Towards a systematic analysis of threats and requirements for private messaging: the case of emailing and instant messaging

Dr. Iraklis Symeonidis
Post-doctoral researcher
SnT - APSIA
University of Luxembourg

Singapore
18 November 2019
Keywords

- Systematic analysis
- Threats and requirements
- Security and privacy
- Private messaging: email and instant messaging

**Aim of this presentation:**
- Stimulate discussions for feedback on our I-D
- Call for contributions
Co-authors Information

Bernie Hoeneisen
Nana Karltetter

Full time post-doctoral researcher
SnT / APSIA
University of Luxembourg

Affiliated post-doctoral researcher
imec-COSIC, KU Leuven
PRIVATE MESSAGE: EMAIL AND INSTANT MESSAGING

STILL A RELEVANT PROBLEM?
Email in numbers

The Widespread Usage of Email

In 2017, global email users amounted to **3.7 billion users** (Statista, 2018)

In 2022, this figure is set to grow to **4.3 billion users** (Statista, 2018)

That’s half of the world’s population

Credits: oberlo.com
Email in numbers

Private Email Traffic Is Declining
The estimated number of emails sent and received each day worldwide (in billions)

<table>
<thead>
<tr>
<th>Year</th>
<th>Business</th>
<th>Consumer</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>100.5</td>
<td>82.4</td>
</tr>
<tr>
<td>2014</td>
<td>108.8</td>
<td>82.6</td>
</tr>
<tr>
<td>2015</td>
<td>116.2</td>
<td>80.2</td>
</tr>
<tr>
<td>2016</td>
<td>123.9</td>
<td>77.5</td>
</tr>
<tr>
<td>2017</td>
<td>132.1</td>
<td>74.5</td>
</tr>
</tbody>
</table>

Source: The Radicati Group
Instant messaging in numbers

Facebook is Ruling The Instant Messaging Market
Communication apps with the most daily active users on Google Play Store*

- WhatsApp: 483.4m
- Facebook Messenger: 397.0m
- imo: 32.8m
- Viber: 20.9m
- Skype: 16.2m
- Truecaller: 12.8m
- UC Browser: 11.3m
- LINE: 10.3m
- WeChat: 7.7m
- Zalo: 7.3m

Facebook’s messaging apps account for 88% of the top ten’s total usage numbers

* in March 2018
Source: Prioridata

Credits: statista.com
Most popular IM app in every country (Android app store ’17)

Credits: www.similarweb.com
PRIVATE MESSAGE: EMAIL AND INSTANT MESSAGING

DO WE HAVE A SYSTEMATIC APPROACH FOR SECURITY AND PRIVACY CHALLENGES?
Security and privacy threats: running examples

- SMTP: No build in security
  - MiTM attacks were trivial
Security and privacy threats: running examples

Gmail analytics

From: unknown@gmail.com
Flight: [details]
On-time - departs in 9 hours 44 mins

<table>
<thead>
<tr>
<th>Time</th>
<th>Terminal</th>
<th>Gate</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:30 AM</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>11:40 AM</td>
<td>2</td>
<td>-</td>
</tr>
</tbody>
</table>

Passenger Information
Name: [redacted]
Confirmation #: [redacted]
Seat: [redacted]

Credits: Google

Snowden revelations 2013

PRISM Collection Details

Current Providers
- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- Skype
- YouTube
- AOL
- Apple
- [other services]

What Will You Receive in Collection (Surveillance and Stored Comm)? It varies by provider. In general:
- Email
- Chat – video, voice
- Video
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Online Social Networking details
- Special Requests

Complete list and details on PRISM web page: Go PRISMTAA

Credits: Guardian

‣ Client-server encryption

‣ Untrusted communication servers
Security and privacy threats: running examples

Synchronizing Key Server (SKS)

- Signing certificates to enhance trust

Certificate poisoning (June’19):

- **Spamming**: rogue signing legitimate certificate - an increase of the certificate size in the Key server - no upper limit in the protocol

- **Aim**: make GnuPG/Enigmail to stop working/make also certificate useless (single cert: ~150k signatures/cert. ~45Mb/cert)

- **Target**: Robert J. Hansen and Daniel Kahn Gillmor - contributors in the OpenPGP community
Security and privacy threats: running examples

Michael Hayden
General and former director NSA/CIA’14

“We kill people based on metadata”

Credits: www.youtube.com

Credits: en.wikipedia.org/

Credits: panoramix-project.eu
Information Disclosure

Why Adding Client-Side Scanning Breaks End-To-End Encryption

BY ERICA PORTNOY | NOVEMBER 1, 2019

- Scanning pictures before sending via private messaging systems
- You cannot check the DB with hashes
- Why not that apply for text?

Credits: eff.org
PRIVATE MESSAGE: EMAIL AND INSTANT MESSAGING

RELATED WORK AND OBJECTIVES?
Related work


State of the art

Secure Messaging Scorecard

<table>
<thead>
<tr>
<th></th>
<th>Encrypted in transit?</th>
<th>Encrypted so the provider can't read it?</th>
<th>Can you verify contacts' identities?</th>
<th>Are past comms secure if your keys are stolen?</th>
<th>Is the code open to independent review?</th>
<th>Is security design properly documented?</th>
<th>Has there been any recent code audit?</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIM</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>BlackBerry Messenger</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

- List of apps + security design features
- Limited categories
- Obsolete
- Only for existing apps
Aim of I-D

Aim of I-D: provide methodology/guide for
- Assessing existing systems
- Designing new private messaging systems

Dimensions/challenges:
- **Technical threats**: security and privacy by design
- **User threats**: backdoors

- As a basis for private messaging standard in a later face (good fit for IETF)
- PEARG to consider adapting this I-D as a WG item (suggestion)
I-D: objectives

- System model:
  - Entities, functionalities
- Adversarial model:
  - Adversaries / adversarial type
- Classes of threats:
  - Technological / user
- Classes of requirements

- Risk - assessment for selection of threats
  - Define risk and evaluation?
  - Primitives (crypto) to mitigate threats / minimize the risk
PRIVATE EMAILING AND INSTANT MESSAGING

THREATS AND REQUIREMENTS?
System model: Email and IM

TE: Trust establishment
ME: Message Exchange
NetND: Networking Nodes

Third Party
Identity, Key (e.g., OpenPGP) Contact Management servers

Email / IM
IM server (e.g., XMPP)
Email servers (e.g., SMTP)

Sender's
Receiver's

Sender
Receiver

Contact Management servers

Email / IM
IM server
Email servers
Adversaries and adversarial model

TE: Trust establishment
ME: Message Exchange

NetND: Networking Nodes

Email / IM

Third Party
Identity, Key (e.g., OpenPGP)
Contact Management servers

IM server (e.g., XMPP)
Email servers (e.g., SMTP)
Sender’s
Receiver’s

Sender
Receiver

Passive / active
Internal / external
Secure and privacy enhancing emailing (challenges)

<table>
<thead>
<tr>
<th>Security Threats</th>
<th>Sec. Requirements</th>
<th>Privacy Threats</th>
<th>Privacy Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>(S)poofing</td>
<td>Entity Authentication</td>
<td>(L)inkability</td>
<td>Unlinkability</td>
</tr>
<tr>
<td>(T)ampering</td>
<td>Data Authentication</td>
<td>(I)dentifiability</td>
<td>Anonymity / Pseudonymity</td>
</tr>
<tr>
<td>(R)epudiation</td>
<td>Non-Repudiation</td>
<td>Non-(R)epudiation</td>
<td>Plausible Deniability</td>
</tr>
<tr>
<td>(I)Information Disclosure</td>
<td>Confidentiality</td>
<td>(D)etectability</td>
<td>Undetectability / Unobservability</td>
</tr>
<tr>
<td>(D)enial-of-Service</td>
<td>Availability</td>
<td>Information (D)isclosure</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>(E)levation of Privilege</td>
<td>Authorisation</td>
<td>Privacy (I)nterdependence</td>
<td>Privacy Independence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Policy and Consent (N)oncompliance</td>
<td>Policy and Consent Compliance</td>
</tr>
</tbody>
</table>
Case 1: STARTTLS and untrusted servers

Identity Management servers (e.g., Pks/Certificates)

TE: Trust establishment

ME: Message Exchange

<table>
<thead>
<tr>
<th>Email servers (e.g., STARTTLS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender’s</td>
</tr>
<tr>
<td>Receiver’s</td>
</tr>
</tbody>
</table>

Email servers: passive adversaries (no confidentiality)

NetND: Networking Nodes

STARTTLS: Client-server
- confidentiality, entity + data authentication

Sender

Receiver
Case 2: S/MiME and Pk spoofing

Identity, Key servers (e.g., S/MiME)

TE: Trust establishment
ME: Message Exchange

NetND: Networking Nodes

S/MiME: End-to-end
- confidentiality, entity + data authentication, non-repudiation of origin

Key managements servers: active adversaries (MiTM - no confidentiality)
Case 2: Certificate poisoning and DoS

- **SKS**: No deletion or modification of a certificate (censorship resistant)
- **OpenPGP**: WoT - self signing certificates

**Certificate Spamming Attack:**
- Flooding a cert with bogus sign
- ~150k sign/cert ~45Mb/cert
Case 1: Non-repudation and plausible-deniability

OTR: End-to-end
- confidentiality, entity + data authentication, forward secrecy, deniability

Requirements can be conflicting
PRIVATE EMAILING AND INSTANT MESSAGING

FUTURE DIRECTIONS?
Future directions: other issues that can affect private messaging

- Usability issues:
  - Key management (e.g., OpenPGP)

Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu

J. D. Tygar
EECS and SIMS
University of California
Berkeley, CA 94720
tygar@cs.berkeley.edu

Why Johnny Still Can’t Encrypt: Evaluating the Usability of Email Encryption Software

Steve Sheng
Engineering and Public Policy
Carnegie Mellon University
shengx@cmu.edu

Levi Broderick
Electrical and Computer Engineering
Carnegie Mellon University
lpb@ece.cmu.edu

Colleen Alison Koranda
HCI Institute
Carnegie Mellon University
ckoranda@andrew.cmu.edu

Jeremy J. Hyland
Heinz School of Public Policy and Management
Carnegie Mellon University
jhyland@andrew.cmu.edu

arXiv:1510.08555v16

Why Johnny Still, Still Can’t Encrypt: Evaluating the Usability of a Modern PGP Client

Scott Ruoti, Jeff Andersen, Daniel Zappala, Kent Seamons
Brigham Young University
{ruoti, andersen} @ isrl.byu.edu, {zappala, seamons} @ cs.byu.edu

SOUPS'06
User threats: backdoors

US, UK and Australia urge Facebook to create backdoor access to encrypted messages
Julia Carrie Wong • Last modified on Fri 4 Oct 2019 02:51 BST
This article is more than 1 month old
Facebook says it opposes calls for backdoors that would ‘undermine the privacy and security of people everywhere’

Australia's Encryption-Busting Law Could Impact Global Privacy
Australia has passed a law that would require companies to weaken their encryption, a move that could reverberate globally.
Lily Hay Newman • 12.07.2018 12:45 PM
Credits: www.wired.com

Backdoors for wiretapping communications

Digital privacy of correspondence
Credits: www.theguardian.com
Future directions: post-quantum key exchange for private messaging

Post-quantum cryptography a major challenge, says expert
November 9, 2018

Post-quantum cryptography will be a major challenge for the next decade at least, according to Bart Preneel, professor of cryptography at KU Leuven University in Belgium.

Bart Preneel:
- "10 years to switch to quantum resistant cryptography"
- "Data needs to be kept confidential for 10 to 50 years,"
- "Organizations should start planning to switch now"
That's all Folks!
THANK YOU!

QUESTIONS?

iraklis.symeonidis@uni.lu

Credits: KU Leuven