

Real-time Communication Security

Dr. Arjan Durresi
Louisiana State University
Baton Rouge, LA 70810
Durresi@csc.lsu.edu

These slides are available at:

<http://www.csc.lsu.edu/~durresi/csc4601-07/>

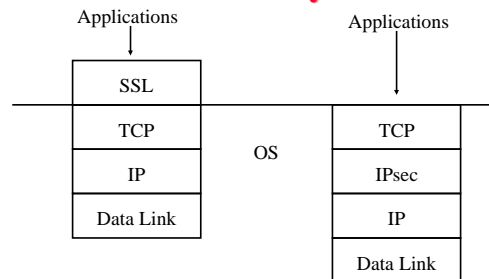


- Layers, Session keys
- Perfect Forward Secrecy
- Denial of Service
- Endpoint Identifier Hiding
- Live Partner Assurance Arranging for Parallel Computation
- Data Stream Protection

Real-time Comm. Sec.

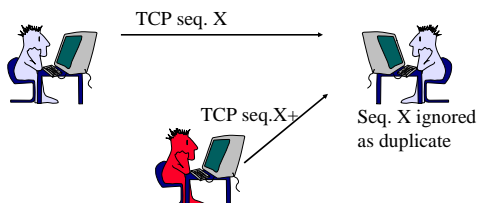
- Real-time protocol - parties negotiate interactively to authenticate each other and to establish a session key
 - IPsec, SSL/TLS, SSH
- Non-real time: email the recipient decrypts and authenticates in non-real-time
- At a minimum, the protocols provide mutual authentication and establish a session key

What Layer?



- Change OS or applications?
- Operating above TCP – problems for TCP

Session Key Establishment



- Protection against session hijacking
- Session key – unpredictable, new for each session
- Both parties should contribute to the session key

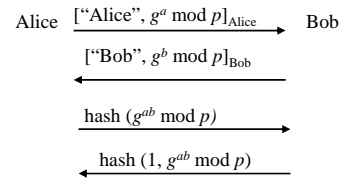
At Layer 3 - IPsec

- IPsec – no need to modify the application
- IP tells to the application only the IP address of the other party, even though IPsec is capable of user authentication
- So the best solution is when both operating system and the applications contribute to security

Perfect Forward Secrecy

- ❑ PFS – impossibility to decrypt the entire conversation without the session key
- ❑ Generate good session keys
- ❑ Protocols without PFS:
 - Using Public key for encryption
 - Kerberos
 - Use of a session key sent encrypted with public key
- ❑ Escrow-foilage – no possible decryption even when having the long-term key

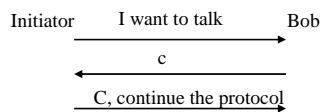
Perfect Forward Secrecy



- Impossible to reconstruct $g^{ab} \bmod p$ without a, b
- Authentication
- Use different hash of $g^{ab} \bmod p$

Denial of Service

- ❑ Force servers to use their resources for authentication attempts
- ❑ Use cookies – an unpredictable number to the other side. Send cookies to the sending IP address and do not do computation until receiving the cookies back
- ❑ Stateless cookies – function of IP address and a secret



Stateless Cookies

- ❑ Cookies – function of the IP address and a secret known by Bob, so he can calculate what cookie he would send to a particular IP address
 - Hash(IP address, secret)
 -

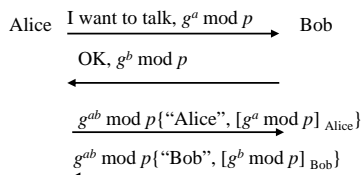
Denial of Service

- ❑ Puzzles – require the initiator to do more computation
 - Ask about a bit of an MD of x
 - Verifying the puzzle is fast, solving is exponential
- ❑ Not much help if the attackers outnumber legitimate users, but it will slow down an attacker
- ❑ Non-hostile users might not mind solving the puzzle but:
 - It will depend on the power of the user's machine
 - Distributed Denial of Service

Endpoint Identifier Hiding

- ❑ Hide the identities of the two communicating parties
- ❑ After establishing a session key, exchange encrypted identities
- ❑ Authenticate each other using the keys associated to their Id.
- ❑ Is it better to protect the initiator's ID or responder's ID?
- ❑ How to protect both IDs?
 - Use a shared secret key
 - Or Bob's public key

Endpoint Identifier Hiding

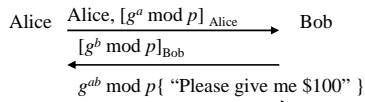


The attacker will discover Alice's identity but not Bob's

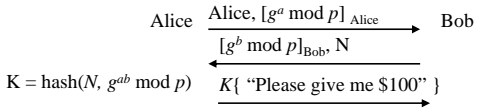
Live Partner Assurance

- ❑ Replay attacks - Replay messages from previous conversations
 - Waste the server resources
 - Make the server repeat actions
- ❑ Bob should realize whether Alice is alive or not
 - Not reusing b – more computations
 - use a nonce for each connection attempt

Live Partner Assurance

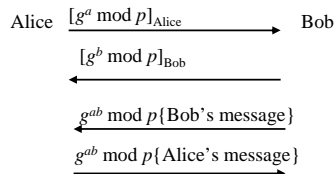


A protocol vulnerable to reuse if Bob reuses b



Using a nonce – make sure it is not replay

Arranging for Parallel Computation



- ❑ Alice and Bob can compute at the same time

Data Stream Protection

- ❑ TCP could fragment packets differently from SSL
- ❑ In IPSec the packets are self-contained for cryptography operations
- ❑ But even IPSec packet could be further fragmented in intermediate links
- ❑ With independent packet – relay attack
 - Have packet sequences – IPSec
- ❑ Negotiating Crypto Parameters
 - More flexible
 - Security flaw

Summary



- ❑ Layers, Session keys
- ❑ Perfect Forward Secrecy
- ❑ Denial of Service
- ❑ Endpoint Identifier Hiding
- ❑ Live Partner Assurance Arranging for Parallel Computation
- ❑ Data Stream Protection