Student Name 1: Damayanti Deb
Student Name 2: Shane Crowley
Student Name 3: Pedro Ruiz

"Critical Infrastructure Security: The Emerging Smart Grid"

Final Exam: Spring 2012

1. Choose one real distributed application program that you are familiar with. Write the following…

Bittorrent is a P2P architecture application that allows for the sharing of files through the use of peers and seeders. Seeders are those users who have a complete file, where as peers only have small parts of a file. The way this application works is a user who wants to share a file, makes use of a tracker which manages connections between peers and generates a torrent file. This user then seeds the file (using the bittorrent file) and then ensures that the generated torrent file is in a location that others can download. The users use a bittorrent client installed on their machine to begin the file transfer. The file when downloaded is broken into small portions and through the use of hashing we can verify the download for each piece of the file completed without errors. As a result of the file being broken into small pieces, it is easier to resume later. Bittorrent also allows for pieces of a file to be skipped if they are not available, so that other portions of the file can be downloaded right away.

In the case of bittorrent, there is only one server, the tracker with everyone else being one of the clients. The tracker (server) manages connections between peers, although there are some trackerless torrents which make use of a distributed database. The tracker accepts requests from new clients and provides them with connection information to begin the downloading process. The clients are split into seeders and peers, the seeders do not issue requests since they have every piece of the file, but receive them and when a certain piece of the file is requested, they send that to the requesting peer. The peers on the other hand must receive and request various portions of the file they need or another peer needs that they have previously downloaded. The only processing that takes place would have to be the internal workings of bittorrent, such as hash checking, determining if we have a piece of file that another peer needs, determining what should be the next piece of file to download from another peer next and which pieces we should skip.

The great thing about bittorrent is there are not many runtime issues. We do not need to worry about low latency as bittorrent is not latency sensitive, high bandwidth is not needed in a P2P architecture, but rather enough peers to seed the file with no more than a cable internet connection. As a result of bittorrents hash checking, we do not need to worry about perfectly consistent/correct replies/answers/service. As for the worst possible limitations that bittorrent could accept, bittorrent was intended to mitigate poor latency, this "Low latency network connections" is irrelevant. As for "High bandwidth available", most of the people on the internet use Cable so for files 25MB and greater I would say you need at the very least a Cable internet connection, dial up modems are too slow but could be tolerated as a last resort, especially for smaller files (assuming there are not better peers to select from). As bittorrents hashing is pretty effective I'd say that as long as there is not a peer transmitting false data intentionally, a solid 5-

10Kb/s correct packets would be reasonable. In summary I'd like to say that bittorrent was designed to mitigate against latency problems, the need for high bandwidth and consistent data being transmitted, and it can deal with pretty much anything that is thrown at it, as long as the transmitted data is legitimate and there are a at least a few peers with high speed connections as peers or seeds.

2. Explain in a paragraph or two in your own words the analogy "Middleware is to socket programming what high-level language programming is to assembler programming".

In order to answer this question we need to define middleware, socket programming, high level languages and assembly programming. Middleware is something that sits between the Application and OS Layer, hiding the details of the OS from the application, allowing for a programmer to make use of local and remote resources through APIs (RMI) using a standard interface. Socket programming is where we open an object or resource in some manner in order to make calls of some kind. A good example of this might be int fd = fopen(FILE, MODE), where a file descriptor is opened by the operating system, then passed to the application, in relation to middleware our file descriptor might be a call to an object via a RMI or something similar to the xml-api framework to make calls to remote objects. High level languages we must keep in mind do not technically exist, we can think of these as Java/C#, these high level languages have variable declarations, functions and other statements converted to assembly programming which are then executed by the machine after being compiled.

The meaning of "Middleware is to socket programming what high-level language programming is to assembler programming" would have to be that middleware and high-level languages depend on socket programming and assembler programming in order to function. We can think of this in terms of independent and dependent factors with middleware and high-level languages being dependent and socket programming and assembler programming being independent. The reason this is true is because middleware is something that hides the internal functionality, so when we make a socket call from our application through a standard format the middleware takes over, communicates with the OS, establishes the connection to a remote server, fetches and returns the data and then even handles the closing of the connection for the remote internet connection and closing the OS file descriptors. The great thing about this would have to be making things easy for programmers, as the hard part is handled by the middleware through a socket call from an application. High-level programming languages are dependent on assemblers to function, as the high level languages do not exist, but are for the most part compiler tricks, with each class and variable being converted by the computer to assembly code before execution. In summary, the analogy is stating that although middleware and high-level language programming are taking over by making programming easier and easier with every iteration for developers and allow for a greater level of stability as a result of so much being done for the programmer already, they are still dependent on the same technology they are trying to replace.

3. Which of the following is false for a NASPInet-like critical infrastructure data delivery service for a power grid:
A. The scale is such that tracking per-flow state at a router (or similar forwarding device) is feasible.
B. The admission control perimeter can be complete.

C. Post-error recovery is sufficient.
D. The predictability of the delivery latency, even in the presence of a small (bounded) number of failures, is very good or better.

4. Which of the following is more burdensome for the application programmer:
A. Remote procedure call
B. Publish-subscribe
C. Remote method invocation
D. Request-reply protocols

5. Which of the following is space-uncoupled:
A. Remote procedure call
B. Publish-subscribe
C. Remote method invocation
D. Request-reply protocols

6. Which is not either a motivating observation or a property provided by P2P systems (i.e., what is false):
A. Compared to exploiting in-network logic, the same level of multicast efficiency and very low delivery latency is achievable (even in the presence of a few faults).
B. CPU/GPU and storage resources are often more abundant "at the edges" of a distributed system.
C. A much larger address space can be handled compared to IPv4 or even IPv6.
D. Using only edge resources means that deployment is much simpler than if in-network logic (e.g., GridStat forwarding engines) were required.

7. Which if the following challenge for the bulk power grid can not be mitigated with much better wide-area communications (and sensors feeding it):
A. The different physics of some kinds of renewable power (e.g., no reactive power) and how that changes the dynamics of a grid at large.
B. Negligible storage of power in the grid.
C. Large numbers of retiring operators who are leaving with a lot of institutional knowledge—intuitive "seat of the pants" understanding—of how their grid operates in many contingencies or unusual situations (and combinations thereof).
D. Increasing stress on grid due to insufficient new transmission capacity compared to increases in both generation and load.

8. Tripwire is a software tool intended to assure integrity of system files by detecting unexpected modifications (such modifications are often a sign of rootkit activity). One version of Tripwire reads the names of the directories to be protected from a configuration file. For each file in the specified directories, Tripwire computes its hash value and stores it in a database. What property must this hash function have?
A. preimage resistance

B. 2nd-preimage resistance
C. collision resistance
D. all of the above

9. SYN cookies (http://cr.yp.to/syncookies.html) are used to mitigate SYN flooding attacks. Which of the following is not used in computing a SYN cookie?
A. Timestamp
B. TCP flags
C. Maximum segment size
D. Port number

10. Suppose you have an intrusion detection system detecting a computer virus on the network with 90% accuracy. Precisely, the IDS detects a connection transferring a virus as an attack with 90% probability and a benign connection as an attack with 10% probability. When 1% of the connections contain a virus, what is the probability that a connection flagged by the IDS as an attack is actually benign?
A. 0–20%
B. 21–50%
C. 51–90%
D. 91–100%

11. The following statements describe Kerberos authentication. Find an incorrect statement.
A. The KDC is a single point of failure.
B. KDC and the ticket-granting server can run on a single machine.
C. Kerberos uses symmetric encryption.
D. Every message in Kerberos authentication is encrypted.

12. Which statement is false?
A. Stuxnet exploited multiple zero-day vulnerabilities.
B. Stuxnet attacked systems from certain vendors only.
C. A network physically separated from the Internet can be infiltrated by Stuxnet.
D. The author of Stuxnet created two fake certificates to sign drivers.

13. The article “W32.Duqu: The precursor to the next Stuxnet” describes Duqu, a threat similar to Stuxnet. Compare Stuxnet and Duqu from the following aspects.
(a) Initial infection
(b) Propagation
(c) Command and control

The Duqu Virus is not a virus, but instead, Duqu, is a Remote Access Trojan (RAT), that has the abilities of a rootkit. Its name comes from the "~DQ" it appends to file names. Symantec quickly

confirmed that Duqu is indeed a branch of Stuxnet when it analyzed research lab samples, and Symantec states that Duqu contains nearly identical code to Stuxnet, but that the identical code has a different purpose than the Stuxnet code. The Stuxnet code basically aims at attacking the scada computers and sabotages the system. The Duqu doesn't sabotage the system. It is merely used to get information out of the system in an encrypted manner., without the user getting to know

(A) INITIAL INFECTION

a. The Duqu arrives as a Microsoft word document that initiates a zero day kernel exploit. Once exploited it drops the installer files that will load the other Duqu components. The Stuxnet arrives through either the internet or any removable disk that is inserted into the system.

   The A variant of DUQU malware drops the following files:

   - %Windows%\system32\Drivers\jminet7.sys - loader driver component
   - %SystemDrive%\inf\netp191.pnf - encrypted main DLL component
   - %SystemDrive%\inf\netp192.pnf - encrypted configuration file

   Similar to Stuxnet, Duqu's driver files are signed with certificates stolen from a Taiwanese company.

   The malware then creates the following launch point:

   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\JmiNET3

   The driver is loaded during system start-up and will be responsible for decrypting and loading the main DLL component.

   The B variant of this malware uses different filenames (cmi4432.sys, cmi4432.pnf and cmi4464.PNF, respectively) and a differently-named launchpoint (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\cmi4432), but further functionality appears to be the same.

b. Another difference in this case between the Duqu and Stuxnet is that the drivers of STuxnet were signed with stolen certificates from the Taiwanese company REALTEK and JMICRON. The Duqu drivers were stolen certificates from the Taiwanese company C_MEDIA ELCETRONICS INCORPORATION.
c. Also the driver used in Stuxnet is MRXCLS.SYS whereas the one used in Duqu is JMINET7.SYS. The main dll of Stuxnet (oam7a.pnf) contains 21 export function but the Duqu dll (netp191.pnf) has only 8 export functions. This indicates that the Duqu does not contain power plant specific functionalities that the STuxnet does.
d. Infection Target: Duqu infection target selection is very similar to the mechanism of Stuxnet. For trusted processes both look up a list of known antivirus products. In Duqu, this

list is stored in 0xb3 0x1f XOR encrypted 0-terminated strings. The only addition in the Duqu Is that of Kaspersky and Chinese rising antivirus.

(B) PROPOGATION

Unlike the Stuxnet which is self propagating the Duqu is not self-propagating. The Stxnet uses P2P(Peer-Peer) using RPCs(Remote Procedure Call), Network Shares, WinCC Databases. The Duqu uses RPC communication.

(C) COMMAND AND CONTROL

While the Stuxnet uses HTTP protocol. The Duqu uses HTTP, HTTPS, Custom protocols to command and control.

14. Read "21 Steps to Improve Cyber Security of SCADA Networks" (http://www.oe. netl.doe.gov/docs/prepare/21stepsbooklet.pdf) from DoE, and answer the follow- ing questions.
(a) If properly implemented, how would each step help preventing Stuxnet attacks?
(b) Are those steps sufficient in preventing future attacks similar to Stuxnet or Duqu? If yes, justify it. If no, extend those steps to prevent such attacks.

The Department of Energy plays a key role in protecting the critical energy infrastructure of the nation as specified in the National Strategy for Homeland Security. In fulfilling this responsibility, the Secretary of Energy's Office of Independent Oversight and Performance Assurance has conducted a number of assessments of organizations with SCADA networks to develop an in-depth understanding of SCADA networks and steps necessary to secure these networks.

The following are the 21 steps that have been taken in order to make the SCADA systems more secure.

1. **Identify all connections to the SCADA networks** : All internal connections like the local area and wide area networks, business networks and connections to the internet or any other means by which the virus can travel should be identified and stringent security should be implemented. Any suspicious file should be discarded immediately. Periodic review of all the connections and their security should help prevent any virus attacks.

2. **Disconnect unnecessary connections to the SCADA network**: The highest degree of security can be obtained if the SCADA system is isolated from all connections especially the internet, which introduces higher security risks. For data transfer to take place between efficiently between the business network and the SCADA network utilization of procedures such as 'Demilitarized zones" and Data warehousing can prove to be secure.

3. **Evaluation and Strengthening the security of the remaining connections to SCADA network** : by conducting penetration testing and Vulnerability analysis of the remaining

connections to the SCADA network the security can be enhanced. At each point of entry Firewall and intrusion detection systems should be implemented in order to further protect the SCADA systems from Stuxnet.

4. **Removing or Disabling of unnecessary services** : Many of the servers used for the SCADA network are built on commercial or open source operating systems. Disabling services such as internet connection, automated meter reading, email services and remote billing system, should help better protect the SCADA network because the virus could be logged on to any such service. A service should only be allowed once it is proven that the benefits outweigh the potential for vulnerability exploitation.

5. **Not relying on propriety protocols for system protection** : Sometimes relying on propriety protocols or factory settings can lead to backdoor going unnoticed thus making the system more vulnerable to the virus attack. Thus all vendors should disclose any backdoor or vendor interfaces to the SCADA systems.

6. **Implementation of security features that are provided by system vendors** : The SCADA systems provided by the vendors should have security features in-built in them. And all the security features should be set to the maximum level in order to further protect the SCADA systems and prevent any virus attack.

7. **Establishing strong control over any medium used as a backdoor** : Modems, wireless and wired connection used for communication and maintenance indicate a backdoor through which the virus can attack the systems. Use of strong authentication protocols before such a connection is established and replacing inbound access with some type of call back system can help remove any vulnerability to such a virus attack, thus making the SCADA system more secure.

8. **Implementing Intrusion Detection System** : Both internal and external intrusion detection system should be implemented which would help in detecting and alerting any malicious activity within and outside the network. An effective reponse protocol should also be implemented along with this.

9. **Performing technical audits** : technical audits prformed on the SCADA systems will help identify the path of least resistance and remove it. Identifying the vulnerabilities and taking corrective actions against them. The system should be retested after corrective action have been taken in order to make sure that the vulnerabilities have been eliminated. This will help prevent any attacker form exploiting the system.

10. **Physical security surveys** : Conducting such surveys should help in identifying single point of failure and help eliminate them and make the systems more secure. Such points would be the telephone/computer network optic cables, radio and microwave links and computer terminals that could be accessed for virus attacks.

11. **Establishing 'Red Teams'** : Establishing 'Red Teams' to identify possible attack scenarios and potential system vulnerabilities and taking appropriate methods in order to remove them to help secure the SCADA system

12. **Defining cyber security roles and responsibilities**: Establishing a cyber security organisational structure that defines the roles and responsibilities of assigned authorities and whom to notify in case of an emergency will help in providing a faster response in case of a virus attack and help preventing it from escalating.

13. **Documentation of network architecture** : There should be a documentation of the kind of information that is contained in a SCADA system i.e which data is important and sensitive. This will help in finding out which system needs a higher level of protection than the other. In case a virus attack it would be clear as to which system contains sensitive data and should be protected first before the virus spreads.

14. **Establishment of a rigorous, on-going risk management process** : Performing a rigorous risk management process including a stage of assessment and a subsequent protection strategy is essential to make routine changes due to rapidly changing technology and new forms of Stuxnet that may come to effect like Duqu.

15. **Establishment of a network protection strategy** : Utilization of technical and administrative controls to mitigate threats from identified risks help preventing single point of failure and contain the impact of any security incidents.

16. **Identifying cyber security requirements** : Formalized policies and procedures are used to establish and institutionalize cyber security program. These policies help every individual identify their responsibilities and consequences if responsibilities are not met. These requirements are used to prevent any threat from the insiders.

17. **Establishment of effective configuration management processes** : These processes help in identifying and controlling any changes in the systems to make sure that the network remains secure.

18. **Self-assessment** : These are processes that include routine scanning for vulnerabilities, automated auditing of the network, assessment of the organization and individual performance to provide a feedback on the effectiveness of the cyber security policy and its implementation.

19. **Establishment of system backup and disaster recovery plan** : Implementation of these plans help in quickly recovering and retrieving important information in case of a virus attack.

20. **Cyber security performance** : When the senior management clearly lists the expectation from the cyber security program, the objective of system security form viruses become

clearer. Holding individuals responsible for their performance ensures that everyone puts in their best effort in following the program.

21. **Programs to help prevent personnel from disclosing sensitive data** : conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, especially their password, and not disclosing them to unauthorized individuals.