Fundamentals of Information Security Series

C836

Instructor: Arthur Moore

Event time: Every Thursday at 6:00PM MST

Instructor intro

- Contact info: Arthur.Moore@wgu.edu
- Number: 1-877-435-7948 Ext. 1554
- Office Hours:
- Monday: 8AM-5PM
- Tuesday: 8AM-5PM
- Wednesday: 8AM-5PM
- Thursday: 8AM-12PM AND 7PM-10PM
- Sunday: 6PM-10PM

As a reminder

- This web series is only to enhance/supplement the course material not to replace it please follow the guidelines as posted below.
- ***It's Highly recommended that you Don't schedule the first assessment until all the materials are covered***.
- -take the preassessment until constantly passing
- -review lessons 1-14 readings (pay close attention to chapters 1 – 6.)
- -complete lessons 1-14 quizzes.
- -complete lessons 1-14 exercises (pay close attention to chapters 1 – 6)
- -watch the videos that are posted in the course tips
- -go over the PowerPoints that are posted in the course tips

What is Cryptology?

- Cryptology is the study of cryptographic algorithms.
- These algorithms convert plaintext (original message) into ciphertext (encrypted/new message).
- Some algorithms work in both directions allowing for the ciphertext to return to the original plaintext form. Other algorithms act as an integrity check only allowing a one-way function.
- Cryptanalysis is the breaking and finding a weakness in the given algorithm.

History

- History is rich with the use of cryptography, with some of the oldest examples being used by the ancient Greeks and Romans. Information was hidden by a wide variety of codes, one extreme example was by tattooing them on the shaved heads of messengers and then allowing the hair to grow, and by a multitude of other methods generally focused on mathematical algorithms.
- Caesar cipher: The Caesar cipher is based on transposition and involves shifting each letter of the plaintext message by a certain number of letters, historically three. The ciphertext can be decrypted by applying the same number of shifts in the opposite direction. This type of encryption is known as a substitution cipher, due to the substitution of one letter for another in a consistent fashion.
- ROT13: ROT13 uses the same mechanism as the Caesar cipher but moves each letter 13 places forward. The convenience of moving 13 places lies in the fact that applying another round of encryption with ROT13 also functions as decryption, as two rotations will return us to the original starting place in the alphabet.

History Continued

- Cryptographic Machines: Before the advent of the modern computer, machines existed that simplified the use of encryption and made more complex encryption schemes feasible. Initially, such devices were simple mechanical machines, but as technology progressed, we began to see the inclusion of electronics and considerably more complex systems.
- The Jefferson Disk, invented by Thomas Jefferson in 1795, is a purely mechanical cryptographic machine. It is composed of a series of disks, each marked with the letters a to z around its edge. On each disk, the letters are arranged in a different order; each disk is also marked with a unique designator to facilitate arranging them in a particular order. The device built by Jefferson contained 36 disks, with each disk representing one character in the message.

History Continued

- German Enigma: The Enigma was created by Arthur Scherbius in 1923 and was used to secure German communications during World War II. In fact, there were several models of Enigma machine, and a variety of accessories and add-ons that could be attached to them. The Enigma I, was developed in 1932.
- The Enigma was based on a series of wheels, referred to as rotors, each with 26 letters and 26 electrical contacts on them, similar in general concept to the Jefferson Disk.
- In order for two Enigma machines to communicate, they needed to be configured identically. The rotors needed to be the same and in the same position, the rings marked with the alphabet on each rotor needed to be in the same position, the rotors needed to be set to the same starting position, and any plugs in the plugboard needed to be configured in the same fashion.

History Continued

- Kerckhoffs' Principle: the second principle has become a tenet of cryptographic algorithms. This idea was later restated by Claude Shannon as "the enemy knows the system"Both versions of this concept mean that cryptographic algorithms should be robust enough that, even though someone may know every bit of the system with the exception of the key itself, he or she should still not be able to break the encryption.
- This idea represents the opposite approach to "security through obscurity" and is one of the underlying principles for many modern cryptographic systems.

Modern Cryptographic Tools

- Symmetric cryptography: Symmetric key cryptography, also known as private key cryptography, utilizes a single key for both encryption of the plaintext and decryption of the ciphertext.
- Asymmetric cryptography: asymmetric key cryptography, also known as public key cryptography, utilizes two keys: a public key and a private key. The public key is used to encrypt data sent from the sender to the receiver and is shared with everyone.
- Hash functions: represent a third cryptography type alongside symmetric and asymmetric cryptography, what we might call keyless cryptography. Hash functions, also referred to as message digests, do not use a key, but instead create a largely unique and fixed-length hash value, commonly referred to as a hash, based on the original message, something along the same lines as a fingerprint. Any slight change to the message will change the hash.
- Digital signatures: Digital signatures allow us to sign a message in order to enable detection of changes to the message contents, to ensure that the message was legitimately sent by the expected party, and to prevent the sender from denying that he or she sent the message, known as nonrepudiation.
- Certificates: are created to link a public key to a particular individual and are often used as a form of electronic identification for that particular person. A certificate is typically formed by taking the public key and identifying information, such as a name and address, and having them signed by a certificate authority (CA).

Symmetric cryptography

- Symmetric cryptography: Symmetric key cryptography, also known as private key cryptography, utilizes a single key for both encryption of the plaintext and decryption of the ciphertext.
- Symmetric key cryptography makes use of two types of ciphers: block ciphers and stream ciphers.
- Block cipher: takes a predetermined number of bits, known as a block, in the plaintext message and encrypts that block. Blocks are commonly composed of 64 bits but can be larger or smaller depending on the particular algorithm being used and the various modes in which the algorithm might be capable of operating.
- Stream cipher: encrypts each bit in the plaintext message, 1 bit at a time.
- A large majority of the encryption algorithms in use at present are block ciphers. Although block ciphers are often slower than stream ciphers, they tend to be more efficient. Since block ciphers operate on larger blocks of the message at a time, they do tend to be more resource intensive and are more complex to implement in hardware or software.
- Block ciphers are also more sensitive to errors in the encryption process as they are working with more data. An error in the encryption process of a block cipher may render unusable a larger segment of data than what we would find in a stream cipher, as the stream cipher would only be working with 1 particular bit.

Symmetric key algorithms

- DES: DES is a block cipher based on symmetric key cryptography and uses a 56-bit key. Although DES was considered to be very secure for some period of time, it is no longer considered to be so.
- 3DES: which is simply DES used to encrypt each block three times, each time with a different key. DES can operate in several different block modes, including Cipher Block Chaining (CBC), Electronic CodeBook (ECB), Cipher Feedback (CFB), Output Feedback (OFB), and Counter Mode (CTR). Each mode changes the way encryption functions and the way errors are handled.
- AES: is a set of symmetric block ciphers endorsed by the US government through NIST, and now used by a variety of other organizations, and is the replacement for DES as the standard encryption algorithm for the US federal government. AES uses three different ciphers: one with a 128-bit key, one with a 192-bit key, and one with a 256-bit key, all having a block length of 128 bits. AES shares the same block modes that DES uses and also includes other modes such as XEX-based Tweaked CodeBook (TCB) mode.
- There are a large number of other well-known symmetric block ciphers, including Twofish, Serpent, Blowfish, CAST5, RC6, and IDEA, as well as stream ciphers, such as RC4, ORYX, and SEAL.

Asymmetric cryptography

- Asymmetric cryptography: asymmetric key cryptography, also known as public key cryptography, utilizes two keys: a public key and a private key. The public key is used to encrypt data sent from the sender to the receiver and is shared with everyone.
- The main advantage of asymmetric key cryptography over symmetric key cryptography is the loss of the need to distribute the key. As we discussed earlier in this lesson, when we use a symmetric algorithm, we need to distribute the key in some way. We might do this by exchanging keys in person, sending a key in e-mail, or repeating it verbally over the phone, but we generally need to communicate the key in an out-of-band manner, meaning that we do not want to send the key with the message, as this would leave our message easily available to an eavesdropper. When we use asymmetric key cryptography, we have no need to share a single key. We simply make our public key easily available, and anyone who needs to send us an encrypted message makes use of it.

Asymmetric key algorithms

- The RSA algorithm, named for its creators Ron Rivest, Adi Shamir, and Leonard Adleman, is an asymmetric algorithm used all over the world, including in the Secure Sockets Layer (SSL) protocol, which is used to secure many common transactions such as Web and e-mail traffic. RSA was created in 1977 and is still one of the most widely used algorithms in the world to this day.
- Elliptic curve cryptography (ECC) is a class of cryptographic algorithms, although it is sometimes referred to as though it were an algorithm in and of itself. ECC is named for the type of mathematical problem on which its cryptographic functions are based.
- ECC has several advantages over other types of algorithms. It has a higher cryptographic strength with shorter keys than many other types of algorithms, meaning that we can use shorter keys with ECC while still maintaining a very secure form of encryption. It is also a very fast and efficient type of algorithm, allowing us to implement it on hardware with a more constrained set of resources, such as a cell phone or portable device, more easily. We can see ECC implemented in a variety of cryptographic algorithms, including Secure Hash Algorithm 2 (SHA-2) and Elliptic Curve Digital Signature Algorithm (ECDSA).
- Several other asymmetric algorithms exist, including ElGamal, Diffie–Hellman, and Digital Signature Standard (DSS). We can also see a variety of protocols and applications that are based on asymmetric cryptography, including Pretty Good Privacy (PGP) for securing messages and files, SSL and Transport Layer Security (TLS) for several kinds of traffic including Web and e-mail, and some Voice over IP (VoIP) for voice conversations. Asymmetric cryptography has allowed many of the modern methods of secure communication to exist and will likely continue to be the basis of them for some time.
- PGP, created by Phil Zimmerman, was one of the first strong encryption tools to reach the eye of the general public and the media. Created in the early 1990s, the original release of PGP was based on a symmetric algorithm and could be put to use in securing data such as communications and files. The original release of PGP was given away as free software, including the source code. At the time of its release, PGP was regulated as a munition under the US International Traffic in Arms Regulations (ITAR) law. Zimmerman spent several years under investigation for criminal activities, as he was suspected of exporting PGP out of the country, which was then illegal and encryption systems were included under arms trafficking regulations.

Hash functions

- Hash functions: represent a third cryptography type alongside symmetric and asymmetric cryptography, what we might call keyless cryptography. Hash functions, also referred to as message digests, do not use a key, but instead create a largely unique and fixed-length hash value, commonly referred to as a hash, based on the original message, something along the same lines as a fingerprint. Any slight change to the message will change the hash.
- Hashes cannot be used to discover the contents of the original message, or any of its other characteristics, but can be used to determine whether the message has changed. In this way, hashes provide integrity, but not confidentiality.
- Some algorithms, such as Message-Digest algorithm 5 (MD5), have been attacked in this fashion, although producing a collision is still nontrivial. When such cases occur, the compromised algorithm usually falls out of common use. Hashing algorithms such as SHA-2 and the soon-to-arrive SHA-3 have replaced MD5 in cases where stringent hash security is required. Many other hash algorithms exist and are used in a variety of situations, such as MD2, MD4, and RACE.

Digital Signatures

- Digital signatures: Digital signatures allow us to sign a message in order to enable detection of changes to the message contents, to ensure that the message was legitimately sent by the expected party, and to prevent the sender from denying that he or she sent the message, known as nonrepudiation.
- To digitally sign a message, the sender would generate a hash of the message, and then use his private key to encrypt the hash, thus generating a digital signature. The sender would then send the digital signature along with the message, usually by appending it to the message itself.
- When the message arrives at the receiving end, the receiver would use the sender's public key to decrypt the digital signature, thus restoring the original hash of the message. The receiver can then verify the integrity of the message by hashing the message again and comparing the two hashes. Although this may sound like a considerable amount of work to verify the integrity of the message, it is often done by a software application of some kind and the process typically is largely invisible to the end user. A digital signature is considered legally binding and if it is lost or stolen must be revoked

Certificates and PKI

- Certificates: are created to link a public key to a particular individual and are often used as a form of electronic identification for that particular person.
- A certificate is typically formed by taking the public key and identifying information, such as a name and address, and having them signed by a certificate authority (CA).
- A CA is a trusted entity that handles digital certificates. One well-known CA, at present, is VeriSign. Additionally, some large organizations, such as the US Department of Defense (DoD), that utilize a large number of certificates may choose to implement their own CA in order to keep costs down.
- A CA is only a small part of the infrastructure that can be put in place to handle certificates on a large scale. This infrastructure is known as a public key infrastructure (PKI).
- A PKI is generally composed of two main components, although some organizations may separate some functions out into more than just these. In a PKI, we often find the CAs that issue and verify certificates and the registration authorities (RAs) that verify the identity of the individual associated with the certificate.
- In PKI, we also deal with the concept of certificate revocation, in the case where a certificate reaches its expiration date, the certificate is compromised, or another reason arises in which we need to ensure that the certificate can no longer be used. In this case, we will likely see the certificate added to a certificate revocation list (CRL). The CRL is a generally public list that holds all the revoked certificates for a certain period of time, depending on the organization in question. An example of the impact to trust relationships from certificates being compromised can be seen when DigiNotar had hundreds of SSL certificates stolen and used by hackers to sign malware with certificates from legitimate companies.

Protecting Data at Rest, in Motion, and in Use

- We can divide practical uses of cryptography into two major categories: protecting data at rest and protecting data in motion.
- Protecting data at rest is important because of the large amount of stored data that can be found on devices such as backup tapes, flash drives, and hard drives in portable devices such as laptops.
- Protecting data in motion is vital as well because of the enormous amount of business that is conducted over the Internet, including financial transactions, medical information, tax filings, and other similarly sensitive exchanges.

Protecting Data at Rest

- Protecting Data at Rest: Data is generally considered to be at rest when it is on a storage device of some kind and is not moving over a network, through a protocol, and so forth.
- Data security: The primary method we use to protect this type of data is encryption, particularly when we know that the storage media, or the media and the device in which it is contained, will be potentially exposed to physical theft, such as on a backup tape or in a laptop.
- Physical security: If we make it more difficult for attackers to physically access or steal the storage media on which our sensitive data is contained, we have solved a large portion of our problem.
- Physical security should be at the core of all our security planning discussions.

Protecting Data in Motion

- Protecting Data in Motion: The primary method of securing data from exposure on network media is encryption, and we may choose to apply it in one of two main ways: by encrypting the data itself to protect it or by protecting the entire connection.
- Protecting the data itself: SSL and TLS are often used to protect information sent over networks and over the Internet, and they operate in conjunction with other protocols such as Internet Message Access Protocol (IMAP) and Post Office Protocol (POP) for e-mail, Hypertext Transfer Protocol (HTTP) for Web traffic, VoIP for voice conversations, instant messaging, and hundreds of others. SSL is actually the predecessor of TLS, and TLS is based heavily on the last version of SSL. The terms are often used interchangeably, and they are nearly identical to each other. Both methods are still in common use.
- Protecting the connection: Another approach we might choose to take is to encrypt all our network traffic with a virtual private network (VPN) connection. VPN connections use a variety of protocols to make a secure connection between two systems. We might use a VPN when we are connecting from a potentially insecure network, such as the wireless connection in a hotel, to the internal resources that are secure behind our company firewalls.
- Two main methods are used at present: Internet Protocol Security (IPsec) VPNs and SSL VPNs.
- An IPsec VPN requires a more complex hardware configuration on the back end and a software client to be installed, whereas an SSL VPN often operates from a lightweight plug-in downloaded from a Web page and a less complex hardware configuration on the back end.

Protecting Data in Use

- Protecting Data in Use: Although we can use encryption to protect data while it is stored or moving across a network, we are somewhat limited in our ability to protect data while it is being used by those who legitimately have access to it. Authorized users can print files, move them to other machines or storage devices, e-mail them, share them on peer-to-peer (P2P) file-sharing networks, and generally make a mockery of our carefully laid security measures.