Final Exam
Daniel Best, Jaymin Pancholi
05/03/2012

1. Choose one real distributed application program that you are familiar with (or could become familiar with if you dont 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.

The Precision Information Environment (PIE) application (http://precisioninformation.org/)is a tool to immerse users into an environment regarding their mission space to help solve theirproblems with use of intuitive displays and available data. The initial demonstration capability used to help facilitate user feed back and drive research revolves around emergency operation center (EOC) staff and their needs during a state of emergency. The tool is currently a 3 tiered client-server application.

The client tier of the application is a thick Java client that is installed on a local system (workstation, touch table, tablet, etc.) and communicates with the server using remote method invocation (RMI). The client requests information about the logged in user, their preferences, data to support visualizations, and current information feeds to display. The client is focused on presentation of the data and allowing client interaction. The server, implemented using JBoss Enterprise Service Bus (ESB) has the ability to implement publish-subscribe features; however, at this time the client polls for information rather than subscribing for it. The application server implements logic needed to support the visual displays and analytics. When necessary, the application server communicates with the database server through object-relational mapping (ORM). Much like RMI abstracts remote procedures calls on objects, hibernate abstracts the underlying database calls through the use of objects. The database server's role is to store data and allow for efficient retrieval of that data when needed by the application server.

• 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.

All three runtime issues are important to PIE. Users interact with the interface and expect information be shown to them quickly when requested. Couple that with a high stress environment (during state of emergency) and users will not tolerate latency issues for very long before they abandon the system. PIE must allow for the decision making process to continue quickly so tasks, such as clearing a road, get accomplished. A component of PIE is to consume feeds of information (Twitter, RSS, Weather data, etc) to help inform the decision making process.

The more feeds added to the system increases the dependency on high bandwidth availability. Finally, because decisions will be made during a state of emergency the outcomes of those decisions have serious implications; therefore the data being presented must be consistent and correct. Many times having the best of all three runtime issues is not feasible and concessions must be made. For PIE, having the data presented be consistent and correct is of the most importance with a low tolerance for the inability to meet that requirement. Low latency network connections is the next most important. Low latency connections allow for interaction with the application, but it also allows for coordination and the decision making process to happen when needed. The final high bandwidth availability can tolerate less than optimal bandwidth since if needed all but the important feeds can be halted to insure the data that most affects decisions is still available.

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”.

Assembler programming is the bare metal level of programing above trying to write a program in binary. To write an assembly language program is doable, and in some cases necessary for highly specialized programs. However, it is very difficult to write a large application in assembly and ensure all of the code is well written and common issues are accounted for. High-level programming allows a developer to construct applications in a way that can account for common mistakes, are easier to read and maintain, and are easier to write large programs. High-level programming abstracts the assembly language underneath to make development easier.

Socket programming is much like assembly language programming where it is a layer above sending binary across the wire. Just like assembly writing a socket programming program is doable and sometimes necessary for specialized programs, it is often best left to middleware. Middleware is like the high-level programming language for network communication. It abstracts the socket programming underneath to make network communication and distributed programs easier to implement.

3. Which of the following is false for a NASPInet-like critical infrastructure data delivery service for a power grid:

C. Post-error recovery is sufficient.

4. Which of the following is more burdensome for the application programmer:

D. Request-reply protocols

5. Which of the following is space-uncoupled:

B. Publish-subscribe

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).

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.

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?
B. 2nd-preimage resistance

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?
C. Maximum segment size

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?
D. 91-100%

11. The following statements describe Kerberos authentication. Find an incorrect statement.
D. Every message in Kerberos authentication is encrypted.

12. Which statement is false?
B. Stuxnet attacked systems from certain vendors only.

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

Duqu	**Stuxnet**
First discovered in Europe.	First discovered in Iran.
Created an initial infection in the system as Remote Access Trojan(RAT).	Created an initial infection in the system by using the hidden autorun command

	codes which were bypassed by windows.
Created dummy .jpg file for initial infection.	Created .lnk and .pif file for initial infection.
Is a remote access trojan which allows the exfiltration of data from target networks.	Is able to inject malicious code onto systems that caused the physical degradation of nuclear centrifuges.
Main target was Industrial Control Systems.	Main target was SCADA systems.

(b) Propagation

Duqu	**Stuxnet**
Used RPC communications for propagation.	Propagated through network shares, MS10-061, MS08-067 and using peer to peer communication.
Not self propagating.	Self propagating
Deletes itself after 36 days.	Does not delete itself

(c) Command and control

Duqu	**Stuxnet**
Uses HTTP & HTTPS to communicate with command and control servers.	Uses HTTP to communicate with command and control serve
Main purpose was as a infostealer to access important data which can be used for future attacks.	Main target was SCADA systems and malfunctioning of SCADA systems.

14. Read "21 Steps to Improve Cyber Security of SCADA Networks" (http://www.oe.netl.doe.gov/do) from DoE, and answer the following questions.

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

i. Identifying all connections of SCADA networks: All the SCADA network connections should be reviewed so that its difficult for worms like stuxnet to propagate and create critical infrastructural damage. In this way tighter security can be implemented on them and chances of future attack can be minimized.

ii. Disconnection of unnecessary connection from SCADA network: If the SCADA network is isolated from the rest of the network than the risk of worm like stuxnet to propagate from the outside network can be reduced as there are no to minimum chances of any kind of worm or virus to attack the network.

iii. Evaluating and strengthening the security of any remaining connections to the SCADA network: The firewalls and intrusion detection systems(IDS) should be implemented at each of the network entry point so there is no breach in the network security. Some strict rules can be made for the access to/from the SCADA network so that there no vulnerability and which can give the robust protection to the system.

iv. Harden SCADA networks by removing or disabling unnecessary services: By removing and disabling the unused and unnecessary devices connected to the SCADA network, the risk of security breach can be mitigated which can be helpful for protection against virus and worms. If this is implemented than propagation like MS10-061 can be prevented.

v. Not relying on proprietary protocols to protect your system: By using the protocols made for the other systems, more security features can be included into the system and thus giving more protection against the attack and reducing the chances of any future attack of stuxnet.

vi. Implementing the security features provided by device and system vendor: After the stuxnet attack on Siemens SCADA system, all the SCADA system manufacturers mush have developed any counterpart to protect against attacks like this, so by installing such software and upgrading it on regular basis future attacks can be mitigated.

vii. Establishing strong controls over any medium that is used as a backdoor into the SCADA network: Some of the communication like modems and wired and wireless networks can be highly vulnerable, so by taking some kind counter action like callback system can be helpful. This helps in prevent the stuxnet attack like CVE-2010-2772 and other kind of discrepencies.

viii. Implementing internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring: The stuxnet worm which was discovered in 2010 bypassed the host IDS installed in the SCADA systems. So by implementing internal and external IDS which notifies administrator and also take preventive measures when some attack is detected making the system secured.

ix. Performing technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns: By performing technical audits periodically on the SCADA devices the vulnerabilities can be avoided. By doing audits and upgrading the system for protection against vulnerabilities, the new threats which have been detected can be prevented.

x. Conducting physical security surveys and assessing all remote sites connected to the SCADA network to evaluate their security: Physical security should be provided to the SCADA control centers and any equipment within the control center which might be vulnerable to the attack should be protected. By doing such the future attacks can be prevented.

xi. Establishing SCADA “Red Teams” to identify and evaluate possible attack scenarios: “Red Teams” should be created using the personnel who has been working with the related areas of SCADA systems. By doing so these personnel can give a better feedback of the weaknesses and how it can be rectified so that it can be safe from the attacks.

xii. Clearly defining cyber security roles, responsibilities, and authorities for managers, system administrators, and users: Specific standards and rules should be made for each organization for protection against cyber attack. Also by assigning special authority to the managers the attacks can be mitigated.

xiii. Documentation of network architecture and identifying systems that serve critical functions or contain sensitive information that require additional levels of protection: Some sensitive information related to the SCADA control center should be documented and made confidential, so that the risk associated with the documents going to wrong hands can be reduced. The key parts of the system should be thoroughly understood and made updated throughout the use.

xiv. Establish a rigorous, ongoing 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

xv. Establishing a network protection strategy based on the principle of defense-in-depth: Defense in depth principle should be considered as the part of security during the development of the system. Also by restricting the personnel just to their job role the security breach chances can be mitigated to huge extent.

xvi. Clearly identifying cyber security requirements: Standard cyber security rules should be established and should be mandated on every organization and its employees for its implementation. Also the consequences of not meeting the requirements should be made aware of to the organization and its employees.

xvii. Establishing effective configuration management processes: When the hardware and software configurations are covered by processes that evaluate and control any changes , the network can be made more secure, mitigating the chances of future attack.

xviii. Conducting routine self-assessments: All the organization must be able to do self-assessments

periodically to check for vulnerabilities. All the organizations must have personnel specializing in root cause analyzing and who must be capable of implementing the corrective actions.

xix. Establishing system backups and disaster recovery plans: All the data recorded by the SCADA system should have backup so that system can be again reconstructed easily after an emergency. Also the mock drill of the data recovery should be conducted on regular basis for ensuring their operability.

xx. Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance: There should be effective communication between the senior managers and the organization for the awareness of the cyber security. This way the chances of an cyber attack can be mitigated, if each and every employee of the organization is aware of the cons of cyber attack.

xxi. Establishing policies and conduct training to minimize the likelihood that organizational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls: The data of the SCADA network should not be made accessible or provided to any stranger or a rookie employee. Only the responsible person should be able to access this data. When personnel are trained not to release data or information to unauthorized people, they become more aware of the risks of their actions. Training on this aspect is essential in preventing any insider attack or outsider for that matter.

(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.

According to me most of the steps are sufficient to prevent the future attacks of stuxned/duqu but there are few steps which needs to be taken care of more deeply. In step 3 they have mentioned to implement IDS for safety but even when stuxnet attacked IDS was implemented on the SCADA systems but it bypassed IDS and affected the system. So more rigorous steps should be taken for implementation of IDS. In step 5 they have mentioned to use other communication protocols for communications between different entities, but according to me by using different communication protocols the system will become more vulnerable to attacks as the attackers can use wide array of different paths and techniques to attack the system.

Considering that Stuxnet initially propagated through a flash drive, Media Protection standard should bed defined. This should define the use of both digital media and non digital Media for SCADA systems. Also in step 16 they have mentioned to increase the security from malicious insider by providing background check and other necessary steps, but even by using background check the operation is not completely safe, so more hard steps should be taken to prevent the attack form the insider. These are the few steps which needs to be taken care of according to me. Also as the use of wireless communication and equipment is increasing in the SCADA network some steps and preventive measures should also be provided so that the attacks caused using the wireless loop holes can be avoided.