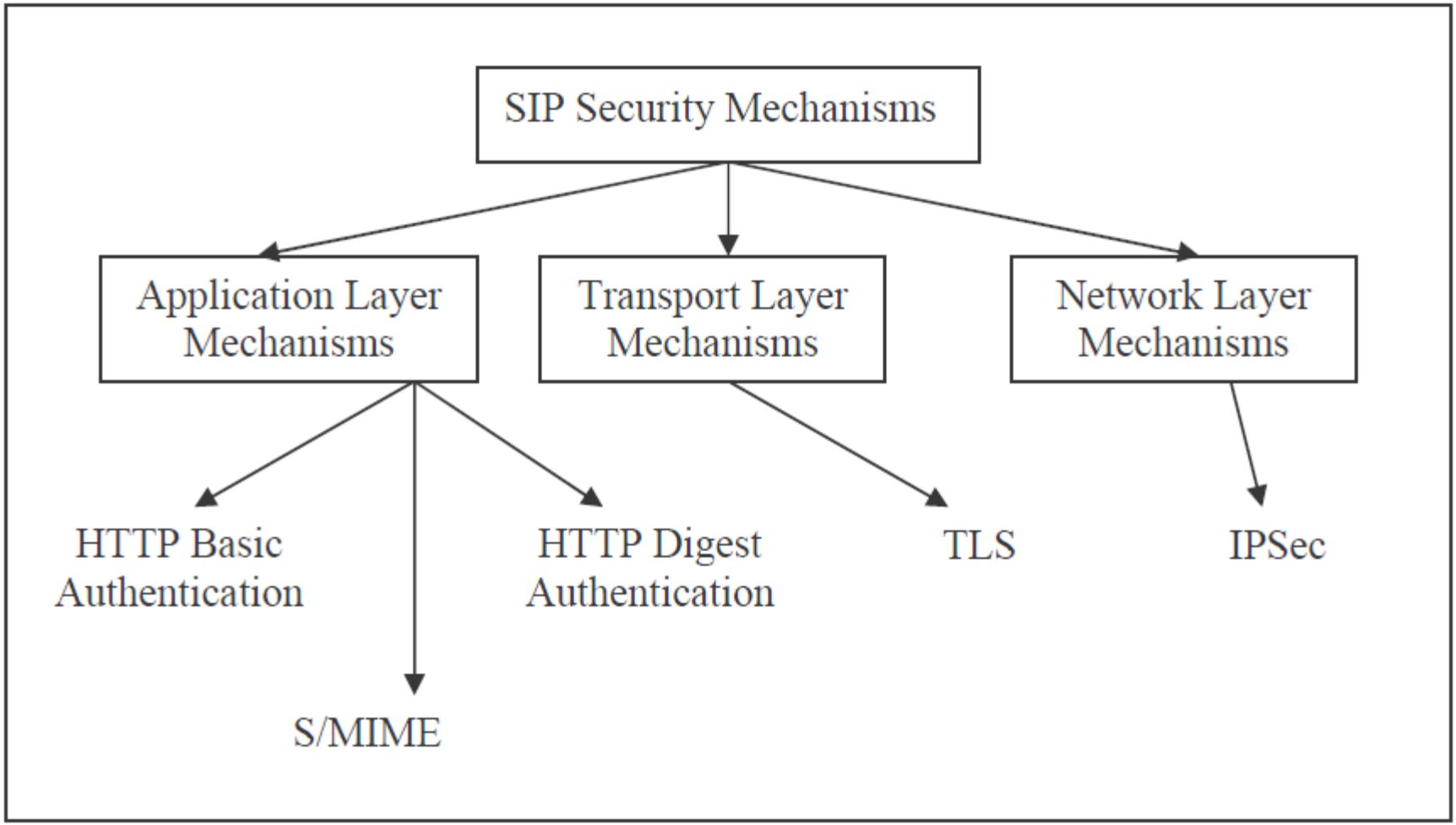
פרק 12

- Authentication Goals
- Attack scenarios
- HTTP digest authentication
- Authentication scheme for a trusted domain
- Authentication Challenges

SIP Security Architecture



Authentication Goals and Methods

- Identifying the source (sender)
  - Object ID in reality should be the same as the object claims to be
- Identifying the Receiver
  - Before sending sensitive data (such as personal information)
- Authentication methods
  - HTTP digest mechanism, transport layer mechanism
  - Secure Multipart Internet Mail Extensions (S/MIME)

Attacks Scenarios

- Hijacking registration of the user client
  - The client sends an REGISTER message to registrar server (includes IP address and contact information of the user)
  - IP Add. & Contact Info. can be used to hijack registration and forward incoming call to SIP phone of the hijacker
  - Hijacker can cheat registrar by first blocking original user's (DoS attacks to the user)

Attacks Scenarios (cont.)

- Hijacking registration of the user client (cont.)
  - The attacker sends it's own registration messages to registrar
    - including the SIP contact information of the original user, but with the changed IP address
  - From the Registrar perspective
    - Only the IP address of the registered user is changed
    - SIP contact is associated to new IP address which is the hijacker's IP address
  - Then Registrar will forward incoming call request to the hijacker instead of the original user

INVITE Spoofing

An example of spoofing the From, Via and Subject header fields in a INVITE request

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP somewhere.com
To: Bob <sip:bob@biloxi.com>
From: Alice <alice@atlanta.com>
Call-ID: a72bcf72f22d
Cseq: 100 INVITE
Contact: <sip:John@somewhere.com>
Subject: Your Friend Alice
…
```

Attacks Scenarios (Cont.)

- SIP calls forwarding
  - SIP calls forwarding to possibly rogue server
    - Exploiting the lack of identifying response messages

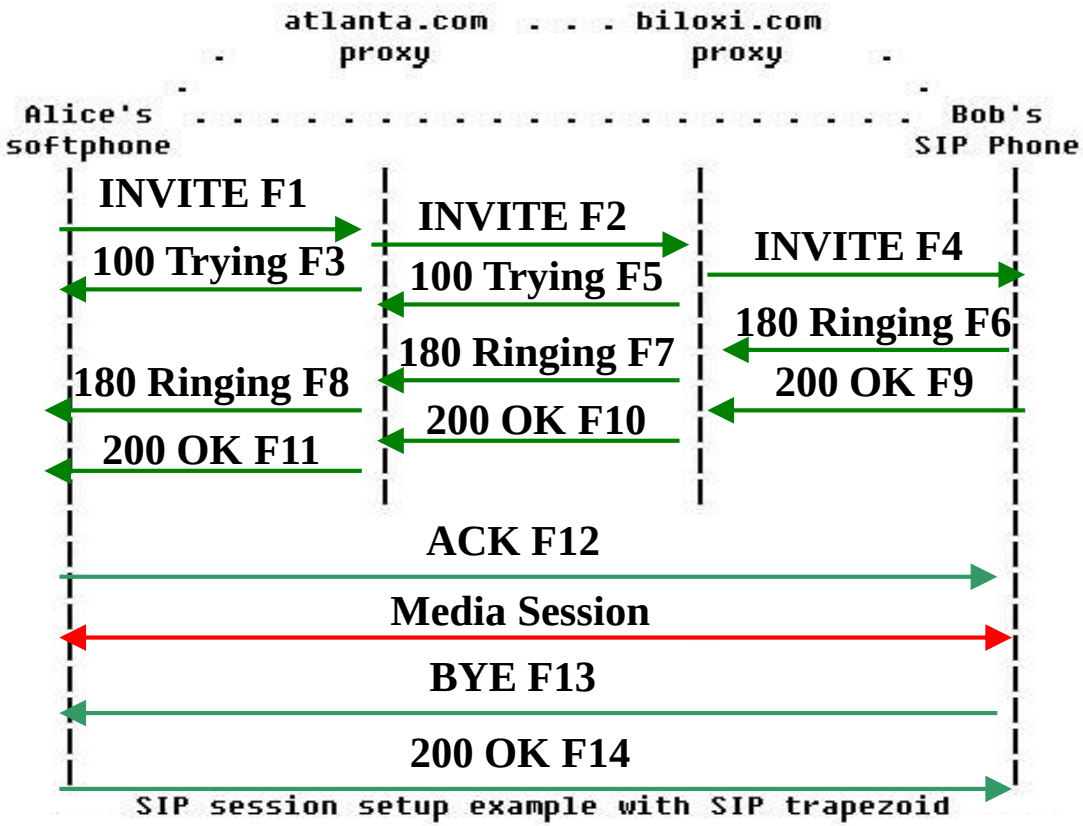
- Attack process: SIP request is send to proxy server of the receiver
  - The attacker hijacks the request message and uses the header fields from that request
  - Then, attacker assigns the response with status code 302 ("moved temporarily“)
  - Message with headers stolen from request message (for example INVITE, incoming call is forwarded to attacker)

Attacks Scenarios (Cont.)

- The two attack scenarios have implications on security and privacy
  - Attacker could get personal and confidential data of the users
  - Rogue party could mislead end users
  - Forward calls to malicious entity
  - Existing call parties could be conferencing with rogue party (interception)

- Two main security mechanisms
  - Authentication
    - To prevent attackers from modifying and/or replaying SIP requests and responses
  - Encryption
    - To ensure confidentiality

Basic Call Flow



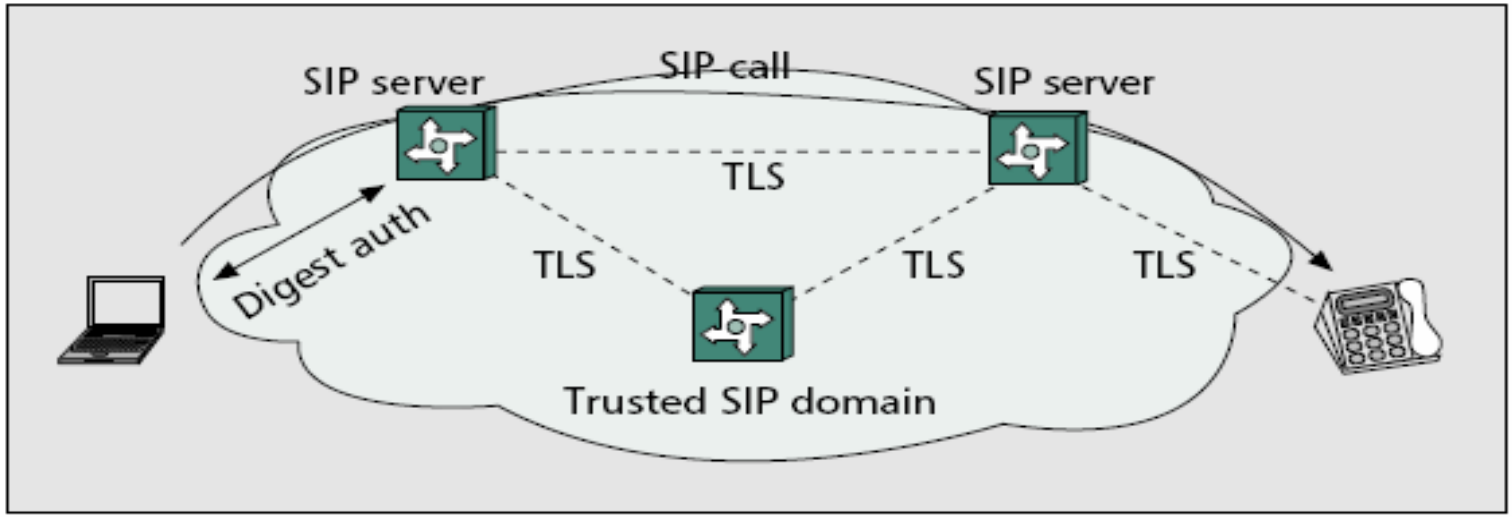
Security Mechanisms

- End-to-end versus hop-by-hop
  - End-to-end security use SIP mechanisms to ensure security
  - Hop-by-hop relies on the security provided by the network
- Examples of hop-by-hop mechanism are Transport Layer Security (TLS) and Internet Protocol Security (IPsec)
- SIP introduces HTTP digest authentication and usage of S/MIME extensions

SIP Methods and Authentication

Method	Purpose	Supports Authentication
INVITE	Initiate a session	Yes
ACK	Acknowledge session initiation	No
OPTIONS	Query server capabilities	No
BYE	Terminate a session	Yes
CANCEL	Cancel a pending request	Yes
REGISTER	Register a user's location	Yes

Security Mechanisms (cont.)

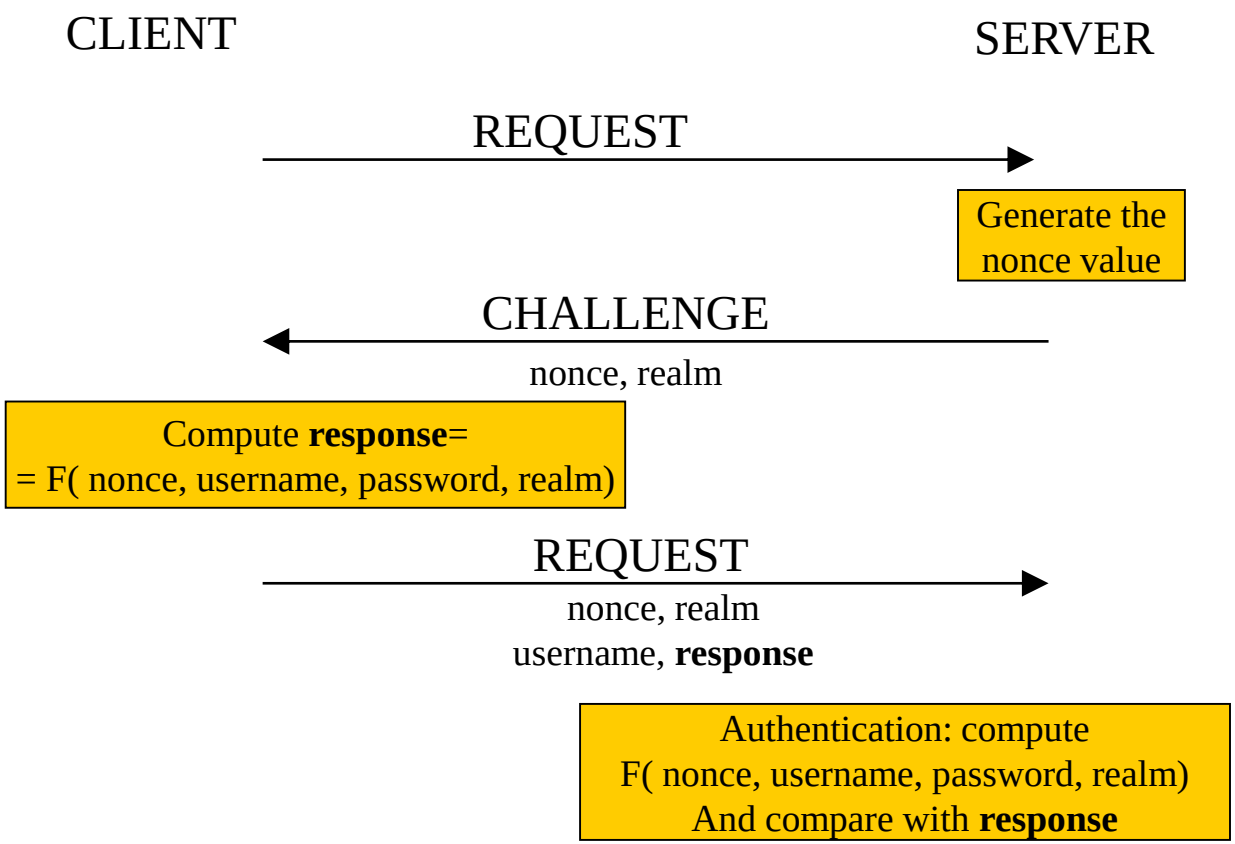


An example of a trusted network scenario

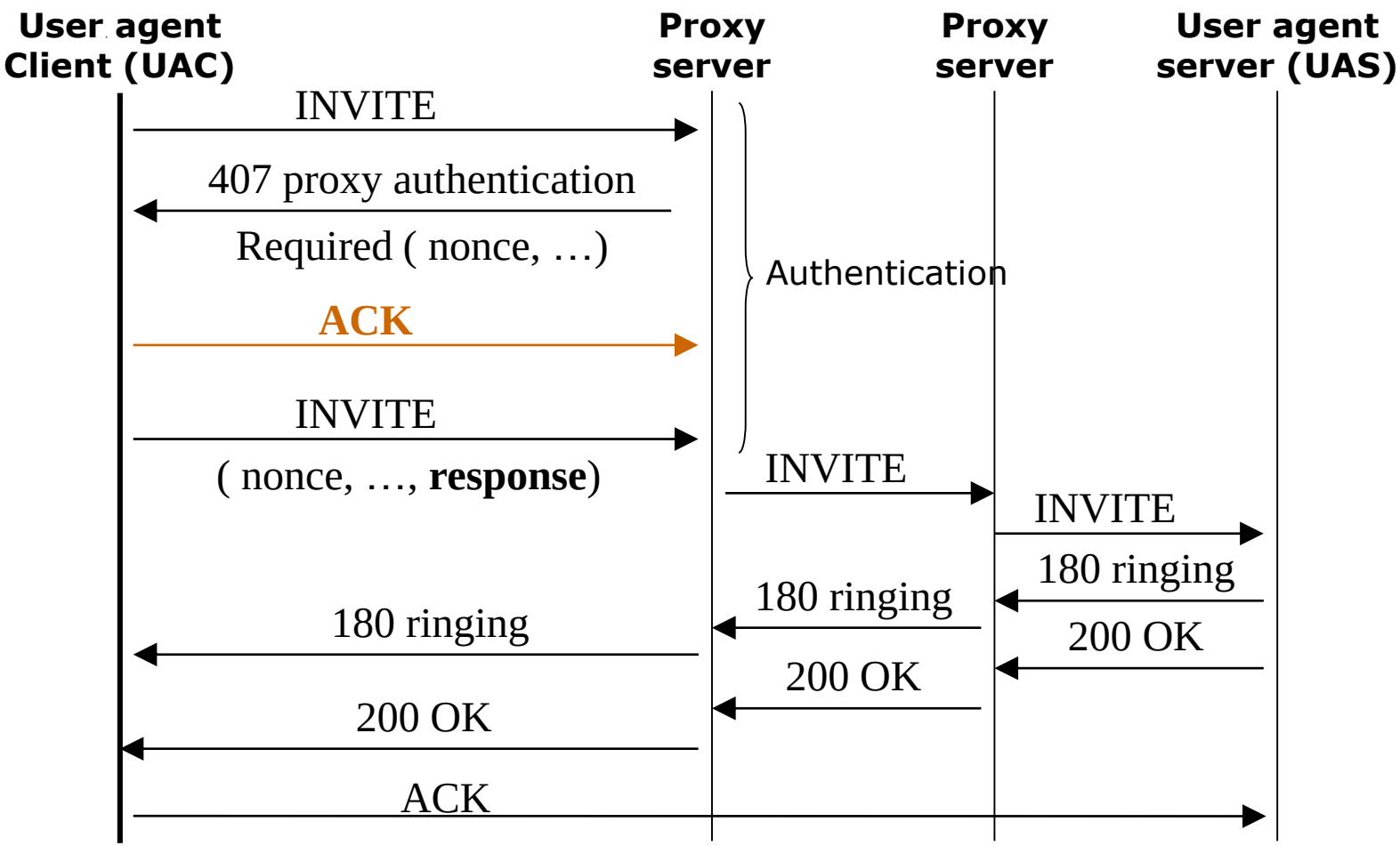
HTTP digest authentication

- HTTP digest is a challenge-response protocol
  - Nonce value is used in challenging the target
  - The response: a checksum of the username, password, nonce value
- The usage: users to users or users to proxies
  - **Not proxies to proxies**
- The security between proxies relies on other mechanisms
  - TLS or IPsec

The Authentication Procedure



The Authentication Procedure (cont.)



HTTP digest authentication

- When a server receives a request message from the client (such as INVITE)
  - it may challenge the sender of the message
    - The server sends an response message containing a nonce value and a realm
    - The response is actually an error message requesting authentication
    - The **realm** in the message is the **digest algorithm** used in this challenge

HTTP digest authentication (cont.)

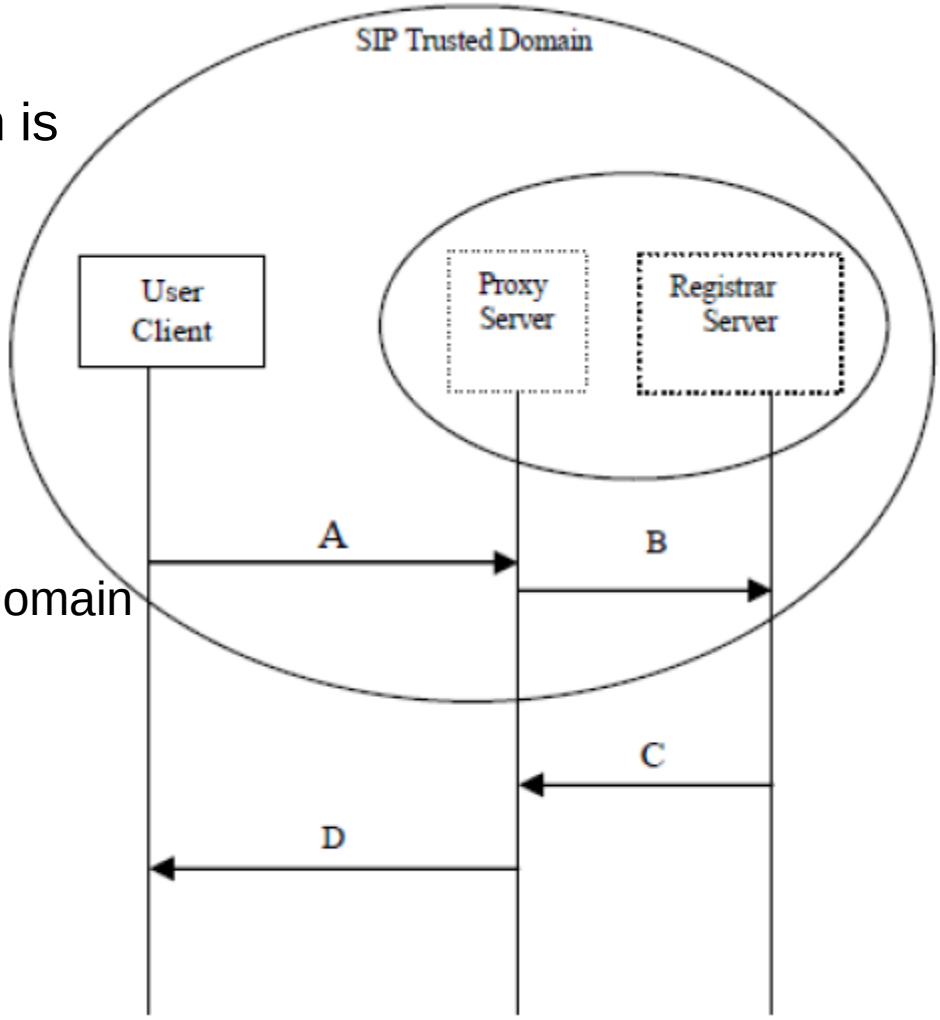
- Nonce value is used in challenging the target
  - The initiator, client, of the request receives the response
    - Computes the response value with nonce value received in challenge and with a username and a secret password
    - The secret password is known by both the client and the server
  - The client sends back the original request message with the computed response value, username, nonce value and realm

Authentication scheme- trusted SIP domain

- The outbound proxy for the domain is at the edge of the domain

  - Authentication of the user client has to be handled by that proxy

  - Proxy and Registrar servers needs to have public key certificates, which are authorized by authorities of that domain



Authentication with trusted SIP domain (cont.)

- The user client registers itself to the registrar server
  - Sends inside the registration message the identity associated to the user client
- The registrar server creates a large Secret number (N) when it receives the registration message
  - Replies to client with a value, which is computed with the **N** value and the identity of the user client
  - This value is the password for the user client

– Then the registrar server computes a number **r**, which is generated with identities of the user client and registrar server

– The user client initiating the call is required to authenticate itself with the outbound proxy of the trusted SIP domain

Authentication with trusted SIP domain (cont.)

- The user client sends request with the parameters as follows
  - User client creates a secret random number R With the password, received in registration
  - The client generates a number n by computing it with the r and the password
  - User client computes a timestamp and a temporary key K
    - K is created with the timestamp and the password
    - The secret random number R is then encrypted with key K
    - Then user client sends the parameter A
    - A consists of n, R encrypted using K, identity of registrar and timestamp

Authentication with trusted SIP domain (cont.)

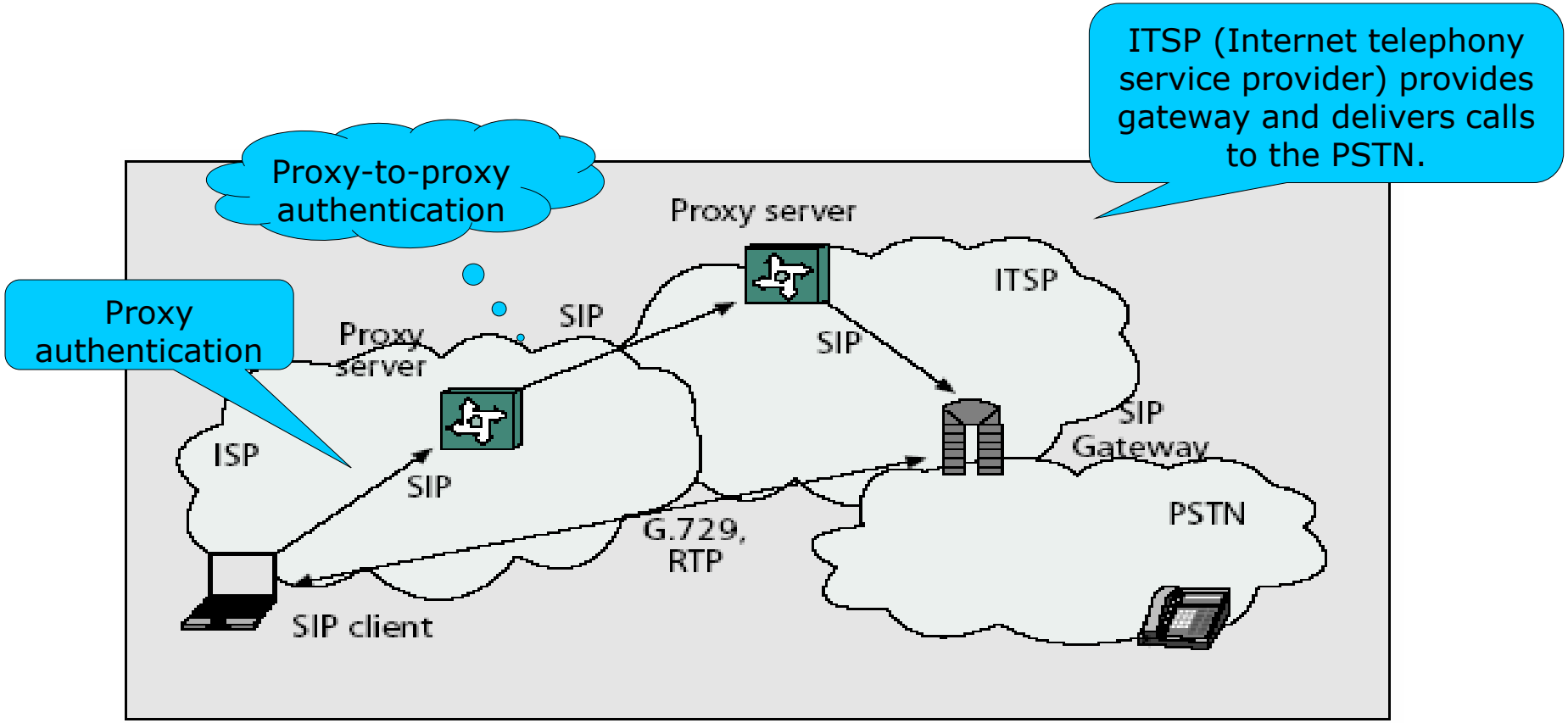
- The Proxy server receives the request A with the parameters
  - Compares the timestamp in A and current time in order to verify that the message is in acceptable timeframe
  - Proxy server verifies the user client with registrar server using the proxy certificate and the parameters received in message A
  - Message B is sent by the proxy to registrar
  - Registrar replies by sending a message C to proxy server, if the user client is identified and authorized in this domain
  - The proxy server then sends to the user client a temporary certificate, which is valid until the timestamp associated with the certificate expires
  - The proxy encrypts the certificate with session key, which is then used for all signalling traffic

Authentication with trusted SIP domain (cont.)

- User client receives the message D containing the encrypted certificate
  - Got a temporary certificate and the session key to continue the call establishment

- Call is established between calling user client and called user's server
  - The identity information is shared
  - The server of the called user verifies the received certificate and if it is valid
  - it saves the session key and allows call to be established to called user client

An Example Scenario of a SIP-Based IP Telephony Service



PC-to-phone call.

Challenges in SIP authentication

- Two major weaknesses in HTTP digest authentication
  - Lack of securing all headers and parameters in SIP
  - The requirement of pre-existing user configuration on servers, which does not scale well

- The authentication scheme for a trusted SIP domain
  - Usage of several hash computations and server certificates
    - Additional load (overhead) and decreases the overall performance of the server
    - If the load increases, the server comes more vulnerable to denial of service attacks

Summary

- Authentication methods
  - HTTP digest
  - Usage of S/MIME in SIP (to be presented)
  - Scheme for a trusted domain
- Security trade-off: Overhead and Performance