# Sample midterm

1. (4 pts) What is IP spoofing? Give an example of at least two uses of IP spoofing by an attacker – how is it used and what advantage does it provide to the attacker.

* IP spoofing is faking the source IP address in packets
* Attacker spoofs his source IP to avoid blame for an attack. Any value can be used as fake source IP (randomly chosen).
* Attacker spoofs one specific IP to place a blame for the attack on that host.
* Attacker performs reflector DDoS attack, spoofs IP of the victim in pkts sent to some servers.
* Attacker spoofs one specific IP that has a trust relationship with victim, with the goal to establish TCP session and use the trust relationship.
* Attacker spoofs one or few IPs that are allowed through the firewall, during his intrusion attempt – sending some exploit through, with fake source IPs.
* Attacker can do a replay attack with some content he’s captured. The IP address is the original source IP in packets (pretty much he’s just repeating what he captured, header and contents).

1. (8 pts) Define the three aspects of security, each in one sentence, and provide an example of a threat and a defense for each aspect.

* Confidentiality – allowing authorized users to access data or resource. Threats = Man in the middle, sniffing, intrusions, breaking crypto. Defenses = encryption is the most frequent defense. For MITM, it matters that we secure key exchange and then encryption works.
* Integrity – data content or some system has not been modified by attacker (behavior or content are as intended by creator). Threats = MITM, changing of data, deleting data, DDoS when the system slows down or crashes, rootkits. Defenses = hashing to detect content modification, signing hash with private key or shared key, DDoS defense, disallowing loadable kernel modules.
* Availability – data or service is available to legitimate users with good QoS. Threats = DDoS, deleting data. Defenses = any DDoS, replication of data.

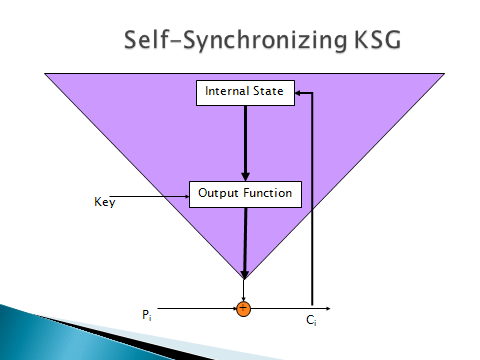
1. (3 pts) What is a polyalphabetic cipher?

Uses multiple mappings, first character is changed to another character using the first mapping, the second character is changed using the second mapping, etc. and then we cycle back when we ran of mappings.

1. (10 pts) Describe how symmetric and asymmetric cryptography work and discuss how their functionalities and costs compare.

* Symmetric: one key is used to encrypt and decrypt. Both parties have the same key.
* Asymmetric: both parties have their private and public key. We can encrypt with public key and decrypt with private or the other way around. We must use keys from the same pair.
* Symmetric crypto: achieves integrity, confidentiality, authentication.
* Asymmetric crypto: achieves integrity, confidentiality, authentication, non-repudiation, encrypting a message so m out of n people can read it, encrypting a message so m people can read it only if they all agree.
* Costs: symmetric is much faster (1500 times). In a group of people we have n\*n keys for symmetric crypto, 2\*n for asymmetric crypto. Symmetric key exchange is performed on demand or out of bounds or there is KDC. Symmetric keys change often, per session, to preserve strength of crypto. Asymmetric key exchange can be performed any time before communication, and it can be in bound (using certificates). Asymmetric keys change rarely (on compromise), can be reused.

1. (10 pts) Draw an architecture of a self-synchronizing key stream generator and explain how it works. What happens if a bit is lost or added to the ciphertext? What happens if a bit is modified in ciphertext?



Bits of ciphertext are returned to the internal state, and bits of internal state are shifted. Internal state or output function depend on the key. Plaintext bits are combined with the output of the KSG. If a bit is lost or added to ciphertext, the generator synchronizes back when the change (loss or addition) falls out of the internal state – if the state is n bits, it synchronizes back after at most n steps. If a bit is modified in cyphertext, this affects n bits of the output, then the generator synchronizes back.

1. (10 pts) Explain how a Diffie-Hellman key exchange works and what makes it hard for a sniffing attacker to learn the key. Does Diffie-Hellman key exchange produce a key for symmetric or asymmetric cipher?

Sender and receiver agree on modulus and base, each chooses a random number known only to that party. Each side takes the base, raises it to the random number, does mod operation and sends the result to the other party. The other party takes this message, raises it to their random number, does mod operation – they both end up with the same key. This is a symmetric key. Attacker doesn’t know random numbers used by the algorithm. To find them he can only use brute force attack because discrete log operation is hard (If you know base B and modulus M, and you don’t know the exponent E – it’s hard getting the exponent from (B^E mod M) – there are no shortcuts.

1. (10 pts) Describe how a server can authenticate a client using a symmetric cipher. How can this be done using an asymmetric cipher? Which approach is better and why?

Server sends a challenge – either random number R or encryption of R – the receiver returns encryption of R or R. In symmetric crypto case one key is used by both parties. In asymmetric crypto the server uses client’s public key. Asymmetric crypto approach is better because it needs no prior trust, nothing is lost if server is compromised.

1. (10 pts) Explain how does Passport service work for single sign-on.
2. Client asks for service from server S
3. Server redirects client to Passport server P
4. P authenticates the client (asks for username/pass for P)
5. P gives client a ticket to the server S (identification or some assertion about the client encrypted with a key shared between P and S)
6. P sets cookies at client
7. Client gives the ticket to S
8. S sets cookies at client

Next time client accesses S, none of the steps are needed. Client just gives the server’s cookie to S. Next time client accesses another server step 3 is not needed because client just gives passport’s cookie to P.

1. (10 pts) How does discretionary access control work? How does mandatory access control work? What are the advantages of one over the other?

Owner controls access to resources in discretionary access control, access control rules speak about each user and each resource. Each user has a clearance level (or classification) each object has a classification, access control rules speak of how to match clearance level to classification, sysadmin sets the rules and the classifications. Discretionary AC is very simple (flexible) – work at fine grain level, add/modify rules whenever new user or resource appears (bad for scalability). Mandatory AC is not very flexible, it is coarse grained but it scales better. (just talking about one of those features – flexibility, fine/coarse grain, scalability is fine)

1. (10 pts) The sample network below should be protected from DNS-based reconnaissance. Web and DNS servers run public services and should be accessible both by internal and external clients, while DB and E-mail server should be accessible only by internal clients. What approach will you use, what changes must be done to your network, what information should be on DNS server(s)? How this all helps protect you from DNS-based reconnaissance?

We’ll use split-horizon DNS. Need another DNS server to be the public server, our current server becomes private DNS server. Web server will have private and public interface. The public DNS server only knows about public Web server’s interface. The private DNS server knows about public DNS server, private Web server’s interface, DB and email servers. External clients know public DNS server’s name. Internal clients are statically configured with private DNS server’s IP. This helps because public DNS only knows about public services and private DNS is not advertised and should also be behind a FW.