Trust Defined

Trust

In the world of IT systems and todays Internet of Everything (IoE), communication is the most popular use of the Internet. When communicating on the Internet, we must be aware of the risks involved in engaging with people we cannot see and may never meet in person because security threats can popup anywhere. Therefore, if we don't know where a link will lead us, nor did we request it, it's safer to not open it for these usually lead to malware infections (including ransomware) or phishing attempts.

New Technologies, New Threats, and New Defenses

A new generation of technology is posing new security risks on all sides. Cloud computing, big data, and especially mobile devices pose complex and growing challenges. The Bring-Your-Own-Device (BYOD) trend is filling workplaces with mobile devices that IT securi teams cannot directly control and that often have serious security gaps.

Digital ID *continue……*

- Strong Identities are released with registration and authentication procedures that guarantee the encryption of any information that passes between the web server and the individual user.
    - Registration – It involves the following processes that make known entity in a given domain.
        - Self-assertion -the user makes a self-assertion of identity and there are no checks.
        - Third-party verification -the verification is left to third-party (i.e. phone number).
        - Direct verification -the verification of identity is direct (i.e. background check of clients)
        - Detailed direct verification -the verification of identity is direct and detailed (i.e. for e-passport)
    - Authentication - It involves the following verification process of the attributes associated with identity.
        - One-factor Authentication – It is the authentication done through something that you know, or you have (i.e. password).
        - Two-factor Authentication - It is the authentication done through something that you know and you have (i.e. token and PIN).
        - Three-factor Authentication – It is the authentication done through something that you know, you are, and you have (i.e. token, PIN, biometric).

Examples of strong identities include:

- Banking Identity
- Account to purchase flights or trains (i.e. Abacus, Amadeus, Apollo, Galileo, Sabre, Worldspan)
- SIM phoneE-Passport (i.e. Department of Foreign Affairs (DFA))
- Health cards (PhilHealth)
- National Service Card (i.e. SSS, GSIS)

Digital Certification

Digital Certificate

A digital certificate is a highly signed statement that binds the identifying information of a user, computer, or service to a public/private key pair. The different fields within a digital certificate are the following:

- Version number - This specifies the version of the X.509 standard being used to create the certificate.
- Serial number - It contains a unique number identifying this one specific certificate issued by a particular certificate authority (CA).
- Signature algorithm - It identifies the hashing algorithim and digital signature algorithm used to digitally sign the certificate.
- Issuer - It identifies the name of the creator who generated and digitally signed the certificate.
- Validity - It specifies the dates and times though which the certificate is valid for use.
- Subject - It specifies the name of the owner of the digital certificate.
- Subject Public Key - It contains the public key being bound to the certified subject.

Digital Certification *continue.....*

- Issuer Unique ID - It is an optional identifier for the creator of the digital certificate.
- Subject Unique ID - It is an optional identifier for the owner of the digital certificate.
- Certificate usage - It specifies the approved use of certificate, which dictates what the user can use this public key for.
- Extensions - They allow a range of optional fields below to be encoded into the certificate to expand the functionality of the certificate.
    - A key identifier (in case owner owns more than one public key)
    - Key usage information that specifies valid uses of key
    - The location of revocation information

Digital Certification *continue.....*

- Identifier of the certificate policy
- Alternative names for the owner

Three (3) types of certificates are available:

- Personal Digital ID or Personal Certificate - These are used for sending personal infromation over the Internet to a website requiring verification of the user's identity. Commonly used in e-mail exchange by individual users.
- Server Digital ID or Website Certificate – It identifies and authenticates the web server and guarantees the encryption of any information passed between the web server and the individual user. Also, enables a specific web server to operate in a secure and authentic way.
- Developers Digital ID - These are used by software developers.

Digital Certification *continue .....*

Intrusion Detection System (IDS) is a system used to detect and prevent a set of actions that aims to compromise the integrity, confidentiality, or availability of a computing and networking resource.

Models of intrusion deection mechanisms:

- Anomaly-based Detection – It detects any action that significatnly deviates from the normal behavior through "learning" systems that work by continously creating "norms" or activities and compares observed activity against expected normal usage profiles "learned".
- Signature-based Detection (a.k.a Misuse Detection) – It catches intrusions by looking for a unique pattern or specific signature on a system and the slight variations of the same activity that produce a new signature.

Intrusion Detection Systems are classified based on their monitoring scope.

- Network-based IDS – It is a system that monitors packets on the network wire and attempts to discover anomalous, inappropriate, or other data that may be considered unauthorized and harmful on a network.
- Host-based IDS - It is a system that detects malicous activities on a single computer through the use of software that monitors security event logs and checks the changes to the system, for example unauthorized login attempts and aberrant file accesses, on the actual target machine.

Digital Certification *continue.....*

PC Card Based Solution

PC card-based solutions can be added to digital IDs and IDSs to establish a network environment that is secured in terms of control of access, identities, software, file storing,e-mails,and so on.

Commonly used PC card-based solutions:

Smart card (a.k.a Security card) – It is a credit card-sized plastic card that contains an embedded computer chip either a memory or microprocessor type that stores and transacts data.

- Functional examples of smart cards are the following:
  - Identification cards (including biometrics)
  - Medical cards
  - Credit and debit cards
  - Access control cards (authenication)

Hardware key (a.ka Dongle) – It is a software copy proterction device that protects a software package agai unauthorized copying.

Password Security

Password Security

The following are not the only ways to keep your password secure, but they are a good start:

- Use passphrases.
- Do not keep your password in open and public spaces.
- Change your password periodically.
- Do not use the same password for everything.
- If you think your password may have been compromised, change it immediately.
- Never tell anyone your password.

Examples:

- A meaningful statement: "Carp3 Diem!"
- Directions to a location: "Down Oak, 2°d on the Right"
- A reference to what you're accessing: "Check ng my Onid-Mail!" *(Note: This is an awesome kind of pass phrase, as you can customize it for any service you use, protecting your accounts from each other).*
- A catchy jingle: "I don't always use passwords, but when I do"

Continue....

The IP packet format consists of these fields:

- Version Field (4 bits) – It indicates the version of IP currently used.
- IP Header Length (IHL) field (4 bits) – It indicates how many 32-bit words are in the IP header.
- Type-of-Service Field (8 bits) – It specifies how a particular upper-layer protocol would like the current datagram to be handled. Datagrams can be assigned various levels of importance through this field.
- Total Length field (16 bits) – It specifies the length of the entire IP packet, including data and header, in bytes.
- Identification Field (16 bits) – It contains an integer that identifies the current datagram. This field is used to help reconstruct datagram fragments.
- Flags Field (4 bits; one is not used) – It controls whether routers are allowed to fragment a packet, and indicates the parts of a packet to the receiver.
- Time-to-Live Field (8 bits) – It maintains a counter that gradually decrements to zero, at which point the datagram is discarded. This keeps packets from looping endlessly.
- Protocol Field (8 bits) – It indicates which upper layer protocol receives incoming packets after IP processing is complete.
- Header Checksum Field (16 bits) – It helps ensure IP header integrity.
- Source Address Field (32 bits) – It specifies the sending node.
- Destination Address Field (32 bits) – It specifies the receiving node.
- Options Field (32 bits) – It allows IP to support various options, such as security.

Continue....

) Data Field (32 bits) - It contains upper-layer information.

The TCP packet format consists of these fields:

) Source Port and Destination Port Fields (16 bits each) - It identifies the end points of the connection.

❯ Sequence Number Field (32 bits) – It specifies the number assigned to the first byte of data in the current message.

) Acknowledgement Number Field (32 bits) - It contains the value of the next sequence number that the sender of the segment is expecting to receive, if the ACK control bit is set.

) Data Offset (a.k.a Header Length) Field (variable length) - It tells how many 32-bit words are in the TCP header.

- o Reserved Field (6 bits) - It contains the various flags:
  - *URG* - It indicates that some urgent data has been placed.
  - *ACK* - It indicates that acknowledgement number is valid.
  - *PSH* - It indicates that data should be passed to the application as soon as possible.
  - *RST* - It resets the connection.
  - *SYN* - It synchronizes sequence numbers to initiate a connection.
  - *FIN* - It means that the sender of the flag has finished sending data.

IP Address Spoofing

Spoofing Attack happens when an attacker impersonates another device or computing system in order to steal data or confidential information, spread malware, bypass access controls, and even launch an attack against network hosts.

IP Address Spoofing is a method of attack, where by network attackers/intruders pretend to be a trusted user to defeat network security measures of the corporate network.

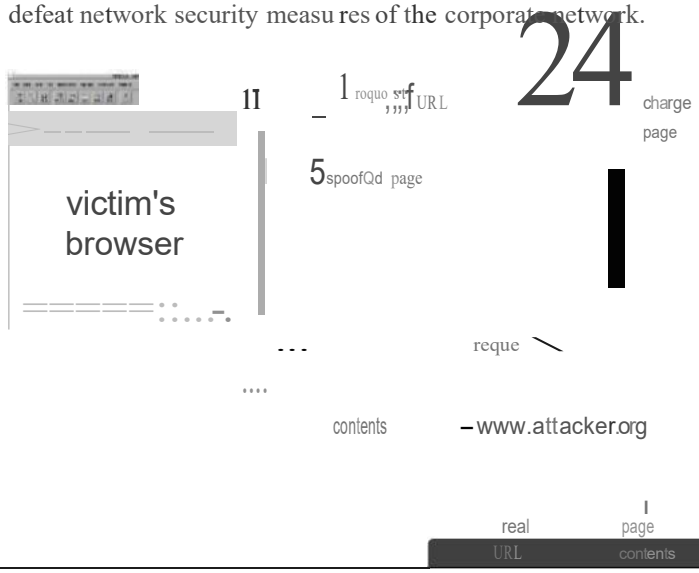

Figure 3 -An example Web transaction during a We

spoofing attack
Source:
http://Iudevsoftwa re.blogspot.com/2014_12_01_archive.html

IP Address Spoofing *continue……..*

The victim requests a web page. The following steps occur: (1) the victim's browser requests the page from the attacker's server; (2) the attacker's server requests the page from the real server; (3) the real server provides the page to the attacker's server; (4) the attacker's server rewrites the page; (5) the attacker's server provides the rewritten version to the victim.

IP Address Spoofing is classified into:

- Non-Blind Spoofing - This takes place when an attacker who happens to be on the same subnet as the target is able to see the sequencing numbers and acknowledgements easily.
- Blind Spoofing - This takes place when an attacker outside the perimeter of the local network sends multiple packets to the target to receive a series of sequence numbers, which are generally used to assemble packets in the order in which they were intended. By taking advantage of knowing the sequence number, the attacker can falsify his identity by injecting data into the stream of packets without having to have authenticated himself when the connection was first established.
- Man in the Middle Attack (Connection Hijacking) - This takes place when an attacker gets between the sender and receiver of information and control the flow of communication and to eliminate or alter the information sent by one of the original participants without their knowledge.

IP Address Spoofing *continue.....*

Countermeasures

Network administrators are tasked to understand the vulnerabilities that exist in the network in order to anticipate possible attacks and implement effective countermeasures.

These are countermeasures that can be implemented in defense against IP Address Spoofing such as:

- Packet Filtering - It analyses the incoming and outgoing packets and inspects them based on the IP addresses of the source and destination with conflicting address information. It is usually a part of a firewall program to protect a local network from unwanted intrusion.
- Avoid IP Address-Based Authentication as much as possible - It makes the system more vulnerable if it relies on IP addresses for authentication insecuring the system since it can easily be spoofed.
- Use Spoofing Detection Software - These are software that inspect and certify data before it is transmitted, and block data if it appears to be spoofed.
- Use Cryptographic Network Protocols - It reinforces spoofing attack prevention attempts by encrypting data before it is sent and authenticating data as it is received.

Buffer overflow *continue.....*

Countermeasures

Understanding buffer overflow is important because the majority of all the existing remote penetration issues in today's internetworking infrastructure uses buffer overflow attacks because the vulnerabilities are common and easy to exploit. Countermeasures to help prevent buffer overflows include:

- Perform thorough input validation – This is the first line of defense against buffer overflows. Although a bug may exist in your application that permits expected input to reach beyond the bounds of a container, expected input will be the primary cause of this vulnerability. Constrain input by validating it for type, length, format, and range.
- When possible, limit your application's use of unmanaged code, and thoroughly inspect the unmanaged Application Program Interface (APIs) – To ensure that input is properly validated.
- Inspect the managed code that calls the unmanaged API to endure that only appropriate values can be passed as parameters to the unmanaged API.
- Use the /GS flag to compile code developed with the Microsoft Visual C++® development system - The /GS flag causes the compiler to inject security checks into the compiled code. This is not a fail proof solution or a replacement for your specific validation code; it does, however, protect your code from commonly known buffer overflow attacks.

Digital ID

A digital ID, or digital identity, is a means by which an entitiy (individual/company) proves their attributes in a specific domain. This implies that one have been granted permission to access information on network devices or services. There are different types of digital identities that, depending on the use and the level of security required, can be divided into two (2) categories:

- Soft Identities are used for sending personal information over the internet to a website, whereby the web server requires verification of the user's identity.
  Examples
  - Email account (private and corporate)
  - Social Network Accounts (i.e. Facebook, Twitter, Google+, Instagram)
  - E-commerce identities (i.e. Amazon, eBay, Lazada, Zalora)