

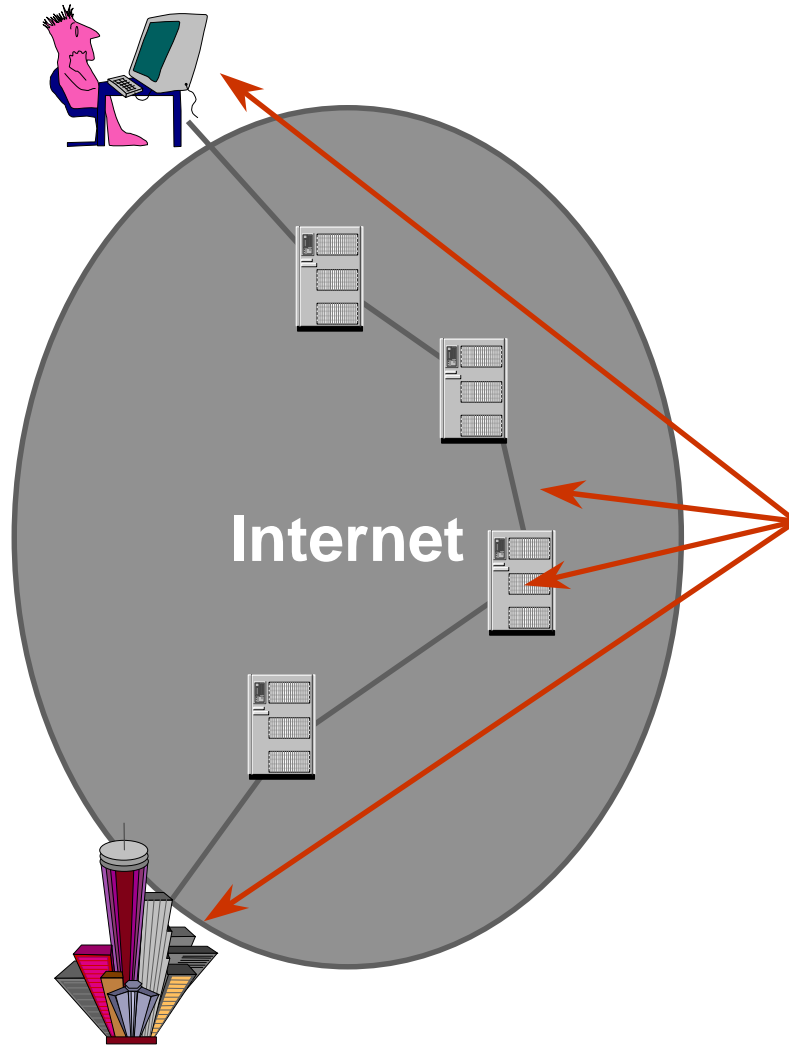
Outline



Secure end-to-end transport



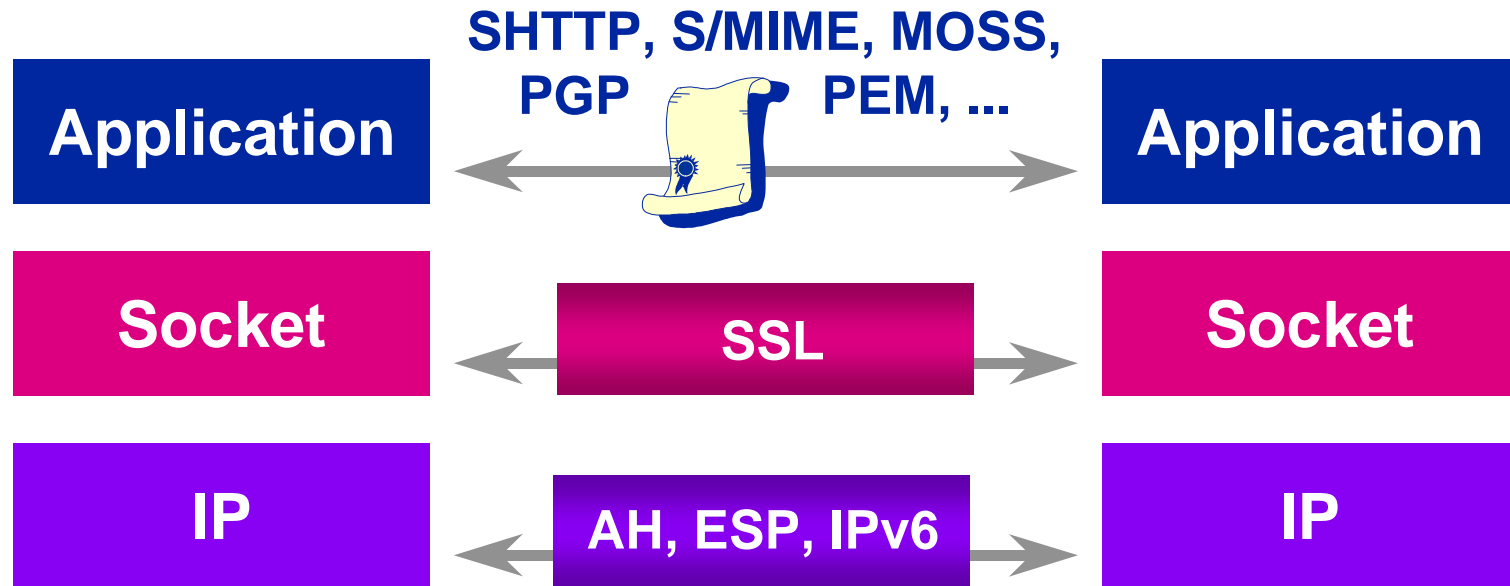
Internet Security: Today



- u **Requirements**
 - u Integrity, Authentication, Confidentiality
- u **Communication**
 - u As “secure” as sending postcards
- u **User Equipment**
 - u Standard PC: Trojan Horses, Virus



Secure End-to-End Transport



u Cryptography

- u Shared/public key encryption (DES, RSA, etc.)
- u Stream/document authentication by MAC (keyed MD5, etc.) or digital signature (RSA, DSS, etc.)
- u Restrictions: national security, law enforcement



Secure Sockets Layer (SSL)



Client

ClientHello

----->

Server

ServerHello
 Certificate*
 ServerKeyExchange*
 CertificateRequest*
 ServerHelloDone

<-----

Certificate*
 ClientKeyExchange
 CertificateVerify*
 [ChangeCipherSpec]
 Finished

----->

[ChangeCipherSpec]
 Finished

Application Data

<-----

Application Data

----->

Client

ClientHello

----->

Server

ServerHello
 [change cipher spec]
 Finished

<-----

change cipher spec
 Finished
 Application Data

----->

Application Data

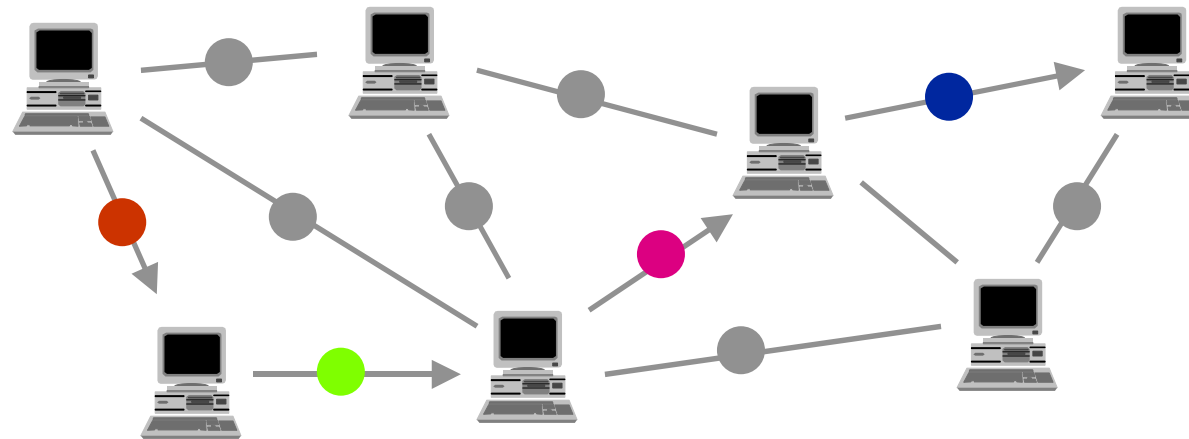
<-----





Anonymous Communication

- u Hide relation between senders and receivers

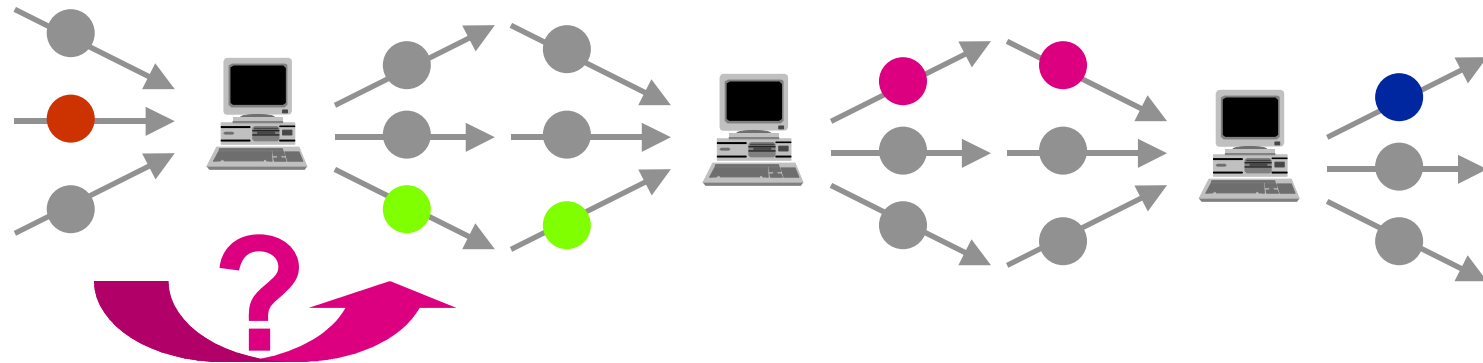


- u **Basic “Mix-Idea”**
 - u Redirect message via several “Mixes”
 - u Each Mix changes appearance of message such that observer cannot relate in/out
 - u Sufficient traffic \Rightarrow anonymity



Anonymous Communication

u Operations of a Mix



u **Contents**

⇒ **Encryption**

u **Time**

⇒ **Delay or reorder**

u **Size**

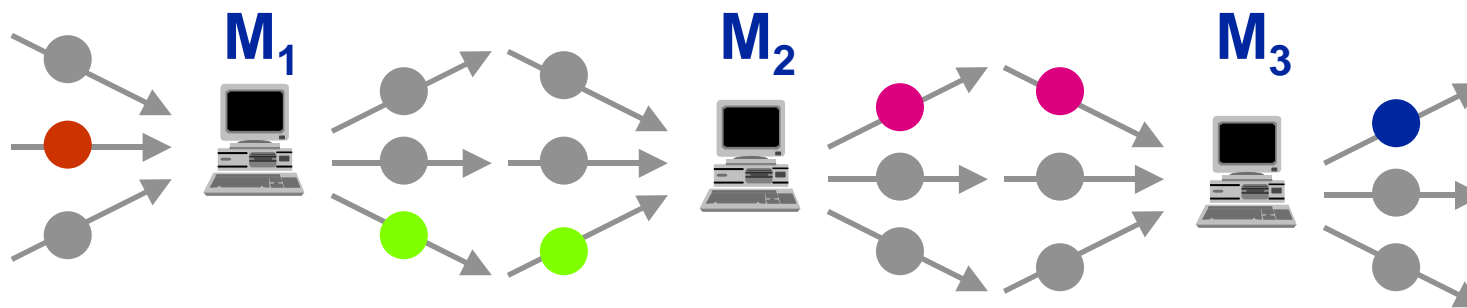
⇒ **Standard packets**

u **Corrupt Mix**

⇒ **Multiple mixes in sequence**

Anonymous Communication

u Cryptographic implementation



u Simple mix message

u $E_1(r_1, E_2(r_2, E_3(r_3, m)))$

u m encrypted for final recipient (pseudonym!)

u route (M_1, M_2, M_3) fixed or randomly chosen

Anonymous Communication

- u **Problem: How to send a message back to anonymous sender?**

⇒ **Anonymous return addresses**

- u S = Sender, R = Recipient

- u S computes “return address”

$$RA := E_1(r_1, k_1, E_2(r_2, k_2, E_3(r_3, k_3, R)))$$

- u R computes mix-message for answer m'

$$RA, m'$$

and sends it to $M_1 \dots$

- u Mixes encrypt it as $k_3(k_2(k_1(m')))$

- u **Efficiency: “short” anonymous channels**