EE 582 Final Exams

# Critical Infrastructure Security: The Emerging Smart Grid

**Submitted by:**

1. Bimal Shah--------------Electrical Engineering
2. Shreya Kodnadu-------Electrical Engineering
3. Christopher Leary-----Computer Science

1. Choose one real distributed application program that you are familiar with (or could become familiar with if you do not 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):

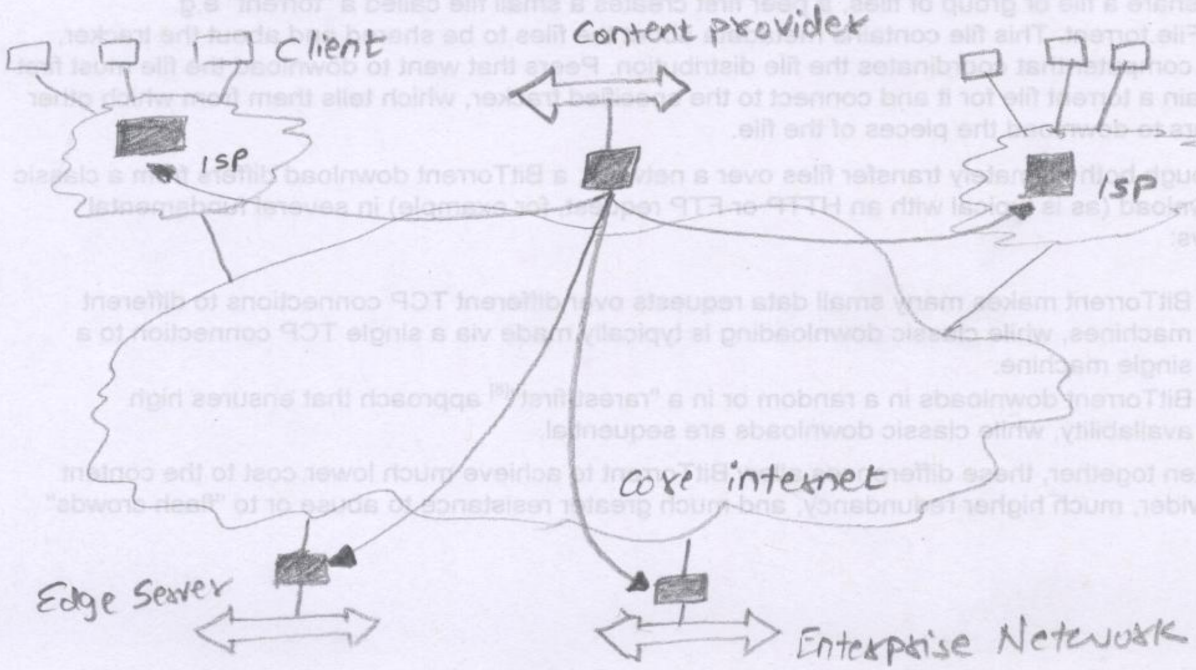
– Low latency network connections
– High bandwidth available
– Perfectly “consistent” and “correct” replies/answers/service versus an inconsistent or approximate reply/answer/service

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.

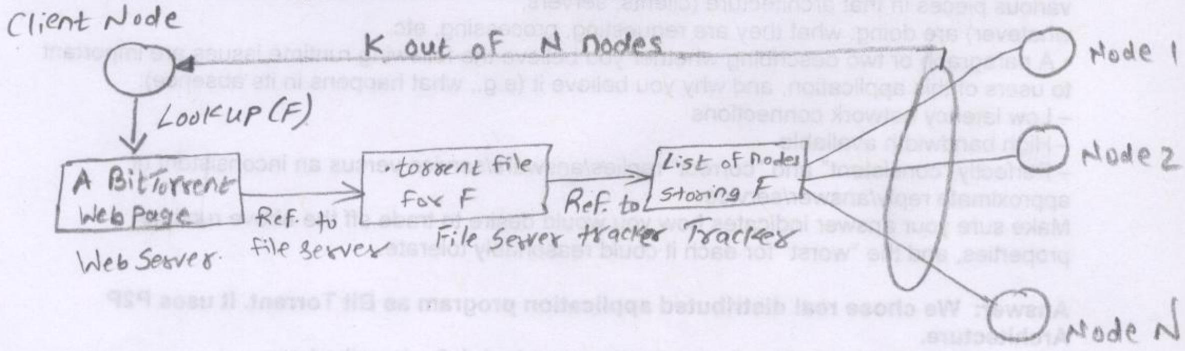
**Answer: We chose real distributed application program as Bit Torrent. It uses P2P Architecture.**

System Architectures for Distributed Systems can be briefly described as:

- **Centralized**: Traditional client-server structure :
  1. Vertical (or hierarchical) organization of communication and control paths (as in layered software architectures)
  2. Logical separation of functions into client (requesting process) and server (responder)
- **Decentralized**: Peer-to-Peer:
  1. Horizontal rather than hierarchical comm. and control.
  2. Communication paths are less structured and have symmetric functionality
- **Hybrid:** combine elements of C/S and P2P
  1. Edge-server systems: e.g. ISPs, which act as servers to their clients, but cooperate with other edge servers to host shared content
  2. Collaborative distributed systems e.g. Bit Torrent, which supports parallel downloading and uploading of chunks of a file. First, interact with C/S system, than operated in decentralized manner.



3. Clients contact a global directory (Web server) to locate a *.torrent* file with the information needed to locate a **tracker**; a server that can supply a list of active nodes that have chunks of the desired file. Using information from the tracker, clients can download the file in chunks from multiple sites in the network. Clients must also provide file chunks to other users



**Bit Torrent-Justification**:

1. Designed to force users of file-sharing systems to participate in sharing.
2. Simplifies the process of publishing large files, e.g. games
   a. When a user downloads your file, he becomes in turn a server who can upload the file to other requesters.
   b. Share the load – doesn't swamp your server

Bit Torrent is a way to transfer files of just about any size quickly and efficiently. It works by breaking files up into small pieces. The file is downloaded piece by piece from one or many different sources. It's efficient because you get faster downloads using a lot less bandwidth. A Bit Torrent client is any program that implements the Bit Torrent protocol. Each client is capable of preparing, requesting, and transmitting any type of computer file over a network, using the protocol. A peer is any computer running an instance of a client.

To share a file or group of files, a peer first creates a small file called a "torrent" e.g. MyFile.torrent. This file contains metadata about the files to be shared and about the tracker, the computer that coordinates the file distribution. Peers that want to download the file must first obtain a torrent file for it and connect to the specified tracker, which tells them from which other peers to download the pieces of the file.

Though both ultimately transfer files over a network, a BitTorrent download differs from a classic download (as is typical with an HTTP or FTP request, for example) in several fundamental ways:

- BitTorrent makes many small data requests over different TCP connections to different machines, while classic downloading is typically made via a single TCP connection to a single machine.
- BitTorrent downloads in a random or in a "rarest-first"[8] approach that ensures high availability, while classic downloads are sequential.

Taken together, these differences allow BitTorrent to achieve much lower cost to the content provider, much higher redundancy, and much greater resistance to abuse or to "flash crowds" than regular server software. However, this protection, theoretically, comes at a cost: downloads can take time to rise to full speed because it may take time for enough peer connections to be established, and it may take time for a node to receive sufficient data to become an effective up loader. This contrasts with regular downloads (such as from an HTTP server, for example) that, while more vulnerable to overload and abuse, rise to full speed very quickly and maintain this speed throughout.

## RUNTIME ISSUES: Bandwidth, Latency, Consistency and Correctness

We just witnessed something that blew my mind. I was downloading something on BitTorrent, and it was downloading at a fairly high rate (~1MB/s). The upload speed was very low (~15kB/s courtesy of lots of seeders).

What surprised me though as that while Bit Torrent was running (and downloading), I couldn't access any webpage, or ping any website. What was even more weird was that Windows was showing me the "I'm connected to the wireless router but there is no internet connection" symbol. Microsoft diagnostics said it couldn't find the DNS server (which explains why I couldn't access/ping web pages). When I looked at the networking tab, of course it showed me plenty of activity courtesy of Bit Torrent. Everything went back to normal as soon as the download finished.

Bit Torrent (or anything else) using excessively large chunks of your bandwidth can saturate your connection. Basically, you're transferring so much at once that other packets end up timing out and getting dropped. Imagine a water pipe, if you try to put too much in it will fill up faster than it can be emptied and start overflowing, losing the water that overflows.
A typical IP (Internet Protocol) request requires you to send some packets to the server you are requesting from, which will then send some packets back - its response. This requires both some upstream and downstream bandwidth. When your upstream bandwidth becomes saturated, you can't send the request. When your downstream bandwidth becomes saturated, you can't receive the response. It is entirely possible for a BitTorrent client to use all your available bandwidth.

Generally, it is best to set your Bit Torrent client to only utilize up to 80% of your upstream and downstream bandwidth, as determined by speed tests. If you require low latency, e.g. online gaming, the percentage should be even lower.

It's also possible for Bit Torrent to overload home modems and routers by opening too many connections, overflowing their NAT tables. The maximum number of connections should therefore be kept at a fairly low level. A maximum of 300 connections globally should be alright. An overflowing NAT table's symptoms will vary from router to router, but often cause them to freeze.

## High Bandwidth:

1. "Bandwidth Allocation is an option that makes Torrent allocate upload bandwidth to the selected torrent job based on the option selected. This option works only if a global maximum upload rate is set, or the selected torrent job each have an individual maximum upload rate set. High will give the selected torrent job more upload bandwidth relative to other torrent jobs of lower bandwidth allocation levels (Low or Normal).
Normal is the default bandwidth allocation given.

Low will give the selected torrent jobless upload bandwidth relative to other torrent jobs of higher bandwidth allocation levels (Normal or High). "It relates only to upload bandwidth and probably will not make much of a difference in download speed. I leave mine on Normal. If you have torrents from a private tracker, then you may wish to set their priority to high.

2. High bandwidth allocation means it will take up more allowing you to download it faster, while downloads of other pages, files etc. will be (potentially) slowed. Select high if it is your priority. If you have a lot of other things happening, depending on your bandwidth, and you want them to keep running select low. With a high-bandwidth, broadband Internet connection, you can watch streaming video and listen to streaming audio. File downloads and uploads are much faster than with a dial-up connection. Also, the price of high-bandwidth Internet connections is lower than ever. Contact your local DSL or cable provider for a list of prices and connection speeds. You may find that these services are less expensive than your current dial-up connection. Higher bandwidth Internet connections allow users to download and upload much larger amounts of data than were previously possible. With a broadband connection, you can both download and upload files that are more than a gigabyte (GB) in size.

## LOW BANDWIDTH:

1. In contrast to a large body of recent work that argues that low-bandwidth clients benefit by strategic behavior, we demonstrate that there is no incentive for low-bandwidth clients to cheat since they actually perform better by enhancing their upload contribution.
2. Our analysis shows that low-bandwidth clients fail to *fairly* utilize their download bandwidth even when there are other peers in the swarm that can offer them good download performance.
3. Based on our analysis, we present a BitTorrent client called BitMate that is designed to enhance the performance of hosts with low-bandwidth connections by maximizing its upload contribution.

Overall, a low-bandwidth BitMate client prefers stable, bandwidth-matched peers over the greedy strategy of vanilla Bit Torrent. Instead of wasting optimistic unchokes on high bandwidth peer, a BitMate client optimistically unchokes those peers that have a similar low-bandwidth. As a result, a BitMate client invests its scarce upload bandwidth on peers that are most likely to reciprocate. At the same time, BitMate leaves the tit-for-tat reciprocal unchoke policy untouched to uphold the fairness of BitTorrent. This leads to both increased performance and fairness since low-bandwidth clients can quickly form mutually beneficial peer-to-peer connections. BitMate outperforms vanilla BitTorrent by as much as 70% in download performance, while at the same time improving upload contribution by an order of magnitude. BitMate also outperforms strategic clients like BitTyrant in low-bandwidth conditions by as much as 60% in download performance.

A block is a piece of a file. When a file is distributed via BitTorrent, it is broken into smaller pieces, or blocks. Typically the block is 250kb in size, but it can vary with the size of the file being distributed. Breaking the file into pieces allows it to be distributed as efficiently as possible. Users get their files faster using less bandwidth.

**Bandwidth Allocation**: This is an option that makes BitTorrent allocate less or more bandwidth toward a torrent .This only affects upload and only if an upload cap is select.

**Latency**: Factors such as latency can reduce the speed of Internet communications. Latency is the time required for a packet of data to travel from its source to its destination. The speed of an Internet connection is defined by both its bandwidth and its latency. Downloads may take a long time on slower broadband connections. Also, bandwidth caps, net congestion and server limits may affect your download speeds.

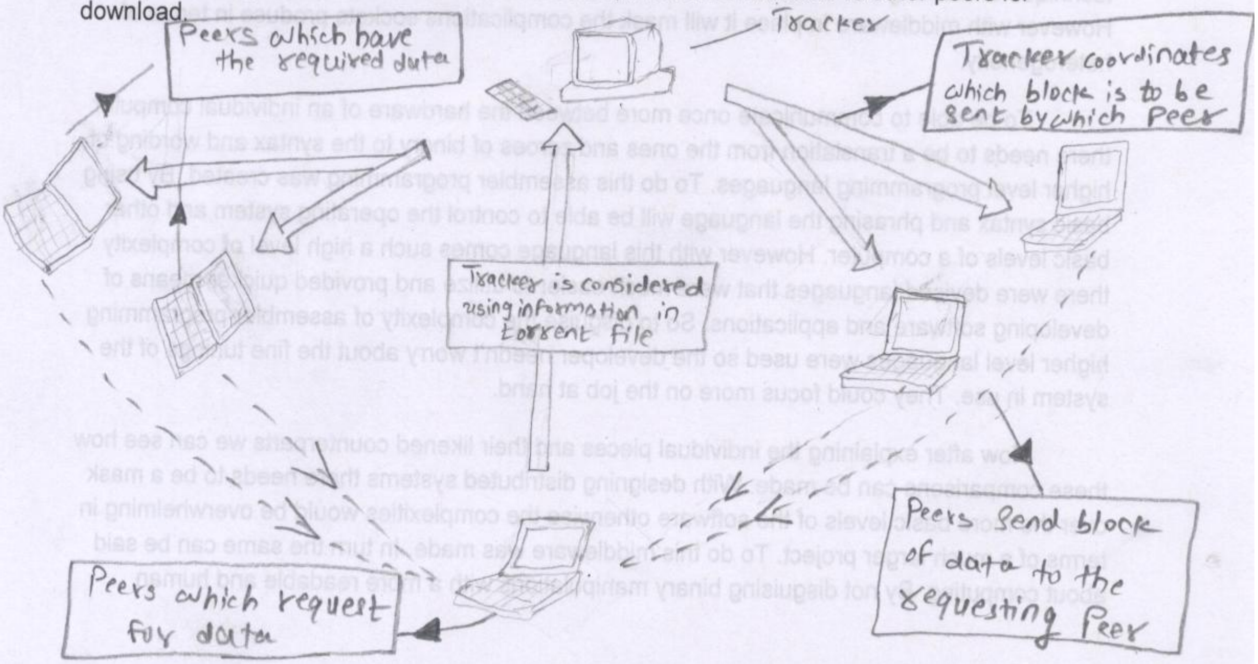
**Extra Explanation**:
Main Elements of Bit Torrent are:

**Torrent**: For every file that is to be shared using BitTorrent ,a corresponding torrent file is required to be made. Also referred to as torrent files, torrent are very small sized files which contain hashed information about the file content and name, length of the file to be shared ,number of blocks of data and the size of each block in which the files contents are to broken and shared. These files also contain the URL of the tracker.

**Tracker**: Every bit torrent network has a unique machine called the tracker. It is centralized entitiy which keeps a record of the peers sharing a particular content and is responsible for coordinating the download of a described file from several peers which are sharing that content. These are several web based tracker software available eg torrents bits which can be run at the tracker. The tracker software allows peers to register with the tracker, login into their account, browse for shared content, download content and upload torrent files .Some tracker software provide additional functionalities like RSS feeds, discussion forums, personal message boards.

**Bit Torrent Client**: This is software which runs at each peer in P2P system and it helps share and download content from other peers. Bitspirit, U torrent is some popular Bit Torrent client software.

**Uploading content**: When a peer wishes to share content with other peers, it creates a torrent file containing the URL of the unique tracker in the system. It then uploads this torrent file on the tracker and share this file for the P2P network using its Bit Torrent client software. This sharing is called seeding of content. Once a file is seeded, it become available to other peers for download.


Peers which have the required data
Tracker
Tracker coordinates which block is to be sent by which Peer
Tracker is considered using information in torrent file
Peers send block of data to the requesting Peer
Peers which request for data

Working of BitTorrent Protocol

**Downloading content**: When a peer wishes to download content from the P2P network, it searches for it on the tracker. If the search is successful, the peer downloads the torrent file for the same. This torrent file is then opened with the Bit torrent client software. Since the torrent file contains the URL of the tracker, the Bit torrent client software contacts the tracker using this URL .The tracker has a list of peers who are sharing the request content. Since the requested content is broken into blocks of fixed size for sharing different peers send different blocks of data to the requesting peer. The tracker coordinates and decides the blocks to be obtained from different peers. These blocks when assembled by the Bit Torrent client complete the file download.

Bit Torrent thus does not adhere strictly to the requirements of a true P2P system and has the feature of centralized control to a certain extent. However the centralized control is only a coordinating agent ; the content is shared not from a single server, but the interaction and exchange of data blocks between several peers.

## 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".

**Answer:** The phrase "Middleware is to socket programming what high-level language programming is to assembler programming" can be explained in a couple of ways. To begin we must talk about each piece to get a basic understanding of what their roles are by themselves. With middleware the goal is to create software that allows communication behind attached nodes in a distributed computing system network. It allows the programmer the ability to focus more on the purpose of the application at hand and to not worry so much on the communication aspects which typically are very error prone and time consuming. It also allows newer applications a higher degree of linking between themselves and older systems that are already in place. To get middleware however there needs to be a connection between the actual hardware and itself. To accomplish this socket programming was devised. This was the original technique of creating interconnection between systems before middleware was planned. However with middleware in place it will mask the complications sockets produce in terms of heterogeneity.

To be able to communicate once more between the hardware of an individual computer there needs to be a translation from the ones and zeroes of binary to the syntax and wording of higher level programming languages. To do this assembler programming was created. By using basic syntax and phrasing the language will be able to control the operating system and other basic levels of a computer. However with this language comes such a high level of complexity there were devised languages that were much easier to utilize and provided quicker means of developing software and applications. So to disguise the complexity of assembler programming higher level languages were used so the developer needn't worry about the fine tunings of the system in use. They could focus more on the job at hand.

Now after explaining the individual pieces and their likened counterparts we can see how these comparisons can be made. With designing distributed systems there needs to be a mask over the more basic levels of the software otherwise the complexities would be overwhelming in terms of a much larger project. To do this middleware was made. In turn the same can be said about computing. By not disguising binary manipulations with a more readable and human friendly approach the amount of time needed to design or implement any sort of application would be geometrically longer. Thus higher level programming languages were created to mask the involvedness of assembler programming.

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.

**Answer: C**

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**

**Answer: D**

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

**Answer: B**

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.

**Answer: C**

7. Which if the following challenge for the bulk power grid cannot 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.

**Answer: B**

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

**Answer: D correct**

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

**Answer: B**

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%**

**Answer: D**

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.**

**Answer: D**

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.**

**Answer: D**

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

**Answer:**

**(a). Initial Infection.**

By exploiting a zero day vulnerability in a Microsoft Word document Duqu can install itself without alerting the user to its presence. Upon the opening of the document Duqu will run an exploit that runs a kernel mode shell code. After the shell code has been put into place it next runs two executable; a driver file and a DLL. When completed the shell code will erase itself leaving no trace of the installation process. Stuxnet also exploits zero day vulnerabilities, four of them, to initiate its infection process. One of these exploits was a LNK vulnerability in which Stuxnet would hijack a shortcut on disk and upon the user clicking on the icon and attempting to run the original program it had pointed too would instead execute the newly planted Stuxnet code. By using this vulnerability the attacker would gain the same user rights as the local user. So while both use zero day vulnerabilities in Windows systems, the specific points of entry and techniques employed are both very different.

**(b). Propagation.**

For propagation Stuxnet and Duqu share a few similarities, mainly the use of passwords and shared folders to circumvent connected systems. Stuxnet had a hardcoded database server password within itself that it used to gain access to shared folders. Once in the folders Stuxnet also utilized another zero day vulnerability in which it would use both remote procedure calls as well as a print spooler service exploit to finally infect a connect system by downloading itself into the %System% directory. While with Duqu it would communicate with its command and control servers to load a keylogger as well as surveillance software so it can gather information about the locally connected systems. To catch network data however Duqu needs to be implanted into a shared folder over the network. Once it has located enough passwords as well addresses to other connected systems the information will be sent back to the C&C servers and from there it will attempt to connect and infect another host.

## (c). Command and Control

In terms of the command and control servers for both worms there are some similarities. Stuxnet starts off first by attempting a connection with a web page. Upon receiving this ping from the worm the C&C server will send a reply back acknowledging it. Next the worm will send back system information like the OS version, machine name, and workgroup name among others. With this new information the C&C server will be able to start the RPC routine and then upon success it will also send a command to execute the encrypted binary code installed by Stuxnet. With Duqu it is sort of similar to Stuxnet in that its command and control server is also used primarily for data storage and future infection data. Duqu upon being installed will begin communicating with its C&C server to get a few executables. One of these being a keylogger, as stated prior in part (b). With this keylogger installed it can now begin to gather sensitive data and passwords in terms of network links the system may have. Upon gathering enough of this data it will send back this information to the C&C server and from there will attempt to establish a new fresh host for infection.

Among these three main topics Stuxnet and Duqu also share some other similarities with each other. One common trait is their intended targets within the Iranian nuclear program. Another is that they both utilize stolen key signatures to bypass initial checks from anti-virus software. On top of these they are both derived from the same source code which makes some think they could both be made by the same people. And perhaps the biggest qualities both Duqu and Stuxnet share is the fact that they both operate on the usage of zero day vulnerabilities.

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?
(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:

Stuxnet is a computer worm. It is the first discovered malware that spies on and subverts industrial systems, and the first to include a programmable logic controller (PLC) rootkit. The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target only supervisory control and data acquisition (SCADA) systems that are configured to control and monitor Power system processes. Stuxnet infects PLCs. Unlike most malware, Stuxnet does little harm to computers and networks that do not meet specific configuration requirements.

The worm consists of a layered attack against three different systems:

1. The Windows operating system,
2. Siemens PCS 7, WinCC and STEP7 industrial software applications that run on Windows and

3. One or more Siemens S7 PLCs.

Steps involved in protection and how they prevent spreading of Stuxnet:

**1. Identify all connections to SCADA networks.**

Stuxnet is initially spread using infected removable drives such as USB flash drives, and then uses other exploits and techniques such as peer-to-peer RPC to infect and update other computers inside private networks that are not directly connected to the Internet. By securing the external sources such as internet, wireless devices and other connections that can allow for Stuxnet to attack, the spreading of this malware can be prevented. Identifying these connections and conducting a thorough analysis of each connection involved lets the user take necessary precautions and install the right protection for each connection involved in the system. This prevents Stuxnet from attacking the system. External connection is one of the sources for Stuxnet to enter into the system. Hence it is important to secure these connections.

**2. Disconnect unnecessary connections to the SCADA network.**

Stuxnet can propagate via the auto run feature, as well as via malformed .LNK files that exploit vulnerability in the Windows shell. This enables Stuxnet to spread easily on network devices. Any connection to another network introduces security risks, particularly if the connection creates a pathway from or to the Internet. Hence it is important to isolate the SCADA network from unnecessary connections and network which pose a security risk and can provide a path for Stuxnet to enter the system. Strategies such as utilization of “demilitarized zones” (DMZs) and data warehousing can facilitate the secure transfer of data from the SCADA network to business networks.

**3. Evaluate and strengthen the security of any remaining connections to the SCADA network.**

Testing or vulnerability analysis of connections to the SCADA network and evaluating the protection posture associated with these pathways is an important step in coming up with solutions or developing robust protection schemes for any pathway to the SCADA network. Evaluating the security risks a network possesses, will give an idea about how well the protection system needs to be devised against malware like Stuxnet.

**4. Harden SCADA networks by removing or disabling unnecessary services.**

SCADA control servers built on commercial or open-source operating systems can be exposed to attack through default network services. Stuxnet is one of those malware attacks which can cause severe damage to the whole system. To the greatest degree possible, it is necessary remove or disable unused services and network daemons to reduce the risk of direct attack from Stuxnet. This is particularly important when SCADA networks are interconnected with other networks. Stuxnet targets the systems that are interconnected and it communicates through P2P network with the infected hosts and spreads to the systems that are not affected by it.

**5. Do not rely on proprietary protocols to protect your system.**

Proprietary protocols sometimes may not be able to give a complete protection to the SCADA system. Stuxnet can misuse this property to gain entry into the system. Stuxnet was devised after through research and it allows an attacker to assume control of critical systems like pumps, motors, alarms and valves in an industrial plant. To prevent such malware from taking advantage of these protocols which have loopholes it is not preferable to not rely on them.

### 6. Implement the security features provided by device and system vendors.

Security features of the SCADA device must be activated completely. Additionally, factory default security settings (such as in computer network firewalls) should be set to provide maximum security. Set all security features to provide the maximum level of security. Spreading of Stuxnet can be prevented by regular updates from anti malware software or windows updates. Just the basic security features on SCADA system may not be sufficient to prevent attacks from malware. Optimum security is utmost necessary for protection from malware like Stuxnet because sometimes even antivirus may not be able to detect such dangerous virus and basic settings may give in to such attacks.

### 7. Establish strong controls over any medium that is used as a backdoor into the SCADA network.

Strong authentication must be implemented to ensure secure communications. Modems, wireless, and wired networks used for communications and maintenance represent a significant vulnerability to the SCADA network and remote sites. **Having proper encryption, key management and appropriate authentication will prevent the attack from Stuxnet.** Disabling inbound access and replacing it with some type of callback system gives high protection to SCADA system.

### 8. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring.

Establishing an intrusion detection strategy that includes alerting network administrators of malicious network activity originating from internal or external sources will enable the system to be prepared for any attacks from malwares such as Stuxnet. Early detection of the virus can prevent the system from undergoing huge damage. Intrusion detection system monitoring 24 hours a day will prevent any intrusion from Stuxnet which can be spread through external sources such as USB drive. Any external source can be first tested for any malicious virus or malware in it and run on a sample system before using it on SCADA system. Logging on all systems and auditing system logs daily to detect suspicious activity can prevent the spreading of virus quickly.

### 9. Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.

Technical audits of SCADA devices and networks are critical to ongoing security effectiveness. Many commercial band open-source security tools are available that allow system administrators to conduct audits of their systems/networks to identify active services, patch level, and common vulnerabilities. System patch needs to be updated regularly. This forms one of the sources for the malware such as Stuxnet to attack. These technical audits can provide some assurance of the system security. These could prevent the attacker from misusing the least resistive or least protective path for Stuxnet.

### 10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.

Identify and assess any source of information including remote telephone/computer network/fiber optic cables that could be tapped; radio and microwave links that are exploitable; computer terminals that could be accessed; and wireless local area network access points. These are the key places through which Stuxnet can gain access into the system. Especially network access points. It uses open network as a medium to communicate to unaffected devices and spreads to those devices as well. This can be prevented by avoiding any unnecessary access to the network or by preventing any live network access points at remote, unguarded sites simply for convenience.

### 11. Establish SCADA “Red Teams” to identify and evaluate possible attack scenarios.

Special team needs to be assigned to identify and analyze the possible attacks on the system. It keeps the system on alert for any possible attacks and people can be prepared before it is too late to identify the attack and rectify the damage it has already caused. People who work on the system every day have great insight into the vulnerabilities of the SCADA network and should be consulted when identifying potential attack scenarios and possible consequences. Various protection strategies can be discussed and implemented for protection.

### 12. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.

Organization personnel need to understand the specific expectations associated with protecting information technology resources through the definition of clear and logical roles and responsibilities. Necessary care should be taken care that the system should not be attacked from an inside resource itself. Responsibility of protecting and accessing system should be carefully assessed before giving it to any person. Establish a cyber-security organizational structure that defines roles and responsibilities and clearly identifies how cyber security issues are escalated and who is notified in an emergency. One of the key ways for the Stuxnet to spread is by external devices which may have been accessed by lot of people working in the organization. Hence it required to clearly identify and give authority to the right people to access or utilize certain system and devices.

### 13. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.

In-depth understanding of the functions that the systems perform and the sensitivity of the stored information is required. Without this understanding, risk cannot be properly assessed and protection strategies may not be sufficient. It is very important to analyze the damage that a malware like Stuxnet can pose and determine the possibilities of elimination of these viruses and the time required to remove them from the system or the amount of protection that may be required. Identifying the systems that perform critical duties could give an idea about the amount of damage the malware could pose and hence appropriate level of protection can be devices for it. If Stuxnet attacks any nuclear system and it takes hold of key functions in the system, it could pose a great danger. Hence the level of protection for such conditions should be thoroughly analyzed and implemented.

### 14. Establish a rigorous, ongoing risk management process.

A thorough understanding of the risks to network computing resources from denial-of-service attacks and the vulnerability of sensitive information to compromise is essential to an effective cyber security program. Risk assessments form the technical basis of this understanding and are critical to formulating effective strategies to mitigate vulnerabilities and preserve the integrity of computing resources. Virus like Stuxnet could be mitigated through understanding the risk that the system is put through and how certain information alone needs the utmost priority before the other information.

### 15. Establish a network protection strategy based on the principle of defense-in-depth.

Defense-in-depth must be considered early in the design phase of the development process, and must be an integral consideration in all technical decision-making associated with the network. It helps in mitigating the risks that have already been identified. Single points of failure must be avoided, and cyber security defense must be layered to limit and contain the impact of any security incidents. This can isolate the damage to a particular location than it spreading continuously.

### 16. Clearly identify cyber security requirements.

Organizations and companies need structured security programs with mandated requirements to establish expectations and allow personnel to be held accountable. A formal program is essential for establishing a consistent, standards-based approach to cyber security throughout an organization and eliminates sole dependence on individual initiative. Strict security policies and protocols must be adhered to, to prevent attacks from Stuxnet. Establish requirements to minimize the threat from malicious insiders, including the need for conducting background checks and limiting network privileges to those absolutely necessary. This allows access only to individuals who need to use the system. Allowing lot of people to access important system data and devices increases the risk of transferring and spreading Stuxnet.

### 17. Establish effective configuration management processes.

Configuration management needs to cover both hardware configurations and software configurations. Changes to hardware or software can easily introduce Stuxnet into the system .network security is compromised in such cases. Hence it is required to evaluate and control any changes in the system.

### 18. Conduct routine self-assessments.

Robust performance evaluation processes are needed to provide organizations with feedback on the effectiveness of cyber security policy and technical implementation. The issues posed by malwares should be analyzed and the right protection should be implemented. Self-assessment processes that are normally part of an effective cyber security program include routine scanning for vulnerabilities, automated auditing of the network, and self-assessments of organizational and individual performance. These help in eliminating virus and any malware in the system.

### 19. Establish system backups and disaster recovery plans.

It is essential to have a system backup and recovery in case it is attacked by dangerous malware such as Stuxnet which can damage all the information present in the system. Recovery plans help in early recovery which can prevent the system from further damage and prevent loss.

### 20. Senior organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.

Effective cyber security performance requires commitment and leadership from senior managers in the organization. It is essential that senior management establish an expectation for strong cyber security and communicate this to their subordinate managers throughout the organization. Without support from the authority and necessary action, malware like Stuxnet can be prevented and removed from the system successfully.

### 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.

Data related to the SCADA network should be given only on a strict, need-to-know basis, and only to persons explicitly authorized to receive such information. The more information revealed about a computer or computer network, the more vulnerable the computer/ network is to Stuxnet. Any requests for information by unknown persons need to be sent to a central network security location for verification and fulfillment. People can be a weak link in an otherwise secure network. Conduct training and information awareness campaigns to ensure that personnel remain diligent in guarding sensitive network information, particularly their passwords.

## Part B:

Protecting SCADA systems is clearly the highest security objectives within these companies, and the most difficult to achieve. For companies that run SCADA networks, Stuxnet shows the harm a determined, highly skilled attacker with ample resources might do**. Having proper encryption and key management possibly could have prevented Stuxnet from attacking the system. Also the steps mentioned above can help in preventing attacks from malware like Stuxnet to a great extent if implemented correctly.** No electronic security perimeters, data diodes or anti-virus software could prevent the Stuxnet from attacking mainly because it was cleverly coded and implemented virus. The main source for Stuxnet was USB drive which was used by individuals in the company. Even though the system is not connected to a potentially insecure network the Stuxnet gained access into the system. In the case of Stuxnet, managed security services would, for example, watch for downloaded data traffic carrying .LNK files, which could potentially be related to one of the now patched zero-day vulnerability exploits used by the threat. Stuxnet can also propagate by exploiting vulnerability in Windows Print Spooler Service. Additionally, Stuxnet exploits an older vulnerability in the Windows Server service. Stuxnet can self-update through a P2P network installed by the worm. This network enables the Stuxnet worm to communicate with other infected hosts. Stuxnet can also propagate by exploiting vulnerability in Windows Print Spooler Service.

The vector for Stuxnet had been data sticks — USB flash drives. Because industrial control systems are often disconnected from the Internet and overall corporate networks for security reasons, thumb drives are frequently used to transfer data to and from such systems and also to implement patch updates. Infected thumb drives carried into organizations by unwary contractors was likely one of the initial propagation methods used to spread the threat. Device control policies can control what files and applications are allowed to run off thumb drives and, if properly set, will prevent malicious executable files, like those used by Stuxnet, from running on targeted systems. Though Traditional protections, such as signature-based antivirus, are the most common method of defending against the initial infection stage. Unfortunately, many modern pieces of targeted malware rely on mutated code that is altered before each new attack and tested against antivirus solutions to ensure it will evade detection. Signature-based detection is ineffective at identifying brand new, never-before-seen malware. Stuxnet like many targeted and non-targeted attacks used previously unknown software vulnerabilities to gain access to susceptible systems. Hence one of the steps such as securing the system against any kind of loopholes should be able to prevent such attacks.