Secure Instant Messaging

Mike Davis, phar@stonedcoder.org

Introduction

- Brief History of IM, and attacks against it
- How IM is being used today, and why these uses make strong security essential
- Current problems and examples
- To-do list for open-source developers

BLAIM

- BLAIM was the first secure instant messenger plugin for the GAIM messaging client
  - Used 2048-bit Diffie-Hellmann for asymmetric key exchange
  - 448-bit blowfish for symmetric cypher
  - Disposable keys, only used during the current online session
  - Earned me my first cease and decist
  - Basically a silly hack

IM-Passe

- IM-Passe was a secure messaging proxy that was an evolution of the BLAIM idea
  - IM-Passe used variable RSA keylengths of 1024-4096 bits
  - 448-bit blowfish for symmetric cypher
  - Secure file transfer
  - Keys were generated only once and re-used
  - Encryption was automatic for known keys
  - Worked for the “big three” messengers: AIM & ICQ, Yahoo, MSN with plugins for Jabber and Excite in progress
  - All protocols were cleanly reverse-engineered from data on the wire

History

- IRC was potentially the first “instant messaging” client, but it doesn’t really fit the model we are used to thinking of it in, so I will not consider it as such for this presentation
- America Online introduced a feature called “instant messaging” usable only by AOL members
- In 1996, and Israeli Software firm named Mirabilis wrote ICQ, creating the standard model as far as look, usability, and sensibility that has been copied, more or less, in every messenger since
- In 1997, AOL released AOL Instant Messenger (AIM)

History (continued)

- By 1998, AOL has purchased Mirabilis, forming the largest Instant Messaging Service
- Soon after Excite, Yahoo, MSN, and other less successful ventures like PowWow followed suit, released hasty mimics to stay in competition.
- By the year 2000, instant messaging had grown popular and stable enough that it began to be incorporated by companies as a standard method of communication

Expanded Use of IM
Leads to more Mature Attacks

- Use of early IM was considered “novelty” or even “kitsch”
- Early attacks and exploits were also light-hearted, and less serious
- The usage has evolved to become more common and serious in nature, so too have the seriousness of the attacks. The maturity of the technology itself, however, has not kept pace.

History of Attacks, Abuse & Exploits

- Early attacks on instant messaging clients were also “novelty” and were focused more on annoying users than anything else
  - Bombs
  - Floods
  - HTML Text Formatting Flaws
  - aim:// Flaws

Modern
Attacks, Abuse & Exploits

- AIM: CAN-2002-0362 – Remote Buffer Overflow
- AIM: CAN-2000-1093 – Remote Buffer Overflow
- AIM: CAN-2000-1094 – Stack Overflow
- MSN: SF-BUG-ID-4316 – Send Messages as an arbitrary user
- AIM: SF-BUG-ID-3408 – Large Buddy Icon DoS
- MSN: SF-BUG-ID-668 – Buffer Overflow
- AIM: SF-BUG-ID-5492 – Buffer Overflow
- ICQ: SF-BUG-ID-5295 – Remote DoS
- ICQ: SF-BUG-ID-7821 – Unauthorized access to remote files

Why You Should Care about IM Security

- Privacy! Messages are sent in the clear, unencrypted.
- Potential for identity theft if attacker can steal identifying information.
- If compromised you system to be used to carry out attacks on other systems.

Why Your Company Should Care About IM Security

- Sanctioned use of IM for inter-office communication, customer support, B2B, etc.
- Instant messaging data can be sniffed off of wireless networks.
- Possible leakage of company infrastructure specifics.
- IM provides an avenue for an attacker to impersonate personnel with even less verification than even a phone.
- Employee contact with outside world can’t be logged for regulation compliance.
- No way to monitor, or enforce company policy regarding contact with customers or partners.

Why We All Should Care About IM Security

- Prevalence in so many homes and offices, could potentially compromise huge numbers of systems behind firewalls by providing a common consistent channel of attack.
- Could provide channel of communication between the attacker and the exploited system
- Potential data loss

Sanctioned Uses of IM

- Customer Service
- Inter-Office, Inter-Department, Inter-Branch Communication
- Status Reports
- Ad-hoc Online Meetings

Unsanctioned Uses of IM

- Chatting with friends and family
- Cybersex
- Group chatting or chat rooms
- Gaming
- “primary means of communication”

Examples of IM Security Gone Wrong

- eFront Systems:
  - eFront's CEO's computer was penetrated by hackers through an "unknown method"
  - An ICQ log was stolen and posted to various websites
  - eFronts financial backers eventually pulled out due to the scandal
- Bugtoaster Inc.
  - Bugtoaster Inc found a method to retrieve MSN passports directly from its location in ram (documented in the microsoft API)
  - While this vulnerability only effected windows 95,98 and ME it is still quite serious due to the nature of MSN Passports!
  - "Microsoft will not be provifing a patch for this because there is nothing to patch" – anonymouse microsoft employee

Current Problem: A

```
T 64.12.200.89:5190 -> 66.246.156.220:49877 [AP]
  *..M.............jdcrunchman....205.188.9.82:5190.........R(.g>.....B..
  ....u..6.........t._.......U.(.?;a.t.B..h..c..`}..AL..."]...,z..e......./
  .7}..NL..,.x..O..Q...f...q.ir?a..........6.I;.gi!...\..U.G...i... .A...^..
  ..r.u.84...Z..qdQd.....Y..#..D......Z6.%.....C%46....v.._P..|6.....i..y.$..
  ..&.E.y.3.8.....crunch@shopip.com.......T.Xhttp://aim.aol.com/redirects/pas
  sword/change_password.adp?ScreenName=%s&ccode=US&lang=en*..N..


T 66.246.156.220:50162 -> 64.12.201.134:5190 [AP]
   ODC2.L.......pn.X.....................`....jdcrunchman.................
   ..<html><body ichatballooncolor="#C0E668" ichattextcolor="#000000"><font
   face="Helvetica" ABSZ=12 color="#000000">I won't be able to do it right
   now...  I'm super busy - here at Hope - doing a demo of the reporter at
   the moment.</font></body></html>
```

Current Problem: Files!

T 64.12.201.130:5190 -> 66.246.156.220:50161 [AP]

<!--The CrunchBox: Designed and programmed by Steven Inness for ShopIP, Inc.-->..<?xml version="1.0" encoding=

"iso-8859-1"?>.<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD

/xhtml1-transitional.dtd">.<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en">.<head>.<title>4XSS - Top pane</title>.<meta http-equiv="Content-Script-Type" content="text/javascript; charset=iso-8859-1" />.<style type="text/css">. body {. background-image: url(/images/metal.gif);. margin: 0px 0px 0px 0px;. padding: 0px 0px 0px 0px;. }.. table {. color: #000000;. font: 300 7pt Helvetica, sans-serif;. }../*Netscape 6 doesn't change from 'link' to 'visited' until page is reloaded.*/. a:link,a:visited {. background-image: url(/images/back_but.gif);. display: block;. color: #000000;. width: 97px;. height: 16px;. padding-top: 3px; /*In Windows IE this does not make text box increase TD box*/. text-decoration: none;. }.. td.b

- remaining packets within this stream were omitted for the sake of brevity

AIM Format String Flaw

- Current and an unknown number of past versions of AIM are vulnerable to a format string flaw embedded into the protocol itself.
  - While the protocol requires direct tinkering with the packet stream this type of attack isn't unheard of, and libraries like "packet purgatory" make it simple with a little ARP spoofing.
  - In the same packet a another potential exploit exists by replacing the "change password" URL within the packet.
  - In past versions of AIM, this packet was vulnerable to "New Update Available" attacks since the url for the software update was provided within the packet also.

A Look at What's Currently Available in "Secure" Messaging

In the marketplace various attempts are made to address individual aspects of security such as…

- » **Strong** encryption of messages
- » Logging for SEC Compliance
- » Verified User Identification
- » Secured File Transfers
- » Hierarchical Policy Management
- » Online Meeting Tools

…but no single client provides all of these protections together

If IM is Going to be Taken Seriously, It's Security Needs to be Taken Seriously

- The clients and the servers need to be fully audited, much like the way Apache and Open SSH are.
- Open protocols standards ought to be developed based on proven security models.
- Some standards for inter-operability need to be developed between networks.
- Clients for corporate installations need a way to distinguish between company and personal communication and features for policy-based management.

Recommendations for Companies Currently Relying on Instant Messaging

None. I'm Sure Microsoft will develop a solution. ☺

- The most that can really be done at this point without a serious effort by the major providers, (AIM, MSN, Yahoo, or Jabber) is to practice standard safe computing practices.
  - Don't do anything really important based on something said in IM without verifying who you are talking to
  - Consider using different usernames for work and personal use
  - Never share sensitive information over IM, (no passwords, credit card numbers, bank or id numbers, secret plans for world domination, Dick Cheney's location, etc.)

Conclusion

- All hope is not lost. People and companies are beginning to address these concerns and are beginning to take security-minded approaches, however, the pressure really has to come from the users for the features to come to fruition.
- Don’t just wait around for AOL to invent a security feature; know what your risks are, where you are vulnerable, and demand serious holistic solutions.

Questions

For further information, and information about my other projects write to me at **phar@stonedcoder.org** or visit my website: **http://www.stonedcoder.org**