XMPP

For Paranoid People

by _NSAKEY

Obligatory self-promotion

- hashcat beta tester
- Tor relay and bridge operator
- ANSI art enthusiast
- "not affiliated with the USA'S NSA" - HardenedBSD.org Donor's page
- "I think you're a Kremlin Troll." - John "20committee" Schindler

30,000 Foot Aerial View

- XMPP
- Prosody For Paranoid Sysadmins
- Evaluation & Summary

What is XMPP?

- Extensible Messaging and Presence Protocol (Formerly known as Jabber)
- It's an open protocol
- jabberd was originally released on January 4, 1999
- IETF XMPP Working Group formed in 2002 [1]
- Messages are XML

Next: XMPP

- What is it?
- Pros
- Cons
- More cons
- Clients
- Servers

Who uses XMPP?

- League of Legends
- Google Talk
- Facebook Messenger
- WhatsApp
- Kik
- Cryptocat
- Smart meters

Good Stuff About XMPP

- Open standard
  - Unlike OSCAR and other 90s protocols
- There are tons of implementations
- Also no need for chat wars [2]

Tell Me More

- Decentralized, allows federation
  - bob@example.com can chat with alice@example.net
- Very easy to roll your own internal server for a company
  - Just use the company domain and disable s2s
  - Most server implementations have a logging module

Bad Things

- The protocol wasn't designed with mobile users in mind [3]
  - Mobile users = SOL
  - Battery life = LOL
  - This is why some chat apps just fork ejabberd and the protocol

Bad Things (cont.)

- No one server has implemented the entire protocol
  - This is because it's so big.
  - ejabberd has the closest to complete implementation
  - Probably not a big deal since nobody cares about most of the protocol

One Last Bad Thing

- Some servers store plaintext passwords
  - This is to mitigate brain damage in older clients
  - ...And partly because ejabberd devs are idiots [4]

Let's Talk About Clients

- Pidgin (Multi-platform; suffers from multiple strains of avian flu)
- Adium (OS X)
- mcabber
- Bitlbee
- ChatSecure (Android)
- Psi/Psi+ (Multi-platform)

Let's Talk About Servers

- The rest of the slides will focus on making your own XMPP server
- If that's not your cup of tea, the following servers all provide Tor Hidden Services:
    - jabber.ccc.de (Avoid; SPREAD OUT)
    - riseup.net (Invite only; mod_otr = optional)
    - otr.im (mod_otr = required)
    - jabber.calyxinstitute.org (mod_otr = required)
    - rows.io

Encryption Manifesto

- As of May 19, 2014 some public servers forced TLS [5]
- Forward secrecy was mentioned, but not required
- Using a Certificate Authority is of course required

Prosody For Paranoid Sysadmins

- So You Want A Server
- Disclaimer
- Requirements
- SSL/TLS
- Forward Secrecy
- Off The Record

So You Want A Server

- Let's assume registration is open
- Let's also assume activists use it
  - And it's a surveillance target
- Let's make The Man's job harder
- But how?

Infosec Hulk Hogan Asks...

Whatcha gonna do when the Five Eyed Boogie Man runs wild on you?

DISCLAIMER

- This threat model is entirely academic
- If a .gov wants to own you, you're toast, as they have more & better resources
- Illegal programs become legal after discovery
    - See Room 641a & FISA Amendments Act of 2008
- The game is rigged, but we can mitigate
    - Somewhat

Requirements

- Force encryption
  - Only use newer TLS versions
  - Weak ciphers get disabled
  - Forward secrecy ciphers only
  - Elliptical Curve Crypto
- Force OTR (Off-The Record)
- Tor onion service
- Disable logging
- New/up-to-date clients
  - Old versions of clients will cry and break

SSL/TLS

- SSL 2/3 have ebola, so use TLS 1.x
- Older TLS versions might be ok
  - For now, so force TLS 1.2 anyway unless you support phones [6]
- Disable weak ciphers
- Disregard client cipher ordering
- See the IM Observatory: https://xmpp.net

Forward Secrecy

- Normally, a key compromise = game over for all past chats
- Not so with forward secrecy
- If the key gets stolen, past chats can't be readily decrypted, but future chats can
    - Session keys needed for decrypt
- tl;dr: EECDH/DHE or GTFO

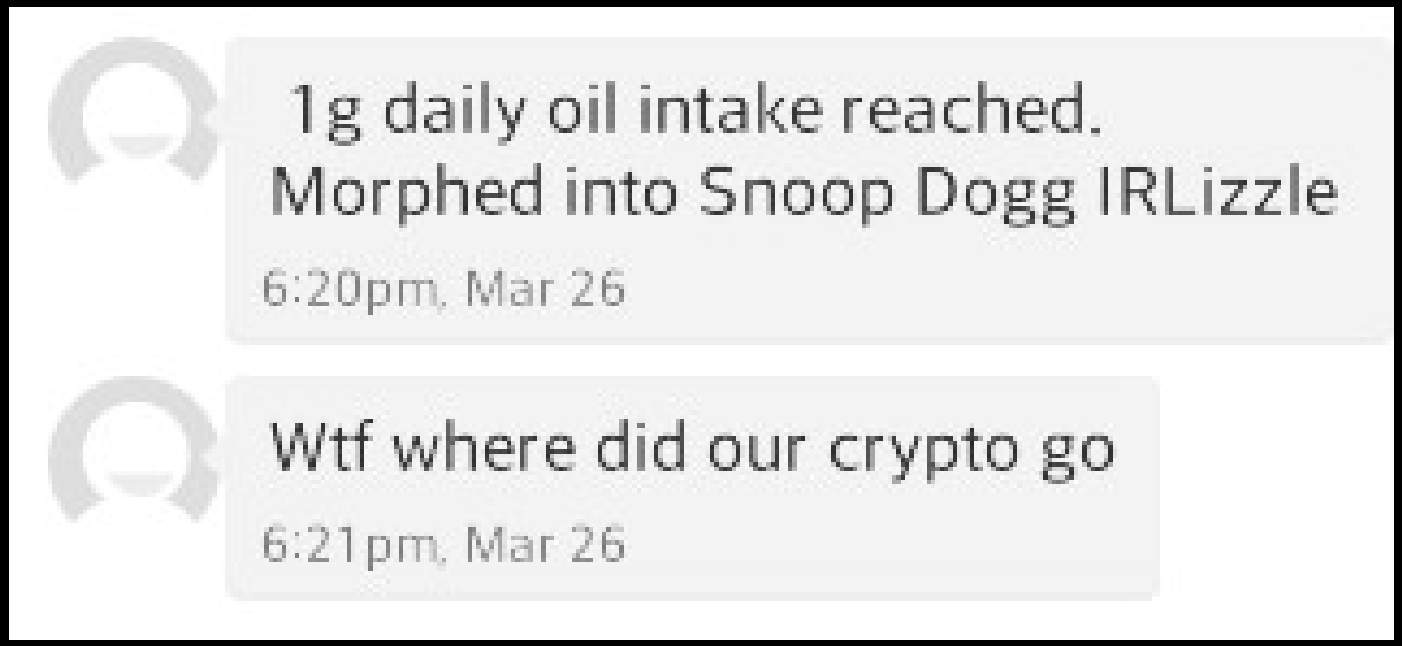
Elliptical Curve Crypto

- This crypto covers session keys
- secp384r1 is the default
- This would be sane if not for the fact that NIST has a tarnished reputation (BLAME THE NSA)
- I chose secp256k1 because...
  - No NIST cooking involved
  - Bitcoin uses it, so if it fails then LOL

Off The Record

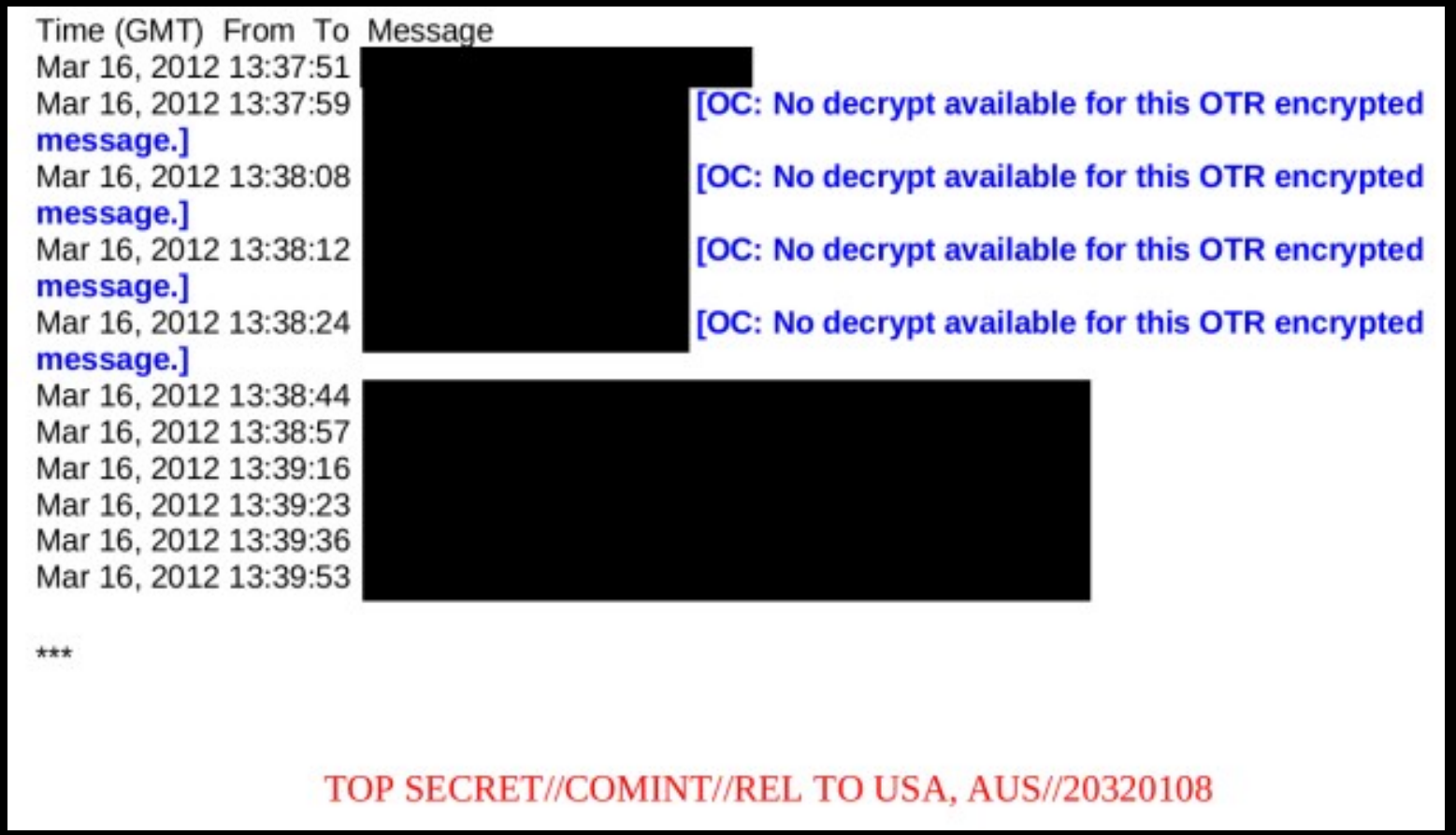
- End to end crypto
- Server can't read cleartext chats
  - Unless there's some active MITMing
  - Why should your users trust you?
- Also uses forward secrecy
- mod_otr for Prosody handles this
- Anyone notice the "FTP" theme yet?

Oh god how did this get in here I am not good with computers



Don't be like this guy.

This Is Why We OTR



Time (GMT)	From	To	Message
Mar 16, 2012 13:37:51	[redacted]		
Mar 16, 2012 13:37:59	[redacted]		[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:08			[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:12			[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:24			[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:44	[redacted]		
Mar 16, 2012 13:38:57			
Mar 16, 2012 13:39:16			
Mar 16, 2012 13:39:23			
Mar 16, 2012 13:39:36			
Mar 16, 2012 13:39:53			

***

TOP SECRET//COMINT//REL TO USA, AUS//20320108

Now isn't that much cooler?

Evaluation & Summary

- Metadata Non-Preservation
- What Do Attackers Get?
- What Do Attackers NOT Get?
- Contact Info
- References/Further Reading
- Questions & Snarky Answers

Metadata Non-Preservation

- .gov PR types like to pretend metadata doesn't matter
  - It's good enough to kill people
- Tor Hidden Services are your friend
  - This is as close to 7 proxies as it gets
  - Any logs will show 127.0.0.1
- But we're disabling logging, too
  - Why? Because subpoenas, that's why

What Do Attackers Get?

- Private key + session keys
  - Your future chats are ownable
- Currently connected users + their IPs
  - This is why we Tor
- Chat frequency (OTRed messages, timestamps, etc)
- Buddy lists + contact names
- Password hashes
  - You're not storing in cleartext, are you?

What Do Attackers NOT Get?

- Past session keys
  - Makes past chat decryption much harder
- Message content
  - mod_otr throws a kink in the works here
- Server logs
  - Since those aren't kept in the first place
- Other timing metadata
  - e.g. Connect and disconnect times

Tell Me How To Do This

- Make a clean Ubuntu or Debian box
- Grab my paranoid-prosody [7] project off GitHub [8]
- Tweak the config and set DNS records
- Get your cert signed by a CA
- Bask in the glow of your perfect IM Observatory score

Contact Me

- E-mail/XMPP: root@abigisp.com
- Twitter: @_NSAKEY
- GitHub: NSAKEY
- Ask for one of my PGP cards, because...

Infosec Hulk Hogan Says...

- To all my little Hulkamaniacs: Say your prayers, take your vitamins, and verify all key fingerprints out of band!

References

1) https://xmpp.org/xmpp-protocols/rfcs/

2) https://nplusonemag.com/issue-19/essays/chat-wars/

3) http://op-co.de/blog/posts/mobile_xmpp_in_2014/

4) https://www.ejabberd.im/plaintext-passwords-db

5)https://github.com/stpeter/manifesto

6)https://blog.thijsalkema.de/blog/2013/09/02/the-state-of-tls-on-xmpp-3/

7)https://abigisp.com/guides/paranoid-prosody.html

8)https://github.com/MSAKEY/paranoid-prosody

Further Reading

- https://en.wikipedia.org/wiki/Comparison_of_XMPP_server_software
- https://prosody.im/doc
- https://otr.cypherpunks.ca/
- https://blog.thijsalkema.de/me/blog//blog/2013/06/11/xmpp-federation-over-tor-hidden-services/
- http://op-co.de/blog/posts/android_ssl_downgrade/
- https://otr.im/chat.html
- http://www.slideshare.net/_NSAKEY/xmpp-47178073

The End

Questions?