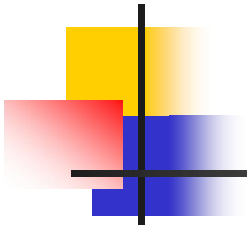


Peer-to-Peer Networking

IM: How Instant Messaging Systems Work

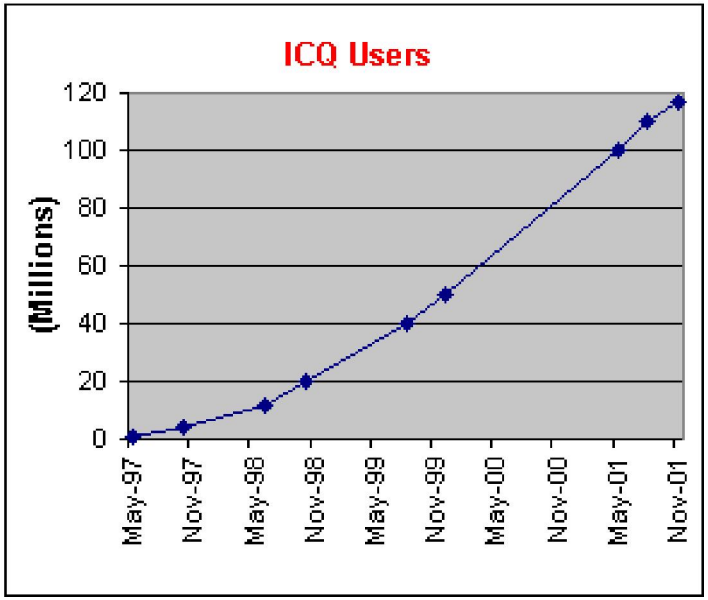
Mohammad iqbal

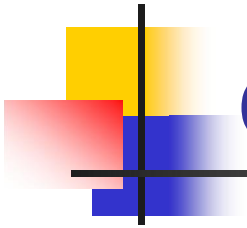
Thanks to : Xinran Wu, Clement Yuen

Gunadarma 2013

Instant Messaging Systems

- ICQ (Mirabilis 1996, Bought by AOL in 1998, $300M)
- AIM (1997), Yahoo (1998), MSN(1999)
- Basic Functions:
  - **Presence (Awareness)**
    - **Status(offline/online/idle)**
    - **Location(office/home/mobile)**
  - **Instant Messaging**
    - **Text/Voice/Video**
    - **Any P2P applications**

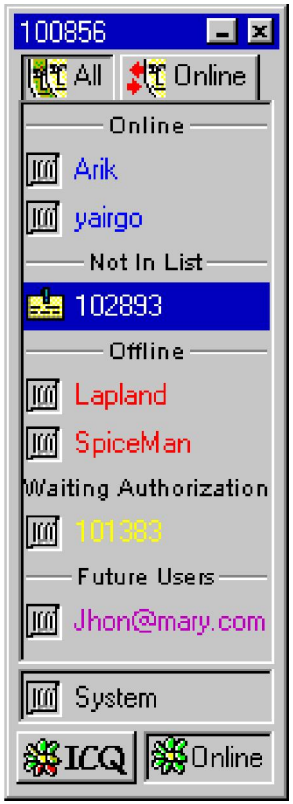


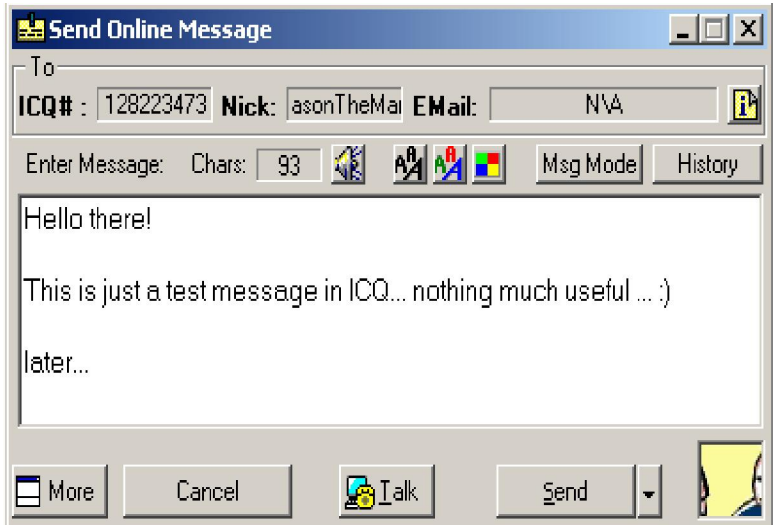


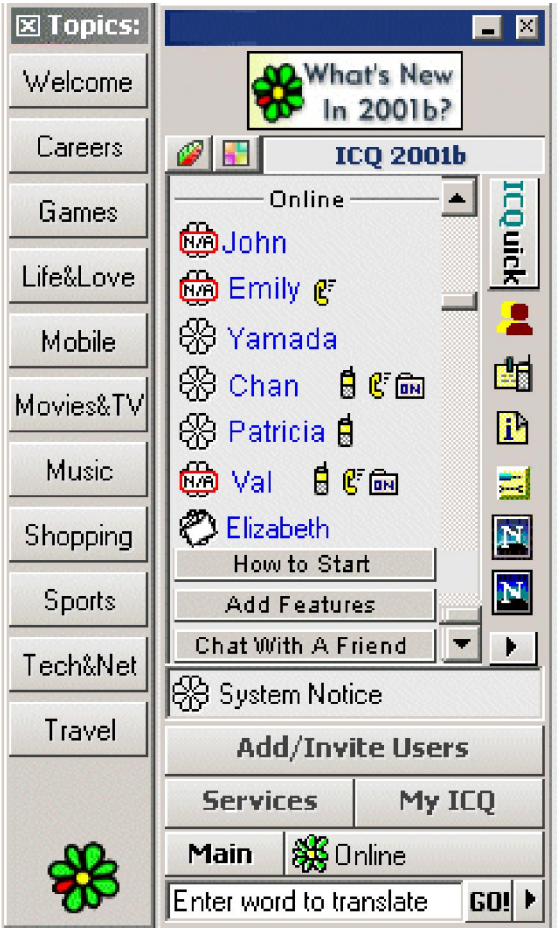
Outline

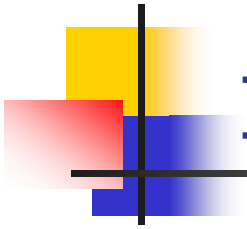
- Introduction to IM
- How ICQ Works
- Problems and Security Concerns in ICQ
- IETF Internet-Drafts for Instant Messaging
  - Model and Terminologies
  - Requirements
  - The PRIM protocol
  - Security Considerations
- Concluding Remarks

ICQ: A Typical Instant Messaging Sys.





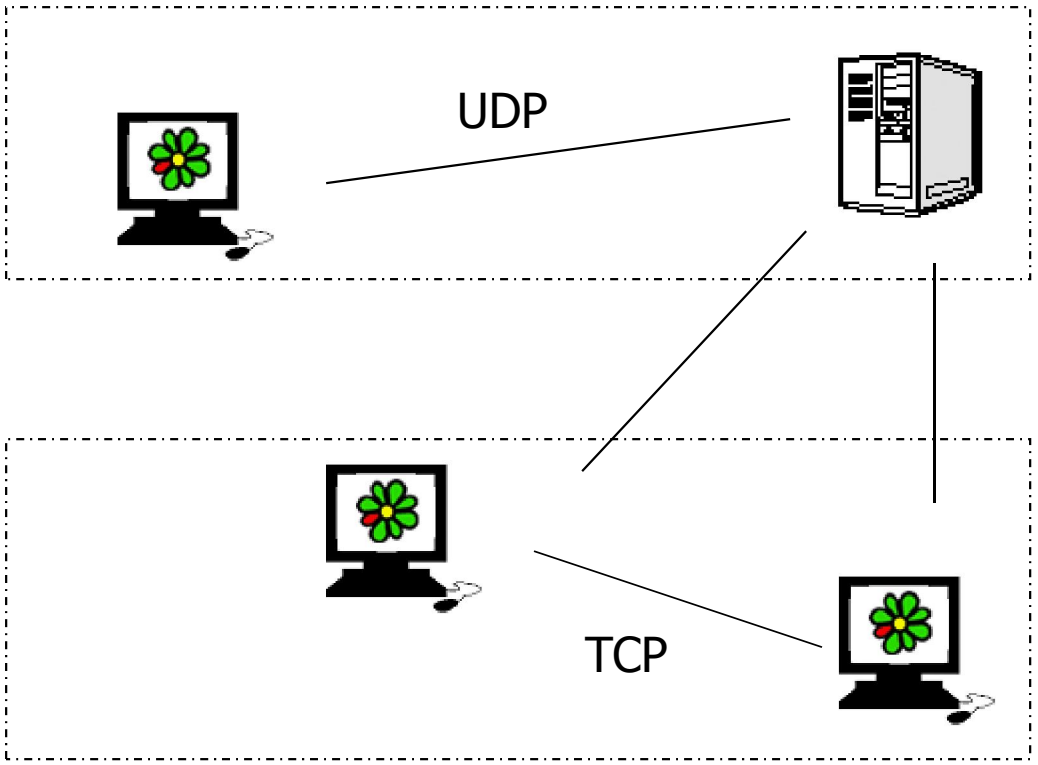




ICQ Protocol

- No official publications
- Info Available is from reverse-engineering the ICQ Protocol
- ICQ Protocols:
  - V1,V2: Simplest Ones
  - V3: Simple Checksum as Security
  - V4: Encryption to Improve the Security
  - V5: Not yet Fully Studied

How Does ICQ Work ?

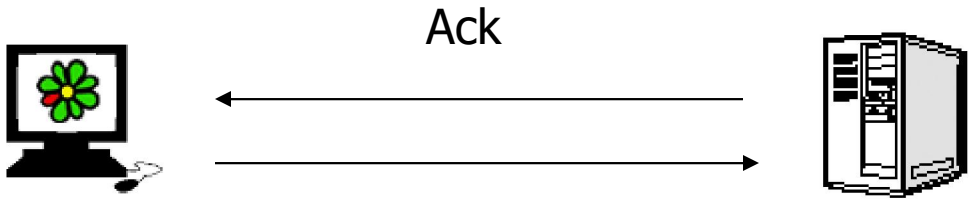


Presence Service

Instant Messaging

Presence Service (1)

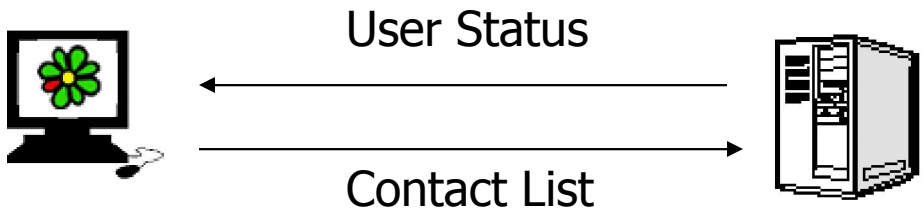
- Create Connection



- "keep active" message
- All UDP packets must be acknowledged by the receiver
- Same UDP packet format
  [SessionID, UIN, FunctionID, Parameters]

Presence Service (2)

- Subscribe to Presence Service



- User will be notified for the Status Change
- Contact List is not stored on server permanently

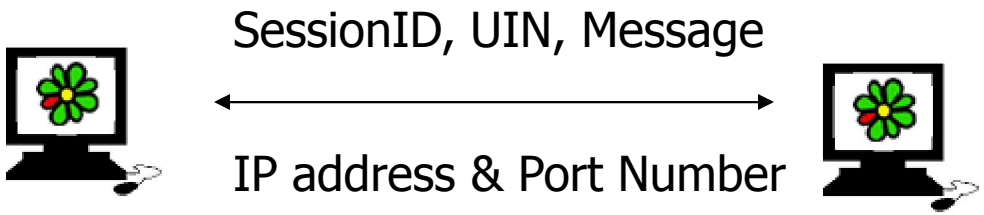
Instant Messaging

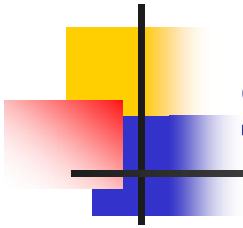
- Receiver is offline:

  Message in UDP to Server

- Receiver is online:

  Build a TCP Connection, open till one side is off.



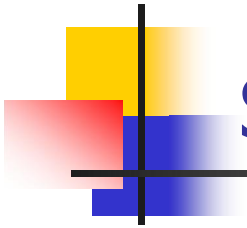


Security on ICQ

"The ICQ protocol is ridiculously simplistic and is riddled with security holes. So is the ICQ software. So ICQ users can be spoofed, have their machine crashed, or have evil haxxors run arbitrary code on their boxes. Geez, these poor users might as well run Internet Explorer!"

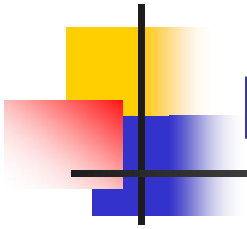
(Source: http://www.insecure.org/sploits/icq.spoof.overflow.seq.html)

- Personal Information Unprotected
- IP Information Exposed
- Client-side operations make ICQ more vulnerable
  - Flooding
  - Spoofing



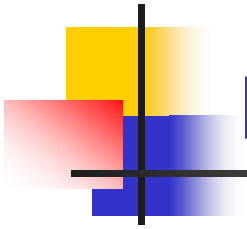
Standardization

- IETF Instant Messaging and Presence Protocol (IMPP) WG
  - Terminologies, model and data formats
  - Specify design goals and requirements
  - Produced RFC 2778/2779 and other I-Ds
- IETF Presence and Instant Messaging Protocol (PRIM) WG
  - Proposes a protocol that minimally satisfies the RFC's



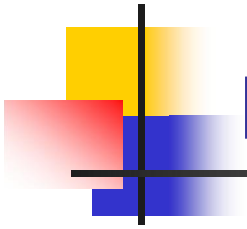
Model and Terminologies

- A *presence and instant messaging system*
  - Provides *presence service* and *instant message service*
  - Presence service accepts, stores and distributes *presence information*
  - Instant message service accepts and delivers *instant messages* to *instant inboxes*
  - Can be regarded and implemented as two independent systems



Model and Terminologies (cont)

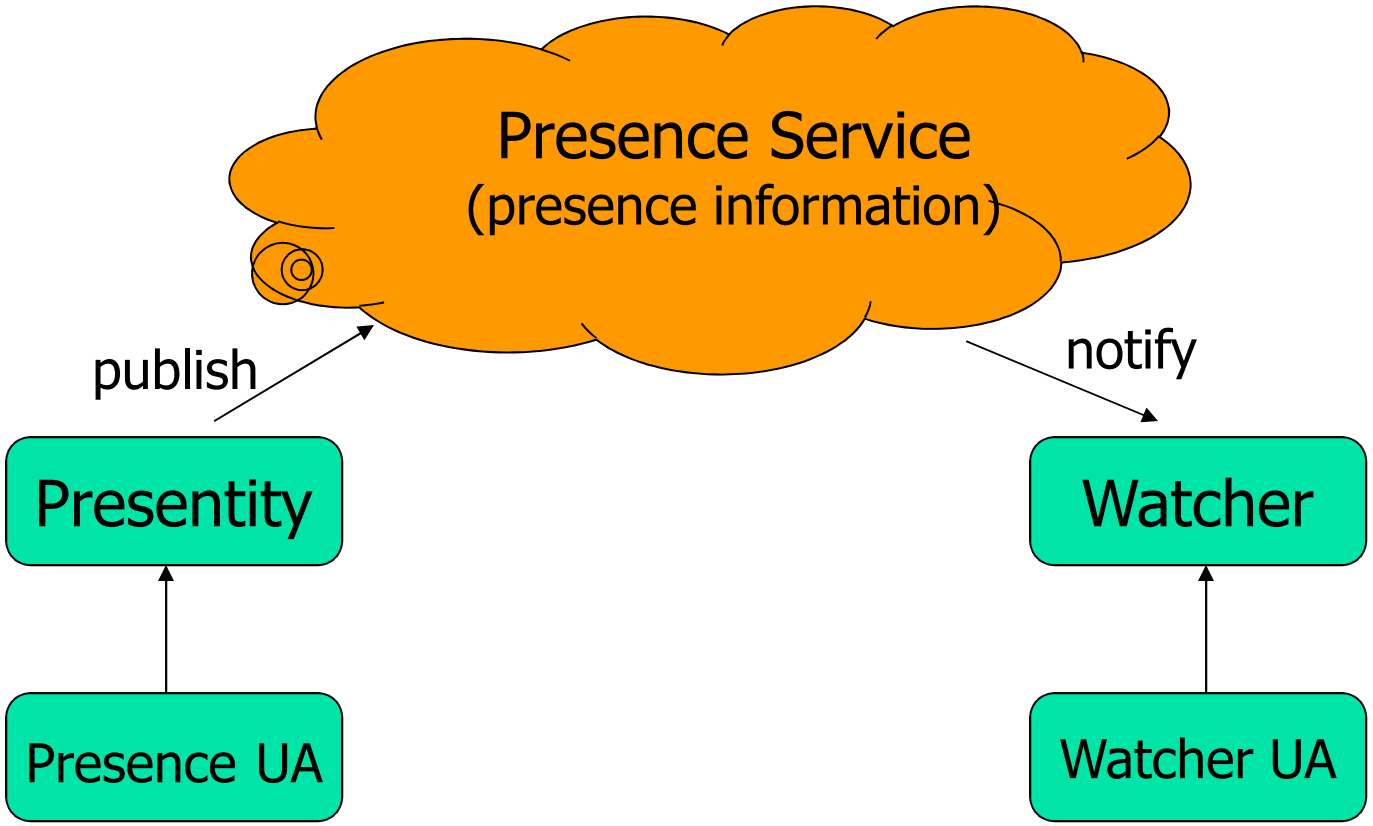
- Presence Service
  - Serves *presentities* and *watchers*
  - Presentities provide presence information
  - Watchers receive presence information
  - May involve multiple servers/proxies across multiple domains (other presence services)
- Watchers
  - Can be classified into *fetchers* and *subscribers*
  - Subscribers request future *notifications* of changes in presence information
- Watcher information can also be distributed



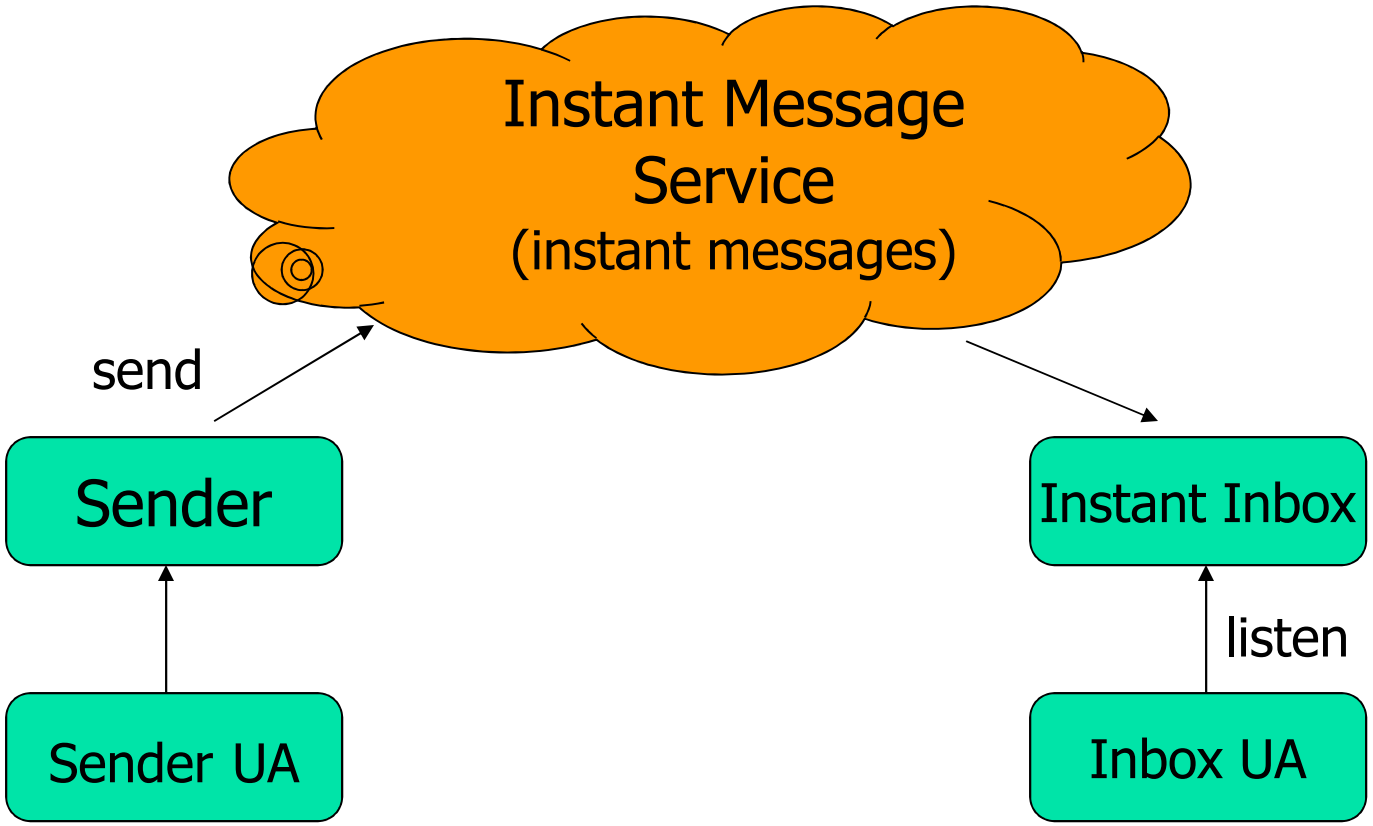
Model and Terminologies (cont)

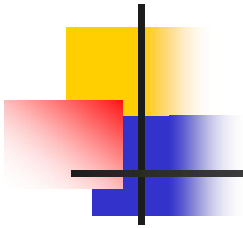
- Instant Message Service
  - Serves *senders* and *instant inboxes*
  - Senders send instant messages to service
  - Messages are then delivered to the inboxes
  - May involve multiple servers/proxies across multiple domains (other IM services)
- *Principals*
  - The "real world" users of the system
  - Interact via *user agents*
  - User agents control access and delivery rules

Presence Service



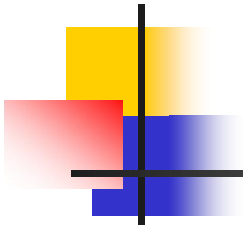
Instant Message Service





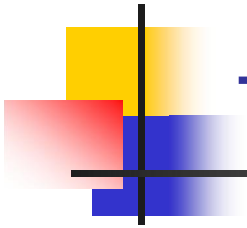
Presence Information

- Consists of multiple *presence tuples*
- Presence tuple
  - *Status* – online/offline,open/close,busy,away
  - *Communication Address*
    - *Communication Means* – instant message service
    - *Contact Address* – instant inbox address



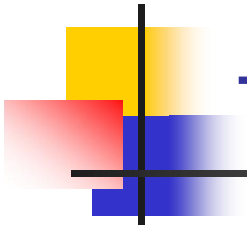
Protocol Requirements

- Independence of presence service and instant message service
- Entities in one domain interoperable with those in other domains
- Scalable – many entities and domains; many subscriptions per subscriber or presentity etc.
- Access control: who can do what
- Must allow operations through proxies and firewalls
- Message encryption and authentication



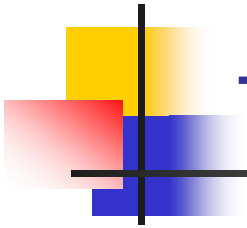
The PRIM protocol

- Designed to allow IM services to be provided by servers distributed across administrative domains
- Client-server (intra-domain) and server-server protocols (inter-domain)
- Assumes TCP as basic transport
- Uses long-lived C-S connections; reduces auth. overhead and firewall friendly
- "Polite blocking" – selective publication of presence information (watcher class)



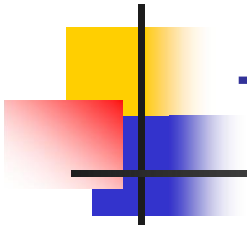
The PRIM protocol (cont)

- Each principal through agents communicates with its own service (home) domain presence/IM servers using client-server protocols
- Presence service
  - Subscription for a presentity in a different domain is forwarded using server-server protocols
  - Likewise for notifications
  - A duration is associated with each subscription
  - A renewal by the user agent or its home presence server is required for continuous subscription



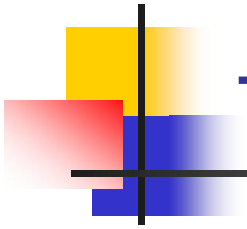
The PRIM protocol (cont)

- Instant Message service
  - IM server provides the instant inbox
  - User agent listens to inbox from which it wants to receive instant messages
  - Inbox is open when at least one principal is listening to it
- Presence/IM identifiers – used to identify presentities and inboxes
  - In the form of URI, e.g. pres:joe@utoronto.ca, im:%22Jane%20Smith%22@domain.com



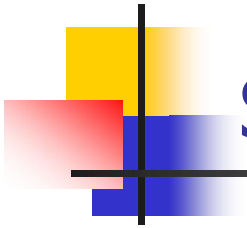
The PRIM protocol (cont)

- Name Resolution – uses DNS
  - Perform SRV RR lookup
- Authentication
  - Performed at connection end-points
  - When succeeds, the other end-point safely accepts requests from presentities/inboxes pertaining to the domain of first end-point
  - Done using the Transport Layer Security (TLS) protocol (out-of-band) (RFC 2246) or Simple Authentication and Security Layer (SASL) (in-band login) (RFC 2222)



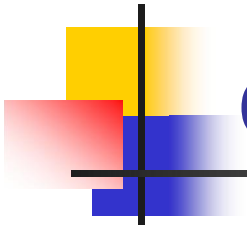
The PRIM protocol (cont)

- Authentication Strength
  - What servers communicate to next hop during a relay
  - “strong”,”medium”,”weak”,”none”
  - Compare with strength of current connection
  - Can be a criterion to reject a command



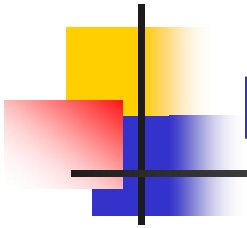
Security Considerations

- Spoofing
  - Authentication of presentities/watchers, senders/inboxes
- Stalking (Privacy)
  - Access rules, visibility rules, polite blocking
- Spam
  - Delivery rules



Conclusion

- IM has become popular in the corporate world
- Current applications: SMS-type chat, real-time collaboration, CRM
- Future applications: Integrate with mobile technologies, PDA, e-commerce, targeted advertisements
- Biggest challenges: different non-standard, non-interoperable implementations, privacy and security issues
- IMUnified – Microsoft, Yahoo, Excite, AT&T etc. to support IETF standards



References

- IETF RFC 2778/2779
- Presence and Instant Messaging Protocol (PRIM) Server-Server Protocol Specification <draft-ietf-prim-server-00.txt>
- Common Presence and Instant Messaging (CPIM) <draft-ietf-impp-cpim-02>
- Common Presence and Instant Messaging: Message Format <draft-ietf-impp-cpim-msgfmt-04.txt>
- CPIM Presence Information Data Format <draft-ietf-impp-cpim-pidf-01.txt>
- http://www.business2.com/webguide/0,1660,40034,FF.html