eXercise In Messaging and Presence Pwnage

fun with XMPP

Ava Latrope

iSEC Partners

Defcon 17

iSEC PARTNERS

Outline

iSEC PARTNERS

Who am I?

- Security Consultant, iSEC Partners
- Prior to that, QA automation for various web 2.0 horrors
- ~~Eats babies~~

iSEC PARTNERS

What is XMPP?

- eXtensible Messaging and Presence Protocol
  - Formerly the Jabber project
- Specialized XML-based protocols, used for:
  - content syndication
  - file sharing
  - ...but, well, still mostly IM.

Why am I picking on it?

- Ubiquity
- Open standard
  - RFC Process
- Many implementation details are at the discretion of the developer
  - ...anyone who's met a developer should be worried by that sentence
- As much fun as you'd expect with regular XML parsing

iSEC PARTNERS

How it works

- Decentralized
  - Addressing via JIDs of the format user@server
- TLS encryption and SASL authentication
- HTTP binding
- XML stream

Common Attributes

- to - recipient JID
- from - sender JID
- id
  - Optional
  - Generated for tracking purposes
  - Scope of uniqueness is flexible
- type
  - Specifies purpose of the stanza
  - Each stanza variety has its own list of acceptable types
- xml:lang
  - Only affects presentation to humans

iSEC PARTNERS

Info/Query

- Request info/receive response
- Child element determines data content
- Requester tracks by id
- Patterned exchange

```
<iq type="result" id="purplece837cfa" to="akl-pc1/acc45887"><bind xmlns="
    urn:ietf:params:xml:ns:xmpp-bind"><jid>test2@akl-pc1/acc45887</jid></bind></iq>
```

Presence

- Publish/subscribe
- Many receive updates from one - 'to' usually omitted
- Seen most frequently in IM applications as contact status updates

```
<presence from='test2@akl-pc1/acc45887' to='avarice@gmail.com'>
<show>away</show>
<priority>0</priority>
<c xmlns='http://jabber.org/protocol/caps' node='http://mail.google.com/xmpp/client/
    caps' ver='1.1' ext='pmuc-v1 sms-v1'/>
<status/>
<x xmlns='vcard-temp:x:update'>
<photo/>
</x>
</presence>
```

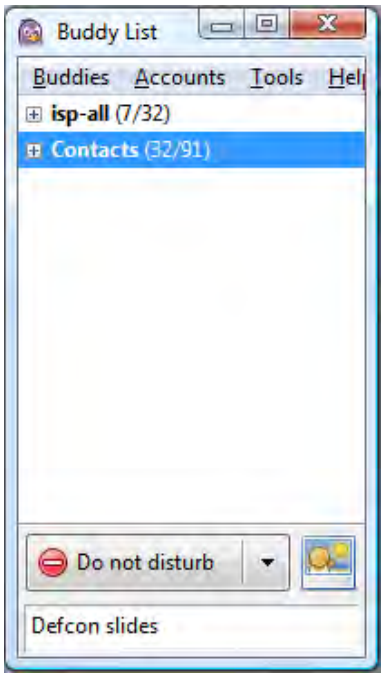
iSEC PARTNERS

Message

Fairly self-explanatory concept so long as you've ever, say, used email.

```
<message type='chat' id='purplece837d83' to='test1@akl-pc1/f9e54d' from='test2@akl-pc1/
      acc45887'>
<x xmlns='jabber:x:event'>
<composing/>
</x>
<active xmlns='http://jabber.org/protocol/chatstates'/>
<body>?OTR:AAIDAAAAAAEAAAABAAAAwEgF/95+kxlcd8Z7I3jdNZtw8d8baZIg5uq0FV3JymhEXf5qJV/6
      P46yjwABFt4UmUqN8BwK7WnWGHlcxsrAvN/FJ4oxSowLYcKRzI/eZoedIFyhlyZBT17Ou1V2+67nnczJOGRq+
      A6wjz0ayoT1iRm1Dx1ZFLvKfRT3uiwbi8AfNG7uCtQAolGKBBp2h7RBVR95NfOrfx8G5Oh6BacdhslcssY0kC3Lwmo29rNOr
      /GVX+9CY0phs8kT+O5cLedhjI8y/+udYAAAAA.</body>
<html xmlns='http://jabber.org/protocol/xhtml-im'>
<body xmlns='http://www.w3.org/1999/xhtml'>?OTR:AAIDAAAAAAEAAAABAAAAwEgF/95+
      kxlcd8Z7I3jdNZtw8d8baZIg5uq0FV3JymhEXf5qJV/6P46yjwABFt4UmUqN8BwK7WnWGHlcxsrAvN/
      FJ4oxSowLYcKRzI/eZoedIFyhlyZBT17Ou1V2+67nnczJOGRq+
      A6wjz0ayoT1iRm1Dx1ZFLvKfRT3uiwbi8AfNG7uCtQAolGKBBp2h7RBVR95NfOrfx8G5Oh6BacdhslcssY0kC3Lwmo29rNOr
      /GVX+9CY0phs8kT+O5cLedhjI8y/+udYAAAAA.</body>
</html>
</message>
```

Pidgin



The IM client formerly known as Gaim
Needed something based on libpurple
Obvious choice with 3 Million users
...especially since it's my default
File transfers
XMPP console

http://www.pidgin.im/

iSEC PARTNERS

Spark

Complement to openfire server
Voice integration
Representative of no-frills clients

http://www.igniterealtime.org/projects/spark/index.jsp

iSEC PARTNERS

Gajim

GTK+
File transfer
Multi-protocol transports

http://www.gajim.org/

Gtalk

~~Skynet~~ Google's pet XMPP project
Jingle
Mobile versions
Offline Messaging

http://www.google.com/talk/

Openfire

- Formerly known as Wildfire
- Popular on corporate networks
- User-friendly, easy to configure
- Admin web interface
- http://www.igniterealtime.org/projects/openfire/

JabberD14

- Modular, certain features can be installed independently
- Written in C/C++
- Complex configuration requires messing directly with XML
- Waning in popularity
- http://jabberd.org/

JabberD2

- Different codebase from JabberD14
- Appear to have kept the project name just to be confusing
- Main distinction seems to be that they're compliant with more RFCs than the original
- http://codex.xiaoka.com/wiki/jabberd2:start

DoS

- Excessive presence traffic makes for high overhead
- Endemic scalability issues in XMPP
- Parser errors tend to be ungraceful

DoS Demo

[DoS demo goes here]

XML Parsing

- Stanza-specific requirements
- Control characters
- Affects on DoS

XML Parsing Demo

[XML parsing demo goes here]

File/Image Upload

- No restrictions on file type
- Relatively new to most feature sets
- Image insertion

File/image Upload Demo

[File/image upload demo goes here]

Features

- HTTP and XMPP
- Intercept mode
- Manual edit
- Command replay
- Multiple concurrent listeners

Persimmon Proxy Demo

[Persimmon Proxy demo goes here]

Download

[Download information goes here]

Features

- Contains all attacks presented here
- GUI interface
- Customization of attacks

XMPP Fuzzer Demo

[XMPP Fuzzer demo goes here]

Download

[Download information goes here]

Summary

- XMPP bugs are still out there
- Here are some tools to help make that more obvious

Resources

- XMPP Foundation
  - http://xmpp.org/
- XMPP: The Definitive Guide: Building Real-Time Applications with Jabber Technologies
  - Peter Saint-Andre, Kevin Smith, Remko Tron on
  - 2009
- Programming Jabber: Extending XML Messaging
  - DJ Adams
  - 2002

iSEC PARTNERS

Questions?

https://www.isecpartners.com