Home Work 2 :

True/False :

1. SHA-3 provides message authentication : True
2. Salting and hashing stored passwords mitigates precomputed offline dictionary attacks : True
3. TCP syn-cookies mitigate memory exhaustion DDoS attacks : True
4. There is a proof that AES provides confidentially against a computationally un constrained attacker : False
5. It is difficult to blindly spoof an IP source address : False

Short Answer :

1. Authentication

Your NYU ID card contains many different factors which may be used for identification, authentication, or authorization. Describe three scenarios in which your NYU ID card is used for each of these. For each scenario, answering the following: (4 points for each scenario)

(a) Which of identification, authentication, and authorization is involved :

- Identification : When an individual presents the ID card at the front desk of the department and claims that he/she is somebody. For eg. I go to the counter and claim that I am Ishita Verma. This is Identification. In this scenario we will be providing our NYU ID card at the front desk.
- Authentication : In Authentication, the other person would verify you are who you are claiming to be. In this scenario, NYU ID information such as university id and Net id will be matched against the NYU database when you swipe your card on the system.
- Authorization : Authorization is the step that happens after identification and authentication. Once you are identified and authorized you are allowed to do what you are supposed to do. In this scenario, if an individual university id and net id is matched with current database, he/she will be allowed to enter the university.

(b) What factors are involved (something you have/are/know/can do)?

For identification student or faculty member should have their NYU ID card, which has University Id and Net Id for claiming their identity. For authentication, you should be currently enrolled in the university, then only your information is going to be matched with current database. Once a student is identified and authenticated, he/she can enter the university and attend his/her respective department classes.

(c) How secure is the security in this scenario? How bad would it be if the security were to be compromised? How likely is it that such an attack would occur? Given these, do you consider the security in place to be sufficient, or do you think the costs of increased security (in terms of money, hassle, etc) would be justified?

The current security system is not sufficient to properly identify and authorize a student or faculty member because there is no biometric recognition involved in the system. For instance , in case of identification, a fake user can swipe the ID at the system, and he/she will be allowed access inside the university, since there is no face recognition or thumb print or retina scan involved. A student or faculty member might lose his/her ID card or the card might get stolen and the malicious user can easily get identified and authenticated, because he is using the NYU ID card of a valid student/faculty member.
Other scenario might include the bar code or the magnetic chip of card getting destroyed which might cause issue while authenticating the user.

2. Cryptography

a. What are the three main classes of security properties that cryptographic techniques offer? What security properties does each of these cryptographic algorithms offer RSA Signature, SHA-3, and AES? (6 points)

Three main classes of security properties that cryptographic techniques must offer are :

1. Confidentiality : Confidentiality means privacy of data. Confidentiality measures are taken to protect the privacy of data, so that it does not reach to wrong people. Data encryption is a common method to ensure confidentiality. A good example would be providing account number or routing number while doing online baking.

2. Integrity : Integrity involves maintaining the consistency, trustworthiness and accuracy of data over its life cycle. When sender sends any data to receiver, it should not be altered by any unauthorized user. Version control might be used to prevent erroneous changes. Some data might include checksums or cryptographic checksums to ensure integrity of data.

3. Availability of data for authorized use : Availability means the system should be available for use by the users all the time. To ensure availability the hardware should be rigorously maintained, performing hardware repair immediately when required. Availability can be hindered by DDoS attack. It's a malicious attempt to bring down networks or other services by overwhelming these resources with too much data or impairing them. This makes devices unavailable for authenticated users.

Security Properties offered by following Algorithms :

1. RSA signature :

- Authentication : To ensure the message is sent by known sender.
- Integrity : The message has not been altered in transit.
- Non-Repudiation : Sender can not deny having sent the message.

2. SHA-3 :

- Integrity : SHA-3 algorithm converts a digital message into a short "message digest". Even a small change in the original message creates a change in the digest, making it easier to detect accidental or intentional changes to the original message.

3. AES :

- Confidentiality : AES uses block cipher to protect classified information.

b. What is the primary weakness of the ECB block cipher mode of encryption? Describe how the CBC block cipher mode of encryption mitigates this flaw? (2 points)

The main weakness of ECB block cipher mode of encryption is that it is not semantically secure. ECB encryption technique involves mapping of identical message blocks into identical ciphertext blocks. If the same message block is encrypted multiple times , it can cause problem and reveal the whole message to attacker if he is able to decrypt the cipher blocks.This can cause a problem because it does not provide message confidentiality.
By analysing the patterns an attacker can deduce properties. CBC (Cipher Block Chaining) is a better version of block cipher encryption. Cipher Block Chaining uses what is known as an initialization vector (IV) of a certain length. One of its important feature is that it uses chaining mechanism that causes decryption of cipher blocks dependent on preceding cipher blocks. This

adds an extra level of complexity to the encrypted data and if you are missing a few blocks in the sequence it becomes impossible to encrypt.

Paper Reviews :

1. Produce a one-page summary of the paper below. In your summary included the novel contributions of the paper beyond prior work, the practical implications of their findings, and a concise summary of the methods of how they conducted their exploration of the problem. (10 points)

This paper throws light on the weakness of Diffie Hellman Key Exchange Algorithm. It is not as secure as it is believed. Diffie Hellman Key Exchange is widely used to establish session keys in IP (Internet Protocol). SSH, IPsec and TLS use Diffie Hellman as key exchange mechanism. Sender and Receiver agree on a prime p and a generator g of a multiplicative subgroup modulo p. By computing discrete logs an attacker can easily find out the shared key. If the attacker makes single large precomputation on p, he can break all Diffie Hellman Exchange made with that prime.

Number Field Sieve is the most efficient discrete log algorithm. It has four different stages. First three stages are dependent on p and involves most of the computation. First stage is polynomial selection, in which a polynomial f(z) is found defining a number field Q(z)/f(z) for the computation. The runtime is very small for this stage. The Second Stage is sieving, one factors ranges of integers and number field elements in batches to find many relations of elements, all of whose prime factors are less than some bound B (called B-smooth). In the third stage, linear algebra, a large sparse matrix consisting of the coefficient vectors of prime factorizations is constructed. The final stage, descent, actually deduces the discrete log of the target y. The first three stages can be done once for a prime p and be repeated for different targets. There are numerous parameter which determines the running time of NFS. Trade off at certain stage will make other stages computation cheap, for example sieving more will result in a smaller matrix, making linear algebra cheaper. These trade offs can quickly compute 512 bit discrete logs and man in the middle attack can be performed on TLS.

TLS most commonly use Diffie Hellman as key exchange mechanism and uses 1024-bit prime. Small number of servers still support legacy “export-grade” Diffie Hellman, that uses 512-bit prime. This fact can be used to perform Logjam attack. The Logjam attack allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography. This allows the attacker to read and modify any data passed over the connection.The attack affects any server that supports DHE_EXPORT ciphers, and affects all modern web browsers. When the experiment was carried on for three 512-bit primes, the

precomputation took 7 days and then the median was of 70 seconds for computation of individual logs.

There is existence of practical attacks against Diffie-Hellman key exchange as currently used by TLS. However, these attacks rely on the ability to downgrade connections to export-grade crypto or on the use of unsafe parameters. The NFS can be extended to attack 768-bit and 1024-bit Diffie Hellman as well. Following protocols will be affected if 1024-bit group were broken : HTTPS (Top 1 Million Domains), HTTPS (Browser Trusted Sites), SSH (IPv4 Address Space), IKEv1 (IPsec VPNS).

Following methods can be used to recover security of Diffie Hellman exchange mechanism, as it used in many mainstream Internet Protocols. Like transition to elliptic curves, increase minimum key strengths, avoid fixed-prime 1024-bit groups and don't deliberately weaken crypto. On the mail Server , the support for export cipher should be disabled and use a 2048-bit Diffie-Hellman group. On the browser, we need to make sure the the latest version are installed and status are checked frequently.

In conclusion, Diffie Hellman is widely used algorithm but it is not as secured as it is supposed to be. So, people need to be aware and work on making their algorithm more secure, so that the system are not vulnerable to attack.

2. Produce a one-page summary of the paper below. In your summary included the novel contributions of the paper beyond prior work, the practical implications of their findings, and a concise summary of the methods of how they conducted their exploration of the problem. (10 points)

This paper discuss about the Mirai Botnet, which emerged in 2016 and startled the internet. It's target were very high profile and this was carried out using DDoS attack. In this paper, author have discussed the rise of Mirai Botnet and effect it had on fragile IoT ecosystem. IoT malware can be very harmful as it could sway access to compromised routers for ad fraud, cameras for extortion, network attached storage for bitcoin mining etc.

The Mirai botnet attack started to appear in early 31 August 2016 and it grabbed headline in mid september 2016. One major event in timeline of Mirai Botnet is release of it's source code. Mirai Botnet targeted devices that run on SSH and telnet. It scans the IPV4 address of the devices and then makes attempt to login in to hardcoded dictionary of IoT. Once it is successful in its

attempt to acquire this information, it sends IPV4 and it's associated credentials to a report server. The Server then asynchronously triggers the loader and infects the device. The Active Mirai attack was carried on Censys, it actively scans the IPv4 address of the devices and collects the data application layer data about hosts. The analysis mainly focused on protocols such as HTTPS, SSH, FTP and Telnet. Mirai first disables outward facing services such as HTTP on attack, so that the devices which are being affected can not get detected. Out of all the devices which were detected , the largests used HTTPS protocol and least used SSH prompts.

Upon the release of Mirai source code many copycats started their own variant of Mirai Botnet. To track the proliferation of Mirai Variants , infrastructure clustering was used.Reverse engineering was implemented for tracking down the variants all trying to leverage the vulnerable IoT. The result showed that multiple variants of Mirai were active simultaneously. The Original Mirai Botnet targeted Kreb and OVH. Mirai largest instance tried to target DYN and other gaming sites. Mirai, third largest variant African telecom operators.

The prevalence of insecure IoT devices on the Internet are the sought target of DDoS attacks.
Mirai and its variants can be averted if best internet security practises are used. Following should be implemented by IoT device makers : Eliminate default Credentials, this will prevent hackers to create a credential master list that allows them to attack number of IoT devices. Auto Patching should be made mandatory. Rate implementing should also be implemented, so that brute force attack can be prevented.