Name: William Fu Date: Jan. 17, 2017

Application Layer Protocol Assignment

Answer the following questions for 3 protocols listed below.

1. What is the protocol used for specifically (essentially define what it is)?

DNS: Domain Name System is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols.

FTP: File Transfer Protocol is the standard network protocol used for the transfer of computer files between a client and server on a computer network. FTP is built on a client-server model architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS)

SSH: Secure Shell is a cryptographic network protocol for operating network services securely over an unsecured network. The best-known example application is for remote login to computer systems by users. SSH provides a secure channel over an unsecured network in a client-server architecture, connecting an SSH client application with an SSH server. Common applications include remote command-line login and remote command execution, but any network service can be secured with SSH. The protocol specification distinguishes between two major versions, referred to as SSH-1 and SSH-2.

2. What are the pros and cons?

DNS:

Pros: Can work across multiple networks. Names of machines are very telling. Does not saturate the local network. High reliability

Cons: Sniffing systems do not have to perform reverse lookups. Sniffing systems can do batch reverse lookups later on

FTP:

Pros: allows you to transfer not only multiple files but multiple directories at one time. Ability to resume file transfer. Ability to schedule transfer. Rate at which files are transferred

Cons: usernames, passwords and files are sent in clear text. Filtering active FTP connections is difficult. Hard to script jobs. Easy for inexperienced users to wipe out work. Inconsistency/inability to track what has been uploaded on the remote system

SSH:

Pros: Security. Safe passwords. Can turn authentication from single to double level (must obtain private key and password). Stronger identity checking. Non- interactive login is possible

Cons: Extra work to setup. Encryption overhead for CPU and bandwidth. If private keys are not protected, security is no better than with password authentication. Not very scalable

3. Is there any history on its origin?

DNS: In 1984, four UC Berkeley students, Douglas Terry, Mark Painter, David Riggle, and Songnian Zhou, wrote the first Unix name server implementation for the Berkeley Internet Name Domain, commonly referred to as BIND. In 1985, Kevin Dunlap of DEC substantially revised the DNS implementation. Mike Karels, Phil Almquist, and Paul Vixie have maintained BIND since then.

FTP: The original specification for the File Transfer Protocol was written by Abhay Bhushan and published as RFC 114 on 16 April 1971. Until 1980, FTP ran on NCP, the predecessor of TCP/IP. The protocol was later replaced by a TCP/IP version, RFC 765 (June 1980) and RFC 959 (October 1985), the current specification. Several proposed standards amend RFC 959, for example RFC 1579 (February 1994) enables Firewall-Friendly FTP (passive mode), RFC 2228 (June 1997) proposes security extensions, RFC 2428 (September 1998) adds support for IPv6 and defines a new type of passive mode.

SSH: In 1995, Tatu Ylönen, a researcher at Helsinki University of Technology, Finland, designed the first version of the protocol (now called SSH-1) prompted by a password-sniffing attack at his university network. The goal of SSH was to replace the earlier rlogin, TELNET, ftp and rsh protocols, which did not provide strong authentication nor guarantee confidentiality. Ylönen released his implementation as freeware in July 1995. In December 1995, Ylönen founded SSH Communications Security to market and develop SSH.

4. Name an application (i.e., Email, Skype etc..) that implements (use) the protocol.

DNS: Servers for large website. Use to remember other computers and network devices IP addresses. DNS is translator between hostname and IP address.

FTP: Internet Explorer. FileZilla

SSH: PuTTY