Week 11: Network Security

Internet Technologies COMP90007

Lecturer: Muhammad Usman

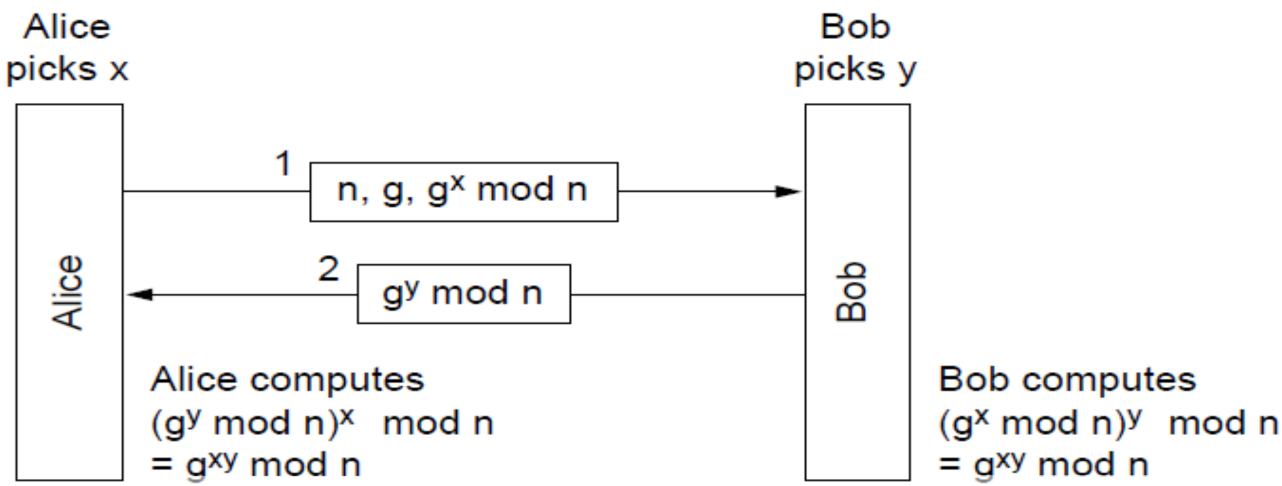
Semester 2, 2020

Authentication

- **Authentication is a primary tenet** of network security
- However, **authentication process itself needs to be secure** also
- A fundamental principle: **minimise the use of permanent keys in establishment of secure connections** (the less packets are exchanged using such keys, the less exposure to potential attackers)
- Four methods in common use:
  - Shared keys
  - Key distribution
  - Kerberos
  - Public keys

Authentication Based on a Shared Secret Key

- How to create a key with Diffie-Hellman key exchange:



Shared secret

Shared secret

Is there a way to break this? Still open to man-in-the-middle attack!

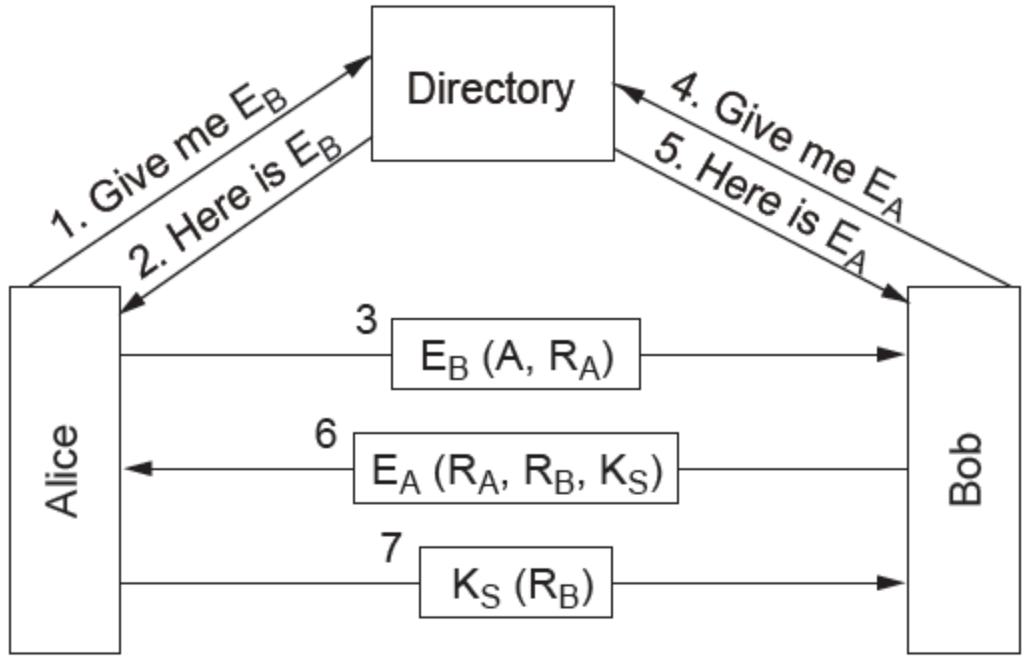
Authentication Using a Key Distribution Center

- In this method, **<u>a trusted intermediary is used</u>** to facilitate
- Users each share a key with a central key distribution centre, and authenticate to the KDC directly
- The KDC acts as a relay between the two parties
- There are issues here as well:
  - Open to **<u>replay-attack</u>**
- Solutions exist to patch the KDC mechanism
  - E.g. timestamps

Authentication Using Kerberos

- Similar to KDC a popular protocol emerged and in frequent use today: Kerberos
- In this method, a multi-component system is required
  - Authentication Server
  - Ticket Granting Server (TGS)
  - Recipient
- Authentication is managed centrally, and then <u>**party to party communication is facilitated by single use tickets**</u>
- Still disadvantages remains: Does not scale to large numbers; different businesses need to trust each other’s TGSs…

Authentication Using Public Key Cryptography



IPSec

- Where to put security?
  - Some say application layer: but users may not want such things
  - Some say lower layers: but not as strong as having it at app layer
  - Outcome is **<u>security can/should be in multiple layers</u>**
- One can put security at application level but also…
- **<u>IPSec (RFC 2401,..) puts it at the network</u>** level as well
- In the IPSec model, **<u>encryption is compulsory, but a null encryption algorithm can be used</u>** between points
- The main IPSec framework features are **<u>secrecy, data integrity, and replay</u>** attack protection
- The IPSec framework allows multiple algorithms and multiple levels of granularity, connection-oriented (**<u>connections are named as SA's security associations</u>**)

IPSec Implementation

- IPSec has two main implementation components
  - Things being added to packets in transit
  - ISAKMP key management: Internet Security Association and Key Management Protocol for establishing keys

- IPSec has 2 modes
  - Transport mode - uses header insertion after IP Header
  - Tunnel mode - uses packet encapsulation

Virtual Private Networks

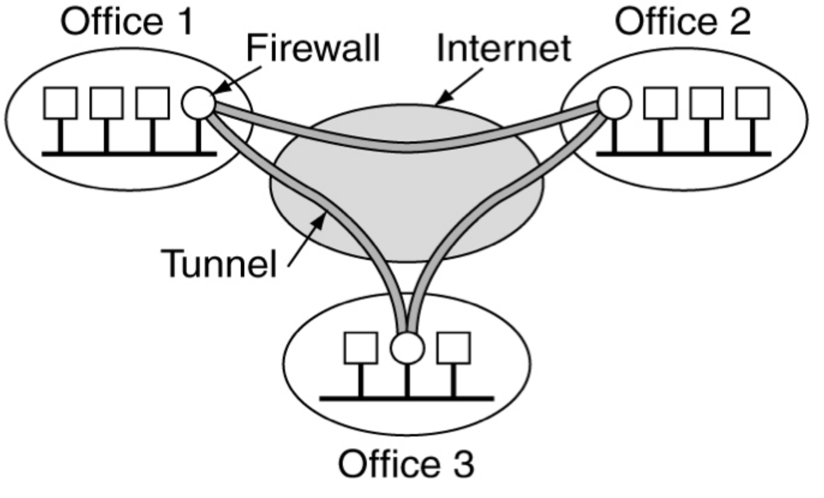
- Unlike a physical network based on leased lines between locations for which secure transit is required

- A Virtual Private Network (VPN) is **a virtual layer on top of an IP network which provides a secure end-to-end connection** over public infrastructure

- A common VPN implementation model:
  - **Use a firewall at each end of a connection**
  - Setup a **SA to create an IPSec tunnel between the two end points**
- Communication on this infrastructure is **transparent to end users**

VPN

A virtual private network



Firewalls

- While IPSec ensures security in transit, a **firewall ensures security at the network perimeter**

- Firewalls are positioned at the network boundary, and **provide a controlled series of routes between the internal and external networks**

- Three characteristics of firewalls
  - All inbound and outbound traffic must transit the firewall
  - Only authorised traffic must pass through the firewall
  - Firewalls should be immune to penetration themselves

Firewall Scope

- Check packets for “bad” packets
  - Administrators can **<u>write rules for this</u>**, e.g., distinguish regular HTTP from P2P related HTTP
- **<u>Not everything is inside the wall</u>**
- Web servers and email servers etc **<u>need to be exposed to allow more open communication</u>**
  - Best firewall is NOT disconnecting everything from the Internet
- Through **<u>further rules packets go in-between this gray area and the LAN</u>**
- Firewalls don’t provide protection against inhouse threats
- Applications can still distribute viruses (via bad attachments for example)

Wireless Security Context

- Wired networks are relatively easy to secure because they require physical access to intercept traffic
- Wireless networks are more difficult to secure because of **omnidirectional signal propagation**
- Additionally by default **most wireless network equipment operates in an insecure and promiscuous manner**
- 802.11 has a native secure protocol, **Wired Equivalency Protocol** (WEP), which is a 40-bit encryption based on RC4 algorithm

Wireless Security Issues

- Two inherent insecurities
  - 40 bit encryption is breakable with low-moderate computational resources
  - RC4 re-uses keys, so capturing a small volume of encrypted traffic will guarantee key identification
- Given these constraints, how can wireless networks be secured?

Securing Wireless

- Additional encryption (128bit WEP)
  - Increased security through longer key lengths
- MAC Address Filtering
  - Only allow specified MAC interfaces to establish connections
- …
- WPA2 (WiFi Protected Access 2)
- …
- Multilayered security
  - Use a VPN over wireless