be followed when shaping a policy:
    -Never conflict with law
    -Stand up in court
    -Properly supported and administered
    -Contribute to the success of the organization
    -Involve end users of information systems
-Enron
-Can you have too many policies?

What Is a Security Policy?

-Policy is a plan or course of action that influences and determine decisions.
-For policies to be effective, they must be:
    -Properly disseminated, read, understood, and agreed to
-Security policy
    -A written document that states how an organization plans to protect the company's information technology assets. It dictates the role that security plays within the organization.

Balancing Trust and Control

-An effective security policy must carefully balance two key elements: trust and control.
-Three approaches to trust:
    -Trust everyone all of the time
    -Trust no one at any time
    -Trust some people some of the time
-Deciding on the level of control for a specific policy is not always clear.
    -The security needs and the culture of the organization play a major role.

Enterprise Information Security Policy (EISP)

-Sets strategic direction, scope, and tone for organization's security efforts.
-Guides development, implementation, and management requirements of

information security program.
-Establishes how a security program will be set up, lays out the program's goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out.
-Must support org vision and mission statements.
-Does not require frequent modification.
-Issued by management official such as head of org or senior official.

Example EISP – CCW

-Protection of Information: Information must be protected in a manner commensurate with its sensitivity, value, and criticality.
-Use of Information: Company X information must be used only for the business purposes expressly authorized by management.
-Information Handling, Access, and Usage: Information is a vital asset and all accesses to, uses of, and processing of Company X information must be consistent with policies and standards.
-Policy Non-Enforcement: Management's non-enforcement of any policy requirement does not constitute its consent.
-Violation of Law: Company X management must seriously consider prosecution for all known violations of the law.
-Industry-Specific Information Security Standards: Company X information systems must employ industry-specific information security standards.
-Use of Information Security Policies and Procedures: All Company X information security documentation including, but not limited to, policies, standards, and procedures, must be classified as "Internal Use Only," unless expressly created for external business processes or partners.
-Security Controls Enforceability: All information systems security. controls must be enforceable prior to being adopted as a part of standard operating procedure.

Issue-Specific Security Policy (ISSP)

-Serves to protect employee and organization from inefficiency and ambiguity; documents how the technology-based system is controlled; and identifies the processes and authorities that provide this control.
-Purpose of ISSP is to show how employees can and cannot use technology, not just for enforcement or prosecution .
-More detailed than EISP.
-Serves to indemnify the organization against liability for an employee's inappropriate or illegal system use.
-Addresses specific security issues that management feels need a more detailed explanation, makes sure employees know how they are to deal with security issues.
-Should address compliance.

-Should have point of contact for further info, guidance or compliance.
-ISSP will require frequent updates.

Types of Security Policies (Continued)

-Most organizations have security policies that address:
-Acceptable use
-Password management and complexity
-Personally identifiable information
-Disposal and destruction
-Service level agreements
-Classification of information
-Ethics

Acceptable Use Policy (AUP)

-Defines the actions users may perform while accessing systems and networking equipment.
-May have an overview regarding what is covered by this policy.
The AUP usually provides explicit prohibitions regarding security and proprietary information. Unacceptable use may also be outlined by the AUP. Acceptable use policies are generally considered to be the most important information security policies.

Password Management and Complexity Policy

-Can clearly address how passwords are created and managed
The policy should also specify what makes up a strong password.

Personally Identifiable Information (PII) Policy

-Outlines how the organization uses personal information it collects

Disposal and Destruction Policy

-Addresses the disposal of resources that are considered confidential
-Often covers how long records and data will be retained
-Involves how to dispose of equipment
-2 people bought 158 recycled computers/hard drives. Of the 129 functioning drives, 69 contained recoverable files, 49 contained significant personal info.

Service Level Agreement (SLA)

-A service contract between a vendor and a client that specifies what services will be provided, the responsibilities of each party, and any guarantees of service.

Service Level Agreement (SLA) Policy

-An organizational policy that governs the conditions to be contained in an SLA. Many SLA policies contain tiers of service.

Classification of Information Policy

-Designed to produce a standardized framework for classifying information assets
-Generally, this involves creating classification categories and then assigning information into these categories.
-Commercial Business Example: Confidential, private, sensitive, public
-Military Example: Top secret, secret, confidential, sensitive but unclassified, unclassified.

Ethics Policy

-Ethics is the study of what a group of people understand to be good and right behavior and how people make those judgments.
-A written code of conduct intended to be a central guide and reference for employees in support of day-to-day decision making.
-Intended to clarify an organization's mission, values, and principles, and link them with standards of professional conduct.

Systems-Specific Policy (SysSP)

-Systems-specific policies (SysSPs) frequently do not look like other types of policy.
-These present the management's decisions that are specific to the actual computers, networks, applications, and data.
-They may often be created to function as standards or procedures to be used when configuring or maintaining systems.

SysSP

-Should be expressed as rules-who can do what to which specific classes and records of data and under what conditions.
-Each type of equipment has its own type of policies
-There are two general methods of implementing such technical controls:
    -Access control lists
    -Configuration rules

Access Control Lists

-In general, ACLs regulate:
    -Who can use the system
    -What authorized users can access
    -When authorized users can access the system
    -Where authorized users can access the system from

-How authorized users can access the system
-Restricting what users can access, e.g., printers, files, communications, and applications.

Configuration Rules

-Configuration rules are the specific configuration codes entered into security systems to guide the execution of the system when information is passing through it.
-Rule policies are more specific to the operation of a system than ACLs, and may or may not deal with users directly.
-Many security systems require specific configuration scripts telling the systems what actions to perform on each set of information they process.

Exceptions to Policy

-Exceptions are always required
    -But they must be managed
-Limiting Exceptions
    -Only some people should be allowed to request exceptions.
    -Fewer people should be allowed to authorize exceptions.
    -The person who requests an exception must never be authorizer.

-Exception must be carefully documented.
    -Specifically what was done and who did each action.
-Special attention should be given to exceptions in periodic auditing.
-Exceptions above a particular danger level
    -Should be brought to the attention of the IT security department and the authorizer's direct manager.

For policies to be effective, they must be:

-Developed using industry-accepted practices.
-Distributed or disseminated using all appropriate methods.
    -Distribution is not always straightforward.
        -Must be able to prove that policy actually reached end user.
-Reviewed or read by all employees.
-Understood by all employees.
    -Effective policy is written at a reasonable reading level, and attempts to minimize technical jargon and management terminology.
-Formally agreed to by act or assertion.
-Uniformly applied and enforced.

---Cryptography Part 1---

What is Cryptography?

-Cryptology, the science of encryption, encompasses two disciplines: cryptography and cryptanalysis.

-Cryptography—from the Greek word "kryptos," meaning "hidden," and "graphein," meaning "to write"—describes the processes involved in encoding and decoding messages so that others cannot understand them.

-Cryptanalysis—from "analyein," meaning "to break up"—is the process of deciphering the original message (or plaintext) from an encrypted message (or ciphertext), without knowing the algorithms and keys used to perform the encryption.

Cryptography versus Steganography

-Steganography

-Hides the existence of the data.

-What appears to be a harmless image can contain hidden data embedded within the image.

-Can use image files, audio files, or even video files to contain hidden information.

What Is Cryptography? (Continued)

Encryption

-Is the process of converting an original message into a form that cannot be understood by unauthorized individuals.

-Encrypt/encipher: to encrypt or convert plaintext to ciphertext.

Decryption

-Change the secret message back to its original form.

-Decipher: to decrypt or convert ciphertext to plaintext.

Encryption Definitions

-Plaintext (not plain text): the original unencrypted message that is encrypted and results from successful decryption. Readable data (by person or computer).

-Cipher: the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components.

-Ciphertext or cryptogram: the unintelligible encrypted or encoded message resulting from an encryption. Neither human or machine can properly process it until it is decrypted.

-Algorithm: the mathematical formula or method used to convert an

unencrypted message into an encrypted message. Set of rules that determines how enciphering and deciphering take place.

-Key: the information used in conjunction with the algorithm to create the ciphertext from the plaintext; it can be a series of bits used in a mathematical algorithm, or the knowledge of how to manipulate the plaintext.

-Keyspace-a range of values that can be used to construct a key. Larger keyspace means more possible keys. Use entire keyspace, pick randomly.

Common Ciphers

-In encryption, the most commonly used algorithms include two functions: substitution and transposition. Two other ciphers are the Vernam and Book (or running key) cipher.

-In a substitution cipher, you substitute one value for another

- -A mono-alphabetic substitution uses only one alphabet
- -A polyalphabetic substitution uses two or more alphabets
- -Caesar cipher.

-The transposition cipher (or permutation cipher) simply rearranges the values within a block to create the ciphertext.

-Simple substitution and transposition ciphers are vulnerable to frequency analysis.

Vernam Cipher

-Also known as the one-time pad, the Vernam cipher was developed at AT&T and uses a set of characters that are used for encryption operations only one time and then discarded.

-The values from this one-time pad are added to the block of text, and the resulting sum is converted to text.

Cryptographic Algorithms

-There are three categories of cryptographic algorithms:

- -Hashing algorithms
- -Symmetric encryption algorithms
- -Asymmetric encryption algorithms

Hashing Algorithms

-Hashing

- -Also called a one-way hash
- -A process for creating a unique “signature” for a set of data
  - -This signature, called a hash or digest, represents the contents.

-Hashing is used only for integrity to ensure that:

- -Information is in its original form
- -No unauthorized person or malicious software has altered the data.

-Hash created from a set of data cannot be reversed

-(12345*143=1,765,335)

Hashing Algorithms (Continued)

-A hashing algorithm is considered secure if it has these characteristics:

-The ciphertext hash is a fixed size (regardless of plaintext size).

-Two different sets of data cannot produce the same hash, which is known as a collision.

-It should be impossible to produce a data set that has a desired or predefined hash.

-The resulting hash ciphertext cannot be reversed

-The hash serves as a check to verify the message contents.

Hashing Algorithms (Continued)

-Hash values are often posted on Internet sites

-In order to verify the file integrity of files that can be downloaded.

Message Digest (MD)

-Message Digest (MD) algorithm

-One common hash algorithm.

-Three versions

-Message Digest 2 (MD2)-developed in 1989, now considered too slow

-Message Digest 4 (MD4)-created in 1990, flawed, too easy to generate collisions.

-Message Digest 5 (MD5)-created in 1991. Successfully attacked in 2004.

Secure Hash Algorithm (SHA)

-A more secure hash than MD: longer hash is harder to attack.

-A family of hashes (SHA-0, SHA-1, SHA-2)

-Should use SHA-2 (224-512 bit hash length).

-SHA-3 currently under development.

-SHA1 collisions in 2005.

Password Hashes

-Another use for hashes is in storing passwords.

-When a password for an account is created, the password is hashed and stored.

-Not really a true hash, but really a one-way function.

-In LM hashes, the password itself is the key.

Symmetric Encryption

-Each of the methods of encryption and decryption described requires that the same algorithm and key are used to both encipher and decipher the message.

-This is known as private key encryption, secret key, or symmetric

encryption.

-In this approach to encryption, the same key—a secret key—is used to encrypt and decrypt the message.

-Symmetric encryption methods are usually extremely efficient and fast, requiring easily accomplished processing to encrypt or decrypt the message (faster than asymmetric).

-Need separate key for each person you want to communicate with. The Number of keys symmetric keys needed is: N(N-1)/2. How many keys needed for 10 people to communicate?

-Biggest challenge in symmetric key encryption is: getting a copy of the key to the receiver.

Symmetric Cryptographic Algorithms (Continued)

-Data Encryption Standard (DES) 1977

-One of the first widely popular symmetric cryptography algorithms.

-DES is a block cipher and encrypts data in 64-bit blocks

-DES is a federally approved standard for non-classified data; it was cracked in 1997 when the developers of a new algorithm, Rivest-Shamir-Aldeman, offered a $10,000 reward for the first person or team to crack the algorithm.

-Fourteen thousand users collaborated over the Internet to finally break the encryption. It took 3 days and 1536 microprocessors.

-Was only intended to be used until the mid-1980s. This same attack might now only take 10 hours.

-Triple Data Encryption Standard (3DES)

-Designed to replace DES

-Uses three rounds of encryption instead of just one, 16 iterations within each round.

-2^56 times stronger than DES, but slow.

Symmetric Cryptographic Algorithms (Continued)

-Advanced Encryption Standard (AES)

-Approved by the NIST in late 2000 as a replacement for DES

-AES performs three steps on every block (128 bits) of plaintext

-Within Step 2, multiple rounds (9-13) are performed depending upon the key size.

-In 1998 (or 1997), it took a special computer designed by the Electronic Freedom Frontier more than 56 hours to crack DES.

-It would take the same computer approximately 4,698,864 quintillion years to crack AES.

-AES was recently “theoretically” broken.

What Does it Mean to Say the Algorithm is Broken?

-Someone was unable to uncover a key that was used during the encryption process. (One key used for one instance of encryption).
-Is the algorithm worthless if it has been broken?

Asymmetric Cryptographic Algorithms

-Also known as public key cryptography
-Uses two keys instead of one
    -The public key is known to everyone and can be freely distributed.
    -The private key is known only to the recipient of the message.
-Either key can be used to encrypt or decrypt the message.
    -However, if Key A is used to encrypt the message, then only Key B can decrypt it; conversely, if Key B is used to encrypt a message, then only Key A can decrypt it.
-Slower than symmetric
-Better key distribution than symmetric
-Better scalability
-Can also provide authentication and nonrepudiation (symmetric cannot provide these).

-Asymmetric cryptography can also be used to create a digital signature.
-A digital signature can:
    -Verify the sender (authentication)
    -Prove the integrity of the message
    -Prevent the sender from disowning the message (nonrepudiation)

Digital Signature

-When the asymmetric process is reversed—the private key encrypts a (usually short) message, and the public key decrypts it—the fact that the message was sent by the organization that owns the private key cannot be refuted.
    -This nonrepudiation is the foundation of digital signatures
    -Often a digital signature is a hash value that has been encrypted by a sender's private key.
-Digital signatures are independently verified by a central facility (Registry) as authentic.
-Using a digital signature doesn't encrypt the message itself. To ensure privacy of the message, it must also be encrypted using the receiver's public key.
-With a digital signature, I'm not releasing/revealing my private key, I'm just using it to encrypt something.

RSA

-The most common asymmetric cryptography algorithm.
-1st public key encryption algorithm developed for commercial use.
-Minimum recommended key length is 1024 bits.

Uses for Cryptography

-File encryption
-Disk encryption
-E-mail security
-Web browsing
-Remote network access

---Cryptography Part 2---

Defining Digital Certificates

-Digital certificate
    -Can be used to associate or "bind" a user's identity to a public key.
    -The user's public key that has itself been "digitally signed" by a reputable source entrusted to sign it.
-Digital certificates make it possible for Alice to verify Bob's claim that the key belongs to him.
-When Bob sends a message to Alice he does not ask her to retrieve his public key from a central site.
    -Instead, Bob attaches the digital certificate to the message.

-A digital certificate typically contains the following information:
    -Owner's name or alias
    -Owner's public key
    -Name of the issuer
    -Digital signature of the issuer
    -Serial number of the digital certificate
    -Expiration date of the public key

Authorizing, Storing, and Revoking Digital Certificates

-Certificate Authority (CA)
    -An entity that issues digital certificates for others.
    -A user provides information to a CA that verifies her identity.
    -The user generates public and private keys and sends the public key to the CA.
    -The CA inserts this public key into the certificate.
    -Can be internal or external.

-Registration Authority (RA)
-Handles some CA tasks such as processing certificate requests and authenticating user.
-A sub-entity of the CA.

-Certificate Revocation List (CRL)
-Lists revoked certificates.
-Can be accessed to check the certificate status of other users.
-Most CRLs can either be viewed or downloaded directly into the user's Web browser.
-Certificate Repository (CR)
-A publicly accessible directory that contains the certificates and CRLs published by a CA.
-CRs are often available to all users through a Web browser interface.

Types of Digital Certificates

-Categories of digital certificates
-Personal digital certificates (mostly used for email)
-Server digital certificates
-Software publisher digital certificates

What Is Public Key Infrastructure (PKI)?

-Public key infrastructure involves public-key cryptography standards, trust models, and key management.
-Public key infrastructure (PKI)
-A framework for all of the entities involved in digital certificates to create, store, distribute, and revoke digital certificates.
-Includes hardware, software, people, policies and procedures.
-PKI is digital certificate management.

Managing PKI (continued)

-Certificate life cycle
-Creation: certificate created & issued, user positively identified.
-Suspension
-Revocation
-Expiration--every certificate issued by a CA must have an expiration date.

Key Management

-Proper key management includes key storage, key usage, and key handling procedures.

Key Storage

-Public keys can be stored by embedding them within digital certificates
-Private keys can be stored on the user's local system
-Private keys can be stored on smart cards or in tokens

Key Handling Procedures

Procedures include:

-Escrow: keys are managed by a third party
-Expiration-frequency of use, sensitivity of information
-Renewal
-Revocation
-Recovery
-Suspension
-Destruction

Trust Models

-Trust may be defined as confidence in or reliance on another person or entity.
-Trust model
  -Refers to the type of trusting relationship that can exist between individuals or entities.
-Direct trust
  -A relationship exists between two individuals because one person knows the other person.
-Third party trust
  -Refers to a situation in which two individuals trust each other because each trusts a third party.

-Direct trust is not feasible when dealing with multiple users who each have digital certificates.
-Three PKI trust models that use a CA
  -Hierarchical trust model
    -I trust the CA, so I trust the certificates the CA issues.
    -Only works on small scale.
  -Distributed trust model
    -CA issues certificates for other CA's, creating a trust chain.
  -Bridge trust model
    -Creates a peer-to-peer relationship between root CA's.
    -A CA exists that does not sign certificates, they just serve as facilitator to interconnect other CA's. Fed/state govt.

Managing Cryptographic Controls

-Don't lose your keys.
-Know who you are communicating with (verify keys).
-It may be illegal to use a specific encryption technique when communicating to some nations.
-Every cryptosystem has weaknesses
-When placing trust into a certificate authority, ask "Who watches the watchers?"
-Security protocols and the cryptosystems they use are installed and configured by humans, and thus they are only as good as their installers.
-As with all other information security program components, make sure that your organization's use of cryptography is based on well-constructed policy and supported with sound management procedures.

---Forensics---

Forensics

-Application of scientific knowledge to legal problems.

What is "Digital Forensics"?

-"Scientific knowledge and methods applied to the identification, collection, preservation, examination, and analysis of information stored or transmitted in binary form in a manner acceptable for application in legal matters."
-Other terms: computer forensics, network forensics, cyber forensics, electronic data discovery, forensic computing.
-Computers have appeared in litigation since the late 1970s.
-The term computer forensics was coined in 1991 at 1st training session of the International Association of Computer Specialists.

Digital Forensics vs. Media Analysis

-Digital forensics involves investigation of crimes against or using digital media, computer technology, or related components.
-Media or root cause analysis: if an organization suspects an attack was successful, they may conduct analysis to determine the path and

methodology used to gain unauthorized access, as well as to determine how pervasive and successful the attack was.

Definition of Crime

-A crime is an offensive act against society that violates a law and is punishable by the government.

-Two important principles in this definition:

-The act must violate at least one criminal law.

-It is the government (not the victim of the crime) that punishes the violator.

Categories of Cybercrimes

-Computer is the crime target: computer as victim

-DDOS, Capturing passwords or other sensitive data

-Computer is the crime instrument: used as a tool to help carry out attack

-Attacking financial systems to steal funds

-Industrial spying

-Computer is incidental to traditional crimes-involved in some secondary manner

Target or instrument?

-Any attack could fall into both categories?

-Instrument-computer is only used as a tool to carry out a traditional crime (theft, destruction, protests). These crimes would take place anyway.

-Target--crime could not take place without a computer

-Why does it matter?

Categories of U.S. Laws

-Criminal law. This includes laws of public order against crimes such as assault, arson, theft, burglary, deception, obstruction of justice, bribery, and perjury. Guilt vs. innocence.

-Law enforcement agencies are responsible for enforcing criminal laws.

-Civil law. This includes contract law, tort law, property law, employment law, and corporate law. Civil law is the branch of laws that generally involve two parties that have a grievance that needs to be settled. Is person liable for act?

-Law enforcement agencies generally have little to do with civil laws.

Computer Fraud and Abuse Act of 1984

-CFAA of 1984

-1st law to define "computer trespass." Illegal to knowingly access a computer without authorization or in excess of authorization.

-Illegal to knowingly transmit program, info, or code and intentionally cause damage to a computer.

-1st real anti-hacking law.

-Amended in 1986 to include stiffer criminal penalties.

-Revised in 1994 to include a civil law component.

-Also amended in 1996, 2001, and 2008.

-Protects government computers and those used in interstate commerce.

-Can be punished by actually committing act or conspiring to do so.

CFAA

-1st person prosecuted was Robert Tappan Morris JR. 1988, crashed 10% of the internet.

-Damage was between 10 and 100 million.

-Sentence was 3 yrs probation, 400 hrs community service, $10,500 fine.

CAN-SPAM

-Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003.

-Act has a very poor record.

-AKA you can spam act.

-IN 2003 SPAM was mostly to get you to buy a product. By 2008, most SPAM is trying to lead you to a website to infect your computer with malware.

-The amount of SPAM has increased 10-fold.

CAN-SPAM

-Government can prosecute spammers.

-ISPs can sue.

-In 2004, most SPAM originated in US (56.7%), by 2008-14.9%.

-Has not increased percent in compliance with unsubscribe option.

-Compliance with accurate subject heading has dropped.

-No increase in inclusion of valid postal address.

Digital Millennium Copyright Act

-Illegal to develop, produce, and trade any device or mechanism designed

to circumvent technological controls used in copy protection.
-Cannot circumvent control even if there is no actual copyright infringement.

Evidence Basics

-Evidence is proof of a fact about what did or did not happen.
-Three types of evidence can be used to persuade someone:
    -Testimony of a witness (direct)-5 senses
    -Physical evidence (circumstantial)
    -Electronic evidence (circumstantial
-Both cybercrimes and traditional crimes can leave cyber-trails of evidence.

Types of Evidence

-Direct: oral testimony that proves a specific fact. Knowledge of the facts is obtained through the 5 senses. Can prove a fact without back-up information to refer to.
-Circumstantial evidence—shows circumstances that logically lead to a conclusion of fact. Told friend would take down eBay.
-Hearsay evidence—secondhand evidence.
    -Computer-generated evidence is typically hearsay evidence.
    -Exceptions exist that allow it to be accepted in court.
-Material evidence—evidence relevant and significant to lawsuit.
-Immaterial evidence—evidence that is not relevant or significant.
-Artifact evidence—change in evidence that causes investigator to think the evidence relates to the crime.
-Inculpatory evidence—evidence that supports a given theory.
-Exculpatory evidence—evidence that contradicts a given theory.
-Admissible evidence—evidence allowed to be presented at trial.
-Inadmissible evidence—evidence that cannot be presented at trial.
-Tainted evidence—evidence obtained from illegal search or seizure.

Steps in the Forensic Examination

-Verify legal authority
    -The Fourth Amendment protects against unreasonable searches and seizures.
-Collect preliminary data.
-Identify relevant items.
-Determine the environment for the investigation.

-Secure and transport evidence.
-Acquire the evidence from the suspect system.
    -Collect as much as you can as soon as you can
    -Forensically clean drive.

-Examiner machine should not be connected to any network.
-Verify copy.
-Analyze copy.

Types of electronic devices relevant to a crime scene:

-Computer systems
-Hard drives
-Thumb drives
-Memory cards
-Smart cards, dongles, biometric scanners
-Answering machines
-Digital cameras
-MP3 players
-PDAs
-Printers
-Removable storage devices-tapes, CDs, DVDs, floppies
-Telephones
-Scanners
-Copiers
-Credit card skimmers
-Fax machines

Acquire the Evidence

-Basic guidelines:
-Wipe all media you plan to use for analysis
-Activate the write protection
-Why?
-Perform a hash of the original drive and of the forensic copy
-Do a physical acquisition to capture space not accessible by the operating system (make bit level copy).

-Make 3-4 copies
-1 to return
-1 marked, sealed, logged with the original
-1 for authentication
-1 for analysis
-Store everything securely
-Very important to maintain chain of custody
-Process is similar for hard drives and removable media

Examining the Evidence

-There are no specific rules for examining evidence due to the variety of cases, but there are general guidelines that should be

considered.

-Exclusion of known files using hash analysis
    -Can exclude 90% of files based on signatures.
-File header and extension
-Obvious files of interest
-Extraction of password-protected files
-Extraction of compressed and deleted files
-Extraction of unallocated space files of interest
-Extraction of file slack space files of interest

Unallocated Space and File Slack

-Unallocated space: space that is not currently used to store an active file but may have stored a file previously.
    -Deleted files are not really deleted. A pointer that is used by the operating system to track down the file is deleted
    -File slack: space that remains if a file does not take up an entire sector. Sophisticated hackers may hide malicious code in slack space. May contain data dumped randomly from memory.
-Unallocated space and slack space can contain important information for an investigator.

The Art of Forensics: Analyzing the Data

-File analysis investigations include:
    -File content
    -Metadata
    -Application files
    -May have file w/out application or application w/out file
    -Directory/folder structure--may reflect intent
    -User configurations--what have they customized

Effective Data Searches

-Carefully prepare and plan the search.
-Confirm or define the objective of the investigation.
-Identify relevant time periods and the scope of the data to be searched.
-Identify the relevant types of data.
-Identify search terms for data filtering to help locate relevant data and filter out what is irrelevant.
-Metadata can be invaluable to the filtering process.
-Find out usernames and passwords for network and e-mail accounts.
-Check for other computers or devices that might contain relevant evidence.

Why Is It Important to Effectively Search Data?

-1KB is about ½ page.

-1MB is about 500 pages.
-1GB is about 160ft stack of paper.
-In Kevin Mitnick's trial, he had 9GB of data.
-This is equivalent to a stack of paper 1440 feet tall.
-A little taller than the World Trade Center towers.
-In these terms, how big of a stack of paper would there be to represent a Terabyte of data? 1TB =1024 GB.

Reporting on the Investigation

-Last step is to finish documenting the investigation and prepare a report on the investigation.
-Documentation should include information such as:
-Notes taken during initial contact with the lead investigator.
-Any forms used to start the investigation.
-A copy of the search warrant.
-Documentation of the scene where the computer was located.
-Procedures used to acquire, extract, and analyze the evidence.

Sources:

----Security+ Guide to Network Security Fundamentals (Third Edition) by Mark Ciampa, ISBN: 1-4283-4066-1

----Management of Information Security (3rd Edition ISBN: 1-4354-884-9) by Michael Whitman and Herbert Mattord or 2nd edition: ISBN: 1-4239-0130-4

----https://secreatine.wordpress.com/2007/11/01/information-assurance-vs-information-security/