Collective Information Security in Large-Scale Urban Protests: the Case of Hong Kong

Martin R. Albrecht, Jorge Blasco, Rikke Bjerg Jensen, Lenka Mareková
Information Security Group, Royal Holloway, University of London
USENIX Security Symposium '21
Grounding
Why Hong Kong?

• Anti-Extradition Law Amendment Bill (Anti-ELAB) protests, 2019-2020

• Highly digitalised: activities and interactions map onto digital communication

• Highly mobile: “pop-up” protests, “be water”, “flash mobs”, “blossom everywhere”¹

• Considered “innovative” in their tactics, e.g. “frontliners”

• Protest tactics imitated elsewhere, e.g. India, Zimbabwe, BLM²


Research methodology

Semi-structured Interviews
• Exploratory; depth not scale
• Interview notes

Participants and recruitment
• Gatekeepers; recruitment challenges
• 11 participants; primary or secondary protest experience

Research ethics
• Approved for self-certification (REC)
• Informed consent
• Study design to minimise the collection of PII

Data analysis
• Inductive coding; three coding cycles (Nvivo 12)

<table>
<thead>
<tr>
<th>ID</th>
<th>Experience</th>
<th>Duration</th>
<th>Medium</th>
<th>Timing</th>
</tr>
</thead>
<tbody>
<tr>
<td>P0</td>
<td>Primary</td>
<td>82 min</td>
<td>Audio</td>
<td>Dec 2019</td>
</tr>
<tr>
<td>P1</td>
<td>Primary</td>
<td>43 min</td>
<td>Audio</td>
<td>Dec 2019</td>
</tr>
<tr>
<td>P2</td>
<td>Primary</td>
<td>64 min</td>
<td>Audio</td>
<td>Feb 2020</td>
</tr>
<tr>
<td>P3</td>
<td>Primary</td>
<td>51 min</td>
<td>Video</td>
<td>Apr 2020</td>
</tr>
<tr>
<td>P4</td>
<td>Secondary</td>
<td>47 min</td>
<td>Audio</td>
<td>Apr 2020</td>
</tr>
<tr>
<td>P5</td>
<td>Secondary</td>
<td>39 min</td>
<td>Video</td>
<td>Jun 2020</td>
</tr>
<tr>
<td>P6</td>
<td>Secondary</td>
<td>62 min</td>
<td>Video</td>
<td>Jun 2020</td>
</tr>
<tr>
<td>P7</td>
<td>Primary</td>
<td>73 min</td>
<td>Audio</td>
<td>Jun 2020</td>
</tr>
<tr>
<td>P8</td>
<td>Secondary</td>
<td>53 min</td>
<td>Video</td>
<td>Jun 2020</td>
</tr>
<tr>
<td>P9</td>
<td>Primary</td>
<td>87 min</td>
<td>Audio</td>
<td>Jun 2020</td>
</tr>
<tr>
<td>P10</td>
<td>Primary</td>
<td>46 min</td>
<td>Audio</td>
<td>Jul 2020</td>
</tr>
</tbody>
</table>
Research Findings
Protest tools

Telegram: “most security”
• Ability to form large and small groups

WhatsApp: “most protesters use WhatsApp too”
• Ability to form close-knit affinity groups

Signal: “you cannot tell people to use Signal”
• Barrier to adoption: phone numbers

“…We have a group on WhatsApp and another one on Telegram, but we use the one on Telegram to talk about our actions [. . .], because we think Telegram is more secure.”

(P9)
Social Organisation

Group types
- Large groups: for organisation, information sharing, collective decision-making, anonymity (infiltration)
- Small affinity groups: for “frontline” trust relations, confidentiality
- Differing security notions depending on group type

Onboarding strategies for affinity groups
- Meet face-to-face during the protests “before moving the connection online” (P4).
- New group members accepted based on group decisions.

“We have another group with a different number which is attached to a different SIM card and completely isolated from the usual groups.” (P2)

“Seeing each other and standing on the front line together is very important for trust.” (P10)
Social Organisation

Collective decision-making
- Real-time voting on “where to go next”
- Security in numbers and tactical buy in from group members
- Group admins as the ‘anonymous leaders’ of the protests

“I only started to use Telegram during these protests. I didn’t use it before. I heard that Telegram is used by terrorists, because it is so secure. And it is used by my group […] I had to conform to be in the group.” (P1)

“The groups have many admins to spread the risk [for the group] to more than one person if one admin is compromised.” (P9)
Indicators of compromise

Monitoring practices (detecting arrest)
- Specific monitoring apps
- Scheduled messages
- Regular messages

Post-compromise practices
- Managing group messages: remote message deletion when a group member is (assumed) arrested
- Managing group membership: remote removal of group members who are (assumed) arrested

“There are some signals that tell me that the person got arrested. For instance on the live location, if they disappear from the map then I know something is wrong [. . .] if I know they have battery and suddenly disappear then I can call them. If no-one picks up the phone for a long time and we can’t find them in the field, then we will track their last location. And then we know whether they have been arrested.” (P1)
Discussion
Collective information security

Collectivity

- Usable security studies generally consider individual users, rather than groups of users. Our work suggests that:

  - Information security in protests rests on collective practices, to fulfil group security needs
  - Information security is negotiated between group members, while security practices are shared between groups

Diversity of social contexts

- Grounding security needs and practices in their specific social settings
- Different higher-risk groups experience distinct security needs
- Moving beyond interview studies to establish actual information security needs of higher-risk groups

---

Designing for protesters’ security needs

- Telegram's bespoke MTProto protocol, beyond secret one-to-one chats, suggests itself as a pressing target for cryptanalysis
- Reliance on trusted third parties (e.g. group administrators as connective leaders)
- Participants’ notions of forward secrecy and post-compromise security do not map onto those used in the cryptographic literature (and vice versa)

Design goals for secure messaging

- Support for both (small) private (confidentiality) and (large) public groups (anonymity)
- Avoid personally identifiable information (e.g. phone numbers)
- Ability for group administrators to control group membership and messages

Broader design goals

- Ability to share live locations securely

Study limitations
Thank you.

A special thank you to all research participants and gatekeepers, without whom this work would not have been possible.