CS2107 Additional Notes

Jothinandan Pillay

Access Control Matrix - The access control matrix can be represented in two different ways: Access Control List or capabilities.

Access Control Model - selective restriction of access to a place or other resource. The access control system/model gives a way to specify and enforce such restriction on the subject, objects and actions.

Access Control List - An ACL stores the access rights to an object as a list.

Action -> executing a program

Advanced Encryption Standard (AES) -> new standard for block cipher. Currently no known attacked on AES. Consists of ECB (Electronic Code Book – No IV) and CBC(Cipher Block Chaining – with IV) as mode of operations.

Alter -> writing, deleting, changing properties of a file.

Anomaly Detection - The IDS attempt to detect abnormal pattern. For e.g. a sudden surge of packets with certain port number.

Attack signature Detection - The attack has specific, well-defined signature. For e.g. using certain port number, certain source ip address.

Authenticity -> owner/origin of message is who he/she claims to be.

Authenticated Encryption -> Supposedly provides confidentiality, authentication and integrity,

Authenticated Key Exchange -> Given protocol that, given the public/private (or symmetric) key, the protocol establishes a symmetric key in both authentic entities. Authenticity protected by mac using t as key. Confidentiality protected by encryption using k as key. So only both sender and receiver should know t and k.

Authentication System -> weak system susceptible to "replay attack": information sniffed from the communicated channel can be used to impersonate the user. Strong system can't be used to impersonate the user and uses challenge-response (unilateral authentication).

Authorization -> function of specifying access rights/privileges to resources, which is related to information **security** and computer **security** in general and to access control in particular.

Automated Checking -> Some automations and tools are possible. For example, taint analysis:

Availability -> information is available to be viewed and not hidden/inaccessible from view upon demand by an authorized entity.

Behavior-based IDS - Can be viewed as a type of anomaly detection that focuses on human behavior. For e.g. The system might keep the profile of each user. It then tries to detect any user who deviates from the profile (e.g. start to download large files).

Bell-LaPadula Model -> For data confidentiality. Restrictions imposed by the Bell-Lapadula Model: The following restrictions are imposed by the model: • no read up: A subject has only read access to objects whose security level is below the subject's current clearance level. This prevents a subject from getting access to information available in security levels higher than its current clearance level. • no write down: A subject has append access to objects whose security level is higher than its current clearance level. This prevents a subject from passing information to levels lower than its current level. (e.g. a clerk working in the highly classified department should not gossip with other staff, in order to prevent leakage).

Blackbox Testing -> tester does not have access to source code.

Biba Model -> For process integrity. Restrictions imposed by the Biba Model: The following restrictions are imposed by the model: • no write up: A subject has only write access to objects whose security level is below the subject's current clearance level. This prevents a subject from compromising the integrity of objects with security levels higher than its current clearance level. • no read down: A subject has only read access to objects whose security level is higher than its current clearance level. This prevents a subject from reading forged information from levels lower than its current level.

Biometric System (Fingerprinting) -> uses unique physical characteristics of a person for authentication. During ***enrollment***, a ***template*** of an user's biometric data is captured and stored (same as bootstrapping in password system). During ***verification***, biometric data of the person-in-question is captured and compared with the template using a *matching algorithm.* The algorithm decides whether to accept or reject. Biometric can be used for *identification* (identify the person from a database of many persons), or *verification* (verify whether the person is the claimed person). Here, we focus on verification.

Birthday Attack -> **birthday attack** is a type of cryptographic attack that exploits the mathematics behind the birthday problem in probability theory. This attack can be used to abuse communication between two or more parties. The attack depends on the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations (pigeonholes).

Blacklist - Accept all packets except those specified in the black-list. (e.g. allow https except ip-address in the black list)

Botnet -> Refer to Lecture Notes Chapter 5 last few slides.

Bound Checks -> Some programming languages (e.g. Java, Pascal) perform bound checking during runtime (i.e. while the program is executing). During runtime, when an array is instantiated, its upper and lower bounds will be stored in some memory, and whenever a reference to an array location is made, the index (subscript) is checked against the upper and lower bound.

Bring Your Own Device -> refers to the policy of permitting employees to bring personally owned devices to their workplace, and to use those devices to access privileged company information and applications.

Cache -> When using a shared workstation (for e.g. a browser in airport), information keyed in could be cached. The next user may able to see the cache. (close the browser when using shared workstation).

Canaries -> Canaries are secrets inserted at carefully selected memory locations during runtime. Checks are carried out during runtime to make sure that the values are not being modified. If so, halts. • Canaries can help to detect overflow, especially stack overflow. This is because in a typical buffer overflow, consecutive memory locations have to be over-ran. If the attacker wants to write to a particular memory location via buffer overflow, the canaries would be modified.

Capabilities - A subject is given a list of capabilities, where each capability is the access rights to an object. “a capability is an unforgeable token that gives the possessor certain rights to an object”

CERT - A Computer Emergency Response Team (**CERT**) is an expert group that handles computer security incidents. Alternative names for such groups include Computer Emergency Readiness Team and Computer Security Incident Response Team (CSIRT).

Certificate -> A ***certificate*** is a digital document that contains ***at least*** the following 4 main items 1) The identity of an owner, for e.g. “alice@yahoo.com” 2) The public key of the owner. 3) The time window that this certificate is valid. 4) The signature of the CA. It also has additional information like the purpose of the public key.

Certificate Authority -> The CA keeps a directory of public keys. The CA also has its own public/private key. We assume that the CA’s public key has been securely distributed to all entities involved. Besides issuing the certificate, the CA is also responsible to verify if the check that the applicant indeed owns the above domain name.

Certificate Chain -> Look at Lecture Notes Chapter 4.

Certificate Revocation -> Non-expired certificates can be revoked for different reasons: Private key was compromise, Issuing CA was compromise, Entity left an organization, Business entity closed. Read more in Lecture notes Chapter 4 Slide 29-30.

Chosen-plaintext attack (CPA) -> a model for cryptanalysis which assumes that the attacker can choose random plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the **attack** is to gain some further information which reduces the security of the encryption scheme.

Ciphertext only attack -> The attackers only have access to ciphertexts. But attackers can still find plaintext if it is an English sentence using exhaustive search (possible but infeasible).

Code Inspection -> Consists of Manual Checking and Automated Checking.

Compartmentalization -> limiting of access to information to persons or other entities on a need-to-know basis to perform certain tasks.

Confidentiality -> content of message not leaked.

Controlled Invocation -> Lecture 6 Slide 39, 41

Covert channel -> type of attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy.

Cryptanalysis -> study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

Cryptographically secure pseudorandom sequence -> security requirement: difficult to distinguish the sequence from a truly random sequence –this is quite a strong requirement. It implies that it is difficult to get the short secret key from the sequence. It also implies that it is difficult to get part of the sequence after seen another part of the sequence.

Cryptography -> referred almost exclusively to encryption, which is the process of converting ordinary information (called plaintext) into unintelligible form (called ciphertext). Decryption is the reverse, in other words, moving from the unintelligible ciphertext back to plaintext. Encryption is just one of the primitives in cryptography. Others include cryptographic hash, digital signature).

Cryptography backdoor -> a method secretly inserted in the cryptosystem by the designer/implementer. It allows the designer/implementer to access the plaintext and/or secret key without having the correct user credentials.

Cryptology -> Cryptography + Cryptanalysis.

CVE -> The **Common Vulnerabilities and Exposures** (**CVE**) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

Data Encryption Standard (DES) -> Exhaustive search. See Lecture 1 Notes.

Decryption order -> a court order that order suspects to decrypt their encrypted data or give up their keys.

Demilitarized zone (DMZ) -> A sub-network that exposes the organization's external service to the (untrusted) Internet.

Denial of Service -> Attack on availability. The prevention of authorized access to resources or the delaying of time-critical operations. Many successful DOS attacks simply flood the victims with overwhelming requests/data. If DDOS (Distributed DOS), attack carried out by large number of attackers. Reflection attack is a type of DOS in which the attackers send requests to intermediate nodes, which in turn send overwhelming traffic to the victim. Indirect, and thus more difficult to trace. Very often, the reflected traffic could be amplified (a single request could trigger multiple responses from the intermediate nodes). Hence, these are also known as *Amplification attacks*.

Dictionary Attack -> The attacker can restrict the search space to a large collection of probable passwords. The collection can include words from English dictionary, known compromised passwords, other language dictionaries, etc.

Discretionary access control - The owner of the object decides the rights.

DNS Spoofing/Cache Poisoning -> a form of computer security hacking in which corrupt Domain Name System data is introduced into the **DNS** resolver's **cache**, causing the name server to return an incorrect result record, e.g. an IP address

Elevated Process -> the interfaces where a user can access the "sensitive" information. - They are the predefined "bridges" for the user to access the data. - The "bridge" can only be built by the root. These bridges solve the problem. However, it is important that these "bridges" are correctly implemented and do not leak more than required. As indicated previously, if the bridge is not built securely, there could be privilege escalation attack.

Elevation of Priviledge -> **Privilege** refers to what a user is permitted to do and so **Elevation of Privilege** is a user receives **privileges** they are not entitled to. EOP allows different access levels which comprises read-only vs. read-write. Where the lower **privileged** user can gain the administrative access known as Vertical **privilege** escalation.

Encryption Scheme -> also known as cipher. Consists of 2 algorithms (encryption, which is plain to ciphertext and decryption, which is cipher to plaintext). An encryption must meet the correctness property:
Correctness: For any plaintext x and key k, Dk (Ek (x)) = x
It also has to be secure. Formulation of security is difficult.
Security: From the ciphertexts, it is "difficult" to derive useful information of the key k, and the plaintext x. The ciphertexts should resemble sequences of random bytes.

End-to-end encryption -> Method of secure communication that prevents third-parties from accessing data while it's transferred from one **end** system or device to another. In E2EE, the data is **encrypted** on the sender's system or device and only the recipient is able 2 decrypt it.

Execution Integrity -> general term for computer security techniques which prevent a wide variety of malware attacks from redirecting the flow of execution of a program

Exhaustive Search -> exhaustively search all the keys (brute force) but may take very long.

Exploits -> a software tool designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware.

Fallback authentication -> alternate ways of authentication if users forget main way. For eg if forget password can use security questions as fall back authentication aka self-services pw reset. Enhances usability, reduces cost but weakens security.

False Match Rate and False Non-Match Rate -> See Lecture Notes Chapter 2. Also includes Equal Error Rate (EER), False to enrol rate (FER) and Failure to Capture rate (FTC).

File system permission -> The file permission are grouped into 3 triples, that define the read, write, execute access for owner, group, other (also called the "world").

FireWall -> Firewall are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures. A Firewall controls what traffic is allowed to enter the network (ingress filtering), or leave the network (egress filtering).

Frequency analysis -> the use of certain letters in certain languages occur more frequently than others. So, if attackers knows the language of the plaintext, he can make use of knowledge of frequency of letters in that language to decipher the plaintext.

Fuzzing -> Fuzzing is a technique that sends malformed inputs to discover vulnerability. There are techniques that are more effective than sending in random input. (detail not required). Fuzzing can be automated or semi-automated.

Graphical password -> an authentication system that works by having the user select from images, in a specific order, presented in a **graphical** user interface (**GUI**)

Greybox Testing -> A combination of white and black box testing

Hardware Random Number Generator -> In computing, a hardware random number generator (HRNG) or true random number generator (TRNG) is a device that generates random numbers from a physical process, rather than by means of an algorithm. The main application for electronic hardware random number generators is in cryptography, where they are used to generate random cryptographic keys to transmit data securely. They are widely used in Internet encryption protocols such as Secure Sockets Layer (SSL).

Hash -> A (cryptographic) hash is a function that takes an arbitrary large message as input, and outputs a fixed size (say 160 bits) ***digest***. **Security requirement**: It is difficult to find two different messages m1, m2 that "hash" to the same digest. That is, h(m1) = h(m2). This is known as ***collision-resistant***. A hash that is collision-resistant is also ***one-way***, that is, given a digest d, it is difficult to find a message m s.t. h (m)=d.

Homomorphic Property -> Nice property of RSA. It is useful (ie blind signature) but also a vulnerability. **Homomorphic** encryption is a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext.

Insider Attack -> The malicious system administrator steals the password file. The system administrator's account is compromised (e.g. password stolen via phishing), leading to lost of password file.

Insider Threat -> An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.

Intrusion Detection System(IDS) -> An IDS system consists of a set of "sensors" gathering data. Sensors could be in the host, or network router. The data are analyzed for intrusion. Two type of IDS

Intermediate Control - Giving access control to groups.

Integrity -> Content of message not modified or changed.

IPSec -> mechanism whose goal is to protect the IP layer.

Iris Recognition -> an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of the irides of an individual's eyes, whose complex random patterns are unique and can be seen from some distance.

Kerckhoff's principle -> a system should be secure even if everything about the system, except the secret key, is public knowledge

Key escrow -> an arrangement in which the keys needed to decrypt encrypted data are held in escrow (in trust) so that, under certain circumstances, an authorized third party may gain access to those keys.

Key exchange/agreement -> the process of establishing a secret between sender and receiver. It is secure against Eve but not against Mallory. The established key can be used to protect (encrypt, mac) subsequent communication between sender and receiver. To protect against Mallory need authenticated key exchange.

Key logger -> captures/records the keystrokes, and sends the information back to the attacker via a "covert channel". Comes in both software (computer viruses) and hardware.

Key size/length -> No. bits required to represent the key. (94 bits for monoalphabetic substitution cipher).

Key space -> set of all possible keys.

Key space size -> total number of possible keys. 27! For monoalphabetic substitution cipher.

Known Plaintext Attack -> a scenario where the attackers have access to pairs of ciphertexts and the corresponding plaintexts and therefore doesn't need to do exhaustive search. If the adversary can successfully derive the key, we say that the scheme is "***not secure under known plaintext attack***" or "***broken under known plaintext attack***". Hence, substitution cipher is not secure under known plaintext attack.

Liveness Detection -> To verify that the entity scanned by the scanner is indeed "live". Used in biometric system scanners.

Login Spoofing -> attacker displays a spoofed login page. Can be prevented by having a secure attention key/sequence. When pressed, the system starts the trusted login processing, (Ctrl, Alt, Del for Windows).

Malware -> or malicious software, is any program or file that is harmful to a computer user.

Mandatory access control - A system-wide policy decides rights of the object.

Man-in-the-middle attack (**MITM**) -> is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

Memory Randomization -> It is to the attacker's advantage when the data and codes are always stored in the same locations. Address space layout randomization (ASLR) (details omitted) can help to decrease the attackers chance of success.

Message Authentication Code (MAC aka keyed hash) -> A keyed-hash is a function that takes an arbitrary large message and a secret key as input, and outputs a fixed size (say 160 bits) ***mac.***
Security requirement: without knowing the key, it is difficult to forge the mac.

Mode of Operation -> In cryptography, an algorithm used in conjunction with a block cipher that makes up the complete encryption algorithm. For example, DES-ECB uses the Data Encryption Standard (DES) block cipher and the electronic code book (ECB) mode of operation

N-Factor Authentication -> Based on something you know (Pw, pin), something you have (token, smart card, mobile phone, ATM card), who you are (biometric).

Network Packet Sniffer -> This allows the sniffer to seize everything that is flowing in the **network**, which can lead to the unauthorized access of sensitive data.

Nonce -> a **nonce** is an arbitrary number that can be used just once in a cryptographic communication.

National Security Agency (NSA) -> a national-level intelligence agency of the US Dept of Defense, which is responsible for global monitoring, collection, and processing of information and data for foreign intelligence and counterintelligence purposes, specializing in a discipline known as signals intelligence (SIGINT).

National Institute of Standards and Technology (NIST) -> a measurement standards laboratory, and a nonregulatory agency of the US Dept of Commerce, whose mission is to promote innovation and industrial competitiveness.

Non-Repudiation -> refers to a situation where a statement's author cannot successfully dispute its authorship or the validity of an associated contract. The term is often seen in a legal setting when the authenticity of a signature is being challenged. In such an instance, the authenticity is being "repudiated". Can achieve using signature but not mac.

Observe -> Reading a file

One-Time Pad -> refer to Lecture Notes Chapter 1. Shown to be “unbreakable” and length of key must be same as plaintext. Basically encrypt PT with key, then for decrypt use CT and same key. Leaks no info about plaintext and keys are generated for each new session.

Ownership Rights -> the rights to a particular information or file. Decided by either the owner of the object or by a system-wide policy.

Packet-Filtering -> Packet filtering inspects every packet, typically only on the packet’s header information. (if the payload is inspected, we call it deep packet inspection (DPI)). Action taken after inspection could be - Allow the packet to pass - Just drop the packet - Reject the packet (i.e. drop and inform the sender) - Log info - Notify system admin - Modify the packet (for more advanced device).

Parametrized Queries (SQL) -> mechanisms introduced in some servers to protect against SQL injection. Queries sent to SQL are explicitly divided by 2 types. The query and the parameters. The SQL parser will know that parameters are data and not “script”. The SQL parser is designed in such a way that it would never execute any script in the parameters. this will prevent most injection attacks..

Password File -> The file is made world-readable because some information in /etc/passwd is needed by non-root program. Note that in earlier version of Unix, the location of “*” was the hashed password H(pw), where H() is some cryptographic hash, and pw the password of the user. Hence, all users can have access to this info (under earlier version of Unix). • The availability of the hashed password allows attackers to carry out offline guessing. Since passwords are typically short, exhaustive search are able to get many passwords. To prevent that, it is now replaced as “*”, and the actual password is stored somewhere else and not world-readable

Password Policy -> Rules set by the organization to ensure that users use strong passwords, and to minimize loss of passwords.

Password Strength and Entropy -> See Lecture Notes Chapter 2.

Password System -> a type of authentication s`ystem. **Bootstrapping** -> Stage 1: Server and a user established a common password. The server keeps a file recording the *identity (aka userid, username)* and the corresponding *password*. **Stage 2: Authentication**. The server authenticates an entity. If the entity gives the correct password corresponds to the claimed identity, the entity is deemed as authentic. Attacks include attacking the bootstrapping, searching for correct pw (guess, dictionary, exhaustive and stealing the pw (eavesdrop (sniff the network, key-logger), phishing, spoofing login screen, cache, insider attack).

Permutation Cipher -> Also known as transposition cipher. The encryption first groups the plaintext into blocks of ***t*** characters, and then applied a secret “permutation” to each block by shuffling the characters. The key is the secret “permutation”, which is an 1-1 onto function *e* from{1,2,..,t} to {1,2,...,t}. The size ***t*** could be part of the key, that is, ***t*** is also kept secret. We can write the permutation ***p*** as a sequence ***p***= (p1 , p2, p3, ... pt) which shift the character at position i (position within the block) to the position pi. Fails under known plaintext attack and easily broken under ciphertext only attack if the plaintext is English.

Pharming -> a cyber attack intended to redirect a website's traffic to another, fake site. **Pharming** can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software.

Phishing -> Same as login spoofing, here, the user is tricked to voluntarily sends the password to the attacker. Phishing attacks ask for password under some false pretense. It is known as a social engineering attack. Usually done through emails but can also be done over phone calls.

Port Knocking -> Use the port as authentication. Only listen to a certain port number. But this is weak because anyone who observes the traffic can find out the port number.

Port Scanner -> A **port scanner** is an application designed to probe a server or host for open ports. Such an application may be used by administrators to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities. Eg, wireshark

Port Scanning -> The process of determining which ports are open in a network

Principals -> the human users. represented by user-identities (UIDs) and group-identities (GIDs).

Principle of Least Privilege -> also known as the principle of minimal privilege or the principle of least authority) requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose"

Privilege - access right. Privilege can also be viewed as a intermediate control.

Privilege Escalation - the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

Protection Rings -> Here, each object (data) and subject (process) is assigned a number. Whether a subject can access an object can be determined by their respective assigned number. Object with smaller number are more important. If a process is assigned a number i, we say that the process runs in ring i. Very often, we call processes with lower ring number as having "higher privilege". A subject cannot access (both read/write) an object with smaller ring number. It can only do so if its privilege is "escalated". (we can also viewed this as a special case of role-based in the sense that the ring number is the "role"). Unix has only 2 rings, superuser and user.

Protocol -> In computer networking, a protocol is a set of rules for exchanging information between multiple entities. A protocol is often described as steps of actions to be carried by the entities, and the data to be transmitted.

Proxy-Re-Encryption -> Proxy re-encryption schemes are cryptosystems which allow third parties to alter a ciphertext which has been encrypted for one party, so that it may be decrypted by another.

Public Announcement -> Type of key distribution. The owner broadcasts her public key. For example, by sending it to friends via email, or publishing it in web-site. Limitations: not standardized, and thus there isn't a systematic way to find/verify the public key when needed.

Public Key Infrastructure -> standardized system that distributes public key. Centred around 2 components: Certificate and Certificate Authority (CA). Limitations/Attacks include implementation bugs, abuse by CA and social engineering.

Public Key Scheme -> Use different keys for encryption and decryption. Given the public key and the ciphertext, but not the private key, it is difficult to determine the plaintext. Without a knowledge of the private key, the ciphertext resembles a sequence of random values. The requirements imply that it must be difficult to get the private key from the public key. Total number of public and private keys is n each. To protect digest, a digital signature is used.

Publicly Available Directory -> If Bob wants to find the public key associated with the name alice@yahoo.com.sg he can search the public directory by querying a server. Anyone can post their public keys in the server. For e.g. https://pgp.mit.edu/. It is not easy to have a "secure" public directory.

Quantum random number generator -> a device which provide a stream of random bits generated using a methods based on the laws of quantum physics. Currently there it is possible to obtain random data generated using methods based on quantum physics using online services or by utilizing specialized hardware.

Race Condition -> Occurs when multiple processes access a piece of shared data in such a way that the final outcome depend of the sequence of accesses.

Retinal Scanning*:* The human retina is a thin tissue composed of neuralcells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique.

Role-based access control -> another form of intermediate control. The grouping is determined by the "role" of the subject. A role associates with a collection of procedures. In order to carry out these procedures, access rights to certain objects are required. If a subject is assigned a particular role, the access rights to the objects can be determined based on the least privilege principle.

Salt -> a salt is random data that is used as an **additional** input to a one-way function that "hashes" data, a password or passphrase. Salts are used to safeguard passwords in storage.

Same-Origin Policy -> A "script" which runs in the browser could access cookies. Which scripts can access the cookie? Due to security concern, browser employs this access control policy: The script in a web page A (identified by URL) can access cookies stored by another web page B (identified by URL), only if both A and B have the same origin. Origin is defined as the combination of protocol, hostname, and port number.

Scripts -> programs that automates the execution of tasks that could alternatively be executed line-by-line by a human operator. Scripting languages are typically "interpreted" instead of being compiled. Well-known examples include PHP, Perl, Javascript, SQL.

Scrypt -> In cryptography, scrypt is a password-based key derivation function created by Colin Percival, originally for the Tarsnap online backup service. The algorithm was specifically designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory.

Searchpath -> When a user types in the command to execute a program, say "su" without specifying the full path, which program would be executed? /usr/bin/su or ./su ? The program to be executed is searched through the directories specified in the searchpath. When a program with the name is found in a directory, the search stops and the program will be executed. Now, it is possible that an attacker somehow stored a malicious program in the directory that appears in the beginning of the search path, and the malicious program has a common name, say “su”. Now, when an user executes “su”, the malicious program will be invoked instead. To prevent such attack, specify the full path.

Security Boundary - the parts of the system that can malfunction without compromising the protection mechanism lie outside this perimeter. The parts of the system that can be used to disable the protection mechanism lie within this perimeter. An important design consideration of the security mechanism is on how to prevent attacker from getting access outside the boundary

Security Information and Event Management (SIEM) - pronounced as “SIM”. Approaches and tools for SOC.

Security Operations Center (SOC) - a centralized unit in an organization that monitors the IT systems and deals with security issues.

Security Questions -> Memorable: If users can't remember their answers to their security questions, you have achieved nothing. Consistent: The user's answers should not change over time. For instance, asking "What is the name of your significant other?" may have a different answer 5 years from now. Nearly universal: The security questions should apply to as wide an audience as possible. Safe: The answers to security questions should not be something that is easily guessed, or research (e.g., something that is matter of public record).

Security Reduction -> A **security reduction** is a particular type of mathematical proof that some **cryptographic** primitive or protocol is **secure. Lecture Notes Chapter 4.**

Security Testing -> attempts to discover intentional attack, and hence would test for inputs that are rarely occurred under normal circumstances. (for e.g. very long names, or names that contain numeric values.)

Security through Obscurity -> to hide the design of the system in order to achieve security.

Self-signed certificate -> identity certificate that is signed by the same entity whose identity it certifies

Shoulder surfing -> Look over the shoulder attack.

Side-channel attack -> any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself.

SIEM -> In the field of computer security, security information and event management software products and services combine security information management and security event management. They provide real-time analysis of security alerts generated by applications and network hardware.

SingCERT - The Singapore Computer Emergency Response Team (**SingCERT**) responds to cyber security incident for its Singapore constituent.

Single sign-on (SSO) -> a session and user authentication service that permits a user to use one set of login credentials (e.g., name and password) to access multiple applications. The service authenticates the end user for all the applications the user has been given rights to and eliminates further prompts when the user switches applications during the same session.

Skimmer (device) -> the slang term for a device used to read and record the magnetic code(s) from a credit card for later fraudulent use.

Smishing -> **SMiShing** is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device.

Sniff -> to illegally listen in to another conversation or communication channel.

Social Engineering -> psychological manipulation of people into performing actions or divulging confidential information

Soft Token -> Lecture Notes Chapter 2 last few slides.

Spam -> spam is unsolicited junk email sent indiscriminately in bulk, often for commercial purposes. Much of it is sent by botnets, networks of virus-infected computers, complicating the process of tracking down the spammers. According to various estimates, about 80% of all email in the world may be spam.

Spamhaus - Computer **Definition**. ... Based in Geneva and London, **Spamhaus** maintains several "block lists;" for example, the **Spamhaus** Block List (SBL) contains the IP addresses of known spammers, and the Exploits Block List (XBL) is a list of compromised computers that send spam without the owner's knowledge.

Spear Phishing -> Phishing can be targeted to a particular small group of users (for example, NUS staff in the above example). Such attack is generally known as ***spear phishing***, which is an example of ***targeted attacks.***

Spoof -> to pretend to be someone else.

SSL/TLS -> sits on top the transport layer

Stack Smash -> A special case of buffer overflow that targets the stack. Buffer overflow on stack is called stack overflow.

Stream Cipher -> Suppose the plaintext is 220 bits, but the secret key is only 256 bits. Steam cipher generates a 220-bit sequence from the key, and takes the generated sequence as the secret key in one-time-pad. The generator has to be carefully designed, so that it gives ***cryptographically secure pseudorandom sequence***.

Steam Cipher with IV -> The IV can be randomly chosen, or from a counter. A long pseudorandom sequence is generated from the secret key together with the IV. The final ciphertext contains the IV, followed by the output of the one-time-pad encryption. (In some documents, the term “ciphertext” does not include the IV. In any case, the IV **must** appear in clear, and every entity can see it). For decryption, the IV is extracted from the ciphertext. From the IV and the key, the same pseudorandom sequence can be generated and thus obtain the plaintext. Read more in Chapter 1 and how C1 XOR C2 = P1 XOR P2.

Subjects -> The entities in the system that operate on behalf of the principals. These are actually processes and are represented by process IDs (PID).

Substitution Cipher -> Plaintext converted into ciphertext using a substitution table. So like maybe a is mapped to c, c is mapped to g, h mapped to x etc. Sub cipher is not secure under known plaintext attack, not secure under ciphertext only attack if plaintexts are made up of a particular language due to the use of frequency analysis.

SUID -> Set UserID (Refer to slides Lecture 6 Slide 52-54).

Superuser -> A special user is the superuser, with UID 0 and usually with the username root. All security checks are turned off for root.

Symmetric Key Encryption -> this scheme uses the same key for encryption and decryption. Total number of keys required is n(n-1)/2. Digest protected using a MAC.

Taint Analysis -> Variables that contain input from the (potential malicious) users are labeled as source. Critical functions are labeled as sink. Taint analysis checks whether the sink's arguments could potentially be affected (i.e. tainted) by the source. If so, special check(for e.g. manual inspection) would be carried out. The taint analysis can be static (i.e. checking the code without "tracing it"), or dynamic (i.e. run the code with some input). E.g. Sources: user input Sink: opening of system files, function that evaluates a SQL command, etc

TOCTOU -> Time of check - time of use - under Race Condition.

Transport Layer Security (TLS) -> protocol to secure communication using cryptographic means. TLS/SSL adopts similar framework and SSL is predecessor of TLS. HTTPS is built on top of TLS.

Type Safety -> Some programming languages carry out "type" checking to ensure that the arguments an operation get during execution are always correct. The checking could be done during runtime (i.e. dynamic type check), or when the program is being compiled (i.e. static type check).

Typosquatting -> is a form of cybersquatting, and possibly brandjacking which relies on mistakes such as typos made by Internet users when inputting a website address into a web browser. Should a user accidentally enter an incorrect website address, they may be led to any URL (including an alternative website owned by a cybersquatter).[1]

The typosquatter's URL will usually be one of five kinds, all similar to the victim site address (e.g. example.com):

- A common misspelling, or foreign language spelling, of the intended site: exemple.com
- A misspelling based on typos: examlpe.com
- A differently phrased domain name: examples.com
- A different top-level domain: example.org
- An abuse of the Country Code Top-Level Domain (ccTLD): example.cm by using .cm, example.co by using .co, or example.om by using .om. A person leaving out a letter in .com in error could arrive at the fake URL's website.

Once in the typosquatter's site, the user may also be tricked into thinking that they are in fact in the real site, through the use of copied or similar logos, website layouts or content. Spam emails sometimes make use of typosquatting URLs to trick users into visiting malicious sites that look like a given bank's site, for instance.

UID (User ID) -> A process is associated with a Real UID and an Effective UID. • The real UID is inherited from the user who invokes the process. For e.g. if the user is alice, then the real UID is alice. • Processes can be created by executing a file. There are two cases: • If the Set User ID (SUID) is disabled (the permission will be displayed as “x”), then the process’ effective UID is same as real UID. • If the Set User ID (SUID) is enabled (the permission will be displayed as “s”), then the process’ effective UID is inherited from the UID of the file’s owner.

Unilateral Authentication -> Unilateral key-exchange protocols are employed in a client-server setting where only the server has a certified public key. The client is then authenticated by sending credentials via a connection that is secured with the key obtained from the protocol.

URL (Uniform Resource Locator) - An url consists of a few components. (see https://en.wikipedia.org/wiki/Uniform_Resource_Locator) 1. scheme, 2. authority (a.k.a the hostname) , 3. path 4. query 5. fragment

Vishing -> telephone equivalent of phishing. It is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.

Vulnerability life cycle -> vulnerability is discovered à affected code is fixed à the revised version is tested à a patch is made public à patch is applied.

Whitebox Testing **-** tester has access to source code.

Whitelist - Drop all packets except those specified in the white-list. (e.g. drop all except http, email protocol, and DNS)

Wireshark -> a packet analyzer that captures traffic sent out to the Internet. Acts as a MITM between network card and OS. Generally captured in data link layer (layer 2).

WPA2 -> provides partial protection at Layer 2 (Link) and at Layer 1 (Physical).

Worm -> A computer **worm** is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on **security** failures on the target computer to access it.

Zero-day vulnerability -> a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw. It has the potential to be exploited by cybercriminals.

Execution Integrity

Memory Integrity

cve

zero-day vulnerability

exploit

People Names Used in Security

Ron Rivest -> cryptographer and is one of the inventors of the RSA algorithm (along with Adi Shamir and Len Adleman). He is the inventor of the symmetric key encryption algorithms RC2, RC4, RC5, and co-inventor of RC6.

Whitfield Diffie -> an American cryptographer and one of the pioneers of public-key cryptography along with Martin Hellman and Ralph Merkle. Their technique became known as **Diffie**–Hellman key exchange.

Alice and Bob -> Sender/Receiver

Eve -> An *eavesdropper*, who is usually a passive attacker. While she can listen in on messages between Alice and Bob, she cannot modify them.

Mallory -> A *malicious attacker*. Associated with *Trudy*, an *intruder*. Unlike the passive Eve, Mallory/Mallet is an active attacker (often used in man-in-the-middle attacks), who can modify messages, substitute messages, or replay old messages. The difficulty of securing a system against Mallory/Mallet is much greater than against Eve.

Trent -> A *trusted arbitrator*, who acts as a neutral third party.

Remarks

- The main strength of RSA and PKC is the "public key" setting, which allows an entity in the public to encrypt without knowing the secret key. This is very useful in ***authentication.*** In practice, PKC is rarely used to encrypt an entire large data file. (if public key encryption is required to encrypt a large file F, it can be efficiently carried out in this way: choose a random AES 128-bit key ***k***, encrypt ***k*** using PKC, and encrypt F using AES with ***k*** as the key).
- *CRCs in **proprietary (relating to owner or ownership)** protocols might be **obfuscated (obscured, made unclear)** by using a non-trivial initial value and a final XOR, but these techniques do not add cryptographic strength to the algorithm and can be **reverse engineered** using straightforward methods**.***
- Encryption is designed to provide confidentiality. It does not provide integrity and authenticity. If want to provide these 2 need to use MAC, signature.
- Difference between hash, mac and signature can be found on last few slides of Lecture notes Chapter 3.
- Crucial difference between human generated password and machine generated key: passwords typically are shorter, and vulnerable under exhaustive search and dictionary attack.
- Offline dictionary attacks: After the attacker logged the traffic, it carries out offline exhaustive/dictionary attack by trying all possible passwords. The offline process could take very long time, but doesn't need to remain connecting to the victim.
- A secure password authenticated key exchange ensure that even if the passwords are short, the adversary can't carry out offline dictionary attack. The adversary could be Eve, or Mallory who pretend to be one of the authenticating party.
- **Don't roll your own crypt**
- **Don't use encryption without message authentication**
- **Be careful when concatenating multiple strings, before hashing.** An error I sometimes see: People want a hash of the strings S and T. They concatenate them to get a single string S||T, then hash it to get H(S||T). This is flawed. The problem: Concatenation leaves the boundary between the two strings ambiguous.
  Example: `builtin`||`securely` = `built`||`insecurely`. Put another way, the hash H(S||T) does not uniquely identify the string S and T. Therefore, the attacker may be able to change the boundary between the two strings, without changing the hash. For instance,

if Alice wanted to send the two strings `builtin`and `securely`, the attacker could change them to the two strings `built` and `insecurely` without invalidating the hash.

- **Make sure you seed random number generators with enough entropy**
- **Don't reuse nonces or IVs**
- **Don't use the same key for both encryption and authentication. Don't use the same key for both encryption and signing.**
- **Don't use a block cipher with ECB for symmetric encryption**

NIST Special Publication 800-63-2

NIST Special Publication 800-63 of June 2004 (revision 2) suggested the following scheme to roughly estimate the entropy of human-generated passwords:[2]

- The entropy of the first character is four bits;
- The entropy of the next seven characters are two bits per character;
- The ninth through the twentieth character has 1.5 bits of entropy per character;
- Characters 21 and above have one bit of entropy per character.
- A "bonus" of six bits is added if both upper case letters and non-alphabetic characters are used.
- A "bonus" of six bits is added for passwords of length 1 through 19 characters following an extensive dictionary check to ensure the password is not contained within a large dictionary. Passwords of 20 characters or more do not receive this bonus because it is assumed they are pass-phrases consisting of multiple dictionary words.

Using this scheme, an eight-character human-selected password without upper case letters and non-alphabetic characters is estimated to have 18 bits of entropy. The NIST publication concedes that at the time of development, little information was available on the real world selection of passwords.

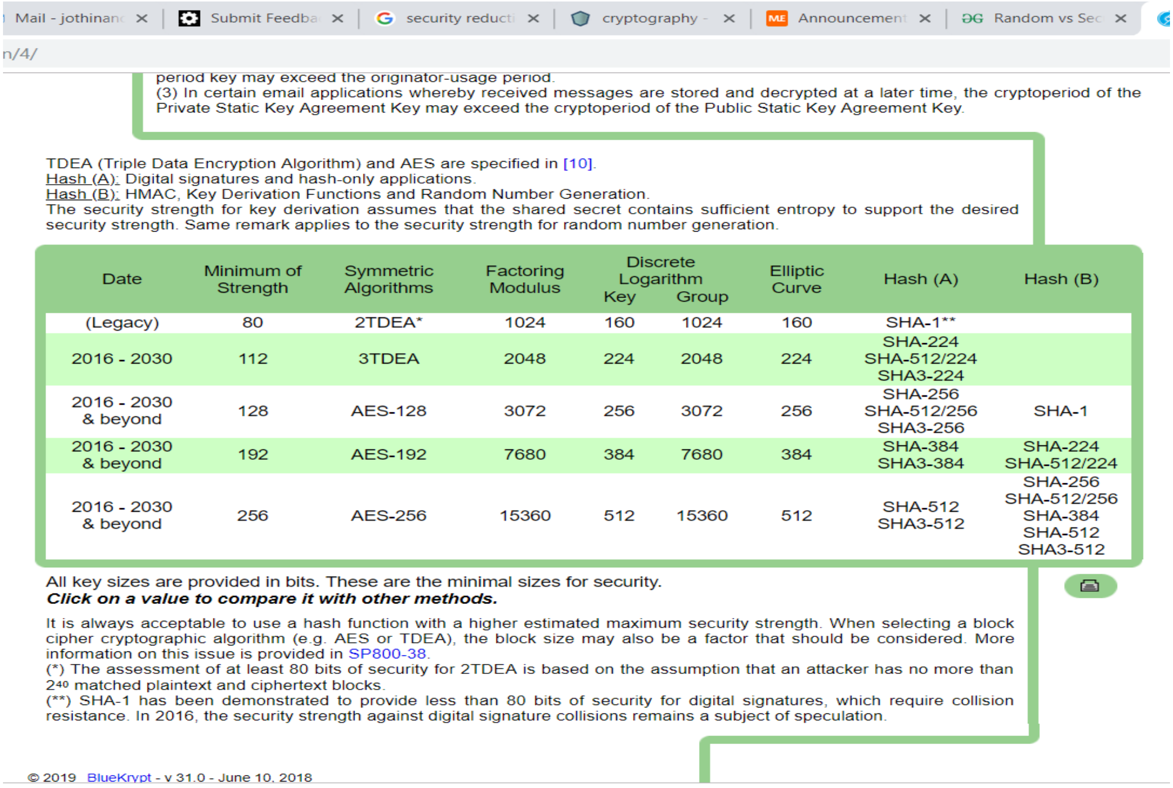
Later research into human-selected password entropy using newly available real world data has demonstrated that the NIST scheme does not provide a valid metric for entropy estimation of human-selected passwords.[11] The June 2017 revision of SP 800-63 (Revision 3) drops this approach

Random vs Secure Random numbers in Java

Prerequisite: Generating Random numbers in Java
java.security.SecureRandom class: This class provides a cryptographically strong random number generator (RNG). A cryptographically strong random number minimally complies with the statistical random number generator tests specified in FIPS 140-2, Security Requirements for Cryptographic Modules, section 4.9.1. Additionally, SecureRandom must produce non-deterministic output. Therefore any seed material passed to a SecureRandom object must be unpredictable, and all SecureRandom output sequences must be cryptographically strong.
java.util.Random class: The classes defined in Random are not cryptographically strong, and the numbers chosen are not completely random because a definite mathematical algorithm (based on Donald E. Knuth’s subtractive random number generator algorithm) is used to select them. Therefore, it is not safe to use this class for tasks that require high level of security, like creating a random password etc.

Random vs SecureRandom

1. **Size:** A Random class has only 48 bits where as SecureRandom can have upto 128 bits. So the chances of repeating in SecureRandom are smaller.
2. **Seed Generation:** Random uses the system clock as the seed/or to generate the seed. So they can be reproduced easily if the attacker knows the time at which the seed was generated. But SecureRandom takes Random Data from your OS (they can be interval between keystrokes etc – most OS collect these data and store them in files – /dev/random and /dev/urandom in case of linux/solaris) and use that as the seed.
3. **Breaking the code:** In case of random, just 2^48 attempts are required, with today's advanced cpu's it is possible to break it in practical time. But for securerandom 2^128 attempts will be required, which will take years and years to break even with today's advanced machines.
4. **Generating Function:** The standard Oracle JDK 7 implementation uses what's called a Linear Congruential Generator to produce random values in `java.util.Random`. SecureRandom implementations are in the form of a pseudo-random number generator (PRNG), which means they use a deterministic algorithm to produce a pseudo-random sequence from a true random seed. Other implementations may produce true random numbers, and yet others may use a combination of both techniques.
5. **Security:** Consequently, the java.util.Random class must not be used either for security-critical applications or for protecting sensitive data.



period key may exceed the originator-usage period.
(3) In certain email applications whereby received messages are stored and decrypted at a later time, the cryptoperiod of the Private Static Key Agreement Key may exceed the cryptoperiod of the Public Static Key Agreement Key.

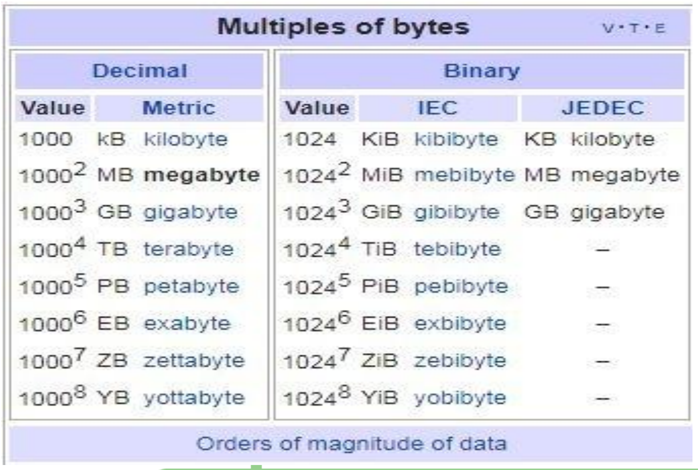
TDEA (Triple Data Encryption Algorithm) and AES are specified in [10].
Hash (A): Digital signatures and hash-only applications.
Hash (B): HMAC, Key Derivation Functions and Random Number Generation.
The security strength for key derivation assumes that the shared secret contains sufficient entropy to support the desired security strength. Same remark applies to the security strength for random number generation.

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm		Elliptic Curve	Hash (A)	Hash (B)
				Key	Group			
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

All key sizes are provided in bits. These are the minimal sizes for security.
Click on a value to compare it with other methods.

It is always acceptable to use a hash function with a higher estimated maximum security strength. When selecting a block cipher cryptographic algorithm (e.g. AES or TDEA), the block size may also be a factor that should be considered. More information on this issue is provided in SP800-38.
(*) The assessment of at least 80 bits of security for 2TDEA is based on the assumption that an attacker has no more than 2^{40} matched plaintext and ciphertext blocks.
(**) SHA-1 has been demonstrated to provide less than 80 bits of security for digital signatures, which require collision resistance. In 2016, the security strength against digital signature collisions remains a subject of speculation.

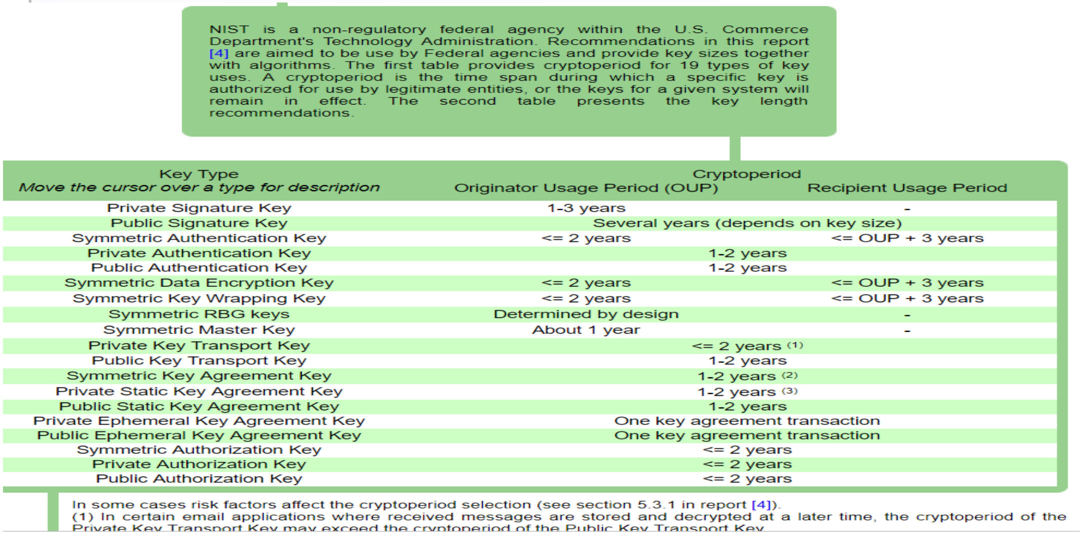
© 2019 BlueKrypt - v 31.0 - June 10, 2018



Multiples of bytes

Decimal			Binary				
Value	Metric		Value	IEC		JEDEC	
1000	kB	kilobyte	1024	KiB	kibibyte	KB	kilobyte
1000^2	MB	**megabyte**	1024^2	MiB	mebibyte	MB	megabyte
1000^3	GB	gigabyte	1024^3	GiB	gibibyte	GB	gigabyte
1000^4	TB	terabyte	1024^4	TiB	tebibyte	–	
1000^5	PB	petabyte	1024^5	PiB	pebibyte	–	
1000^6	EB	exabyte	1024^6	EiB	exbibyte	–	
1000^7	ZB	zettabyte	1024^7	ZiB	zebibyte	–	
1000^8	YB	yottabyte	1024^8	YiB	yobibyte	–	

Orders of magnitude of data



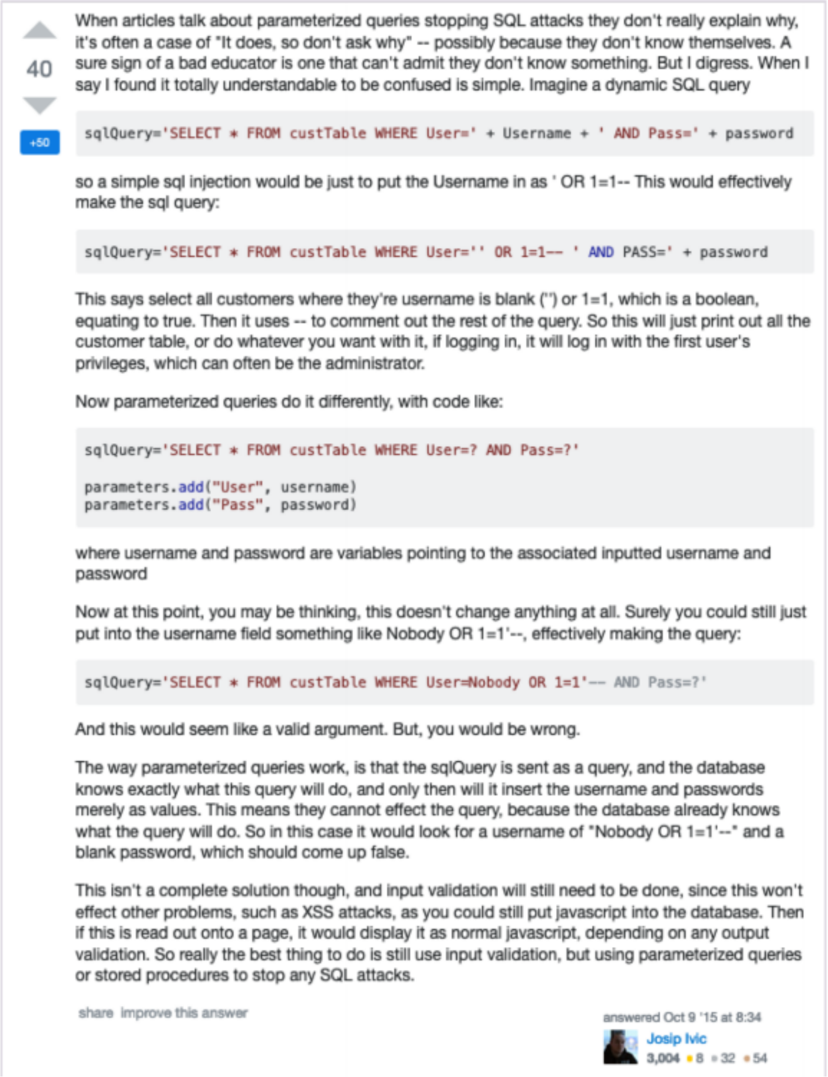
NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. Recommendations in this report [4] are aimed to be use by Federal agencies and provide key sizes together with algorithms. The first table provides cryptoperiod for 19 types of key uses. A cryptoperiod is the time span during which a specific key is authorized for use by legitimate entities, or the keys for a given system will remain in effect. The second table presents the key length recommendations.

Key Type	Cryptoperiod	
Move the cursor over a type for description	Originator Usage Period (OUP)	Recipient Usage Period
Private Signature Key	1-3 years	-
Public Signature Key	Several years (depends on key size)	
Symmetric Authentication Key	<= 2 years	<= OUP + 3 years
Private Authentication Key	1-2 years	
Public Authentication Key	1-2 years	
Symmetric Data Encryption Key	<= 2 years	<= OUP + 3 years
Symmetric Key Wrapping Key	<= 2 years	<= OUP + 3 years
Symmetric RBG keys	Determined by design	-
Symmetric Master Key	About 1 year	-
Private Key Transport Key	<= 2 years (1)	
Public Key Transport Key	1-2 years	
Symmetric Key Agreement Key	1-2 years (2)	
Private Static Key Agreement Key	1-2 years (3)	
Public Static Key Agreement Key	1-2 years	
Private Ephemeral Key Agreement Key	One key agreement transaction	
Public Ephemeral Key Agreement Key	One key agreement transaction	
Symmetric Authorization Key	<= 2 years	
Private Authorization Key	<= 2 years	
Public Authorization Key	<= 2 years	

In some cases risk factors affect the cryptoperiod selection (see section 5.3.1 in report [4]).
(1) In certain email applications where received messages are stored and decrypted at a later time, the cryptoperiod of the Private Key Transport Key may exceed the cryptoperiod of the Public Key Transport Key.

Parameterized Queries

- Parameterized queries are mechanisms introduced in some SQL servers to protect against SQL injection. Here, queries sent to the SQL are explicitly divided to two types: the queries, and the parameters.
- The SQL parser will know that the parameters are “data” and are not “script”. The SQL parser is designed in such a way that it would never execute any script in the parameters. This check will prevent most injection attack.
- The stack overflow post gives a good explanation of parameterized queries.
- *(optional) Will this stop all scripting attacks? No. There are many forms and depending on applications. E.g. it can’t stop XSS.*



When articles talk about parameterized queries stopping SQL attacks they don't really explain why, it's often a case of "It does, so don't ask why" -- possibly because they don't know themselves. A sure sign of a bad educator is one that can't admit they don't know something. But I digress. When I say I found it totally understandable to be confused is simple. Imagine a dynamic SQL query

```
sqlQuery='SELECT * FROM custTable WHERE User=' + Username + ' AND Pass=' + password
```

so a simple sql injection would be just to put the Username in as ' OR 1=1-- This would effectively make the sql query:

```
sqlQuery='SELECT * FROM custTable WHERE User='' OR 1=1-- ' AND PASS=' + password
```

This says select all customers where they're username is blank ('') or 1=1, which is a boolean, equating to true. Then it uses -- to comment out the rest of the query. So this will just print out all the customer table, or do whatever you want with it, if logging in, it will log in with the first user's privileges, which can often be the administrator.

Now parameterized queries do it differently, with code like:

```
sqlQuery='SELECT * FROM custTable WHERE User=? AND Pass=?'

parameters.add("User", username)
parameters.add("Pass", password)
```

where username and password are variables pointing to the associated inputted username and password

Now at this point, you may be thinking, this doesn't change anything at all. Surely you could still just put into the username field something like Nobody OR 1=1'--, effectively making the query:

```
sqlQuery='SELECT * FROM custTable WHERE User=Nobody OR 1=1'-- AND Pass=?'
```

And this would seem like a valid argument. But, you would be wrong.

The way parameterized queries work, is that the sqlQuery is sent as a query, and the database knows exactly what this query will do, and only then will it insert the username and passwords merely as values. This means they cannot effect the query, because the database already knows what the query will do. So in this case it would look for a username of "Nobody OR 1=1'--" and a blank password, which should come up false.

This isn't a complete solution though, and input validation will still need to be done, since this won't effect other problems, such as XSS attacks, as you could still put javascript into the database. Then if this is read out onto a page, it would display it as normal javascript, depending on any output validation. So really the best thing to do is still use input validation, but using parameterized queries or stored procedures to stop any SQL attacks.

answered Oct 9 '15 at 8:34
Josip Ivic
3,004 ● 8 ● 32 ● 54