

# Strong Encryption over the MSN Instant Messenger Network

Private Communications over  
Public Chat Networks

By: Anthony Lander  
anthonylander@yahoo.com

# Introduction

- What's the problem?
  - Privacy in normal life vs private on the net
- Do we really need encryption?
  - Secure data
  - Secure communications
    - Email, IM – Comparable adoption pattern?
- The ultimate goal

# Roadmap

- Understanding strong encryption
- MSN Instant Messenger & Pongo
- Adding strong encryption to MSN IM
- Question Period

# Strong Encryption

- Symmetric ciphers
- Asymmetric ciphers
- Key exchange

# Symmetric Ciphers



- There's only one key
- Can encrypt and decrypt messages
- Fast and strong
  - 128 bit key is considered secure (Schneier 154)
- Examples
  - 3DES, IDEA

# Asymmetric Ciphers



- “Lock” and “key” are separate
- Public key can encrypt messages
- Only private key can decrypt them
- Computationally expensive
- Bit for bit, not as strong as symmetric
  - A128-bit IDEA key much, much stronger than even a 2048-bit RSA key (Schneier 162)
  - Consider key lifetime



# Key Exchange

- Out of band exchange
  - Email, in person, by phone
  - Trusted 3<sup>rd</sup> parties
- In band exchange
  - Secure key exchange algorithms
    - eg Diffie-Hellman

# Putting It All Together

- Storing documents securely
- Transferring documents securely
- Chatting securely

# Storing Documents Securely

- Small documents
  - Public key alone
- Large documents
  - Public key + symmetric key
- Free software
  - PGP
  - GNU Privacy Guard (GPG)

# Transferring Documents Securely

- Usually relies on public key exchange
- E-mail integration
  - Painless on Unix/Linux/BSD
    - kmail, mutt, et al + GPG
  - Varying degrees of pain on Windows
    - Eudora + PGP
    - Conspicuous-Lack-of-Integration award: **Outlook!**
      - plugins are available, though
  - Web-based e-mail
    - HushMail

# Chatting Securely

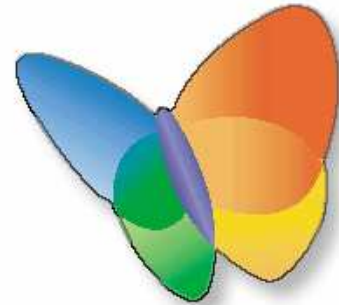
- Coming up!

# Roadmap

- Understanding strong encryption
- **MSN Instant Messenger & Pongo**
- Adding strong encryption to MSN IM
- Question Period

# MSN Instant Messenger

- Real-time chat protocol
  - Text chat
  - File transfers
  - Voice and video
- Ubiquitous
  - Currently *100 million* active users
    - ref: <http://tinyurl.com/fw1c>



Butterfly logo (c) and TM Microsoft Corp.

# Protocol Overview

- Server mediated communications
- Notification server
  - Contact list, online status
- Switchboard server
  - Chat session

# Notification Server

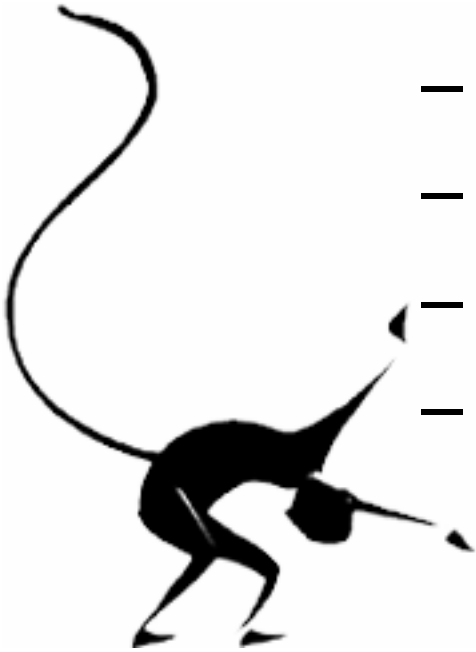
- Login manager
- Online status
  - eg, Online, Away, On the Phone
- Contact list management

# Switchboard Server

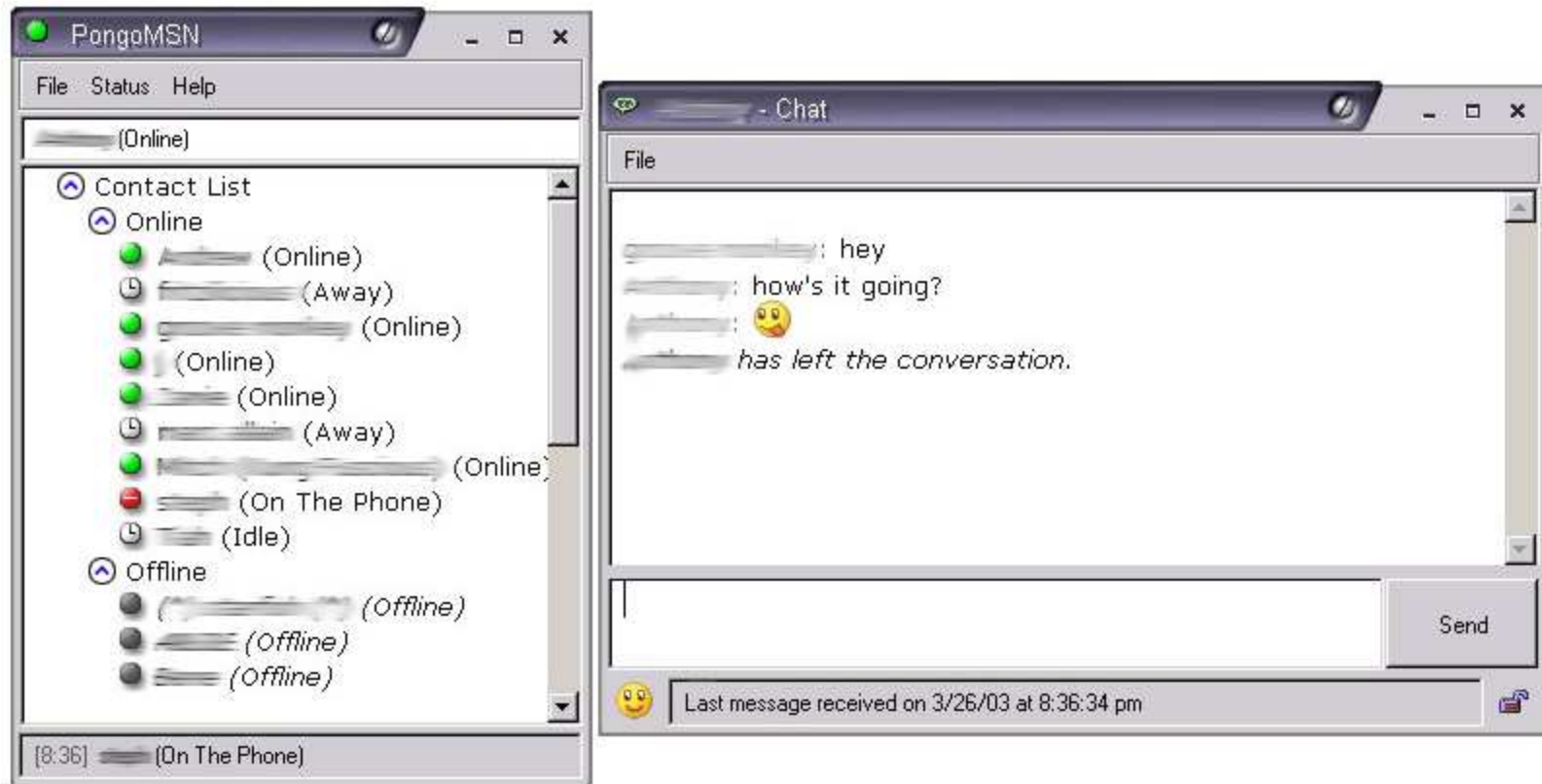
- Mediates a single chat session
  - Participants may join and quit at any time
  - Relays messages to all participants
- Uses MIME messages
  - eg, Text/Plain, text/x-msmsgsinvite
- Extensible
  - Unhandled MIME types are ignored

# Pongo

- MSN Instant Messenger client
  - Written in VisualWorks Smalltalk
  - Open source (Artistic license)
  - <http://pongo.sourceforge.net>
  - Stand alone, or Integrated with BottomFeeder



# Pongo Features



# Roadmap

- Understanding strong encryption
- MSN Instant Messenger & Pongo
- **Adding strong encryption to MSN IM**
- Question Period

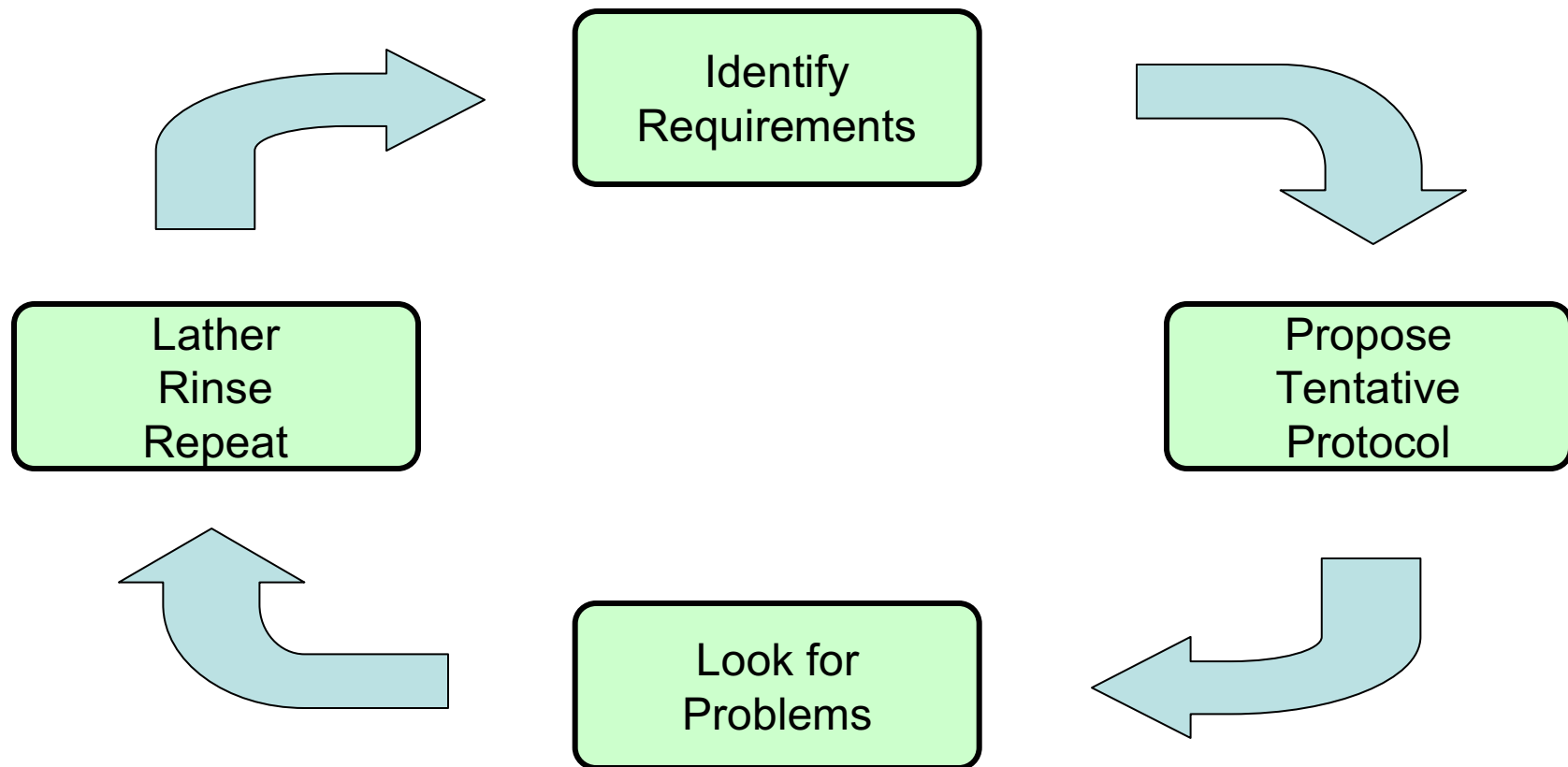
# Crypto Over Chat

- Requirements
  - Private conversation over a public server
  - More than 2 participants
  - Participants don't share a secret key
  - Easy enough for my Mom to use

# Basic Encryption Protocol

- Establish conversation
- Handshake
  - Agree upon a what sort of encryption to use
- Negotiate
  - Agree on a secret key (or use public keys)
- Establish a secure session
  - Chat ...
- Tear down the session
- Disconnect the conversation

# Refinement Strategy



# Proposal #1

- Negotiate
  - Use Diffie-Hellman to exchange an *ephemeral symmetric session key*
- Establish a secure session
  - Exchange messages encrypted with the symmetric key
- Tear down the session
  - Send an encrypted termination message

# Problems

- Monkey in the middle attack
  - In-band key exchange over a public server



# Proposal #2

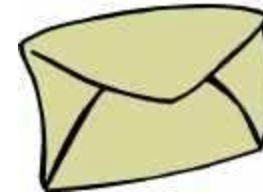
- Negotiate
  - Use **public keys** to exchange an ephemeral session key
- Establish a secure session
  - Exchange messages encrypted with the session key
- Tear down the session
  - Send an encrypted termination message

# Problems

- What happens after a participant leaves?
  - He can still “listen in” on the conversation

# Proposal #3

- Package each message in an *envelope* which contains:
  - Ephemeral key for this message, encrypted to each recipient
  - Message encrypted with ephemeral key



# Proposal #3 ...

- Negotiate
  - Gather each participant's public key
- Establish a secure session
  - Generate a session key for each message
  - Encrypt message with session key
  - Encrypt a copy of session key with each participant's public key
- Tear down the session
  - Send an encrypted termination message

# Summing Up

- Layering secure encryption on MSN is definitely possible
- Tradeoffs to consider:
  - Security
  - Efficiency
  - Convenience

# Roadmap

- Understanding strong encryption
- MSN Instant Messenger & Pongo
- Adding strong encryption to MSN IM
- **Question Period**

Questions...?

# References

- Pongo MSN Client
  - <http://pongo.sourceforge.net>
- The Passphrase FAQ
  - <http://www.stack.nl/~galactus/remailers/passphrase-faq.html>
- GNU Privacy Guard
  - <http://www.gnupg.org>
- Cryptlib
  - <http://www.cs.auckland.ac.nz/~pgut001/cryptlib/index.html>
- Diceware
  - <http://world.std.com/~reinhold/diceware.html>
- Applied Cryptography, 2<sup>nd</sup> Edition
  - Schneier, Bruce. New York: Wiley & Sons, 1996.

# References ...

- Hypothetic.org – MSN Protocol Overview
  - <http://www.hypothetic.org/docs/msn/index.php>
- Encrypted web-mail
  - <http://www.hushmail.com>
- The History of Alice and Bob
  - <http://tinyurl.com/fwgd>
- Implementor's forum for crypto over chat
  - <http://www.chat.solidhouse.com/smsn/>