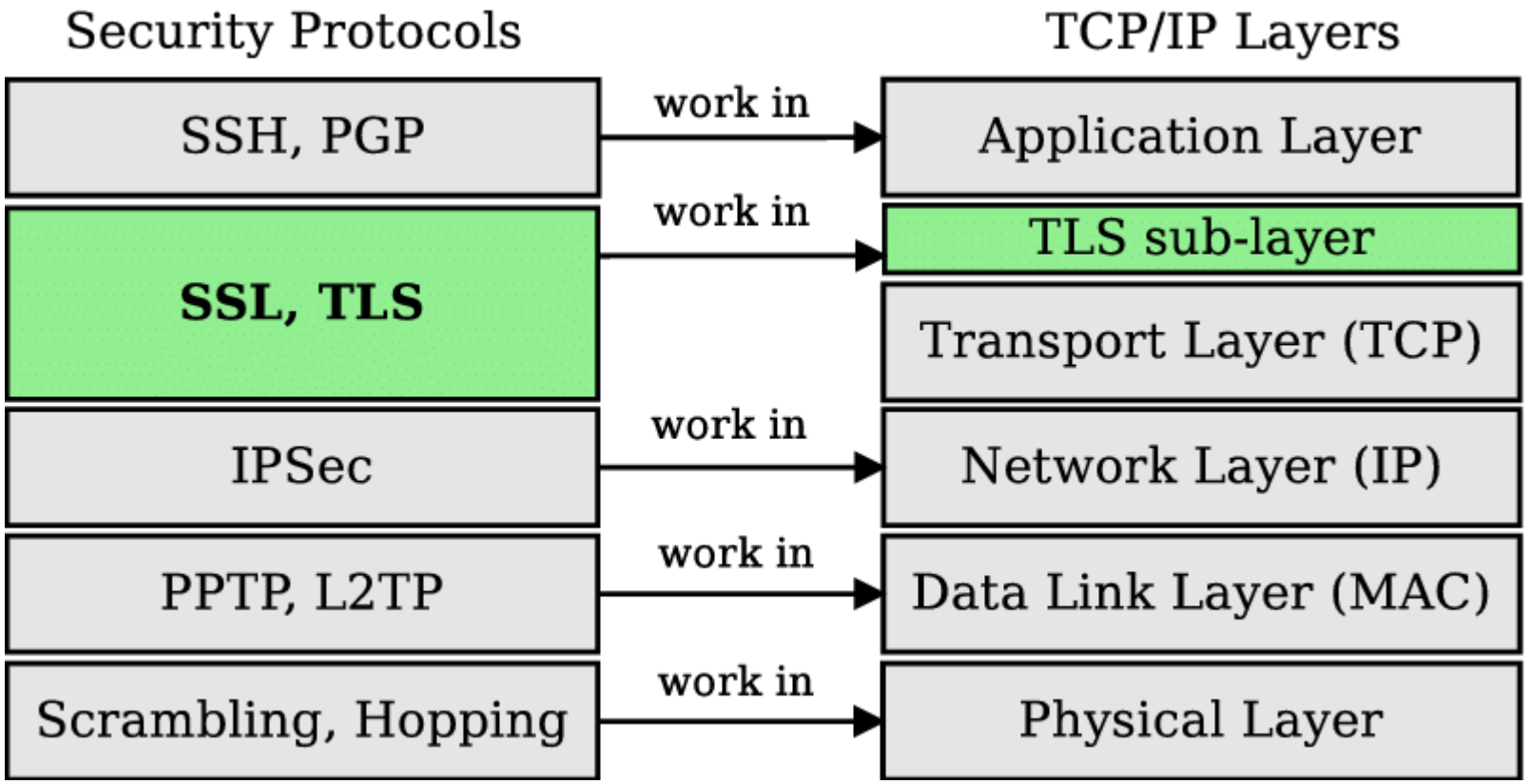
Tutorial 6

An Important Pic

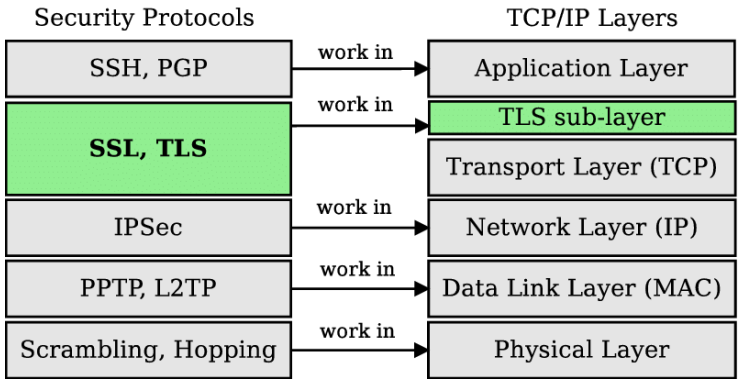


About 79,700,000 results (0.29 seconds)

22 TCP

Changing the Default SSH Port

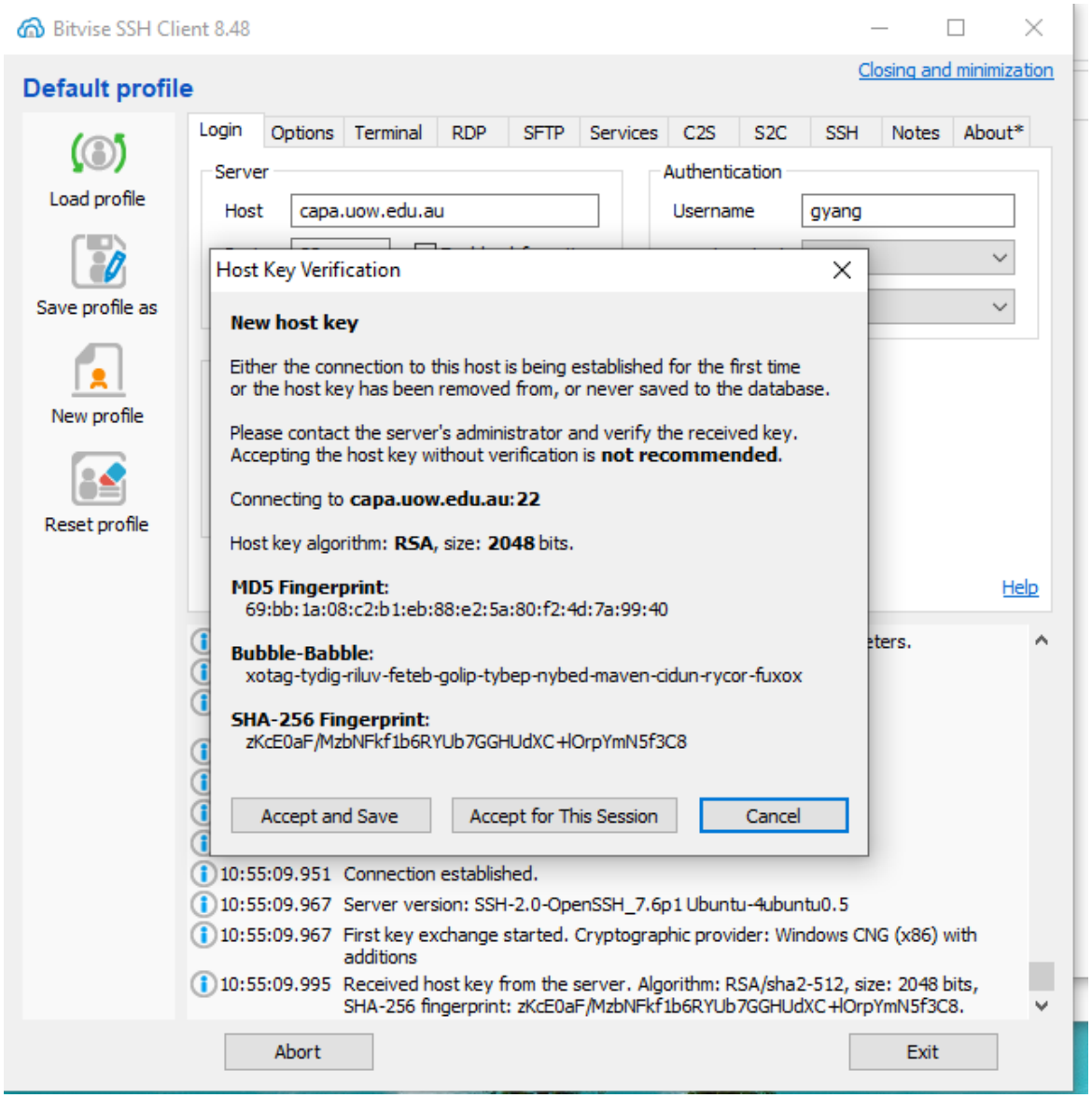
Port Number	Service	Description
22	**TCP**	Secure Shell (SSH) communication.
23	TCP	Used by the Telnet protocol.
25	TCP	The default port for relaying emails via SMTP.
53	DNS	Port for transferring Domain Name System (DNS) queries.

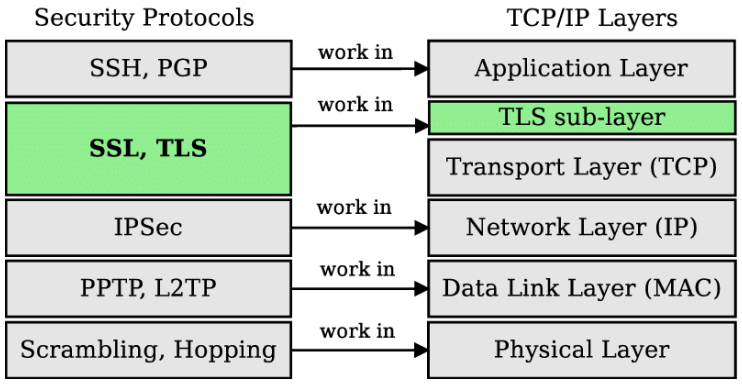


1.Alice is using computer A and Bob is using computer B. Alice doesn't know B before. Can you use SSH to have a secure communication (B is the host)?

- No. SSH protocol doesn't use certificates. Alice must **SECURELY** get Bob's public key first. (see the next page)

SSH Key Fingerprints





2.Bob is hosting a web server via port number 80 in his company. However, the firewall in his company has blocked all requests sent to port number 80. How can Bob visit the website homepage at home using SSH?

❖ The key solution is called port-forwarding.

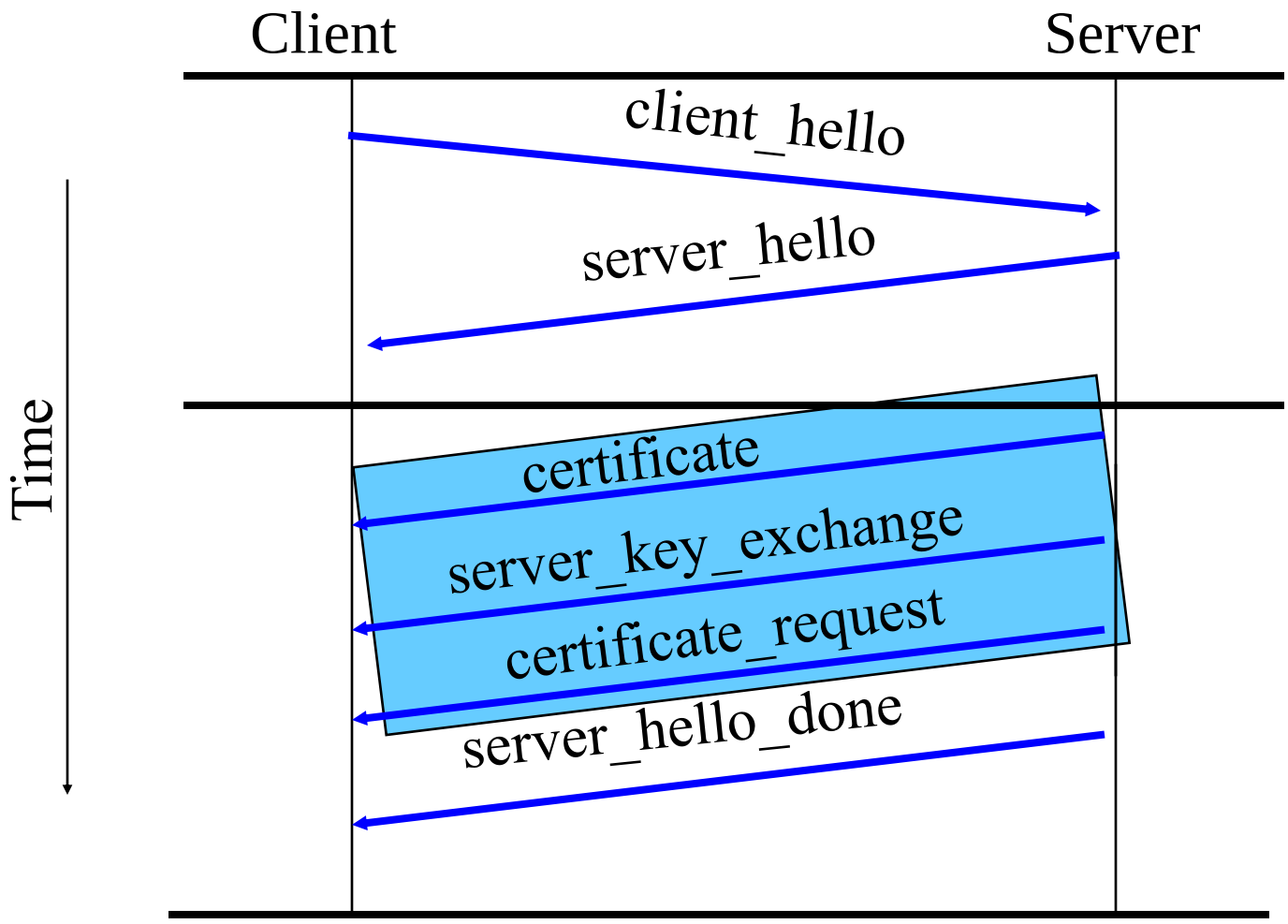
2.Bob is hosting a web server via port number 80 in his company. However, the firewall in his company has blocked all requests sent to port number 80. How can Bob visit the website homepage at home using SSH?

- suppose that the browser should visit www.com.au:80
- The SSH client at home will monitor the port 8015 and forward the received access request via SSH channel to the SSH server at company.
- Now, Bob at home visit www.com.au:80 via 8015.
- The SSH server will send the website request to port number 127.0.0.1:80 (local device and no block) and get the response.
- The response will be forwarded to Bob's home via SSH channel.
- The Bob at home can request the website info.

SSL/TLS

Handshake Protocol Action

First Half

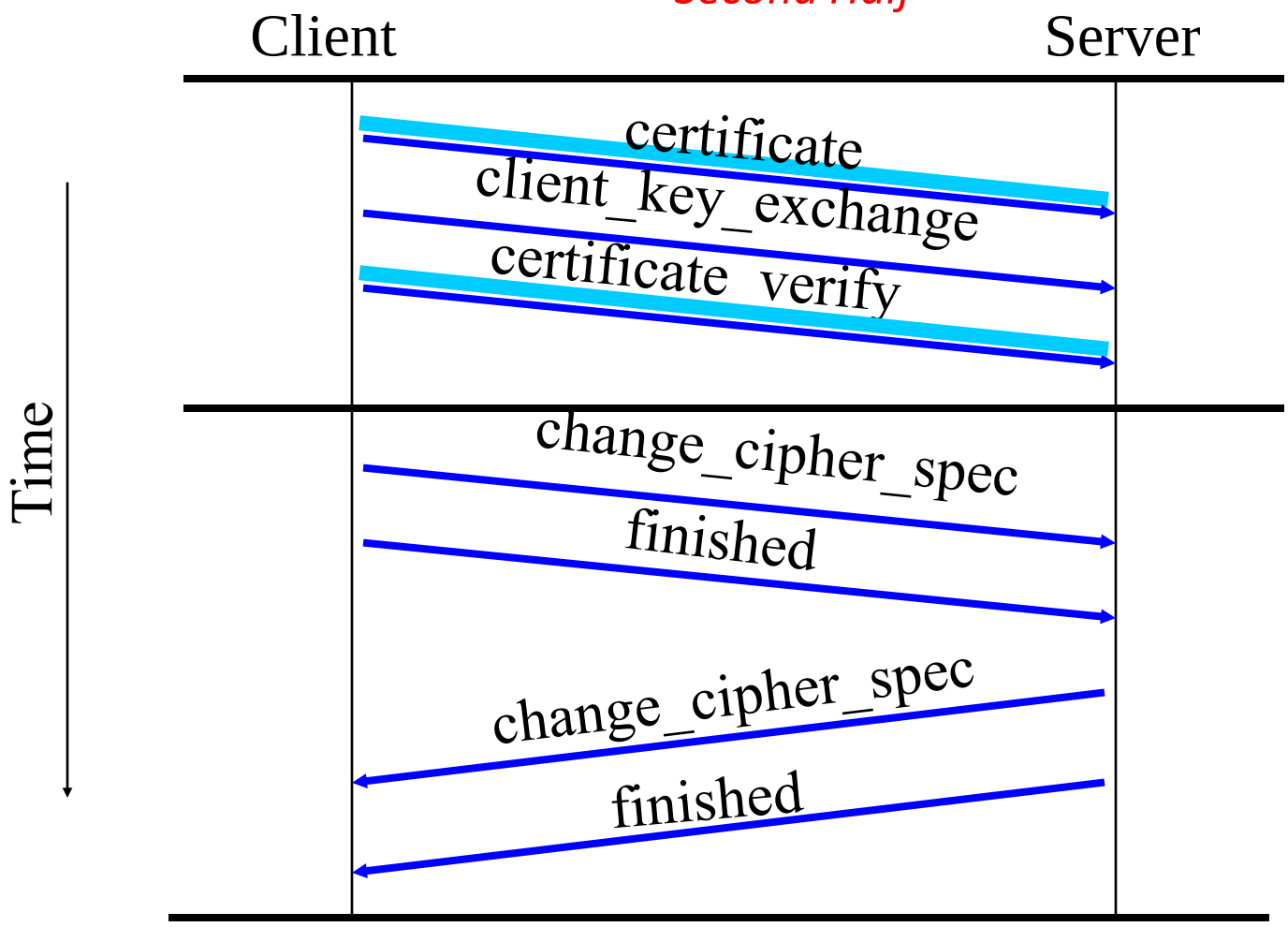


Establish security capabilities, including protocol version, session ID, cipher suite, compression method and initial random numbers.

Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase

Handshake Protocol Action

Second Half



Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

Change cipher suite and finish handshake protocol.

NOTE:- Shaded transfers are optional or situation-dependent messages that are not always sent.

1. Explain how pre_master_secret in SSL is sent to the server using RSA key transport.

This is a sketch of the RSA key exchange method.

A→ B: RA, Hello

B→ A: CertB, Hello, RB.

A→ B: Pre-master-secret encrypted under Bob's public key.

2. What is the advantage of Ephemeral Diffie-Hellman key exchange method over the RSA key transport method?

RSA key transport does not provide forward-secrecy.
If the server's long-term key associated with the Cert is compromised, all the previous sessions are compromised.
Ephemeral Diffie-Hellman can provide forward-secrecy by using ephemeral (or one-time) Diffie-Hellman key exchange in each handshake.

3. Consider the SSL Handshake Protocol. Why does not the action of the client validating the certificate presented by the server authenticate the server to the client?

The certificate contains Server's ID, Public key, Timestamp,... and has been signed by a trusted authority. It can be sent by any one since the certificate is public.
The server is only authenticated when it uses its private key to sign the key exchange message.

4. Is SSL or IPSec sufficient for electronic commerce applications? Justify your answer.

SSL provides client-server authentication (both ways) and encrypts message flows between client and server. It can protect secret information such as credit card numbers or PINs.

It becomes insufficient when the dealer (server) requires a client to sign a credit card payment. The SSL signing functions are used for authentication only. It does not provide flexible signing capability to the application layer.

More complicate payment systems require special payment software to ensure all security issues are addressed. For example, Secure Electronic Transaction (SET) provides more security features than those of SSL.

IPSec ensures the authenticity and confidentiality of network traffic, but it does not provide these features at the application layer. For example, it cannot handle the authenticity of a user.

5. Two computers A and B are running TLS protocols. Now, all applications communicating between A and B cannot be seen by a hacker. Is this correct? Justify your answer.

- No. Only those applications running TLS protocol will be protected. For example, two applications 1 and 2, which send data to port number X and Y of B computer. If X is a normal port number without protection of TLS, then the application 1 is not secure (unless there is another security protection at the application level).