Network Security
CS 239
Security for Networks and System Software
April 29, 2002

Outline

- Catching up on certificates
- Basics of network security

Certificates

- An increasingly popular form of authentication
- Generally used with public key cryptography
- A signed electronic document proving you are who you claim to be

Public Key Certificates

- The most common kind of certificate
- Addresses the biggest challenge in widespread use of public keys
- Essentially, a copy of your public key signed by a trusted authority
- Presentation of the certificate alone serves as authentication of your public key

Implementation of Public Key Certificates

- Set up a universally trusted authority
- Every user presents his public key to the authority
- The authority returns a certificate
  - Containing the user's public key signed by the authority's private key

Checking a Certificate

- Every user keeps a copy of the authority's public key
- When a new user wants to talk to you, he gives you his certificate
- Decrypt the certificate using the authority's public key
- You now have an authenticated public key for the new user
- Authority need not be checked on-line

Scaling Issues of Certificates

- If there are ~550 million Internet users needing certificates, can one authority serve them all?
- Probably not
- So you need multiple authorities
- Does that mean everyone needs to store the public keys of all authorities?

Certification Hierarchies

- Arrange certification authorities hierarchically
- The single authority at the top produces certificates for the next layer down
- And so on, recursively

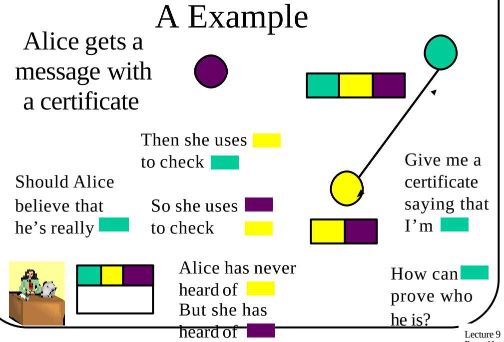
Using Certificates From Hierarchies

- I get a new certificate
- I don't know the signing authority
- But the certificate also contains that authority's certificate
- Perhaps I know the authority who signed this authority's certificate

Extracting the Authentication

- Using the public key of the higher level authority, extract the public key of the signing authority from the certificate
- Now I know his public key, and it's authenticated
- I can now extract the user's key and authenticate it

A Example



Certificates and Trust

- Ultimately, the point of a certificate is to determine if something is trusted
  - Do I trust the request to perform some financial transaction?
- So, Trustysign.com signed this certificate
- How much confidence should I have in the certificate?

Potential Problems in the Certification Process

- What measures did Trustysign.com use before issuing the certificate?
- Is the certificate itself still valid?
- Is Trustysign.com’s signature/certificate still valid?
- Who is trustworthy enough to be at the top of the hierarchy?

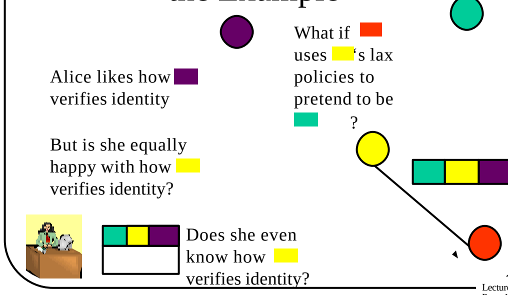
Trustworthiness of Certificate Authority

- How did Trustysign.com issue the certificate?
- Did it get an in-person sworn affidavit from the certificate’s owner?
- Did it phone up the owner to verify it was him?
- Did it just accept the word of the requestor that he was who he claimed to be?

What Does a Certificate Really Tell Me?

- That the certificate authority (CA) tied a public/private key pair to identification information
- Generally doesn’t tell me why the CA thought the binding was proper
- I may have different standards than that CA

Showing a Problem Using the Example



Another Big Problem

- Things change
- One result of change is that what used to be safe or trusted isn’t any more
- If there is trust-related information out in the network, what will happen when things change?

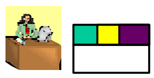
Revocation

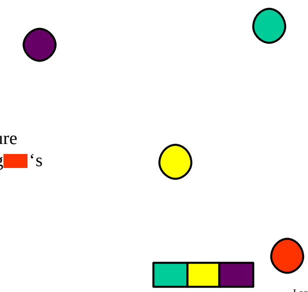
- A general problem for keys, certificates, access control lists, etc.
- How does the system revoke something related to trust?
- In a network environment
- Safely, efficiently, etc.

Revisiting Our Example

Someone discovers that has obtained a false certificate for

How does alice make sure that she's not accepting 's false certificate?





The Web of Trust Model

- Public keys are still passed around signed by others
- But your trust in others is based on your personal trust of them
  - Not on a formal certification hierarchy
  - "I work in the office next to Bob, so I trust Bob's certifications"

Certificates in the Web of Trust

- Any user can sign any other user's public key
- When a new user presents me his public key, he gives me one or more certificates signed by others
- If I trust any of those others, I trust the new user's public key

Limitations on the Web of Trust

- The web tends to grow
  - "I trust Alice, who trusts Bob, who trusts Carol, who trusts Dave, . . ., who trusts Lisa, who trusts Mallory"
  - Just because Lisa trusts Mallory doesn't mean I should
- Working system needs concept of degrees of trust

Advantages and Disadvantages of Web of Trust Model

+ Scales very well
+ No central authority
+ Very flexible
– May be hard to assign degrees of trust
– Revocation may be difficult
– May be hard to tell who you will and won't trust

Some Important Network Characteristics for Security

- Degree of locality
- Media used
- Protocols used

Degree of Locality

- Some networks are very local
  - E.g., an Ethernet
  - Only handles a small number of machines, mostly related ones
- Other networks are very non-local
  - E.g., the Internet backbone
  - Vast numbers of users/sites share bandwidth

Implications of Locality

- Truly local networks may gain from physical security
- Relative trustworthiness of all participants may help
- Common interests of all on a local network may be helpful, too
- Wide area networks generally harder

Network Media

- Some networks are wires or cables
- Other networks run over the telephone lines
- Other networks are radio links to satellites
- Other networks are broadcast radio links

Implications of Media Type

- Wires can sometimes be physically protected
- Radio links generally can't
  - Though power and technology requirements for satellite links may provide some help

Protocol Types

- TCP/IP is probably the most widespread
  - But it only specifies some common intermediate levels
  - Other protocols exist above and below it
- And, in places, other protocols replace TCP/IP
- And there are lots of supporting protocols
  - Routing protocols, naming and directory protocols, network management protocols

Implications of Protocol Type

- The protocol defines a set of rules that will always be followed
  - But usually not quite complete
  - And they assume everyone is at least trying to play by the rules
  - What if they don't?
- Specific attacks exist against specific protocols

Threats to Network Security

- Pretty much the usual suspects:
  - Wiretapping
  - Impersonation
  - Message confidentiality
  - Message integrity
  - Denial of service

CS 239, Spring 2002 — Lecture 9 Page 31

Why Are Networks Especially Threatened?

- Many “moving parts”
- Many different administrative domains
- Everyone can get some access
- In some cases, trivial for attacker to get a foothold on the network
- Networks encourage sharing
- Networks often allow anonymity

CS 239, Spring 2002 — Lecture 9 Page 32

What Can Attackers Attack?

- The media connecting the nodes
- Nodes that are connected to them
- Routers that control the traffic
- The protocols that set the rules for communications

CS 239, Spring 2002 — Lecture 9 Page 33

Wiretapping

- An obvious network vulnerability
  - But don’t forget, “wiretapping” is a general term
    - Not just networks are vulnerable
- **Passive wiretapping** is listening in illicitly on conversations
- **Active wiretapping** is injecting traffic illicitly

CS 239, Spring 2002 — Lecture 9 Page 34

Wiretapping on Wires

- Signals can be trapped at many points
- Actually tapping into some physical wires is possible
- Other “wires” are broadcast media
  - **Packet sniffers** can listen to all traffic
- Subverted routers and gateways also offer access

CS 239, Spring 2002 — Lecture 9 Page 35

Wiretapping on Wireless

- Often just a matter of putting an antenna up
  - Though position may matter a lot
  - Generally not even detectable that it’s happening
- Active threats are easier to detect
  - And, for satellites, technically challenging

CS 239, Spring 2002 — Lecture 9 Page 36

Impersonation

- A packet comes in over the network
  – With some source indicated in its header
- Often, the action to be taken with the packet depends on the source
- But attackers may be able to create packets with false sources

Methods of Network Impersonations

- Even in standard protocols, often easy to change fields in a header
  – When created or later
  – E.g., IP allows forging "from" addresses
- Existing networks have little or no built-in authentication

Authentication to Foil Impersonation

- Higher level protocols often require authentication of transmissions
- Much care required to ensure proper authentication
- And not having authentication underneath can cause many problems
- Authentication schemes are rarely perfect

Violations of Message Confidentiality

- Other problems can cause messages to be inappropriately divulged
- Misdelivery can send a message to the wrong place
  – Clever attackers can make it happen
- Message can be read at an intermediate gateway or a router
- Sometimes an intruder can get useful information just by traffic analysis

Message Integrity

- Even if the attacker can't create the packets he wants, sometimes he can alter proper packets
- To change the effect of what they will do

Methods of Attacks on Message Integrity

- Replacing part of a packet
- Changing headers to alter destination of a packet
  – Or its source
- Inserting improper packets into a proper packet stream

Denial of Service

- Attacks that prevent legitimate users from doing their work
- By flooding the network
- Or corrupting routing tables
- Or flooding routers
- Or destroying key packets

How Do Denial of Service Attacks Occur?

- Basically, the attacker injects some form of traffic
- Most current networks aren't built to throttle uncooperative parties very well
- All-inclusive nature of the Internet makes basic access trivial
- Universality of IP makes reaching most of the network easy

Some Sample Attacks

- Smurf attacks
- SYN flood
- Ping of Death

Smurf Attacks

- Attack on vulnerability in IP broadcasting
- Send a ping packet to IP broadcast address
  - With forged "from" header of your target
- Resulting in a flood of replies from the sources to the target
- Easy to fix at the intermediary
  - Don't allow IP broadcasts to originate outside your network
- No good solutions for victim

SYN Flood

- Based on vulnerability in TCP
- Attacker uses initial request/response to start TCP session to fill a table at the server
- Preventing new real TCP sessions
- SYN cookies and firewalls with massive tables are possible defenses

Normal SYN Behavior

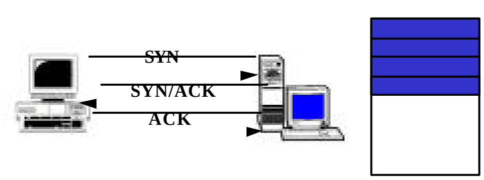
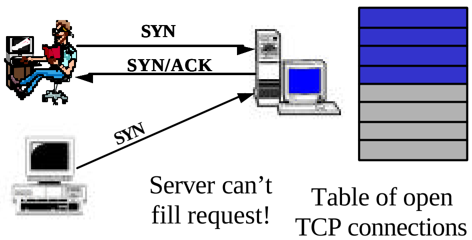
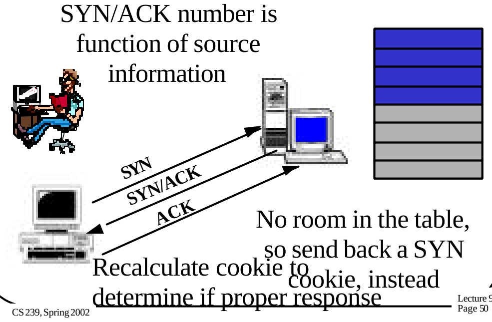


Table of open TCP connections

A SYN Flood



SYN Cookies



The Ping of Death

- IP packets are supposed to be no longer than 65,535 bytes long
- Can improperly send longer IP packets
- Some OS networking software wasn't prepared for that
  - Resulting in buffer overflows and crashes
- Can filter out pings, but other IP packets can also cause problem
- OS patches really solve the problem

Network Security Mechanisms

- Again, the usual suspects -
  - Encryption
  - Authentication
  - Access control
  - Data integrity mechanisms
  - Traffic control

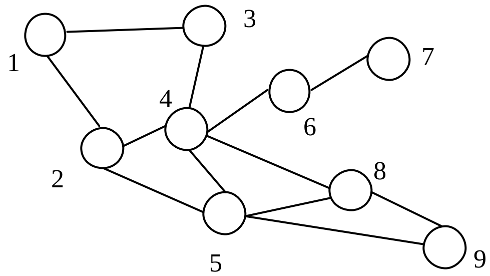
Encryption for Network Security

- Relies on the kinds of encryption algorithms and protocols discussed previously
- But network security tends to only worry about the data transport issues
- Which leads to an important question -

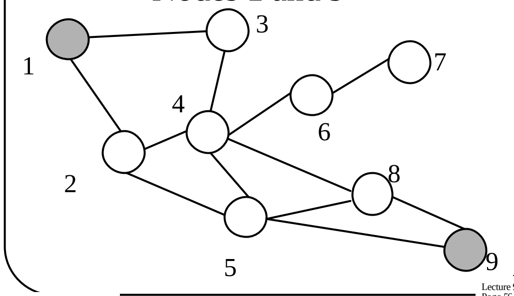
Link Encryption vs. End-to-End Encryption

- Should encryption be applied between pairs of hosts?
- Or should encryption be applied between the endpoints of applications?

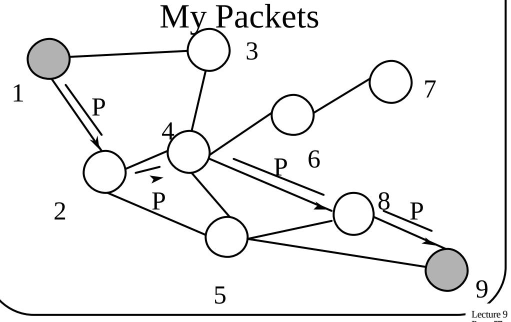
Clarifying the Question



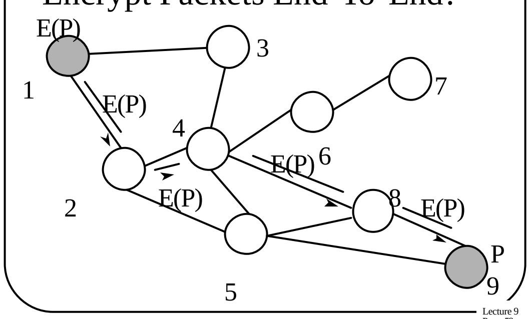
I Want to Communicate Between Nodes 1 and 9



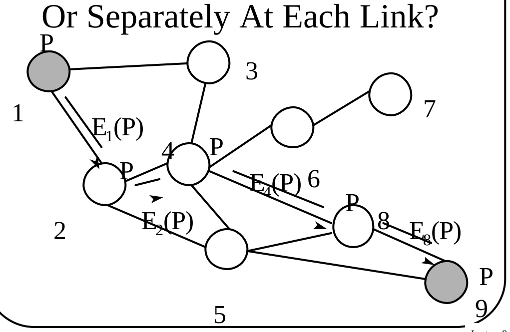
Some Path Will Be Chosen For My Packets



Encrypt Packets End-To-End?



Or Separately At Each Link?



Well, What Difference Does It Make?

- The two methods have very different characteristics
  - Level of user/application involvement
  - Scaling properties
  - Trust requirements
  - Adaptability of transmission

Link Level Encryption

+ Transparent to the user
+ Scaling related to number of links
+ Limits encryption to where it’s needed
+ Can adapt data in transit
– Not as much user/application control
– May be applied unnecessarily
– Must trust intermediate nodes

End-To-End Encryption

+ Greater possibilities for user control
+ Need not trust network components
+ Easier to apply selectively
– More user/application intervention required
– Data stream can’t be adapted (much)
– Scaling related to logical connections

Authentication for Network Security

- Various entities need to be authenticated
  - Hosts to hosts
  - Users to hosts
  - Hosts to users
- Because of inherent insecurities of networks, cryptographic methods used

Access Control

- When a node is put on a network, potentially all its resources become available over the network
- How do we control who can access resources?
- And how?

Data Integrity Mechanisms

- Bad things can happen if attackers can change data values
  - Either while in transit in the net
  - Or by remotely accessing a machine
- How do we keep our data intact?

Checksums, Secure Hashes, and Digital Signatures

- Checksums can tell us if the data has changed
  - If the checksum hasn’t been altered
- Secure hashes use cryptographic techniques
  - If the hash is protected
- Digital signatures provide full protection
  - At full cryptographic costs

Traffic Control Mechanisms

- Filtering
  - Ingress filtering
  - Egress filtering
- Protection against traffic analysis
  - Padding
  - Routing control

Ingress Filtering

- As packets enter router/switch/firewall, apply filtering rules
- Typically, drop packets not meeting some criteria
- Common example is firewall filtering
- Ingress filtering can help detect packets with bad "from" addresses
  - But only if forged address is "inside"

Egress Filtering

- Routers/switches/firewalls filter packets leaving them
- To catch packets likely to cause trouble
- Egress filtering is commonly prescribed to handle forged "from" addresses
  - Only let out packets with "from" addresses in your domain
  - But not widely used
  - Since it provides few benefits to its user

Padding

- Sometimes you don't want intruders to know what your traffic characteristics are
- Padding adds extra traffic to hide the real stuff
- Requires that fake traffic is not differentiable from real
- Usually means encrypt it all
- Must be done carefully, or clever attackers can tell the good stuff from the noise

Routing Control

- Use ability to control message routing to conceal the traffic in the network
- Especially important when trying to handle **covert channels**
  - Encapsulated users or programs trying to leak information out