SSL and TLS

- SSL – Secure Socket Layer
- TLS – Transport Layer Security
- The common standards for securing network applications in Internet
  - E.g., web browsing
- Essentially, standards to negotiate, set up, and apply crypto

The Basics of SSL

- Usually a client/server operation
- Client contacts server
- A negotiation over authentication, key exchange, and cipher takes place
- Authentication is performed and key agreed upon
- Then all packets are encrypted with that key and cipher at application level

Common Use

- Server authenticates to client using an X.509 certificate
  - Typically, client not authenticated
    - Though option allows it
- Client provides material to server to derive session key
- Client and server derive same session key, start sending encrypted packets

Crypto in TLS/SSL

- Several options supported
- RSA or elliptic curve for PK part
- AES, DES, 3DES, or others for session cryptography
- Not all are regarded as still secure
- Chosen by negotiation between client and server

Use of SSL/TLS

- The core crypto for web traffic
- Commonly used for many other encrypted communications
- Used in all major browsers
- Usually not part of OS per se
  - But all major OSes include libraries or packages that implement it

Security Status of SSL/TLS

- Kind of complex
- SSL is not very secure
- Early versions of TLS not so secure
- Later versions of TLS fairly secure
  - Depending on cipher choice
- Recent chosen-plaintext attacks shown to work on all versions
  - In special circumstances

Virtual Private Networks

- VPNs
- What if your company has more than one office?
- And they're far apart?
  - Like on opposite coasts of the US
- How can you have secure cooperation between them?
- Could use leased lines, but . . .

Encryption and Virtual Private Networks

- Use encryption to convert a shared line to a “private line”
- Set up a firewall at each installation’s network
- Set up shared encryption keys between the firewalls
- Encrypt all traffic using those keys

Actual Use of Encryption in VPNs

- VPNs run over the Internet
- Internet routers can't handle fully encrypted packets
- Obviously, VPN packets aren't entirely encrypted
- They are encrypted in a tunnel mode
  - Often using IPSec
- Gives owners flexibility and control

Key Management and VPNs

- All security of the VPN relies on key secrecy
- How do you communicate the key?
  - In early implementations, manually
  - Modern VPNs use IKE or proprietary key servers
- How often do you change the key?
  - IKE allows frequent changes

VPNs and Firewalls

- VPN encryption is typically done between firewall machines
  - VPN often integrated into firewall product
- Do I need the firewall for anything else?
- Probably, since I still need to allow non-VPN traffic in and out
- Need firewall “inside” VPN
  - Since VPN traffic encrypted
  - Including stuff like IP addresses and ports
  - “Inside” can mean “later in same box”

VPNs and Portable Computing

- Increasingly, workers connect to offices remotely
  - While on travel
  - Or when working from home
- VPNs offer a secure solution
  - Typically as software in the portable computer
- Usually needs to be pre-configured

VPN Deployment Issues

- Desirable not to have to pre-deploy VPN software
  - Clients get access from any machine
- Possible by using downloaded code
  - Connect to server, download VPN applet, away you go
  - Often done via web browser
  - Leveraging existing SSL code
  - Authentication via user ID/password
  - Implies you trust the applet . . .
- Issue of compromised user machine