Networking Security Research Journal

CIT 288

Chaz Davis

BCTC
Spring 2020

February 12, 2020

Contents

Chapter 1

Research
Chapter 02

Network Security **CIT 288**
Spring 2020 Chaz Davis

What are the essential ingredients of a symmetric cipher?

- plain text
- Encryption Algorithm
- Secret Key
- Cipher Text
- Decryption Algorithm

How many keys are required for two people to communicate via a symmetric cipher?

1, the same key thats used to encrypt the message is used to decrypt the message

What are two principal requirements for the secure use of symmetric encryption?

- A strong encryption algorithm. The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession.
- Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

List three approaches to message authentication

- Using conventional encryption

- Using Public-key encryption
- Using a secret value

What is message authentication?

small block of data, that is appended to a message to assure that the sender is authentic and that the message is unaltered.

Briefly describe the three schemes found in figure 2.3

- A
- B
- C

What properties must a hash function have to be useful for message authentication?

- Plain text
- Encryption Algorithm
- Public and Private keys
- Cipher text

List and briefly describe three uses of a public-key cryptosystem

- Encryption/Decryption: The sender encrypts a message with the recipients public key.
- Digital Signature: The sender "signs" a message with its private key.
- Key Exchange: Two sides cooperate to exchange as a session key. Several different approaches are possible, involving the private keys of one or both parties.

What is the difference between a private key and a secret key?

The key used in conventional encryption is typically referred to as a secret key. the two keys used for public-key encryption are referred to as the public key and the private key.

What is a digital signature?

A mechanism for authenticating a message. Bob uses a secure hash function, sch as SHA-512, to generate a hash value for the message and then encrypts the hash code with his private key, creating a digital signature. Bob sends the message with the signature attached. When Alice receives the message she calculates a hash value for the message, decrypts the signature using Bob's public key and compares it to Bob's hash value. If the two hash values match, Alice is assured that the message must have been signed by Bob. It is important to emphasize that the digital signature does not provide confidentiality.

What is public-key certificate?

A certificate consists of a public-key plus a user ID of the key owner, with the whole block signed by a trusted third-party (= certificate authority CA) The user can then publish the certificate and anyone needing the users public-key can obtain the certificate and verify that it is valid by means of the attached signature.

How can public-key encryption be used to distribute a secret key?

- Digital Envelope
- Prepare a message
- Generate a random symmetric key that will be used the time only
- Encrypt that message using symmetric key encryption with the one-time key.
- Encrypt the one-time key using public-key encryption

Chapter 2

Research
Chapter 03

Network Security **CIT 288**
Spring 2020 Chaz Davis

Question

An early attempt to force users to use less predictable passwords involved computer-supplied passwords. The passwords were eight characters long and were taken from the character set consisting of lowercase letters and digits. They were generated by a pseudorandom number generator with 2^{15} possible starting values. Using the technology of the time, the time required to search through all character strings of length 8 from a 36-character alphabet was 112 years. Unfortunately, this is not a true reflection of the actual security of the system. Explain the problem.

i) answer Analyze the actual security of the computer supplied passwords: In the early days to select strong passwords, the computers use a psuedo random number generator to generate passwords which are 8 characters in lengths using 36 character alphabets. the number of possible strings that can be generated using 36 characters with a length of eight characters is 36^8 which is aproximately equal to 2^{41} But the psudorandom generator can produce 2^{15} passwords. as a result, the number of passwords that needs to be looked at to hack is only 2^{15}. Therefore, this system does not provide much security.

Question

A phonetic password generator picks two segments randomly for each six-letter password. The form of each segment is CVC (consonant, vowel, consonant), where V = < a, e, i, o, u > and C = V . What is the total password population? What is the probability of an adversary guessing a password correctly?

i) part a: answer the password generator generates 6 letter passwords randomly which consist of two segments. the segment is

- The segment is of the form CVC (consonant, vowel, consonant)

  Vowels consist of 5 letters

  Consonants consist of 21 letters

- 6 letters the 6 letter password is of the form CVCCVC

- The total number of passwords that a phoetic password generator can generate is $21x5x21x21x5x21$ which is equal to: 4,862,025.

ii) part b: answer The probability to guess a password correctly is calulated using the following formula:

$$\text{Probability of correct number of guesses} = \frac{1}{\text{Total password population}} \tag{2.1}$$

Here, the total password population is 4,862,025; substitute it in the above formula to find the probability.

$$\text{Probability of correct password guesses} = \frac{1}{4,862,025} \approx 2x10^{-7} \tag{2.2}$$

So, the probability to guess a correct password by an adversay is approximately equal to $2x10^{-7}$ (2.3)

Question

It was stated that the inclusion of the salt in the UNIX password scheme increases the difficulty of guessing by a factor of 4096. But the salt is stored in plaintext in the same entry as the corresponding ciphertext password. Therefore, those two characters are known to the attacker and need not be guessed. Why is it asserted that the salt increases security? i) answer Salt: An extensively employed password security is the usage of a salt value and hashed passwords. This password scheme is found on all UNIX systems as weall as on other operating systems.

the salt has certain features that increase the security of the password scheme

- Different salt values for the same password
  - Salt averts duplicate passwords in the password file
  - Even when two end-users pick the same password, those passwords will be given different salt values.
  - For this reason, the hashed password of the two end-users will be different
- Increase the difficulty of guessing a pasword
  - Salt significantly increases the difficulty of dictionary attacks
  - If salt is of "b" bit length, then the number of possible passwords is amplified by a factor of "2^b".

So, for those reasons, it is understood that the salt increases security

Question

Assuming you have successfully answered the preceding problem and understand the significance of the salt, here is another section. Wouldn't it be possible to thwart completely all password crackers by dramatically increasing the salt size to, say, 24 or 48 bits?

i) answer Protecting the security of the system completely from password crackers does not depend on the salt size but depends on the user population size. Using the hash function of the cipher password and the randomly generated salt and both are stored in the password file. Increasing the size of salt leads to resolve problems of two users having the same salt. *Because, if the salt is the same for more users then the attacker needs to do seperate encryptions for each password of the user* So, increasing the sie of salt through bits, such as 24 or 48, does not protect the security of the system completely from all password crackers.

Question

A relatively new authentication proposal is the Secure Quick Reliable Login (SQRL) described here: `https://www.grc.com/sqrl/sqrl.htm`. Write a brief summary of how SQRL works and indicate how it fits into the categories of types of user authentication listed in this chapter.

i) answer SQRL logs into websites for you. instead of using a username, email, and password, SQRL uses an app to login to SQRL aware sites. When it logs you in it uses a long string of code that looks like: E6Qs2gX7W-Pwi9Y3KAmbkuYjLSWXCtKyBcymWIoHAuo
Your SQRL identity is different for every websitem but its always the same long code for each individual website that you've visited before. this means that websites never know who you are, but they do know when "You'' return.

It seems to me that it is almost like anEncrypted API that acts as a multi factor authentication, but as a single factor authentication. very interesting, and even stores data from the websites within its own crypt instead of letting that data be stored on websites where breaches and such happen. ill be very insterested to see where they go with this, it took 6 years for steve to get it out from the first time he talked about it. and it just came out. but already is getting traction with Os's and Websites alike. and has a setup for shared use authenticator, for sites like netflix, where several people can all login to the same account each from their own setup, but all as the same Netflix account identity.

Question

In general terms, what are four means of authenticating a user's identity?

i) answer

- Something the individual **knows**:
  - a password
  - a Personal Identification Number (PIN)
  - answers to prearranged questions
- Something the individual **possesses** (these are known as tokens):
  - Electronic key-cards
  - smart cards
  - physical keys
- Something the individual **is**(static biometrics):
  - Fingerprint

  - retina
  - face

- Something the individual **does**(dynamic biometrics):
  - voice recognition
  - handwriting characteristics
  - typing rhythm

Question

What are two common techniques used to protect a password file?

i) answer

- **Using a salt** this is stored in plain text with the hash from (salt + password)
- **Password File Access Control** The hashed passwords are kept in a seperate file from the user IDs refferred to as shadow password file. Only priveledged users have access to this file.

Question

Explain the difference between a simple memory card and a smart card.

i) answer

- **Memory Card** stores but does not process data
- **Smart Card** Has a micrprocessor, different types of memory, I/O ports, etc. May also have a cryptocoproccessor and an embedded antenna.

Question

Define the terms false match rate and false nonmatch rate, and explain the use of a threshold in relationship to these two rates.

i) answer

- **False Match Rate** It measures the percent of invalid inputs which are incorrectly accepted.
- **False Non Match Rate** It measures the percent of valid inputs which are incorrectly rejected.

By moving the threshhold, the probabilities can be altered but note that a decrease in false match rate doesn't necessarily result in an increase in false non-match rates, and vice versa

Question

Describe the general concept of a challenge-response protocol.

i) answer The host generates a random number r and returns it to the user (=challenge). In addition, the host specifies two functions, a hash function h() and another f() to be used in the respomse. The user calculates $f(r', h(P'))$, where r' = r and P' is the user's Password. When the response arrives, the host compares the incoming result to the calculated $f(r, h(P))$ and if it matches the user is authenticated. Advantages: Only the hashes of the passwords have to be stored and they do not have to be transmitted directly, so it cannot be captured during transmission.

bonus data

- Linux Encryption Method
  - 12-bit salt to mod DES into one way hash
  - zero value repeated 25 times
  - output translated into 11 character sequence

Chapter 3

Research
Chapter 04

Networking Security **CIT 288**
Spring 2020 Chaz Davis

What is a Trust Framework? Give at least one real-world example of its use in Microsoft or Linux offerings

In digital identity systems, a trust framework functions as a certification program. It enables a party who accepts a digital identity credential (called the relying party) to trust the identity, security, and privacy policies of the party who issues the credential (called the identity service provider) and vice versa.

A trust framework is primarily a legal framework that captures a set of activities and responsibilities of participatin entities in a way that it promotes trust among those entities. Trust framework may or may not be accompanied by technical spec.

Who is OIX? ICF? ICAM? OITF? OIDF? What is the mission of each of these?

- OIDF The OpenID Foundation is an international nonprofit organization of individuals and companies committed to enabling, promoting, and protecting OpenID technologies. OIDF assists the community by providing needed infra- structure and help in promoting and supporting expanded adoption of OpenID.

- ICF The Information Card Foundation is a nonprofit community of companies and individuals working together to evolve the Information Card ecosystem. Information Cards are personal digital identities people can use online, and the key component of identity metasystems. Visually, each Information Card has a card-shaped picture and a card name associated with it that enable people to organize their digital identities and to easily select one they want to use for any given interaction.

- OITF The Open Identity Trust Framework is a standardized, open specification of a trust framework for identity and attribute exchange, developed jointly by OIDF and ICF.

- OIX The Open Identity Exchange Corporation is an independent, neutral, international provider of certification trust frameworks conforming to the Open Identity Trust Frameworks model.

- AXN An Attribute Exchange Network (AXN) is an online Internet-scale gateway for identity service providers and relying parties to efficiently access user-asserted, permissioned, and verified online identity attributes in high volumes at affordable costs

Explain what an AXN does.

- Subjects These are users of an RP's services, including customers, employees, trading partners, and subscribers.

- Attribute providers (APs) APs are entities acknowledged by the community of interest as being able to verify given attributes as presented by subjects and which are equipped through the AXN to create conformant attribute credentials according to the rules and agreements of the AXN. Some APs will be sources of authority for certain information; more commonly APs will be brokers of derived attributes.

- Identity providers (IDPs) These are entities able to authenticate user credentials and to vouch for the names (or pseudonyms or handles) of subjects, and which are equipped through the AXN or some other compatible Identity and Access Management (IDAM) system to create digital identities that may be used to index user attributes.

There are also the following important support elements as part on an AXN:

- Assessors Assessors evaluate identity service providers and RPs and certify that they are capable of following the OITF provider's blueprint.

- Auditors These entities may be called on to check that parties' practices have been in line with what was agreed for the OITF.

- Dispute resolvers These entities provide arbitration and dispute resolution under OIX guidelines.

- Trust framework providers A trust framework provider is an organization that translates the requirements of policymakers into an own blueprint for a trust framework that it then proceeds to build, doing so in a way that is consistent with the minimum requirements set out in the OITF specification. In almost all cases, there will be a reasonably obvious candidate organization to take on this role, for each industry sector or large organization that decides it is appropriate to interoperate with an AXN.

How are capability tickets utilized?

capability ticket A discretionary access control technique organized by subject. For each subject, the capability ticket lists objects and their permitted access rights by this subject.

When it is desired to determine which subjects have which access rights to a particular resource, ACLs are convenient, because each ACL provides the information for a given resource. However, this data structure is not convenient for determining the access rights available to a specific user.

Decomposition by rows yields capability tickets. A capability ticket specifies authorized objects and operations for a particular user. Each user has a number of tickets and may be authorized to loan or give them to others. Because tickets may be dispersed around the system, they present a greater security problem than access control lists. The integrity of the ticket must be protected, and guaranteed (usually by the operating system). In particular, the ticket must be unforgeable. One way to accomplish this is to have the operating system hold all tickets on behalf of users. These tickets would have to be held in a region of memory inaccessible to users. Another alternative is to include an unforgeable token in the capability. This could be a large random password, or a cryptographic message authentication code. This value is verified

by the relevant resource whenever access is requested. This form of capability ticket is appropriate for use in a distributed environment, when the security of its contents cannot be guaranteed.

The convenient and inconvenient aspects of capability tickets are the opposite of those for ACLs. It is easy to determine the set of access rights that a given user has, but more difficult to determine the list of users with specific access rights for a specific resource.

Briefly define the difference between DAC and MAC.

Discretionary Access Control

- the control access is defined based on the requestor identity and the access rule authorizations.
- It permits the requestors only to perform the allowed activity
- The above policy is termed as a discretionary
- Because the entity must have access rights to permit another entity by its own decision
- It enables another entity to access some resource

Mandatory Access Control

- The control access is defined based on comparing the security labels with the security clearances.
- The security label indicates whether the system resource is sensitive or critical.
- The security clearance refers the system entities which are eligible to access the certain resources.
- The above policy is termed as mandatory
- Because the entity may or may not have eligibility to access the resource by its own decision and enable another entity to access some resource.

How does RBAC relate to DAC and MAC?

RBAC is a Role Based Access Control. The user roles are defined within the system and the access allowed based on the given roles.

All three are not mutually exclusive and the access control mechanism can employ two or all the three of the policies to cover different types of system resource.

The RBAC may use the discretionary or the mandatory mechanism for user roles.

List and define the three classes of subject in an access control system.

Access Control System The access control system is embodied in the authorization database. It states the types of permitted access, circumstances for the permission and who are all permitted.

- The access control system defines the three classes of the subject with different access rights:

- Owner
- Group
- World

What is the difference between an access control list and a capability ticket?

Access Control Lists can be simply explained as the mechanism that allows the permission on who can access the object. Capability Ticket refers to the process that shows what objects are allowed to access and what operations are allowed on it.

In the NIST RBAC model, what is the difference between SSD and DSD?

SSD is a constraint of the National Institute of Standards and Technology role based access(NIST RBAC) model. It enables a set of mutually exclusive roles. If one role is assigned to a user from a set, then the user may not be assigned to any other roles from that set. DSD is a constraint of NIST RBAC model. DSD relation is used to limit the permissions available to the user. DSD places constraints on the role which is activated within or across a user's session to limit available permissions.

What is a protection domain?

A protection domain is a grouping of code source and permissions. A protection domain represents all the permissions that are granted to a particular code source. In the default implementation of the Policy class, a protection domain is one grant entry in the file.

UNIX treats file directories in the same fashion as files; that is, both are defined by the same type of data structure, called an inode. As with files, directories include a nine-bit protection string. If care is not taken, this can create access control problems. For example, consider a file with protection mode 644 (octal) contained in a directory with protection mode 730. How might the file be compromised in this case?

If the file's octal code is 644 then that represents

- read and write access for the owner
- read access to the group
- read access to the everyone else

If the directory's octal code is 730 then that represents

- read and write and execute access for the owner
- write and execute access to the group
- and null value access for all other users

Since the file has only read permission for the group and others, the file has no write and execute permissions for the group and others. Whereas the directory has the write and execute permissions for the users group. So, the member of the group may change the content of the file or the file may be deleted. Thus, the permissions given to the file are of no use. The file has read permission for everyone else whereas the directory has no permission for others. Thus, the content of the file cannot be read by the others. The permissions given to the file are of no use.

What is a session?

A session is a temporary and interactive information exchange between two or more communicating devices. A browser may be making a series of http requests and transactions all initiated by the same user. Typically a session is started when a user authenticates their identity using a password or another authentication protocol.

Give a brief overview of credential management.

Credential Management is the set of practices that an organization uses to issue, track, update, and revoke credentials for identities within their context.

Chapter 4

Research
Chapter 05

Networking Security **CIT 288**
Spring 2020 Chaz Davis

What is a relational database and what are its principal ingredients?

Relational database is a set of multiple data organized by tables, records, and columns and it creates the relationship between the database tables.

- the principal ingredients for a relational database
  - the main ingredient is a table
  - the table contains the set of data that consists of rows and columns
  - Rows are reffered as the tuples of records
  - columns are reffered to as attributes
  - the primary key is used for unique identification of a row in a table

How many primary keys and how many foreign keys may a table have in a relational database?

In a relational database. a primary key is a key that is used for identifying and defining the characteristics uniquely for each row. A primary key may have a single attribute or multiple attributes. a foreign key attribute of one table is a foreign key for another table. In a logical way, the foreign key is used to establish a link between two tables.

Explain the nature of the inference threat to an RDBMS.

An inference threat is the process of doing the authorized queries and collect the unauthorized data from the legal response received. it is related to database security. The problem of inference arises from when the grouping of the number of data items is more sensitive than the data item of individual or grouping the data items can be used to deduce the higher sensitivity of data.

What are the disadvantages of database encryption?

There are two difficulties for database encryption:
Key management - only authorized users are allowed to access the decryption key for data. Because, database is typically accessed by a large number of users and applications. So, database encryption is a complex task to provide the security keys to those selected portion of database to authorized users and applications.
Inflexibility - database encryption is more complex to search the records in database when the part of the database or entire database is encrypted.

What is an SQLi? How does one attack using this method?

There are several types of SQL injection attacks: in-band SQLi (using database errors or UNION commands), blind SQLi, and out-of-band SQLi.

Define Defensive coding.

Defensive Coding is developing a system that behaves in a predictable manner despite unexpected conditions or inputs. Defensive coding can generally be broken down into three main areas. Clean Code. Testable Code. Validation.

What is an attribute in a database. Give an example.

An attribute is a characteristic. It is a database component, such as a table. It may be a database field or instances in the row of a database.

Explain cascading authorizations. Is there a ”downside ” to this method of security?

Cascading Authorization is a grant option that allows the access rights to cascade through the multiple users. When the user has an access rights of the grant option to another user. Therefore, passing the access rights of the grant option of certain tables to multiple users in a cascade manner, known as cascading authorization.

What is an in-band attack? Is there such a thing as an out-of-band attack?

In-band SQLi is the most common and easy-to-exploit of th SQL injection attacks. In-band injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results. There is such a thing as Out-of-band injection. Its not very common, mostly because it depends on features being enabled on the database server being used by the web application. Out-of-band injection occurs when an attacker is unable to use the same channel to launch the attack and gather results.

What is ”blind” SQL injection?

Blind SQLi is also called boolean based injection. It is an inferential injection technique that relies on sending a SQL query to the database which forces the application to return a different result depending on whether the query returns a TRUE or FALSE result. Depending on the result, the content within the HTTP response will change, or remain the same. This allows an attacker to infer if the payload used returned true or false,

even though no data from the database is returned. This attack is typically slow since an attacker would need to enumerate a database, character by character.

Chapter 5

Research
Chapter 06

Networking Security **CIT 288**
Spring 2020 Chaz Davis

Briefly describe the four generations of anti-virus software

Anti-virus: The computer software that is used to avoid, catch, and eliminate malicious software is known as anti-virus

- **Four generations:**

  first generation avs is required to have "simple scanners" to determine the malware

  second gen avs is required to have "heuristic scanners" to search for possible malware occassion using heuristic rules or needs an "integrity checking" to determine changed files

  third gen avs is required to have "activity traps" in an infected program to determine malware by its measures rather than its structure.

  fourth gen avs is required to have "Full Featured Protection" This full featured protection uses a collection of anti-virus techniques packages used in conjunction with activity trap components and scanning.

Describe some malware countermeasure elements.

- **Prevention** this measure prevents Mal ware from getting into the system or blocking its capability to change the system through policy, awareness, susceptibility, mitigation, and threat detection
- **Detection** the measure determines the positions of the Mal ware
- **Identification** detects the specific malware that has infected the system
- **Removal** removes all elements of malware virus from every infected system so it cannot propagate further.

What is the difference between a backdoor, a bot, a keylogger, spyware, and a rootkit? Can they all be present in the same malware?

- **Backdoor** it is a secret admission point into a system or program that permits an important person who is concious of the backdoor to get access without going through the common security access procedures
- **Rootkit** collection of programs implemented on a system to sustain secret access to that system with administrator rights, while hiding proof of its presence to the most extent possible
- **Bot** a threat to the network resources and computational of the infected system for use and it is done by the attacker
- **Keylogger** software which records every keystroke on the infected machine to permit an attacker to observe responsive information especially the information that contains the login and password credentials
- **Spyware** an attack that causes the machine to permit observing of the range of action on the system, observing the history and content of browsing action, dynamically changes the data exchange between the browser and websites

Yes, all can be present within the same malware.

What is "Ransomware"?

A type of malicious software designed to block access to a computer system until a sum of money is paid. Files are encrypted. Like an RSA encryption, where the attacker has the unencryption key and until paid you are locked out.

What means can a worm use to access remote systems to propagate?

The mechanisms that worm can use to spread:

- Email or instant messenger
- File sharing
- Remote execution capability
- Remote file access or transfer capability
- Remote login capability

Assume you have found a USB memory stick in your work parking area.

What threats might this pose to your work computer should you just plug the memory stick in and examine its contents? In particular, consider whether each of the malware propagation mechanisms we discuss could use such a memory stick for transport. What steps could you take to mitigate these threats, and safely determine the contents of the memory stick?

When a memory stick is plugged into the computer which was found in the parking area may create a variety of threats to the confidentiality, integrity, and availability of the system
*The memory stick may transmit an ”executable virus” or ”macro virus” on to the system**
Executable virus - Executable program files are affected by machine executable virus and these program files work with specific operating system and in some cases it is based upon the hardware platform.
Macro virus - Files with macro or scripting code are affected by macro viruses and its support effective content in a field of user document types and is translated by an application
*The memory stick may transmit a ”malicious worm”**
Worm - While viewing the memory stick, worm runs automatically and infects other appropriate files as a virus on the system
*The memory stick may contain a trojan horse**
Trojan horse - malicious piece of code that is delivered through the mail or web page or through the USB drives that causes damage to the data or system

Steps to mitigate the problem:

- the user should scan the memory stick with appropriate up-to-date avs
- the user could check the memory stick in a controlled environment.

  for example a live boot linux or emulation environment

Consider the following fragment:

```
legitimate code
if data is Friday the 13th;
crash_computer();
legitimate code
```

What type of malware is this?
The type of malware being used is a logic bomb, which is a key part of data corrupting malware.

- It is code inserted in malware that is placed to ”explode” when certain actions are met
- The actions take place in the given fragment, it checks the data with appropriate day and date that is Friday the 13th
- If the condition is met it calls the function crash_computer()
- For a logic bomb, the example conditions hat can be used as triggers are as follows
- The presence or absence of devices or files on the system
- An appropriate date or day of the week
- Software with appropriate version or configuration
- The application executed by the appropriate user
- Once activated, a bomb may change or delete data or complete files, or other damage

Chapter 6

Research
Chapter 07

Networking Security **CIT 288**
Spring 2020 Chaz Davis

What types of packets are commonly used for flooding attacks?

- **Types of packets:**

  ICMP

  UDP

  TCP SYN

What is "backscatter traffic?" Which types of DoS attacks can it provide information on? Which types of attacks does it not provide any information on?

In computer network security, backscatter is a side-effect of a spoofed denial-of-service attack. In this kind of attack, the attacker spoofs (or forges) the source address in IP packets sent to the victim. In general, the victim machine cannot distinguish between the spoofed packets and legitimate packets, so the victim responds to the spoofed packets as it normally would. These response packets are known as backscatter.

If the attacker is spoofing source addresses randomly, the backscatter response packets from the victim will be sent back to random destinations. This effect can be used by network telescopes as indirect evidence of such attacks.

The term "backscatter analysis" refers to observing backscatter packets arriving at a statistically significant portion of the IP address space to determine characteristics of DoS attacks and victims.

Define a distributed denial-of-service (DDoS) attack.

Denial of service attack is a malicious attempt by an individual or group of people to attack any network or website and abrupt the service for the people who are using those network or websites.

It prevents the authorized use of networks, systems or applications with the help of resources such as memory, bandwidth, CPU and disk space.

Considering your answer from question 3, is a normal DoS attack from a small number of hosts effective in today's bandwidth heavy networks? Why or why not?

Yes, if the attacker employs a basic tactic – more resources wins this game. If they can overload your resources, the attack is successful.

It is quite easy for attackers to achieve their goals. Most website owners are leveraging shared hosts and the ones with virtual private server (VPS) environments are often set up in the smallest tiers and configurations.

This attack can be measured in bits per second.

Volume-based DDoS attacks include:

- **UDP floods**
- **ICMP floods**
- **Ping floods**

So, my answer is, no. The larger the network, the larger the botnet to be used.

Define a reflection attack.

The attacker sends the network packet with a spoofed source address to service runs on the network server and the server responds back to this packet by sending it to the spoofed address that belongs to authentic attack target.

This is referred to as reflection attack
* I the attacker sends multiple numbers of requests attached all with same spoofed source addresses to the number of servers
* The resulting flood of responses for those requests devastates the targets network link. It is the fact that the normal server systems used with intermediaries and if the handling of packets is entirely predictable. Then, these attacks are easier to deploy and harder to trace back to the actual attacker.

Define an amplification attack.

Amplification attack is different from the reflector attack and it is used to transmit a packet with spoofed source address to the target system through mediators.
* After transmission, it generates multiple responses for each original packet transmitted and it is achieved by sending the original request to some other network by broadcasting the address.
Finally, the host on the entire network responds to the request and generates a huge number of responses alternatively it uses service called DNS which generates a longer response than the original request

What is the primary defense against many DoS and DDoS attacks, and where is it implemented?

The main critical component of dos attack is the use of spoofed source addresses

The spoofed addresses both makes it difficult to understand the originating system of direct and distributed DDoS attacks and they are used to direct the reflected or amplified traffic to the target system. So, it is recommended to limit the ability of systems to send the packets with spoofed source addresses.

Implementation

The spoofed address filtering must be implemented and needs to be done close to the source packet with the help of routers or gateways by identifying the valid address range of incoming packets.
Normally, this is the ISP that provides the network connection for an organization or users from home
ISP knows which address belongs to which customers
Therefore, it is best to ensure whether all the packets from the customers use valid source addresses

What defenses are possible against a DNS amplification attack? Where must these be implemented? Which are unique to this form of attack?

For an individual or company running a website or service, mitigation options are limited. This comes from the fact that the individual's server, while it might be the target, is not where the main effect of a volumetric attack is felt. Due to the high amount of traffic generated, the infrastructure surrounding the server feels the impact. The Internet Service Provider (ISP) or other upstream infrastructure providers may not be able to handle the incoming traffic without becoming overwhelmed.

- Reduce the total number of open DNS resolvers By having poorly configured DNS resolvers exposed to the internet, all an attacker needs to do is discover it.
- Source IP Verification Because the UDP requests being sent by the attacker's botnet must have a source IP spoofed to the victim's IP address, a key component in reducing the effectiveness of UDP-based amplification attacks is for ISPs to reject any internal traffic with spoofed addresses.

What measures are needed to trace the source of various types of packets used in a DoS attack? Are some types of packets easier to trace back to their source than others?

There are various measures used to trace the source of various types of packets used in the DOS attack:

- the organization may wish to ask the ISP to trace the flow of packets to identify the source
- If the packets are used with spoofed addresses then it is difficult and time consuming to trace back the packets whereas if they are used with nonspoofed addresses then it is easy to identify the source

Are packets easier to trace back:
No! Traversing is neither easy nor automated, to trace back the source of various types of packets than other packets. This requires cooperation from the network providers to traverse these packets.

Is it always possible to trace the general geographic source of a DDoS attack?

An IP address traceback tasks can be performed in three ways: cache mining mode, online mining mode, and offline mining mode. During this attack, the eight to 12 pieces of DDoS data generated in one hour need to be analyzed and handled at a high speed.

- **High-speed memory mining:** The mined data, saved in the memory, can be quickly invoked and reused for progressive queries.

  Mining a big amount of data consumes a lot of cluster memory. So, the cache mode is applicable only for mining data generated in one day.

  It is recommended that a filter be used to filter the data in advance.

- **Online mining mode:** After mining conditions are typed, a filter will be automatically generated accordingly.

  The filter directly queries the raw flow table without waiting for a cache to be created, thus making query to a specific analysis scenario fast and convenient.

  This mode is applicable to one-time queries of data generated within one day.

- **Offline mining mode:** This can be used for analyzing data generated within more than one day.

  The required data is first queried and then compressed (by combining small files).

  The created physical table is saved in the hard disk for future reuse.

  Due to the big amount of data, conditions should be configured, such as a specified IP address to be queried.