Financial Cryptography - Feb 27, 2006

A Protocol for Secure Public Instant Messaging

Mohammad Mannan and Paul C. van Oorschot

Digital Security Group

Carleton University, Canada

Outline

- IM overview and motivation
- Instant Messaging Key Exchange (IMKE) – the protocol
- Security comments

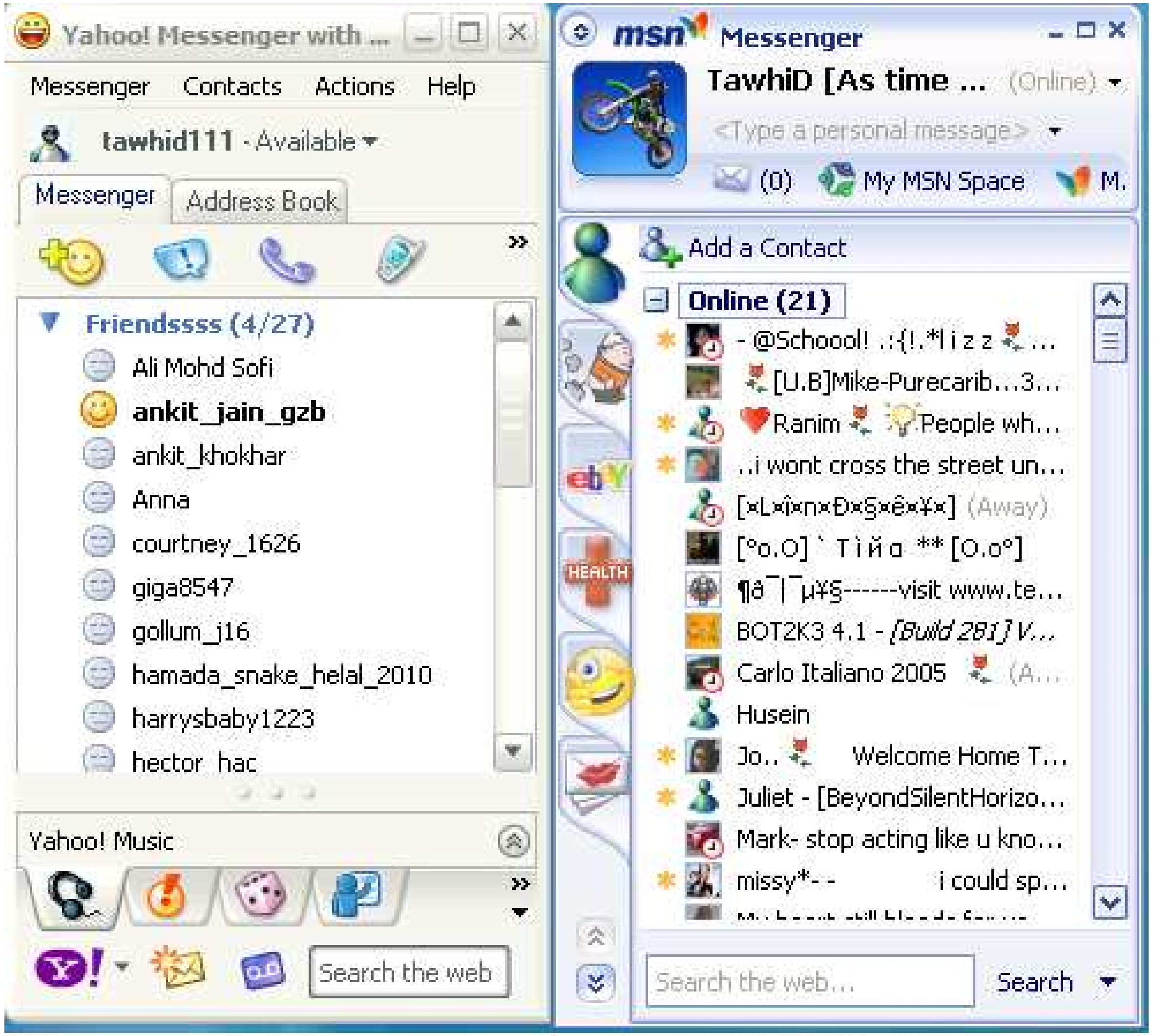
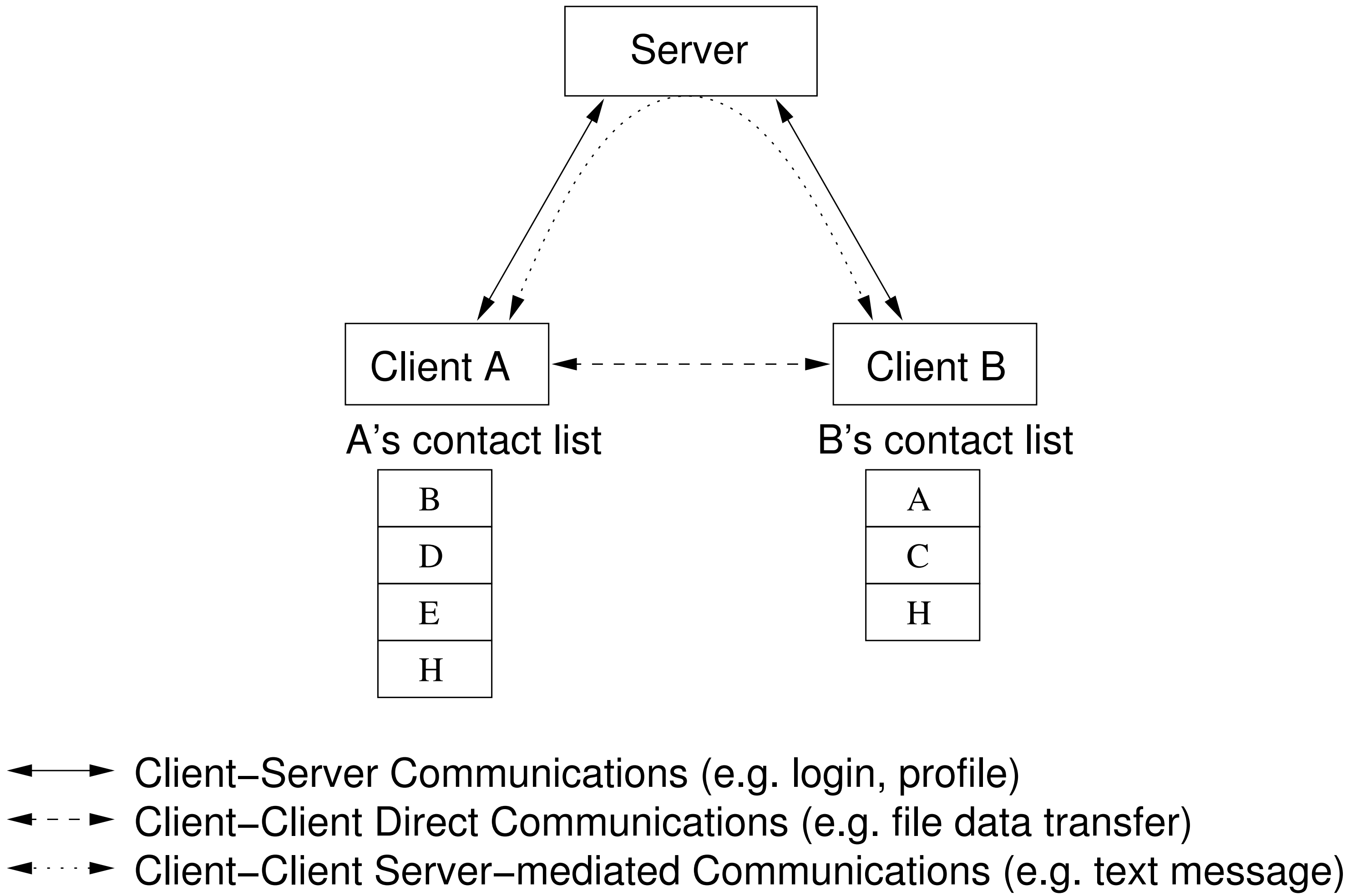


Figure 1: IM in action

IM communication model



Do we need secure IM?

- IM is a popular application
  - instant communication (home users)
  - instant collaboration (enterprise users)
- Number of users : MSN 185m, Yahoo! 82m, AOL 61m[a]
- 13 of Fortune 50 companies were affected by IM-related security incidents in the last 6 months[b]
- IMlogic was bought by Symantec (Jan. 2006)

[a] Source: ComScore Media Metrix, Aug. 2005

[b] Source: IMlogic, Nov. 2005

IMKE - motivation

1. Existing solutions have drawbacks
   - SSL: relayed user messages are visible to IM server
   - client plug-ins: client-server messages are plaintext
   - secure protocols: not designed for integration
2. Strong password protocols do not fit
   - efficiency
   - simplicity

IMKE - goals

1. Mutual assurance of identity
2. Secure communications (“C.I.A.”)
3. Forward secrecy
4. Repudiation (!)
5. Replay detection
   - authentication phase: ✓
   - text message / file transfers: standard techniques

IMKE - notation

A, B, S	IM users *Alice* and *Bob*, and IM server
ID_A	User ID of A
P_A	Password shared by A and S
R_A	Random number generated by A
$\{data\}_K$	Secret-key encryption of $data$ using key K
$\{data\}_{E_A}$	Public-key encryption of $data$ using A's public key KU_A
K^s_{AS}	Symmetric (s) session encryption key shared by A and S
$[X]_{AS}$	MAC output of X under the symmetric MAC key shared by A and S

IMKE - features

- Comparing IMKE re: offline dictionary attack avoidance
  1. password-only (eg. EKE): $\{KU_A\}_{P_A}$
  2. known server public key (eg. Halevi-Krawczyk): $\{P_A, R\}_{E_S}$
  3. IMKE: $\{K_{AS}\}_{E_S}, \{P_A\}_{K_{AS}}$
- Public key protocol independence
- IM server works as an online public key distribution center
- Secure communications between users who share no long-term secret
- Dynamic client public keys

IMKE - message summary (1)

Phases	*Message Labels*	*Messages*
Authentication and Key Exchange		A generates a dynamic public/private key pair A, S authenticate each other using shared password A, S establish a session key A's public key is sent to and stored by S
Public Key Distribution		A communicates to S a desire to talk to B S forwards B's public key to A (and A's to B)
Session Key Transport		A, B authenticate each other using the received public keys A, B establish a session key

IMKE - message summary (2)

Phases	*Message Labels*	*Messages*
Authentication and Key Exchange	$a1$	$A \rightarrow S : ID_A, \{K_{AS}\}_{E_S}, \{KU_A, f_1(P_A)\}_{K_{AS}}$
	$a2$	$A \leftarrow S : \{R_S\}_{E_A}, \{f_2(P_A)\}_{K_{AS}}$
	$a3$	$A \rightarrow S : f_3(R_S)$
Public Key Distribution	$b1$	$A \leftarrow S : \{KU_B, ID_B\}_{K^s_{AS}}, [KU_B, ID_B]_{AS}$
	$b2$	$B \leftarrow S : \{KU_A, ID_A\}_{K^s_{BS}}, [KU_A, ID_A]_{BS}$
Session Key Transport	$c1$	$A \rightarrow B : \{K_{AB}\}_{E_B}, \{R_A\}_{K_{AB}}$
	$c2$	$A \leftarrow B : \{R_B\}_{E_A}, \{f_6(R_A)\}_{K_{AB}}$
	$c3$	$A \rightarrow B : f_7(R_A, R_B)$

$$K^s_{AS} = f(K_{AS}, R_S), \quad K^s_{AB} = f(K_{AB}, R_B)$$

IMKE - security

- Formal proofs: ✗
- BAN-like analysis (outline): ✓
- AVISPA protocol analysis tool: ✓

  `http://www.scs.carleton.ca/~mmannan/avispa-imke/`

IMKE - attacks not addressed

1. Keyloggers can collect passwords
2. A false public key of S on client allows offline dictionary attacks
3. Malicious IM server may forward false client public keys (MIM)
4. IM worms

IMKE - implementation

1. Integrated with Jabber
2. Usable performance
   - authentication time doubles, but still less than 0.5 second
   - little effect on text messaging and bulk data transfer
3. Incrementally deployable

Concluding remarks

1. Secure IM: becoming increasingly important

2. IMKE: simple, integratable

3. Main lesson from IMKE implementation: practical today