Final Exam

Ron Haley
Idris Mawleed

1. Choose one real distributed application program that you are familiar with (or could become familiar with if you don't know any (!!!)). Write the following:

- **A paragraph or two giving an overview of the application. Make sure to include which generic architecture (client-server, publish-subscribe, P2P, . . .) you believe best categorizes the application, and why it does so. Be sure also to describe what application-specific activities the various pieces in that architecture (clients, servers, whatever) are doing: what they are requesting, processing, etc.**

iTunes is a popular distributed application program that many people are familiar with. Its purpose is a large application and media distribution center that provides some key features; it allows the ability to rank items based on number of downloads by other, this allows iTunes to make suggestions based on the users previous purchases and the ranking of similar files. It allows users to leave feedback that can be useful to other users debating a certain purchase. It also provides the ability to sample or preview items in real-time.

iTunes utilizes the client-server architecture, which provides the ability to handle multiple users simultaneously. iTunes is the server in this architecture, it provides and maintains the database that stores all the media and application files, it also stores the user information and history for ranking, verification, and purchasing capabilities. The server handles requests from the client which include; user authentication, file transfer requests, and user click history. The server then replies with user account information and file handling (listing, sampling, and transferring).

The iTunes application, installed on the client’s computer, is the graphical user interface for the server that provides access to the iTunes server and files in its database. It is responsible for requesting lists of files available for purchase along with past user history then displaying that data.

- **A paragraph or two describing whether you believe the following runtime issues are important to users of this application, and why you believe it (e.g., what happens in its absence):**

- **Low latency network connections**
- **High bandwidth available**
- **Perfectly "consistent" and "correct" replies/answers/service versus an inconsistent or approximate reply/answer/service**

Make sure your answer indicates how you would desire to trade off the above runtime properties, and the "worst" for each it could reasonably tolerate.

As a user of iTunes, low latency would probably be the most important issue during runtime; one of the best features is the ability to sample music of preview movies, this would become less useful if the network speed decreases due to high latency which would lead to buffering during sampleing. Low latency usually means higher available bandwidth which is ideal for downloading files from iTunes, quick download time is good but I would trade download time to have a consistent network speed with low latency.

Latency and bandwidth issues are important in regards to the perfoemance of the application, but consistent and correct replies could be the most important issues during runtime. iTunes would not be useful if the customers pay for a certain file and in return download a file that was not intended. This would defeat the ultimate goal and use of iTunes,. Therefore, I would trade all performance issues to guarantee that the application would perform accurately and reliably like it was intended.

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".

Middleware is a computer software that provided services to software application, and it's not part of an operating system, not a database system, and neither is it part of one software application. Middleware makes it easier for software developers to perform communication, so they can focus on the purpose of their application. Middleware is used for software that enables communication and management of data in the distrubuted applications. Middleware is the software between the operation system and applications on the distributed computing system.

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

The initial infection of the W32 Duqu virus was discovered around September 1, 2011, in Europe; it created files with the file name prefix "~DQ". The Stuxnet worm was discovered in June 2010, it initially spreads via Microsoft Windows indiscriminately, but itarget only Siemens supervisory control and data acquisition (SCADA) systems.

(b) Propagation

The W32 Duqu virus is a remote access Trojan that does not self-replicate and is designed to remove itself after 36 days. The virus installs a infostealer that could record keystrokes and gain other system information. The Stuxnet virus is an Internet worm and was designed to spread to 3 other systems through a usb device so the system does not have to be connect to the Internet. The intent of the virus is to look for a particular model of Programmable Logic Controller (PLC) made by Siemens and reads and changes particular bits of data in the controlled PLCs.

(c) Command and control

The W32 Duqu virus uses HTTP and HTTPS to communicate with a command-and-control (C&C) server, this allows attackers to download additional executables through the server which include infostealer that can perform actions such as enumerating the network, recording keystrokes, and gathering system information. The information is logged to a lightly encrypted and compressed local file, which then must be exfiltrated out. Using the C&C protocol, allows downloading or uploading what appear to be JPG files. However, in addition to JPG files, additional data for exfiltration is encrypted and sent, and likewise received. The Stuxnet virus actually does not do anything to the infected Windows computers, unless they contain the target device (a particular model of PLC made by Siemens). It is responsible for installing its own driver into Windows to allow the attackers control of the system, then removing itself after a certain number of days which due to an error in the code did not happen.

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 following questions.

(a) If properly implemented, how would each step help preventing Stuxnet attacks?

1. **Identify all connections to SCADA networks-** this would allow SCADA networks to verify that all connections are safe or at least identify possible vulnerabilities from certain connection and enable proper precautions to be enacted.

2. **Disconnect unnecessary connections to the SCADA network-** by isolating SCADA from unnecessary connections, you will limit the number of security risks (eliminating the number of possible intrusion access points that Stuxnet could use).

3. **Evaluate and strengthen the security of any remaining connections to the SCADA network-** by conducting these penetrating test, you are pinpointing possible weaknesses which allows you to develop a plan to address and monitor them for a Stuxnet worm.

4. **Harden SCADA networks by removing or disabling unnecessary services-** by not permitting these service or features, you are limiting the number of possible ways that Stuxnet could attack.

5. **Do not rely on proprietary protocols to protect your system-** these protocols do not provide the proper security needed to protect against a worm such as Stuxnet

6. **Implement the security features provided by device and system vendors-** since older SCADA system do not have security features utilizing the ones provided by vendors provides at least some sort of protection against Stuxnet.

7. **Establish strong controls over any medium that is used as a backdoor into the SCADA network-** implementing strong authentication ensures secure communication to trusted devices making it harder for an attack.

8. **Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring-** this would provide all day monitoring of the system from internal and external attacks. Stuxnet can spread from internal usb devices, this would provide the monitoring to detect it.

9. **Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns-** this will help to identify all paths connected to the system and is a tool to identify any paths that could be vulnerable to attacks which would allow for proper handling of these paths,

10. **Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security-** this would help to identify any unprotected access points to the network internally (like phone lines, computer systems, etc) this will allow proper measures to take place and make the more secure.

11. **Establish SCADA "Red Teams" to identify and evaluate possible attack scenarios-** brainstorming possible attacks could help identify vulnerabilities or even future weaknesses in the system that Stuxnet could use to infect the system.

12. **Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users-** management might not have a technical background, by defining rules and regulations, it could help to eliminate vulnerability in the system cause by human error or even the possibility of uploading the Stuxnet worm unknowingly.

13. **Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection-** having documentation will allow anyone the ability to know and understand the security measure for

the system and can limit infections caused by human error.

14. **Establish a rigorous, ongoing risk management process- t**his will help by providing thorough strategies to handle and paln for possible risks like the Stuxnet worm.

15. **Establish a network protection strategy based on the principle of defense-in-depth-** this is beneficial when designing a secure system and will help to limit single points of failure.

16. **Clearly identify cyber security requirements-** this will allow people to be held accountable if they are responsible for infecting the system with a virus like Stuxnet.

17. **Establish effective configuration management processes-** this will ensure that any changes to hardware or software will not induce vulnerabilities to the system which could lead to a possible attack.

18. **Conduct routine self-assessments-** this will help to identify if the procedures established are outdated or not effective. This will allow the system to stay up to date with the latest security techniques to help protect against updated versions of viruses.

19. **Establish system backups and disaster recovery plans- this** will allow the ability to recover or restore the system if a possible attack like the Stuxnet occurs.

20. **Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance-** these rules need to be enforced and people need to be held accountable, that should come from upper management, this will ensure all measure are being enforced in regards to preventing or monitoring possible attacks like Stuxnet.

21. **Establish policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls-** by releasing data on a need to know basis and to only those authorized can help prevent data ending up with those that could potentially use it to cause harm to the system; will increase the security of the system.

(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.

There is really no set of instructions or steps that can completely prevent attacks like Stuxnet or Duqu. However, these steps are sufficient in that they set up requirements that if followed correctly, will provide constant monitoring of the system and all connections associated with it, and requires consistent testing and evaluation of the system to ensure security, all while holding those responsible for ensure that the steps are followed correctly.