The Glass Archive: Digital Security for Your Institution, and Yourself

Talking Tech
2/8/17
Ethan Gates, NYU-MIAP
and Nicole Martin, Human Rights Watch/NYU-MIAP
Personal Messaging
Mobile/Texting Apps and Calls

- SMS/cell networks
- End-to-end encryption
- Metadata
- Forward Secrecy
- Transparency
SMS/cell networks
End-to-End Encryption

- Is data encrypted in transit?
- Is data encrypted on a provider’s servers?
- If data is encrypted, does provider still have ability to decrypt it ("zero knowledge")?
Metadata

- Who did I talk to/chat/text?
- When?
- For how long?
- Subject lines?
- Read receipts?
- Geolocation?
Forward Secrecy

- Are public/session keys truly ephemeral?
- How long does service provider keep your encrypted data?
Transparency

- Is the code open-source?
- Are security measures documented, provided to the public?
- Has the code been recently audited by an independent, named security team/firm?
Let’s compare!

<table>
<thead>
<tr>
<th>Service</th>
<th>End-to-End</th>
<th>Metadata - What can others see?</th>
<th>Forward Secrecy</th>
<th>Transparency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook Messenger</td>
<td>Secret Conversations - ✔️</td>
<td>Secret Conversations - really really depends Otherwise - ❌</td>
<td>Secret Conversations - ✔️</td>
<td>😑 😑</td>
</tr>
<tr>
<td>Google Hangouts/Chat</td>
<td>❌</td>
<td>errything</td>
<td>❌</td>
<td>😑 😑</td>
</tr>
<tr>
<td>iMessage</td>
<td>✔️</td>
<td>really really depends</td>
<td>✔️</td>
<td>😊 😊</td>
</tr>
<tr>
<td>Signal</td>
<td>✔️</td>
<td>Are you using Signal? If so, when?</td>
<td>✔️</td>
<td>😍 😍 😍 😍 😍</td>
</tr>
<tr>
<td>Skype</td>
<td>❌</td>
<td>errything</td>
<td>❌</td>
<td>😑 😑</td>
</tr>
<tr>
<td>Slack</td>
<td>❌</td>
<td>errything</td>
<td>❌</td>
<td>😑 😑</td>
</tr>
<tr>
<td>Snapchat</td>
<td>❌</td>
<td>errything</td>
<td>❌</td>
<td>😑 😑</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>✔️</td>
<td>really really depends</td>
<td>✔️</td>
<td>😊 😊</td>
</tr>
</tbody>
</table>

Key:
- 😊 = well-documented security
- 😞 = unpublished independent code audits
- 😞 😞 = unpublished independent code audits
- 😍 😍 😍 😍 😍 = we have alternative facts
Web Traffic

Browsers, Networks and Tracking

- Wifi networks
- HTTPS
- Trackers
- Transparency
- Tor
Open/Public Wifi Networks
HTTPS

- Incorporates usual HTTP web communication with TSL/SSL (Transport Security Layer or older Security Socket Layer) encryption protocol
- Adds authentication via public key verification
- Public keys are trusted according to certificate authorities (GlobalSign, GoDaddy, Symantec, etc.)
Trackers

- It’s all about the 🍪 🍪 🍪

- Small pieces of text downloaded to your browser to record preferences, configuration, activity

- Can be set by “first-party” (the site you’re on) or “third-party” (advertisers, hosts of embedded information)
Common Tracker-Blocking Extensions

- AdBlock Plus
- Disconnect
- Ghostery
- Privacy Badger

- HTTPS Everywhere (not a tracker-blocker, but forces HTTPS encryption where available)

❤ = open-source
Transparency

Firefox

Chromium

QupZilla

Pale Moon
(Windows, Linux only)

Tor
Tor

[Diagram showing Tor network with entry guard, middle relay, and exit relay.]
Tor

![Tor Network Diagram](image)
Personal Data

Personal Drives, Social Media and Cloud Services

- Hard drive/solid-state encryption
- Encrypted cloud services
- Phone encryption
- Passwords, passwords, passwords
Personal Hard Drive/SSD Encryption

For Mac OS:

FileVault

For Windows:

BitLocker
Security-Focused Cloud Services

**Zero Knowledge:**

- **CertainSafe**
  (min. 100 GB for $12/month; targeted more at enterprise use)
- **Mozy**
  (zero knowledge optional, $6/month for 50 GB)
- **SpiderOakONE**
  (min. 100 GB for $5/month, up to 1 TB for $12/month)

**Some Knowledge:**

- **Boxcryptor**
  (extension for common services)
- **Carbonite**
  ($60/yr, unlimited)
- **SOS Online Backup**
  ($60/yr, unlimited)
Phone Encryption

- It’s done for you!
- …but you can make it better
Passwords

We’re all doing it wrong.
Does the XKCD method hold up?
Password Managers

- **1password**
  ($3/month, web access or stand-alone apps)

- **Encryptr**
  (free, stand-alone app only)

- **KeePass**
  (free, stand-alone app only)

- **LastPass**
  (free or premium $1/month accounts, web access/extensions only)
Email

We All Need It To Have Jobs

- End-to-end encryption services
- PGP-enabled clients
End-to-End Services

- **LavaBit**
  ($15/yr for 5 GB storage; $30/yr for 20 GB)

- **MailFence**
  (free, 200MB limited account; 2,50€/month or 7,50€/month plans)

- **ProtonMail**
  (free, 500MB limited account, based in Switzerland, premium plan available)

- **TutaNota**
  (free, 1 GB limited account; premium 1,00€/month plan)
PGP-Enabled Clients

- Postbox
- Thunderbird
- Mailvelope (webmail extension)
Lock-and-Key: Encryption Activity!
Threat Modeling
Who are you?

- Journalist
- Archivist at human rights organization
- Documentary filmmaker
- Citizen activist/protestor
- Academic or student
- Private/public employee
- Librarian
- Grassroots volunteer/organizer
- Gamer or member of other active online community
- Active social media user
- Woman, POC, and/or LGBTQ community member
What are your concerns?

- Mass state surveillance
- Doxxing
- MITM (Man-in-the-middle) attacks
- Employer surveillance
- Targeted government persecution
- Being arrested during protest/activist actions
- Data breaches from social media or storage services
- Personal or job-related systems administration
HEARTBLEED MUST BE THE WORST WEB SECURITY L A S E R EVER. WORST SO FAR. GIVE US TIME.

I MEAN, THIS BUG ISN'T JUST BROKEN ENCRYPTION. IT LETS WEBSITE VISITORS MAKE A SERVER Dispense RANDOM MEMORY CONTENTS.

IT'S NOT JUST KEYS. IT'S TRAFFIC DATA, EMAILS, PASSWORDS, EROTIC FANFICTION.

IS EVERYTHING COMPROMISED?

WELL, THE ATTACK IS LIMITED TO DATA STORED IN COMPUTER MEMORY. SO PAPER IS SAFE. AND CLAY TABLETS. OUR IMAGINATIONS, TOO. SEE, WE'LL BE FINE.

Constant vigilance!

https://xkcd.com/1353/
Recommended Reading/Resources

- Electronic Frontier Foundation: [https://www.eff.org/](https://www.eff.org/)
  - Surveillance Self-Defense project: [https://ssd.eff.org/en](https://ssd.eff.org/en)