WA Assignment

3180103570 卢佳盈

Q1 Cryptography

a

> What is the difference between symmetric cryptography and asymmetric cryptography?

1. Symmetric cryptography use the same key to encrypt and decrypt, but asymmetric cryptography use two different keys(private key to decrypt & public key to encrypt).
2. Symmetric cryptography uses less time in encryption and decryption than asymmetric cryptography.
3. Asymmetric cryptography is more secure because the transmission from private key to public key is unidirectional.

b

> Given that both types of cryptography can protect security, why should we still need both of them?

Both cryptography has its own advantages and disadvantages.

When we are concerning about security, asymmetric cryptography is better because it does not need the channel to convey the key, which is a problem for symmetric encryption.

But if we need to encrypt a lot of data, we prefer to symmetric cryptography because its cost is lower.

c

> What is the algorithm framework of RSA?

use Alice call to Bob as an example

Generate the keys

1. Alice randomly select 2 unequal prime numbers P and Q, we can assume that $P = 61$ and $Q = 53$
2. Calculate $n = P \times Q = 61 \times 53 = 3233_{(10)} = 110010100001_{(2)}$. (Actually, the length of RSA key is 1024b, even 2048b)
3. Calculate the Euler function $\phi(n)$

$$\phi(n) = (p-1) \times (q-1)$$
$$\phi(3233) = (61-1) \times (53-1) = 3120$$

4. Randomly select a number $e \in (1, \phi(n))$, where e and $\phi(n)$ are coprime. There, we assume that Alice select $e = 17$.
5. Calculate the module inverse element d of e to $\phi(n)$, which means

$$e \times d \equiv 1 \mod \phi(n)$$

   We can use *extended Euclidean algorithm* to get a workable $d = 2753$ with $e = 17$ and $\phi(n) = 3120$
6. Encapsulate (n, e) as public key, (n, d) as private key. For Alice, the public key is $(3233, 17)$, and the private key is $(3233, 2753)$

Encryption

If Bob want to send message m to Alice, he should use the public key (n, e) from Alice to encrypt m. (m should be an integer and smaller than n), which means get the following number c:

$$m^e \equiv c \mod n$$

With the public key $(3233, 17)$ and assuming Bob want to send $m = 65$. We can get $c = 2790$ because $65^{17} \equiv 2790 \mod 3233$. So, Bob send 2790 to Alice.

Decryption

After receiving $c = 2790$ from Bob, Alice should use the private key $(3233, 2753)$ to decrypt it.

$$c^d \equiv m \mod n$$
$$2790^{2753} \equiv 65 \mod 3233$$

Therefore, Alice know the origin message from Bob is 65.

Q2 Cryptography

a

> Given an n-bit password, what is the average trying time for cracking the password using a brute force attack? Provide the detailed derivation.

$$\frac{1 + 2 + 3 + \cdots + 2^n}{2^n} = \frac{2^n + 1}{2}$$

b

> How does a replay attack work? How to address it?

Replay attack is a kind of network attack, which means the attacker repeatedly sends the network packet intercepted from the user to the server, in order to attack the data validity.

We can use timestamp, one-time session key or the way of challenge and response to address it.

c

> How does a man-in-the-middle attack work? How to address it?

Man-in-the-middle attack(MIMT attack) means that the attacker will create independent connections with both ends of the communication and exchange the data of both sides. Both sides of the communication think they are talking directly to each other through a private connection even though it is truly controlled by the *mid-man*. In this case, the attacker can intercept the communication between the two sides and insert new content.

1. The client sends the request to the server and it is intercepted by the mid-man.
2. The server sends the public key to the client.
3. The mid-man intercepts the public key and keeps it in its own hands. Then it will generate a forged public key and send it to the client.
4. After receiving the forged public key, the client generates the encrypted hash value and sends it to the server.

5. The middleman obtains the encrypted hash value and decrypts it with his private key to obtain the true secret key. At the same time, a fake encrypted hash value is generated and sent to the server.
6. The server decrypts with the private key to obtain the false key. Then the encrypted data is transmitted to the client.

Defense ways:

- Use "https" instead of "http".
- Never connect to public Wi-Fi directly and enable the VPN. VPN can encrypts the internet connection to protect the private data when using public Wi-Fi.
- Install a comprehensive internet security solution, that is because MITB always use malware to attack.

d

> How does a relay attack work in wireless communication? How does distance bounding work against a relay attack?

For example, when Alice is trying to send a request to Bob, the attacker can intercept it and replace the request with his own request. Meanwhile, when Bob sends the response to Alice, the attacker can also intercept and replace it.

Distance bounding can help both sides of the communication to check whether the response time is impractically long. For example, if the time is much longer than RTT, which is the theoretically time cost of sending messages between Alice and Bob, the message can be refused.

Q3 Secure Routing

a

> What are the key features of the five typical delivery schemes?

1. Unicast: deliver a message to a single specific node
2. Broadcast: deliver a message to all nodes in the network
3. Multicast: deliver a message to a group of nodes
4. Anycast: deliver a message to any one out of a group
5. Geocast: deliver a message to a group of nodes based on geographic location

b

> What is the framework of the Dijkstra algorithm

1. Initiation:
    - S only contains the source point v, $S = \{v\}$ and distance of v is 0
    - U contains vertices except v
    - If v has an edge with the vertex in U, $< U, v >$ weight the value, otherwise, the value is infinity
2. Select the vertex k with the smallest distance v from U and add k to S.
3. Take k as the new consideration and modify the distance of each vertex in U which distance to v through k is shorter than without it.

4. Repeat 2 and 3 until all vertices are contained in S.

c

> What is the framework of the Bellman-Ford algorithm?

1. Initiation: Set the distance array of all vertices except starting point s to infinity, $d[v] = \text{inf}$, $d[S] = 0$
2. Iteration: Traverse each edge of the graph, relax the two vertices of the edge once, until no point can be relaxed again

   relaxed: Every successful relaxation operation means that we find a new shortest path
3. Judgment of negative cycle: if the iteration exceeds V-1 times, there is a negative cycle

d

> How does prefix hijacking work?

- User Alice wants to connect to website B, attacker Charles says that he has a path to website B, so, request data from Alice will be sent to Charles, but actually he doesn't have a path to B
- User Alice wants to connect to website B, attacker Charles says that he has a path to website B, which is shorter than other paths, so, request data from Alice will be sent to Charles, but actually his path is longer.

e

> How does RPKI work? Why is it insufficient for secure routing?

1. Verify the code number resource allocation relationship by issuing RPKI resource certificate.
2. The autonomous network is authorized to send route origin notification to IP address prefix by issuing ROA. ROA binds the as number of the autonomous network to the IP prefix.
3. The above resource certificates and ROA signatures are stored and published on the publishing point maintained by each Ca, which constitutes the RPKI database.
4. RPKI relying party (RP) is responsible for downloading these certificates and signatures from rpki database on a regular basis, and verifying their validity, so as to obtain the real authorization relationship between IP prefix and as number.

Insufficient because malicious router can pretend to connect to the valid origin.

Q4 DDoS

a

> What is the difference between DoS attacks and DDoS attacks?

DDoS is a method of DoS attack.

DoS(Denial of Service): The purpose of DoS attack is to make the computer or network unable to provide normal service.

DDoS(Distributed Denial of Service): It means that with the help of client / server technology, multiple computers are combined as an attack platform to launch DDoS attacks on one or more targets, thus doubling the power of denial of service attacks.

b

> How does the TCP SYN Flood attack work?

TCP SYN Flood uses a defect of TCP protocol by sending a large number of forged source address attack messages to the port where the network service is located. Therefore, the semi-open connection queue in the target server is full so that other legitimate users will be refused to access.

The attacker will send a large number of TCP SYN packets to the victim in a short time. As long as these SYN packets have different source addresses, the victim (server) will allocate a specific data area for each TCP SYN packet. This will cause a lot of system burden to the TCP server, and eventually lead to the system can not work properly.

c

> How does the solution of SYN Cookies against TCP SYN Flood attacks work?

SYN Cookies uses a special algorithm to generate the sequence number. This algorithm takes into account the fixed information of the other party's IP, port, own IP and port, as well as some fixed information that the other party can't know, such as MSS and time. After receiving the other party's ACK message, it recalculates it to see whether it is the same as Sequence number-1 in the response message, so as to decide whether to allocate TCB resources.

d

> How does the DNS Amplification Attack work? How to defend against it?

DNS Amplification is an asymmetric DDoS attack, in which the attacker sends out smaller query requests with false target IP, which makes the cheated target become the receiver of larger DNS response. With these attacks, the attacker can saturate the network by consuming bandwidth continuously.

Defend:

1. Prepare enough network bandwidth to defend small-scale rainstorm like active attacks
2. Make sure have an emergency number at hand that can connect with the ISP anytime, anywhere. If there is such an active attack, you can always establish contact with the ISP and let them filter out such an active attack in the upstream.
3. Ensure that DNS servers that can be accessed from the external network only implement circular network queries for their own Internet, rather than detailed addresses on other Internet big data.

Q5 Blockchain

a

> What are the key cryptographic techniques used in blockchain? What are they used for therein?

RSA algorithm is the key cryptographic techniques used in blockchain.

For example, if Alice owns a bitcoin and wants to make a transaction to Bob, he will use his private key to make a digital signature on the transaction to prove the authenticity of the transaction.

b

> How is double spending addressed in blockchain?

Double Spending means the same amount of money (digital currency) is paid twice or more.

- If Alice simultaneously puts $sn1$ related Alice Bob and Alice Charlie in Block B , other will easily spot that there are 2 transactions in a block.
- If Alice first pays $sn1$ to Bob, and after a while, pays sn1 to Charlie . Then sn1 appears in two in fields in prev-blocks, others can easily spot it.
- I f Alice pays $sn1$ to Bob, wait till accepted; then repays sn1 to Charlie, compute another longer fork then there appear two forks. Blocks will only follow the longest fork, which means that only one will be accepted.

The block will be accepted until at least 5 more blocks follow it to make the transaction safe.

c

> How does Proof of Stake work and save blockchain from intensive computation?

Before user add a block to the blockchain, he has to find a nonce x, such that $h(blockheader, x) <= target$, this requires intensive computation. And the block is accepted after 5 more blocks follow it, so it has to catch up at l east 5 blocks, which is almost impossible only if attacker controls 51% of total computation power.

Q6 Secure Connection

a

> How does a DNS hijacking attack affect network security?

1. **DDoS attack using DNS server:** Suppose that the attacker knows the IP address of the attacked machine, and then the attacker uses this address as the source address to send the parsing command. In this way, when the DNS server recursively queries, the DNS server responds to the initial user, who is the victim. If the attacker controls enough broilers and repeatedly performs the above operation, the attacker will be attacked by DDoS with response information from DNS server.
2. **DNS cache infection:** The attacker uses DNS request to put the data into the cache of a vulnerable DNS server. These cache information will be returned to the user when the customer has DNS access, so as to guide the user's access to the normal domain name to the page set by the intruder, such as hanging horse, fishing, etc. Or obtain the user's password information through forged e-mail and other server services, causing the customer to encounter further infringement.
3. **DNS information hijacking:** Before the DNS server, the attacker gives the false response to the user, thus deceiving the client to visit the malicious website. Suppose that a packet submitted to a domain name server for domain name resolution is intercepted, and then a false IP address is returned to the requester as the response information according to the interceptor's intention. At this time, the original requester will connect the false IP address as the domain name it wants to request. Obviously, it has been cheated to other places and can't connect to the domain name it wants to connect.
4. **DNS redirection:** If the attacker redirects the DNS name query to a malicious DNS server. Then the resolution of the hijacked domain name is completely under the control of the attacker.
5. **ARP Spoofing:** ARP spoofing by forging IP address and MAC address can generate a lot of ARP traffic in the network and block the network. As long as the attacker continuously sends forged ARP

response packets, the IP-MAC entry in the ARP cache of the target host can be changed, resulting in network interruption or man in the middle attack.

6. **Local hijacking:** After the computer system is infected by Trojan horse or rogue software, there may be abnormal access to some domain names.

b

> What is the protocol framework of HTTPS?

HTTPS adds a TLS/SSL protocol in HTTP.

1. The server generates public and private keys with RSA Algorithm.
2. The server sends the public key to the client in the certificate and self saves the private key.
3. The client checks the validity of the certificate to an authoritative server. If the certificate is valid, certificate to an authoritative server. If the certificate is valid, the client generates a random number, which is used as the communication key. We call it a symmetric key.
4. The server uses key decryption to obtain the symmetric key, and the two parties then encrypt and decrypt the communication with the symmetric key.

c

> How does a user verify a certificate for determining the authenticity of the website it connects to?

1. Check the certificate is issued by a trusted CA
2. Check the fully qualified hostname in the request URL is match to the certificate owner
3. Check the certificate is in valid date range
4. Check the certificate is not in a revocation list
5. Check 1-4 are recursively applied to every certificate in the trust chain

d

> When is a certificate chain required? How to authenticate a certificate chain?

When we need to verify that the CA issuing the user entity certificate is authoritative and trusted, we require a certificate chain. The requirement of certificate chain authentication is that each certificate in the path from the final entity to the root certificate is valid, and each certificate should correctly correspond to the authoritative trusted CA issuing the certificate.

Q7 Wi-Fi Security

a

> What key properties of wireless communication make it more vulnerable to attacks than wired communication?

- Wireless network usually includes **broadcast communication**, which is easier to be eavesdropped and interfered than wired network
- Wireless networks are more vulnerable to **eavesdropping and interference**

- Wireless networks are more vulnerable to active attacks by **exploiting communication protocol** vulnerabilities

b

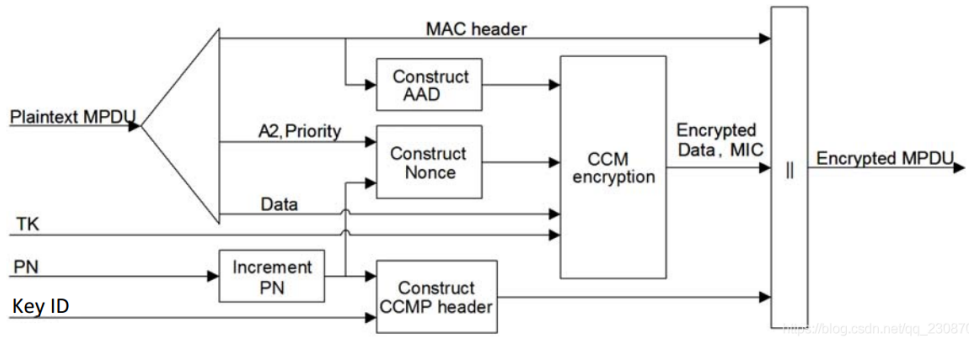
> Why is WEP insecure?

1. WEP can be cracked by packet capture.
2. WEP is cracked by taking advantage of the defects of the encryption system. By collecting enough data packets and using the analytical encryption algorithm, the password can be restored.
3. WEP is the security mechanism of link layer, the decryption process is just a simple negation.

c

> How does IEEE 802.11i provide a higher security guarantee than WEP?

IEEE 802.11i specifies a CCMP data encryption, which is based on the "advanced encryption standard" AES encryption algorithm to implement stronger encryption and information integrity checks.



CCMP Encryption Framework

Q8 Anonymous Communication

a

> Why is current Internet communication vulnerable to anonymity or privacy leakage?

For users communicating over the Internet, their devices are assigned IP addresses, which are usually fixed in one or more communication sessions. It can be used to infer the user's key privacy and the attacker can monitor user's process by easily monitoring the IP address.

b

> In which scenarios do users require the communication anonymity or privacy as concerned in sub-question a?

1. Unmonitored access to health and medical information
2. Preservation of democracy: anonymous election/jury
3. Censorship circumvention: anonymous access to otherwise restricted information

c

> How to use proxies to secure communication anonymity? What are the possible limitations?

How to use: The client first connects with the proxy server, then obtains the required network protocol from the agent, and then establishes the connection through the target network.

Limitation:

1. Need a trusted third party proxy
2. Anonymity largely depends on the (likely unknown) location of attacker
3. The attacker can use flow analysis to discover the sender's real destination

d

> How does Onion Routing provide a better guarantee for anonymity?

Send information:

1. Connect to Tor entry
2. Randomly select a series of Tors
3. Relay messages across them
4. Tor exit relays message to destination

Reply information:

1. Reply traffic from destination traverses the reverse path
2. Maintains a bidirectional persistent multi-hop path between source and destination

In onion routing network, messages are encrypted layer by layer like onion packets, which are sent through a series of network nodes called onion routers. Each Onion Router will decrypt the outermost layer of the packets until the destination decrypts the last layer, so the destination can obtain the original message. Through this series of encryption packaging, each network node (including the destination) can only know the location of the previous node, but can not know the whole sending path and the address of the original sender.

e

> How to infer anonymity or privacy of Onion Routing traffic?

- **Path Selection Attack**: weight nodes by self-reported bandwidth; select each node using weighted probability distribution;
- **Counting Attack**: Correlate incoming and outgoing flows by counting the number of packets.
- **Low Latency Attack**: Tor router assigns each anonymous circuit its own queue; Dequeue one packet from each queue in round-robin fashion.
- **Cross Site Attack**: Search the accounts on public websites

---

Q9 Authentication Efficiency

> Consider a time-consuming authentication scenario where a database records all secret keys of a large number of users. When the system authenticates a user, it first issues a challenge message to the user. The user then uses his/her key to encrypt the challenge and then returns the encrypted challenge to the system. The system then encrypts the challenge using one key in the database after another and compares the result with the received encrypted message. Once a match is found, the

> system accepts the user. Otherwise, the user is denied. This authentication protocol surely takes a lot of time and computation.
>
> Design a possible solution to speed up the authentication process.

When the client responses, it can return its ID and encrypted message back, in order to reduce the calculation time. The system can firstly issues a challenge massage to the user when authenticating, then the user can encrypt the challenge and returns it back to the system with ID. Finally, the system can get the key through the given ID.

Q10 SHINE YOUR WAY

a

> Do you aim for a research output from the course project? To what extent do you devote your time and energy to it? How do you overcome the associated challenges?

Yes, I think I learned a lot from the project with PanZY, ZhenH and TangSZ. Actually, before learning WA, I don't have any experience with Computer Security, so I thank a lot to my teammates for helping me get started cryptography. We reading the related paper together and discuss with each other regularly. With their help, I also learned a lot of basic knowledge of information security, which is like opening the door to a new area for me.

b

> Do you think that you have gradually cultivated a research/security mindset? What is the most useful idea that you learned during this process?

Yes. I think the most useful idea is always being optimistic and encourage myself. In the process of completing the project, we encountered many difficulties. I find it impossible to overcome difficulties when I am in a very negative state.

c

> Provide an example to showcase how you leverage that useful idea to facilitate problem solving in study or life.

I used to be a very negative person. In the last semester, I even fell into excessive anxiety and self doubt, when I think I cannot do anything well and I won't have a good future. But in kg's class, I feel the power of optimism inexplicably. I can tell myself "xixi" when I'm in trouble, also I can use "wow" to encourage myself when I have finished some work. In addition, I also began to try to show myself. All thanks to Kg as well as all friends in WA class.

Question Designed

a

> Which topic among the lectures you would like to consider?

DoS attack

b

> Describe a (sufficiently complex) question.

In order to implement the classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity if the link to the target organization. Consider an attack using ICMP echo request(ping) packets that are 500 bytes in size(ignoring framing overhead). How many of these packets per second must the attacker send to flood a target organization using a 0.5Mbps link? How many per second if the attacker uses a 2Mbps link? Or a 10Mbps link?

c

> Provide also a correct sample solution.

0.5Mbps:

$$\frac{0.5Mbps}{500B/packet} = 125packets/s$$

2Mbps:

$$\frac{2Mbps}{500B/packet} = 500packets/s$$

10Mbps:

$$\frac{10Mbps}{500B/packet} = 2500packets/s$$