Security vulnerabilities in the Internet and possible solutions

Presentation by

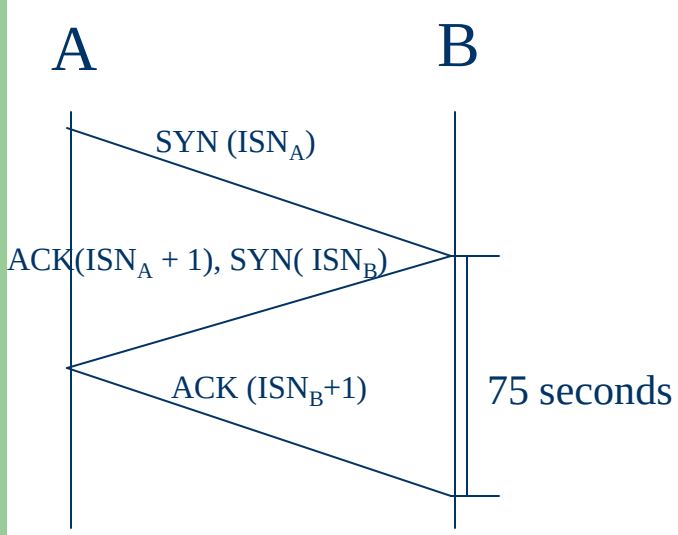
Hemant Kumar

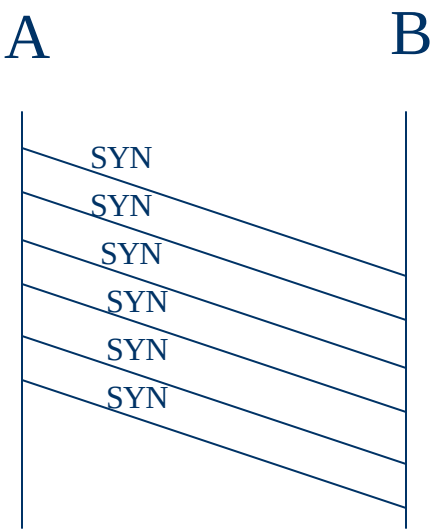
History

- TCP/IP Suite designed in early 1980s
- No thought to security
- With widespread usage comes widespread abuse

Attacks on TCP/IP

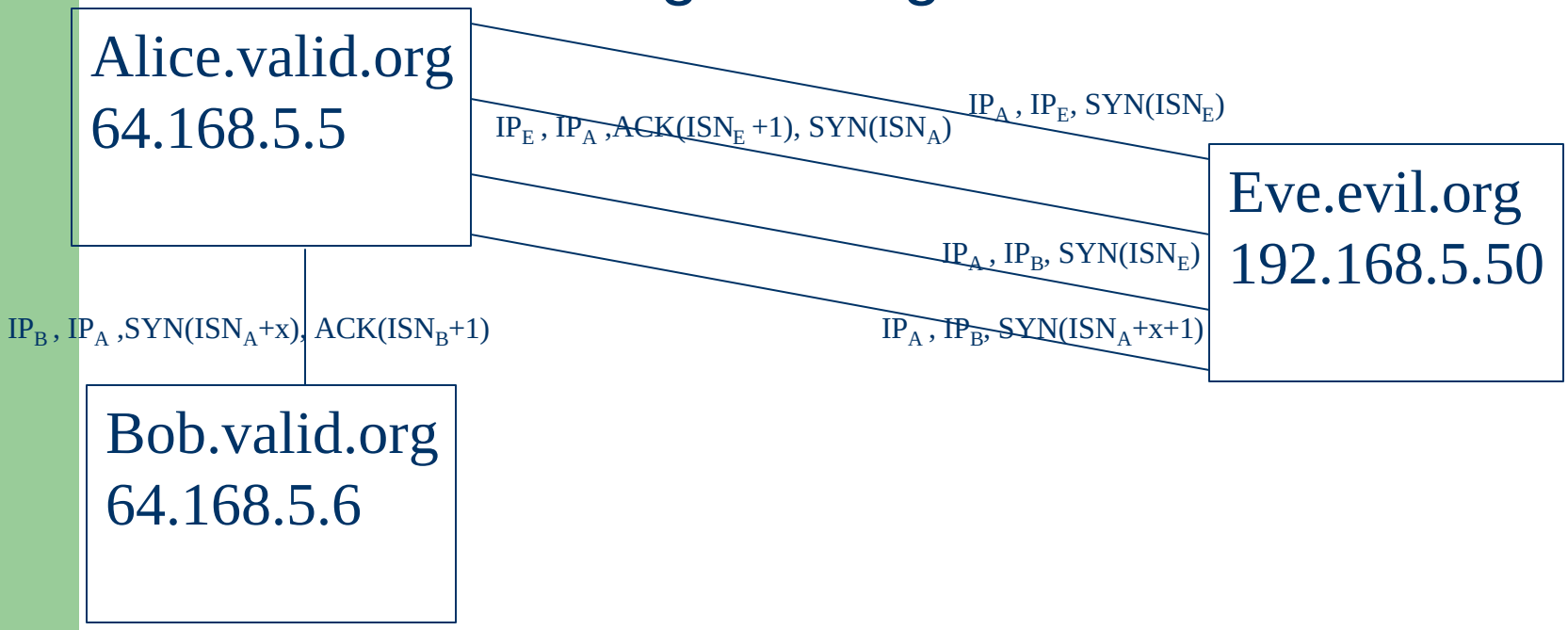
- SYN-Flood, Smurf and UDP flood attacks
  Tools : Trinoo, Stacheldraht, Trinity, Shaft, TFN





IP Spoofing

- Faking the source address in IP packets
  - relies on ISN guessing



ICMP Misuse

- Denial of Service - Destination unreachable, Time to live exceeded
- Redirect through attacker - ICMP Redirect
- Port Scanning and Network mapping – ICMP request reply (e.g. Cheops)

Connection Hijacking

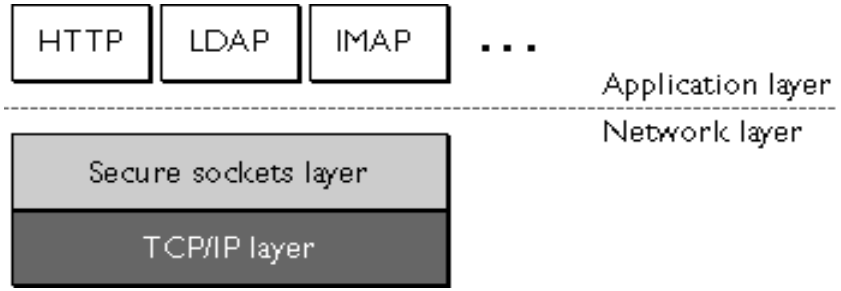
- Defeats one time authentication methods (e.g. rlogin, ftp etc)
  - needs to snoop traffic
  - bring down the client by DoS
  - Spoof the client

Snooping

- Shared transmission media (e.g. ethernet, wireless)
- Compromised infrastructure elements (e.g.routers)

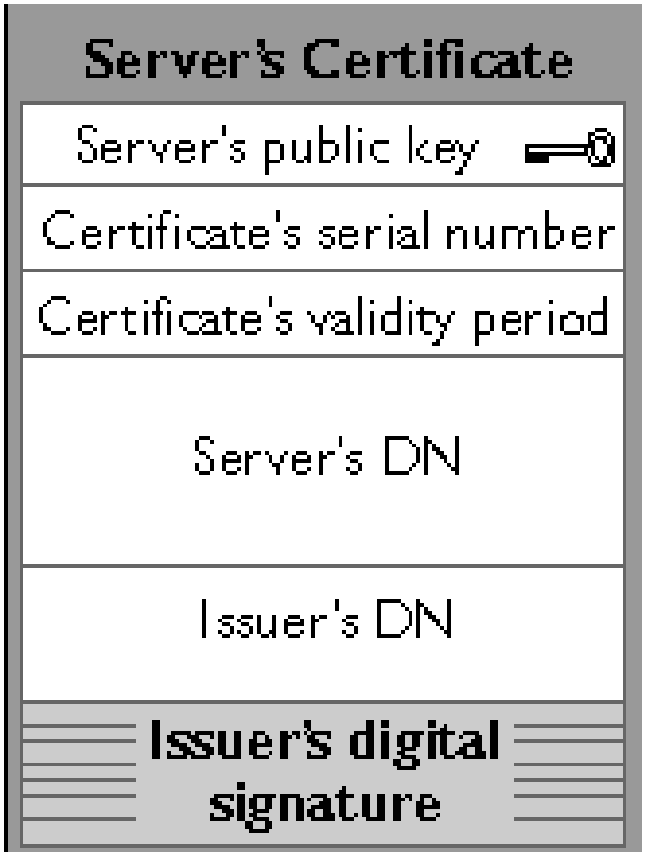
Secure Socket Layer

- Addresses security on Transport layer
- Uses Digital Certificates of entities to authenticate and share key.
- Digital Certificates are issued by Certifying authorities whose public key is embedded inside the browsers.
- No setup required at client end for individual connection (if client authentication is not required)
- Commonly used scheme for client-server communication HTTPS, SFTP, POP3S, NNTPS, LDAPS are plain protocols inside SSL.



Digital Certificates

1. Chose a public key/private key
2. Give public key to a certifying authority
3. CA verifies antecedents and signs the public key/Distinguishing name combination



IPSec

- Provides security on network layer.
- Comes with IPv6, also available with IPv4.
- Commonly used to make VPN connections.
- Highly flexible. Allows user to:
  - select which aspects of security to address (authentication, confidentiality, integrity, replay protection.)
  - choose encryption algorithm, key parameters, signature etc.
  - granularity with which the security services are applied.
- Two parts :
  - Security Association and Key Management
  - Security Headers (Authentication header, Encapsulating Security Payload)

IPSec

Internet Security Association and Key Management Protocol (ISAKMP)

-Used for negotiating options between two ends.

Authentication header

-Inserted between IP and payload

-Ensures data integrity & authentication but payload is still plaintext

Encapsulating Security Payload

-Inserted between IP and payload

-Ensures integrity, authentication, replay protection & confidentiality

Denial of Service protection

- Still being researched
- An interesting aspect is that encryption might increase possibility of DoS.
- Some preliminary methods include
  - Ingress filtering
  - IP traceback
  - Server side methods