Secure Messaging

36C3. WILL SCOTT
Secure Messaging

- Identify Adversaries & Threats
- Existing Mechanisms
- Remaining Challenges
Direct

Adversary: Network Observer

Adversary: Malicious Software
• Encryption
• Message Expiry
• OS Sandboxing / Isolation
Centralized

Facebook, whatsapp, slack, irc, wire, threema, etc.
Centralized

Adversary: Local Network
Adversary: Data Center
Adversary: Hacked Server
Adversary: Government
Adversary: ISP
Adversary: Acquisition

Acquisition
• Encryption
• Message Expiry
• OS Sandboxing / Isolation
• Traffic Obfuscation
• Server Hardening
Centralized

**PROS.**
- Availability
- Multiple devices, mobile push

**CONS.**
- Centralized Costs
- Legal/Regulatory
Federated
'Decentralized'
'Decentralized'

Ricochet.im

Tox.chat
• Encryption
• Message Expiry
• OS Sandboxing / Isolation
• Traffic Obfuscation
• Server Hardening
ENRPTION
No Encryption

We should consider switching to more private methods of communication...

Bob
192.168.0.1
hostname.tld

FROM: Alice
Transport Encryption
E2E Encryption

To: Bob
E2E Encryption

Signal Protocol
https://signal.org/docs/

OTR
https://otr.cypherpunks.ca/

OMEMO
https://conversations.im/omemo/
• Connection Establishment

• Deniability
Connecting

Who is bob? who do I trust to map "bob" to an identity?
Connecting

“WhatsApp” Would Like to Access Your Contacts
Upload your contacts to WhatsApp’s servers to help you quickly get in touch with your friends and help us provide a better experience.

Don’t Allow  OK

Welcome to WhatsApp

“You know 12 people from Instagram
Ann Glenn, Toni Marciliana, and 10 other

Continue

“Twitter” Would Like to Access Your Contacts
We will securely upload your contacts to help you connect with friends and suggest users to follow on Twitter.

Don’t Allow  OK

“Riot.im” Would Like to Access Your Contacts
In order to show you which of your contacts are already using Riot or

Don’t Allow  OK

michaelkirk commented on Sep 27, 2016 - edited

I agree that the wording is lacking.

FYI - We hash the numbers on your device and upload the hashes to the server to compute an intersection without ever sending the plain text phone numbers of your contacts to the server.
Connecting

+ ORAM

Pseudonyms

https://github.com/signalapp/contactdiscovery-service
Connecting

SKS Keyserver Network Under Attack

This work is released under a Creative Commons Attribution-NoDerivatives 4.0 International License.

Executive Summary

In the last week of June 2019 unknown actors deployed a certificate spamming attack against two high-profile contributors in the OpenPGP community (Robert J. Hansen and Daniel Kahn Gillmor, better known in the community as "rjh" and "dkg"). This attack exploited a defect in the OpenPGP protocol itself in order to "poison" rjh and dkg's OpenPGP certificates. Anyone who attempts to import a poisoned certificate into a vulnerable OpenPGP installation will very likely break their installation in hard-to-debug ways. Poisoned certificates are already on the SKS keyserver network. There is no reason to believe the attacker will stop at just poisoning two certificates. Further, given the ease of the attack and the highly publicized success of the attack, it is prudent to believe other certificates will soon be poisoned.

https://gist.github.com/rjhansen/67ab921ffbf4084c865b3618d6955275f
Connecting

TOFU

https://en.wikipedia.org/wiki/Tofu
Pond

(Note: recent events have lead to these topics being in the news quite often in recent weeks. However, Pond is not a reaction to those events - it was started nearly a year ago.)

For secure, synchronous communication we have OTR and, when run over Tor, this is pretty good. But while we have secure asynchronous messaging in the form of PGP email, it's not forward secure and it gratuitously leaks traffic information. While a desire for forward secure PGP is hardly new, it still hasn't materialised in a widely usable manner.

Additionally, email is used predominately for insecure communications (mailing lists, etc) and is useful because it allows previously unconnected people to communicate as long as a (public) email address is known to one party. But the flip side to this is that volume and spam are driving people to use centralised email services. These provide such huge benefits to the majority of email communication, so it's unlikely that this trend is going to reverse. But, even with PGP, these services are trusted with hugely valuable traffic information if any party uses them.

So Pond is not email. Pond is forward secure, asynchronous messaging for the discerning. Pond messages are asynchronous, but are not a record; they expire automatically a week after they are received. Pond seeks to prevent leaking traffic information against everyone except a global passive attacker.

https://github.com/agl/pond
Friday, October 21, 2016

Yes, we can validate the WikiLeaks emails

Recently, WikiLeaks has released emails from Democrats. Many have repeatedly claimed that some of these emails are fake or have been modified, that there's no way to validate each and every one of them as being true. Actually, there is, using a mechanism called DKIM.

DKIM is a system designed to stop spam. It works by verifying the sender of the email. Moreover, as a side effect, it verifies that the email has not been altered.

Hillary's team uses "hillaryclinton.com", which as DKIM enabled. Thus, we can verify whether some of these emails are true.

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
  d=hillaryclinton.com; s=google;
  h=from:mime-version:references:in-reply-to:date:message-id:subject:to:
  :
  bh=EH1yNFKU1g6KhzxpAJQtxaW82g5+cTT3q1zIb0pG0RY=;
  b=Jg8tkuhI1dCythkYCrUMjPIAjNhDVpFtyvuy+RpUR/kqQjR8+W23zacIh0DtV7qUGD
  mzaviTrNm18Ds2aU1zEFjxhJHtgKT42zhRiqDS27fgba8iFMKCyDgApGHfemnQz+Bl+hN
  2OHb/plm mop+1leM8ELXHhhr60/Sd4c/3BOy8=
Forward Secrecy

<Message>
My next public key is

<Message>
My next public key is

<Message>
My last private key was

<Message>
my next public key is...
• Encryption

• **Message Expiry**

• OS Sandboxing / Isolation

• Traffic Obfuscation

• Server Hardening
EXPIRY
Expiry

The "screenshot" adversary
Expiry
(the forensic adversary)

GrayKey / Cellebrite
or "ADB" on android

• Encryption
• Message Expiry
• OS Sandboxing / Isolation
• Traffic Obfuscation
• Server Hardening
ISOLATION
Tinfoil Chat

https://github.com/maqp/tfc
Recovery & Backups

Cloud Key Vault
Overview

HSMs running custom secure code connected to Apple cloud

"Behind the Scenes with iOS Security" - Ivan Krstić. Blackhat 2016
• Encryption
• Message Expiry
• OS Sandboxing / Isolation
• Traffic Obfuscation
• Server Hardening
Obfuscation

To: safe.com
To: chat provider

DOMAIN FRONTING
Obfuscation

Russia’s game of Telegram whack-a-mole grows to 19M blocked IPs, hitting Twitch, Spotify and more

Ingrid Lunden  @ingridlunden  /  12:50 pm PDT  •  April 19, 2018

As the messaging app Telegram continues to try to evade Russian authorities by switching up its IP addresses, Russia’s regulator Roskomnadzor (RKN) has continued its game of *whack-a-mole* to try to lock it down by knocking out complete swathes of IP address. The resulting chase has ballooned to nearly 19 million IP addresses at the time of writing, as tracked by unofficial RKN observer
Figure 2. Overall architecture of our approach for reconstructing transcripts of VoIP conversations from sequences of encrypted packet sizes.

Activity
MECHANISMS

- Encryption
- Message Expiry
- OS Sandboxing / Isolation
- Traffic Obfuscation
- Server Hardening
Server Hardening

Skype's China spying sparks anger

John Ruwitch, Emma Graham-Harrison

HONG KONG/BEIJING (Reuters) - Savvy Internet users in China began avoiding the version of Skype offered by its Chinese partner two years ago, but news it filtered and recorded text messages has sparked new worries about the global firm’s commitment to privacy.

The U.S.-owned Web communications firm faces a backlash at home and in China for apparently allowing core principles to be compromised in order to meet the demands of Chinese censors, analysts warned.

https://www.reuters.com/article/us-china-skype-censorship/idUSTRE49238X20081003
Server Hardening

Messing app Wire confirms $8.2M raise, responds to privacy concerns after moving holding company to the US

Ingrid Lunden, Natasha Lomas / 5:13 pm PST • November 13, 2019

Big changes are afoot for Wire, an enterprise-focused end-to-end encrypted messaging app and service that advertises itself as “the most secure collaboration platform”. In February, Wire quietly raised $8.2 million from Morpheus Ventures and others, we’ve confirmed — the first funding amount it has ever disclosed — and alongside that external financing, it moved its holding company in the same month to the US from Luxembourg, a switch that Wire’s CEO Morten Brogger described in an interview as “simple and pragmatic.”
Server Hardening

Message Metadata:

- Size
- Source
- Destination
Link-ability

To: Bob
Link-ability

https://katzenpost.mixnetworks.org/
Private Information Retrieval
### Private Information Retrieval

#### Exclusive Or

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>0</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The table illustrates the exclusive or (XOR) operation, where the result is 1 if the inputs are different, and 0 if they are the same.
Private Information Retrieval
Private Information Retrieval

- (PIR) Talek - https://github.com/privacylab/talek
- (PIS) Express - https://github.com/SabaEskandarian/Express