**CPSC525 Assignment2**

Jiashan Li 10171607

Q1. Word Count: 233 Bishop, chapter 12, 12.2.3, 12.2.5.

In my opinion, the open source development model promotes the security of a software. Firstly, the principle of open design indicates that the security of a mechanism should not depend on the secrecy of its design or implementation. Even you cryptograph the source code, the attacker could even find it by searching through garbage receptacles or find the vulnerability by analysis. Secondly, based on the principle of economy of mechanism, which is defined as security mechanisms should be as simple as possible, we find that cryptographic software is pretty complicated to develop cause cryptography is a highly mathematical subject. So it against this design principle. Since the source code is public to everyone, more people can inspect the source code to find and fix a possible vulnerability. This can lead to both faster discovery of unintentional security vulnerabilities and prevention of intentional vulnerabilities in the code put there by the developers themselves. Because the code could be seen by others, it forces people to write more clear code, and to adhere to standards. In this way, the there will be less mistakes and bugs exist in the code. Also, the end-user of open source code has the ability to modify source to implement any extra features of security they may wish for a specific use. In conclusion, It is much better to use the open source design pattern to improve the software security.

Q2. Word Count: 253 Pfleeger et al, Section 2.1, P40

The text based password and the non-text based password for Android phone is the most common authentication mechanism to unlock the screen. The non-text based password requires the user to tap symbols within a randomly generated matrix or a sequence of points on a photo. Certificates are another popular authentication mechanism we use, when you want to log into your account, it will send you an email or test message based on the email address and phone number you bind when you register the account to let you to confirm. A Smart card is a security chip, embedded in a credit card or badge. That chip provides safe storage for cryptographic keys used by authentication and encryption algorithms. When the user input the card, the phone or the laptop will know it is the owner. Biometric authentication covers fingerprints, voiceprints, iris scans, handwritten signatures are also used when user would like to unlock the phone. This one, in my opinion, is the safest way to identify no one will do this instead of the owner. There are some authentication based on proximity. Smartphone may stay unlocked indefinitely while communicating with the user’s Bluetooth headset. permitting connections with mobile devices that pass through a checkpoint and denying connections outside that area. In these four authentication mechanisms, the password is based on something the user knows. Certificates, Smart card and proximity based on something the user has (like a phone number or a connected Bluetooth). And the handwritten signature based on something the user is.

Q3. Word Count: 226 Gollman, Chapter6.

The operating system has a lot of methods to utilize modern computer architecture to enhance security. For example, operating system can decide the access control. It implements both the underlying tables supporting access control and the mechanisms that check for acceptable uses. Making objects safe from users who do not have rights. Another example is the virtualization, in which the operating system presents each user with just the resources that class of user should see. So if the user A only has the right to access data A, so he is unable to get to, or even know the existence of B resources. Under this condition, B resources are safe. Another way is separation and protection, it means the operating system keeps one user’s objects separate from other users. With this form of protection, the owner of an object could declare if the object is public, if it is not, no one can access it except the owner to make the object safe. The operating system can also deal with hardware and memory protection. A fence is use to prevent a faulty user program from destroying part of the resident portion of the operating system. Another way to protect memory is dividing a program into many small pieces. OS maintains a table mapping segment id to physical address. In this way, Physical addresses cannot be forged.

Q4. Word Count: 247 Pfleeger et al. Section 2.2 after p80

The Access Control List is a representation of a column of the access control matrix which shows what kind of right does the subject own to deal with the object. It is Efficient to find out all the accesses that can be performed over a given object. There is one such list shows all subjects who should have access to the object and what their access is. And there are some significant advantages to this approach. The access control list representation can include general default entries for any users. In this way, specific users can have explicit rights and all other users can have a default set of rights. With this organization, all possible users of the system can share a public program or file without the need for an entry for the object in the individual directory of each user. A Capability List is a representation of a row of the Access Control Matrix. It is efficient to revoke all access rights of a user. The advantage of a Capability List is ease of revocation. If the user is removed from the system, the Capacity List shows all object to which the user access so that those rights could be removed easily and make the list clear. The Capability is an unforgeable token that gives the possessor certain rights to an object. It provides better support for least privilege and prevent the confused deputy problem. Also it eliminate the need to refer to objects by name.

Q5. Word Count: 226 Pfleeger et al.Section 3.1

Stack smashing and heap corruption are both buffer overflow vulnerability. So they are both serious problems of security. Firstly, they can both lead to privilege escalation, the attacker may replace code in the system space, in this way, the attacker regains control from the operating system, possibly with raised privileges. Secondly, they can both be produced by a memory overwriting, most people accidentally put one more element in an array or append an additional character into a string. However sometimes even worse, malicious exploitation of buffer overflows occurs. Not only does the attacker overrun allocated space, but the attacker also uses the overrun to execute instructions to achieve the next step in the attack. Thirdly, stack smashing and heap corruption can both occur with many kinds of data, ranging from arrays to parameters to individual data items, although some of them are easy to prevent, such as checking an array’s dimension before storing, most of them are hard. Because they are both buffer overflow problems, they occur because attacker can write directly to particular memory addresses and language and compiler allows inappropriate operations on certain data types. They can be solved and protected by code analyzers, which could help to detect unsafe conditions. Also we can enforce containment to avoid them, such as separating sensitive areas from the running code and its buffers and data space.

Q6. Word Count: 228 Smith & Marchesini, 6.1 P131

I think the stack smashing is a pretty serious problem in security vulnerability and the address randomization is an important way to deal with it. It prevents an attacker from using the same attack code to exploit the same flaw in multiple randomized instances of a single software program. The workers should go through the knowledge of the Linux patch PaX Project. PaX randomly offsets the base of the stack in increments of 16 bytes, combining random placement of the actual virtual memory segment with a sub-page stack gap. Pax also optionally randomizes the mmap() base and the executable base of programs. This substantially lowers the probability of a successful attack by requiring the attacking code to guess the locations of these areas. When

Randomized mmap() base is enabled, PaX randomly shifts the mmap() base, affecting the positioning of all libraries and other non-specific mmap() calls. Attackers requiring a function in a certain library must guess where that library is loaded in virtual memory space to call it. This makes return-to-libc attacks difficult. When combining a non-executable stack with mmap() base randomization, the difficulty in exploiting bugs protected against by PaX is greatly increased due to the forced use of return-to-libc attacks. In conclusion, PaX is an essential way to realize the address randomization and workers should be familiar with all procedures in PaX to adopt address randomization.

Q9. Word Count: 456

On October 21 2016, Dyn received a global DDoS attack on its DNS infrastructure. DNS is an essential component of all Web sites, anytime you send an e-mail or browse a Web site, your machine is sending a DNS look-up request to your Internet service provider to help route the traffic, so this attack makes people feel hard to access websites. The DDoS attack overwhelms a DNS server with lookup requests, rendering it incapable of completing any. That’s what makes attacking DNS so effective. Rather than targeting individual sites, an attacker can take out the entire Internet for any end user whose DNS requests route through a given server. In this serious attack, more than a dozen major websites experienced outages and other technical problems. They included The New York Times, Twitter, Pinterest, Reddit, GitHub, Etsy, Tumblr, Spotify, PayPal, Verizon, Comcast, EA, the Playstation network, and others. DDoS enables multiple machines to generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and shut down. Typically, computers become bots when attackers illicitly install malware that secretly connects the computer to a botnet, attackers then perform tasks such as sending spam, hosting or distributing malware, or attacking other computers. The DDoS attacks work in phases. In the first phase, the attacker compromises the weak machines in the network from around the world. In the second phase, a set of tools is installed on the compromised systems to attack the victims by controlling them from a C&C server. This, after all, will end up completely crashing a website for periods of time. The type of DDoS this time is called Flood or volumetric attacks, which seeks to consume all the available bandwidth of or to a data center or a network, such as UDP floods, ICMP floods and DNS reflection. As a result, the legitimate user is no longer able to connect or access the desired servers or applications. DDoS attacks are increasing in frequency and impact. Inherent limitations in today’s infrastructure make DDoS a very realizable risk. The attack not only cause inconvenience to the users to access the website, the most serious impact is organization suffer a financial and brand perspective loss. The company brand and reputation damaged, contract and violations of service level agreements breached, shareholder confidence lost. In conclusion, DDoS attacks are largely adopted in cyberwarfare to hit a country’s critical infrastructures. Enterprises must pay attention to this threat and properly assess their environment and monitoring capability to protect and defend against these aggressive attacks. As DDoS attacks continue to evolve, it is critical not to underestimate the threat.