**Security and Support in IT G (6689) – Assignment 1**

**Submitted by:**

**Name: Tenzin Dendup**

**Student ID: u3149399**

**Answers:**

1. ‘Automation for uniformity’ mainly refers to automation of operating system installations, configuration and updates for desktop computers to maintain uniformity.

Automation is a good solution because it:

* results in machines which are uniform and identical in their configuration and setup.
* leads to easier support and management of desktop computers.

In an organization with 15 desktops, I would implement a fully automatic system if all the desktops have identical hardware. Fully automatic system is chosen because:

* automation will save time and resources during installation phase and subsequent user support
* automation will result in consistent and uniform desktop computers.

A fully automatic system will not be opted if the hardware is not identical across all the 15 computers since this might result in the system administrator having to prepare separate automatic system for each hardware type.

1. Following are the technologies used in server computers to improve reliability, availability and performance:

* Redundancy – This includes redundant power supplies, multiple network connections, backups (full and n+1)
* Hot-swappable components – components which can be plugged in without having to halt the server computer, which avoids downtime
* RAID – Redundant Array of Independent Disks. Depending on its configuration, RAID provides difference features like reliability, availability, performance and capacity.
* Load balancers – both hardware or software implementation of load balancers which will distribute service request loads across multiple servers

1. The “Scope of Coverage” of a Helpdesk operation is a policy defining the scope of support provided by the help desk. It mainly defines what is being supported, who will be supported, when is the support provided and for how long the average support request takes to complete.
2. Trusted certificate authority are companies or government organizations which are trusted to issue digital identification certificates. These certificates are used to verify the identity of people or organizations to enable secure communication. They are important because they play a crucial role to establish trust between entities like IT departments or universities and students involved in the communication process.

To guarantee the authenticity of announcements, the department or the university can use public-key certificate. A public-key certificate consists of public key and identity of the university signed by a trusted certificate authority. In order to send announcements to students the university will take the following steps:

1. get the university’s public key certificate from a trusted certificate authority
2. Prepare the announcement message
3. Generate hash of the message
4. Encrypt the hash using university’s private key
5. Send the message and encrypted hash together with the public key certificate to the student

At the students’ side, they will take the following steps:

1. Decrypt the hash using university’s public key
2. Generate hash of the received message
3. Compare the two hashes to check if they are same or not

The fact that the public key certificate is signed by the trusted certificate authority ensures that the public key belongs to the university. Match between generated hash and decrypted hash ensures that the message is authentic and not changed by someone. And the students being able to decrypt the hash using university’s public key means that it was encrypted by university’s private key which ensures that the message was prepared and send by the university.

**References**:

1. Thomas A. Limoncelli, Christina J. Hogan and Strata R. Chalup, “*The Practice of System and Network Administration*” Second Edition, Addison-Wesley, 2007
2. William Stallings and Lawrie Brown, “*Computer Security: Principles and Practices*” third edition, Pearson Education Limited, 2015.