Security Protocols
CS 239
Computer Security
February 10, 2003

Outline

- Societal issues and cryptography
- Key recovery cryptosystems
- Designing secure protocols
- Basic protocols
  - Key exchange

Legal and Political Issues in Cryptography

- Cryptography is meant to help keep secrets
- But should all secrets be kept?
- Many legal and moral issues

Societal Implications of Cryptography

- Criminals can conceal communications from the police
- Citizens can conceal taxable income from the government
- Terrorists can conceal their activities from governments trying to stop them

Problems With Controlling Cryptography

- Essentially, it's mostly algorithms
- If you know the algorithm, you can have a working copy easily
- At which point, you can conceal your secrets from anybody
  - To the strength the algorithm provides

Governmental Responses to Cryptography

- They vary widely
- Some nations require government approval to use cryptography
- Some nations have no laws governing it at all
- The US laws less restrictive than they used to be

The US Government Position on Cryptography

- All forms of cryptography are legal to use in the US
- **BUT**
  - Some minor restrictions on exporting cryptography to other countries
- The NSA used to try to keep a lid on cryptographic research

US Restrictions on Cryptographic Exports

- Rules changed in 2000
- Greatly liberalizing cryptographic exports
- Almost all cryptography is exportable
- Exception is for government use by a handful of countries
  - Those the US government currently doesn't like

Cryptographic Source Code and Free Speech

- US government took Phil Zimmermann to court over PGP
- Court ruled that he had a free-speech right to publish PGP source
- Eventually, appeals courts also found in favor of Zimmermann

Other Nations and Cryptography

- Generally, most nations have few or no restrictions on cryptography
- A group of treaty signatories have export restrictions similar to US's
- Some have strong restrictions
  - China, Russia, Vietnam, a few others
- A few have laws on domestic use of crypto
  - E.g., Australia, UK, India have laws that demand decryption with court order

Key Recovery Cryptosystems

- An attempt to balance:
  - Legitimate societal security needs
    - Requiring strong encryption
  - And legitimate governmental and law enforcement needs
    - Requiring access to data
- How can you have strong encryption and still satisfy governments?

Idea Behind Key Recovery

- Use encryption algorithms that are highly secure against cryptanalysis
- But with mechanisms that allow legitimate law enforcement agency to:
  - Obtain any key with sufficient legal authority
  - Very, very quickly
  - Without the owner knowing

Proper Use of Data Recovery Methods

- All encrypted transmissions (or saved data) must have key recovery methods applied
- Basically, the user must cooperate
  - Or his encryption system must force him to cooperate
  - Which implies everyone must use this form of cryptosystem

Methods to Implement Key Recovery

- Key registry method
  - Register all keys before use
- Data field recovery method
  - Basically, keep key in specially encrypted form in each message
  - With special mechanisms to get key out of the message

Problems With Key Recovery Systems

- Requires trusted infrastructures
- Requires cooperation (forced or voluntary) of all users
- Requires more trust in authorities than many people have
- International issues
- Performance and/or security problems with actual algorithms

The Current Status of Key Recovery Systems

- Pretty much dead
- US tried to convince everyone to use them
  - Skipjack algorithm, Clipper chip
- Very few agreed
- US is moving on to other approaches to dealing with cryptography

Basics of Security Protocols

- Work from the assumption (usually) that your encryption is sufficiently strong
- Given that, how do you design the exchange of messages to securely achieve a given result?
- Not nearly as easy as you probably think

Security Protocols

- A series of steps involving two or more parties designed to accomplish a task with suitable security
- Sequence is important
- Cryptographic protocols use cryptography
- Different protocols assume different levels of trust between participants

Types of Security Protocols

- Arbitrated protocols
  - Involving a trusted third party
- Adjudicated protocols
  - Trusted third party, after the fact
- Self-enforcing protocols
  - No trusted third party

Participants in Security Protocols

Alice

Bob

Carol

David

And the Bad Guys

Eve

And sometimes Alice or Bob might cheat

Mallory

Who only listens passively

Who is actively malicious

Trusted Arbitrator

Trent

A disinterested third party trusted by all legitimate participants

Arbitrators often simplify protocols, but add overhead

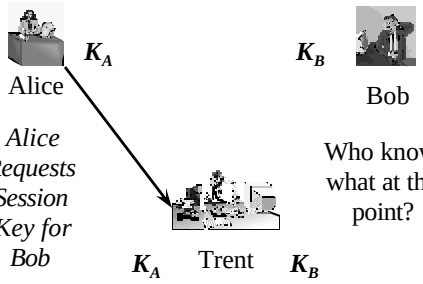
Key Exchange Protocols

- Often we want a different encryption key for each communication session
- How do we get those keys to the participants?
  - Securely
  - Quickly
  - Even if they've never communicated before

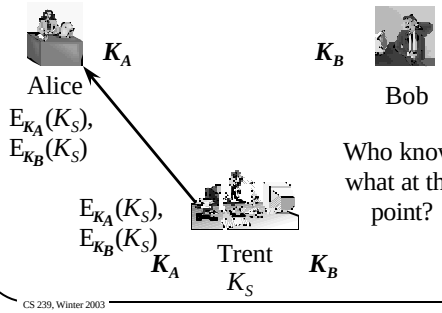
Key Exchange With Symmetric Encryption and a Arbitrator

- Alice and Bob want to talk securely with a new key
- They both trust Trent
  - Assume Alice & Bob each share a key with Trent
- How do Alice and Bob get a shared key?

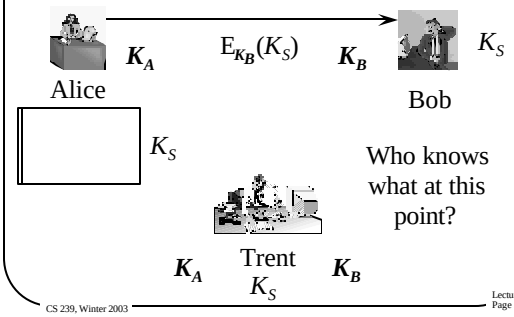
Step One



Step Two



Step Three



What Has the Protocol Achieved?

- Alice and Bob both have a new session key
- The session key was transmitted using keys known only to Alice and Bob
- Both Alice and Bob know that Trent participated
- But there are vulnerabilities

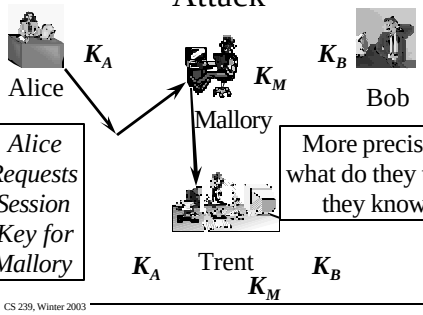
Problems With the Protocol

- What if the initial request was grabbed by Mallory?
- Could he do something bad that ends up causing us problems?
- Yes!
- (And there are also replay problems)

The Man-in-the-Middle Attack

- A class of attacks where an active attacker interposes himself secretly in a protocol
- Allowing alteration of the effects of the protocol
- Without necessarily attacking the encryption

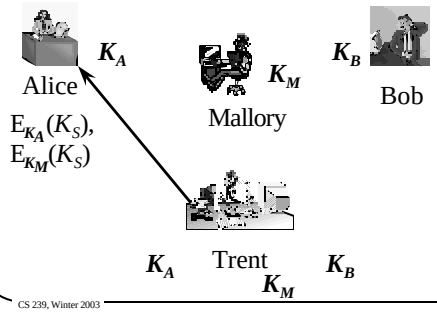
Applying the Man-in-the-Middle Attack



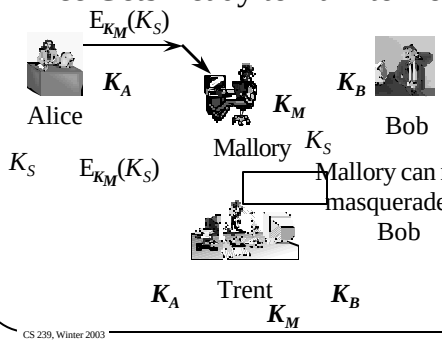
Alice Requests Session Key for Mallory

More precisely, what do they think they know?

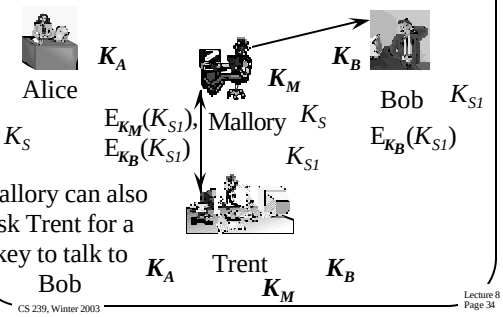
Trent Does His Job



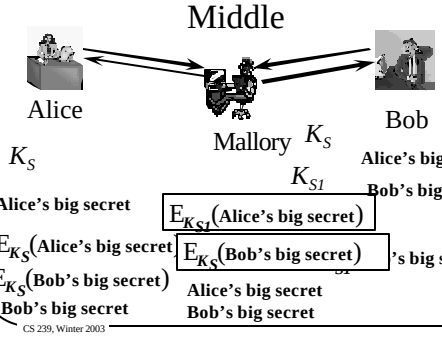
Alice Gets Ready to Talk to Bob



Really Getting in the Middle



Mallory Plays Man-in-the-Middle



Defeating the Man In the Middle

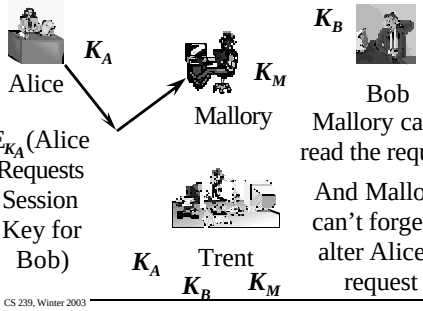
- Problems:

1). Trent doesn't really know what he's supposed to do

2). Alice doesn't verify he did the right thing

- Minor changes can fix that
  1). Encrypt request with K_A
  2). Include identity of other participant in response - $E_{K_A}(K_S$, Bob)

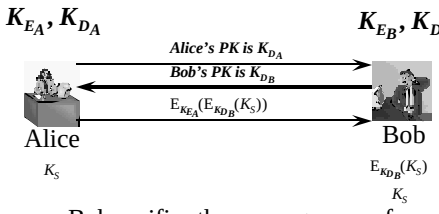
Applying the First Fix



Key Exchange With Public Key Cryptography

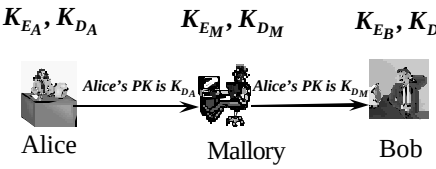
- With no trusted arbitrator
- Alice sends Bob her public key
- Bob sends Alice his public key
- Alice generates a session key and sends it to Bob encrypted with his public key, signed with her private key
- Bob decrypts Alice's message with his private key
- Encrypt session with shared session key

Basic Key Exchange Using PK



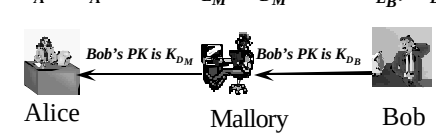
Bob verifies the message came from Alice
Bob extracts the key from the message

Man-in-the-Middle With Public Keys



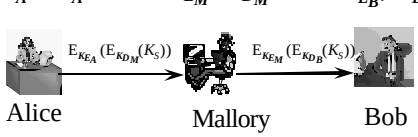
Now Mallory can pose as Alice to Bob

And Bob Sends His Public Key



Now Mallory can pose as Bob to Alice

Alice Chooses a Session Key



Bob and Alice are sharing a session key
But they're unknowingly sharing it with Mallory, too

Defeating This Man-in-the-Middle Attack

- Use Rivest and Shamir's *interlock protocol*
- Doesn't require any authorities
- Essentially, send stuff in pieces of an encrypted whole
- The man in the middle has little chance of correctly dealing with pieces

Using the Interlock Protocol

- Alice sends Bob her public key
- Bob sends Alice his public key
- Alice encrypts the message in Bob's public key and sends half of it to Bob
- Bob encrypts his message in Alice's public key and sends half of it to Alice
- Alice sends her other half to Bob

Continuing the Interlock Protocol

- Bob puts Alice's two halves together and decrypts
- Bob sends the other half of his encrypted message to Alice
- Alice puts Bob's halves together and decrypts

Why Does This Protocol Help?

- Because the man in the middle must provide half of an encrypted message before he gets all of it
- Consider one part of the attack -
  - Mallory wants to translate the message in Alice's public key into Mallory's public key

What Does Mallory Do?

- Mallory has deceptively sent out her public key to Bob and Alice
  - Claiming it's theirs
  - And Mallory knows their public keys
- Alice send Mallory half of an encrypted message
- Now Mallory must send Bob half an encrypted message

Mallory's Situation

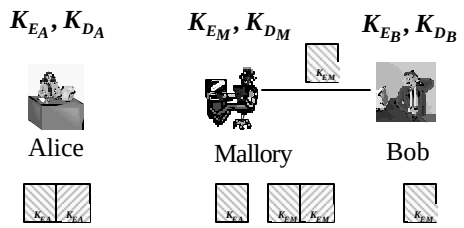
K_{E_A}, K_{D_A} K_{E_M}, K_{D_M} K_{E_B}, K_{D_B}

Alice Mallory Bob

Mallory's Problem

- Mallory can't yet decrypt Alice's message
  - Since he only has half of it
- Mallory must provide Bob two matching halves eventually
  - And one right now
- Mallory's only choice is to generate a new message before he knows the real message

Mallory's Only Option



Why Is This A Problem For Mallory?

- Mallory must now spoof proper contents of Bob and Alice's conversation
- Without knowing the real contents until later
- Bob and Alice are likely to notice problems quickly

Is This Generally Feasible?

- Not really
- Assumes Bob has a useful, unguessable message before Alice's message arrives
- Not really the way the world works
- If Mallory can guess Bob's message, he can play the standard man-in-the-middle game

Diffie/Hellman Key Exchange

- Securely exchange a key
  - Without previously sharing any secrets
- Alice and Bob agree on a large prime n and a number g
  - g should be primitive mod n
- n and g don't need to be secrets

Exchanging a Key in Diffie/Hellman

- Alice and Bob want to set up a session key
  - How can they learn the key without anyone else knowing it?
- Protocol assumes authentication
- Alice chooses a large random integer x and sends Bob $X = g^x mod\ n$

Exchanging the Key, Con't

- Bob chooses a random large integer y and sends Alice $Y = g^y \bmod n$
- Alice computes $k = Y^x \bmod n$
- Bob computes $k' = X^y \bmod n$
- k and k' are both equal to $g^{xy} \bmod n$
- But nobody else can compute k or k'

Why Can't Others Get the Secret?

- What do they know?
  - n, g, X, and Y
  - Not x or y
- Knowing X and y gets you k
- Knowing Y and x gets you k'
- Knowing X and Y gets you nothing
  - Unless you compute the discrete logarithm to obtain x or y