

# SGFR:

## Secure Groupware for First Responders

<http://cs.uccs.edu/~sgfr/>

Contact: [chow@cs.uccs.edu](mailto:chow@cs.uccs.edu)

A NISSC Sponsored Project

C. Edward Chow (PI)

Chip Benight (PI)

Ganesh Godavari

Department of Computer Science

Part of this work is based on research sponsored by the Air Force Research Laboratory, under agreement number F49620-03-1-0207. it was sponsored by a NISSC summer 2003 grant.

# Goal of SGFR

- SGFR: Secure Groupware for First Responder:
- The goal is to design a framework for enhancing groupware packages such as instant messenger and video conferencing tool,
  - with security through
    - scalable group key management (Keystone from UT Austin), and
    - secure model secure group policy management (Antigone from U. Michigan)
  - With stress level and tool usage effectiveness evaluation
- This is a joint project with Dr. Chip Benight of psychology department.
- The enhanced secured groupware will be tested in a field trial with City's Emergency Response team.

# SGFR Features

## **Security Enhanced Groupware**

Instant messenger  
(JabberX)

## **Psychology Evaluation**

Stress Level Tracking  
Effectiveness of Tool Usage  
(Keyboard/Mouse Event Tracking,  
History of Commands, Mistakes,  
Popup Quiz?)

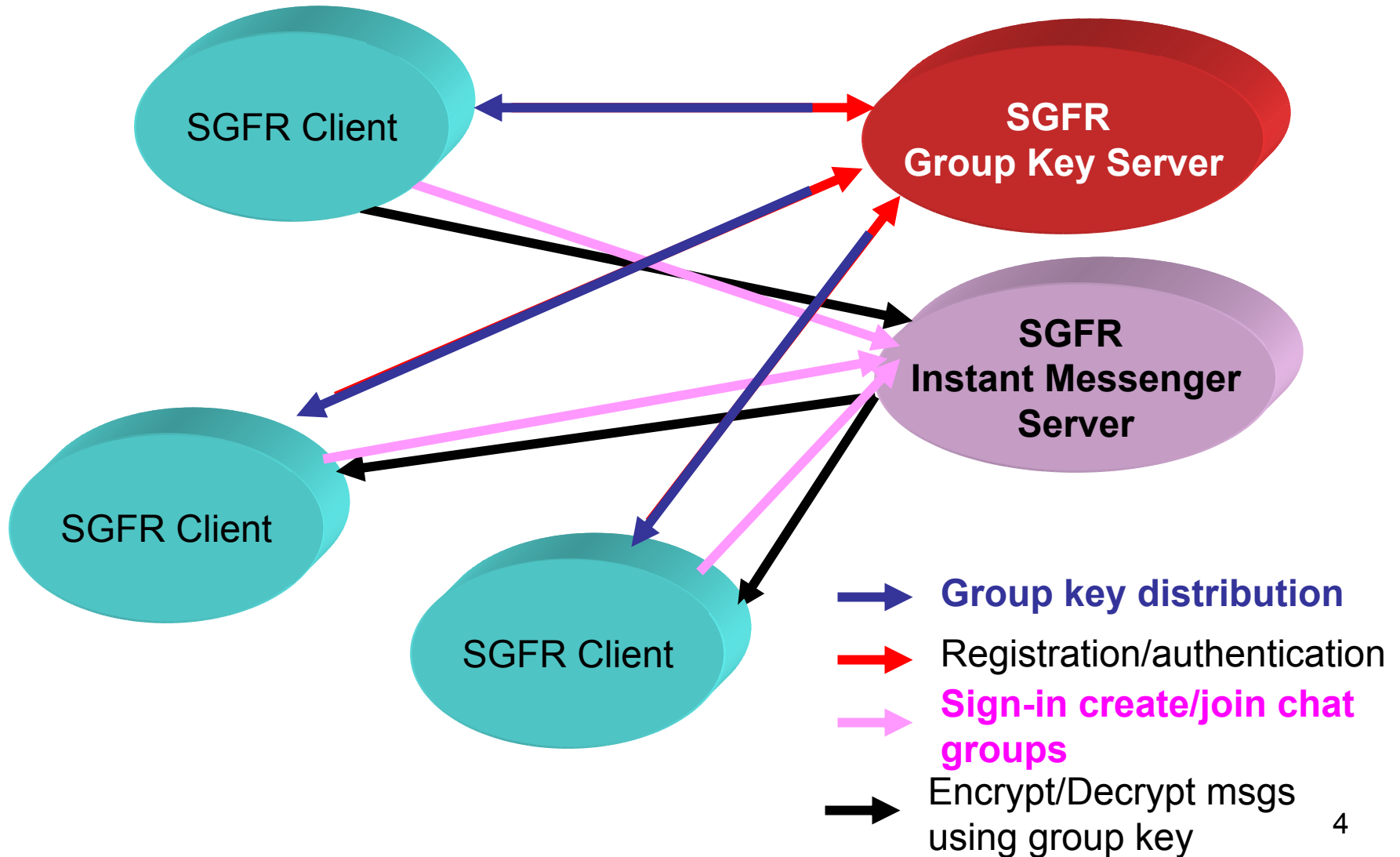
## **Group Key Management**

Secure Group  
Rekeying system  
(Keystone)

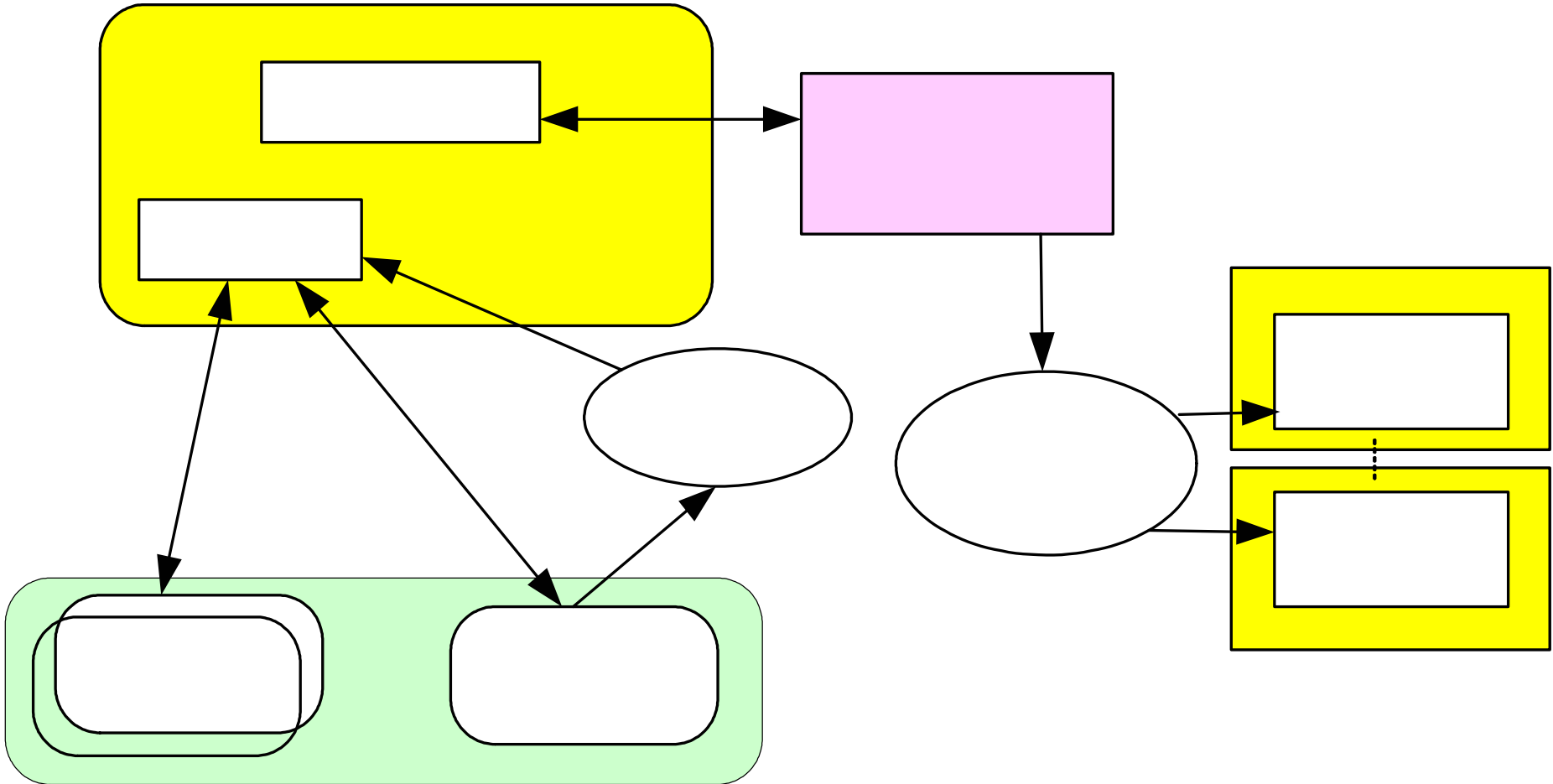
## **Group Communication Server**

Instant Messaging Server  
(Jabber)

# SGFR System Architecture



# SGFR System Operation



# Associate JabberX client with Keyserver and Jabber server

- Users login to the Jabber server
- If login successful, the client registers with the Keyserver.
- When a user creates/joins a group, the Keyserver gives a key to the client.
- When a user leaves the group, the Keyserver generates a new key for the remaining members of the group.

```

[root@oblib keystone1.0]# ./keyserver0
pid 23976 in progress
pid 23976 exited
group g1 key (100000,2): 5def1274 eca51de5 5d30b65f 9cf37007 5def1274 eca51de5
req rekey: [N(100002,1)] [N(100000,2)] (108)
join rekey
0105006c 00000000 00000002 00000001
1351d29c 44625901 42e5f4b5 b9852684
d5892548 061fdf6a 1885d461 a168d3e1
c7da83ba 6eae79ec 5857d567 77906ade
f635e06c a3ba820a dbda1127 9004f194
388eb20e c6857b75 8a9fa8f8 1a168074
9240821e b3cf284b 3e1624f1
JL_JL1:
rekey msg 0 (g1):
pid 24020 in progress
pid 24020 exited
req rekey: [N(100003,1)] [N(100000,3)] (108)
join rekey
0105006c 00000000 00000003 00000001
b316f5e9 9244c27f e7bfc2d5 c40f3ccd
46ea5a55 58316b96 488ad2e3 c8d012a2
17b481c6 b2c72901 905b97ee 45986e56
0a7131ef c8dc57ac 92b575a6 94294a8f
b600cc55 5ca76321 728022af 4a07ad99
e684e16a 7e9612b6 e3643ec2
JL_JL1:
rekey msg 0 (g1): [j(100000,3)(100000,2)]
rekey msg 132
01040084 00000000 00000001 00000001
0402002c 000186a0 00000002 000186a0
00000003 1fbacec6 2146f863 6d1c2425
0569e904 755c0800 37c32ae8 07000048
00000000 d6f50b30 911f653b bdae8c07
cf337be1 5bdcd195 d9fb4e2d 678fb7f4
82631594 329be29a bbb32e24 4e73c9f6
920ead76 20024322 4ea758de f77360fb
300a7d46
group g1 key (100000,4): 4dcd385a f96e9452 ac8cb02c e705cdae 4dcd385a f96e9452

```

↑  
**First group key  
assigned to group**

**Second group key  
assigned to group  
When a member  
joined**

↓

```

Joining g1@conference.oblib.uccs.edu...

```

```

*** ayen is available.

```

```

*** ganesh is available.

```

```

decryption of the string gone wrong error -2

```

```

*** ganesh has become available

```

```

<ganesh> ganesh is here

```

```

<ayen> good that u r

```

```

GChat [g1@conference.oblib.uccs.edu]

```

```

Online [ganesh@oblib.uccs.edu/JabberX]

```

```

jx> []

```

**User ganesh joining group g1**

```

Joining g1@conference.oblib.uccs.edu...

```

```

*** ayen is available.

```

```

*** ayen has become available

```

```

<ayen> hello

```

```

*** ganesh is available.

```

```

*** ganesh has become available

```

```

<ganesh> ganesh is here

```

```

<ayen> good that u r

```

```

GChat [g1@conference.oblib.uccs.edu]

```

```

Online [ayen@oblib.uccs.edu/JabberX]

```

```

jx> []

```

**User ayen joining group g1**

**Output of the Keystone Server**

```

0040 d1 24 3c 6d 65 73 73 61 67 65 20 74 79 70 65 3d .<message type=
0050 27 67 72 6f 75 70 63 68 61 74 27 20 74 6f 3d 27 'groupchat' to='
0060 57 6b 67 6f 64 61 76 61 40 6f 62 6c 69 62 2e 75 gkgodava@oblib.u
0070 53 63 73 2e 65 64 75 2f 4a 61 62 62 65 72 58 27 ccs.edu/ JabberX'
0080 20 66 72 6f 6d 3d 27 67 31 40 63 6f 6e 66 65 72 from='g 1@confer
0090 55 6e 63 65 2e 6f 62 6c 69 62 2e 75 63 63 73 2e ence,oblib,u
00a0 55 64 75 2f 67 61 6e 65 73 68 27 20 63 6e 75 3d edu/ganesh' cnu=
00b0 27 27 3e 3c 62 6f 64 79 3e 78 47 62 61 72 37 39 '<body>xGbar79
00c0 33 78 31 67 3d 3c 2f 62 6f 64 79 3e 3c 2f 6d 65 3x1q=
00d0 73 73 61 67 65 3e /body></me
ssage>

```

Packet captured by Ethereal Packet Sniffer

Encrypted "Hello"

Surrounded by <body>tag

```

File Edit View Terminal Go Help
[root@oblib jabber-1.4.2]# ./jabberd/jabberd -c jabber.xml
20030916T10:09:23: [notice] (-internal): initializing server
20030916T10:09:54: [notice] (update.jabber.org): bouncing a packet to jsneupdate
.jabber.org/1.4.2 from localhost: Server Connect Timeout
20030916T10:09:54: [alert] (localhost): hostname naps back to ourselves!
20030916T10:09:54: [notice] (localhost): failed to establish connection
20030916T10:09:54: [warn] (localhost): dropping a packet to localhost from jsmeu
pdate.jabber.org/1.4.2: Server Connect Failed

```

Output of the Jabber server running on a machine

# Testing Results

Table 1 time taken for client registration group join, group leave

Runs	Client Registration Time (ms)	Group Join Time (ms)	Group Leave Time (ms)
1	279.62	233.46	135.54
2	249.28	652.74	126.78
3	253.93	706.04	769.08
4	259.46	118.15	434.12
Avg/Run	260.5725	427.5975	366.38

Table 2 time taken for file transfer

File size	Time Taken (ms)
8.5K	35302.47
25K	105986.05
60K	305934.53
195K	1007949.38

# Conclusion

- A secure group communication software package SGFR v.0 was developed.
  - Use Digital Certificate to authenticate client access.
  - Group keys are distributed when members join/leave or based on some time period.
  - Group key is used to encrypted the messages.
  - Enhance text-based chat with remote file download and remote display.
- Ported the SGFR v.0 to run on handheld devices include PDA running Linux and Sony PalmTop.

# Future work

- Improve the file transfer capability using Reliable Multicast Transport Protocol.
- Improve Keystone's error handling mechanism between keyserver/registrar and client manager.
- Improve Keystone client manager by moving it into socket layer and providing socket layer API between a client manager and data processor.
- Integrate with Wireless Sensor Networks and improve security of their operations.