Critical Infrastructure Security: The Emerging Smart Grid
Final Take-Home Exam
Spring 2012
(Due on May 3)

Casey Clayton Neubauer, Ming Meng, Paul Elliot McKinley,

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.
- 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.

Massively Multiplayer Online Games (MMOs) are an example of a distributed system. The underlying architecture of most such systems are client/server, because users typically download a "game client", which then connects to a server, which is typically proprietary and maintained by employees of the game company. Most or all data is stored on the server side of the system, and is sent when requested by the client. Users type or send commands from the clients which are then processed by the server, with results being sent back to the client. For example, if a player presses a key to move in a certain direction, the command is sent to the server, and the result is sent back to the client. The user then observes that in the game, they have then moved that distance. The server handles coordination of clients. For example, if a player interacts with another player, the server must receive and interleave the messages between the two players correctly. Otherwise the players will perceive events of the interaction happening in an inconsistent order.

Low latency connections are important for this distributed system, because otherwise users will experience "lag" (a similar word used to describe latency) and the game will become more and more unplayable. The amount of required minimum latency varies depending upon the specific game, and is often tolerable up to a point; however latency in excess of a few hundred milliseconds is immediately obvious to even a human. High bandwidth is important for the server, because it must handle many connections simultaneously. With a lower available bandwidth, the server would not be able to service as many clients, which would translate to less players, which would mean less paying customers for the game company. Finally, "consistent" or "correct" replies would be more important than partial or approximate replies, because partial replies would lead to inconsistent results between clients.

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 layer that is between the application and operating system. It allows for the ability to gain access to sockets, instead of dealing with sockets directly. High-level programming language is a layer that allows people to develop software but it is converted to assembly language later. It gives the ability to write a program that works on a computer and not have to develop using the assembly language directly.

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

Answer: C

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:

Answer: D

A. Remote procedure call
B. Publish-subscribe
C. Remote method invocation
D. Request-reply protocols

5. Which of the following is space-uncoupled:

Answer: B

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):

Answer: A

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 of the following challenge for the bulk power grid cannot be mitigated with much better wide-area communications (and sensors feeding it):
Answer: B
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?
Answer: B
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?
Answer: B
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?
Answer: A

A. 0–20%
B. 21–50%
C. 51–90%
D. 91–100%

11. The following statements describe Kerberos authentication. Find an incorrect statement.

Answer: D

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?

Answer: D

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

Stuxnet:

Stuxnet exploits the Microsoft Windows Shortcut 'LNK/PIF' Files Automatic File Execution Vulnerability in order to spread. The worm drops a copy of itself as well as a link to that copy on a removable drive. When a removable drive is attached to a system and browsed with an application that can display icons, such as Windows Explorer, the link file runs the copy of the worm.

Duqu:

In one case, Duqu arrived at the target using a specially crafted, Microsoft Word document. The Word document contained a currently undisclosed 0-day kernel exploit that allows the attackers to install Duqu onto the computer unbeknownst to the user.

(b) Propagation

Stuxnet:

Infecting WinCC machines via a hardcoded database server password.
Propagating through network shares.
Propagating through the MS10-061 Print Spooler Zero-Day Vulnerability
Peer-to-peer communication and updates
Propagating through the MS08-067 Windows Server Service Vulnerability

Duqu:

Network spreading: The first step is to copy Duqu onto the target computer over a

shared folder. The infecting computer is able to authenticate to the target by using the credentials intercepted by the keylogger. The next step is to trigger execution of that copied sample on the target computer. This is done by creating a scheduled task on the target computer, which executes the copied version of Duqu. At this point Duqu is running on the target computer.
(c) Command and control
Stuxnet:
Test network connectivity;
Send basic information about the compromised machine;
C&C response to execute RPC routine;
C&C response to execute encrypted binary code.

Duqu:
Duqu uses HTTP and HTTPS to communicate with a command-and-control (C&C) server that at the time of writing is still operational. The attackers were able to download additional executables through the C&C server, including an 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.

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?
Answer:
For those steps which focus on specific actions to be taken to increase the security of SCADA networks, the sixth step " Implement the security features provided by device and system vendors. " can largely prevent Stuxnet because it exploits system vulnerabilities which can be patched. Also, since Stuxnet can also propagate through network share and p2p communication, the first three steps can be helpful in that they can stop the communication of Stuxnet.

(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.
Answer:
Yes, since Duqu infects system through a word document exploit, thus "steps which focus on management actions to establish an effective cyber security program" can prevent such attack in that these steps request users to take precautions during operation. Such as " 12. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users. " and " 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. "