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

Martin R. Albrecht, Jorge Blasco, **Rikke Bjerg Jensen,** Lenka Mareková

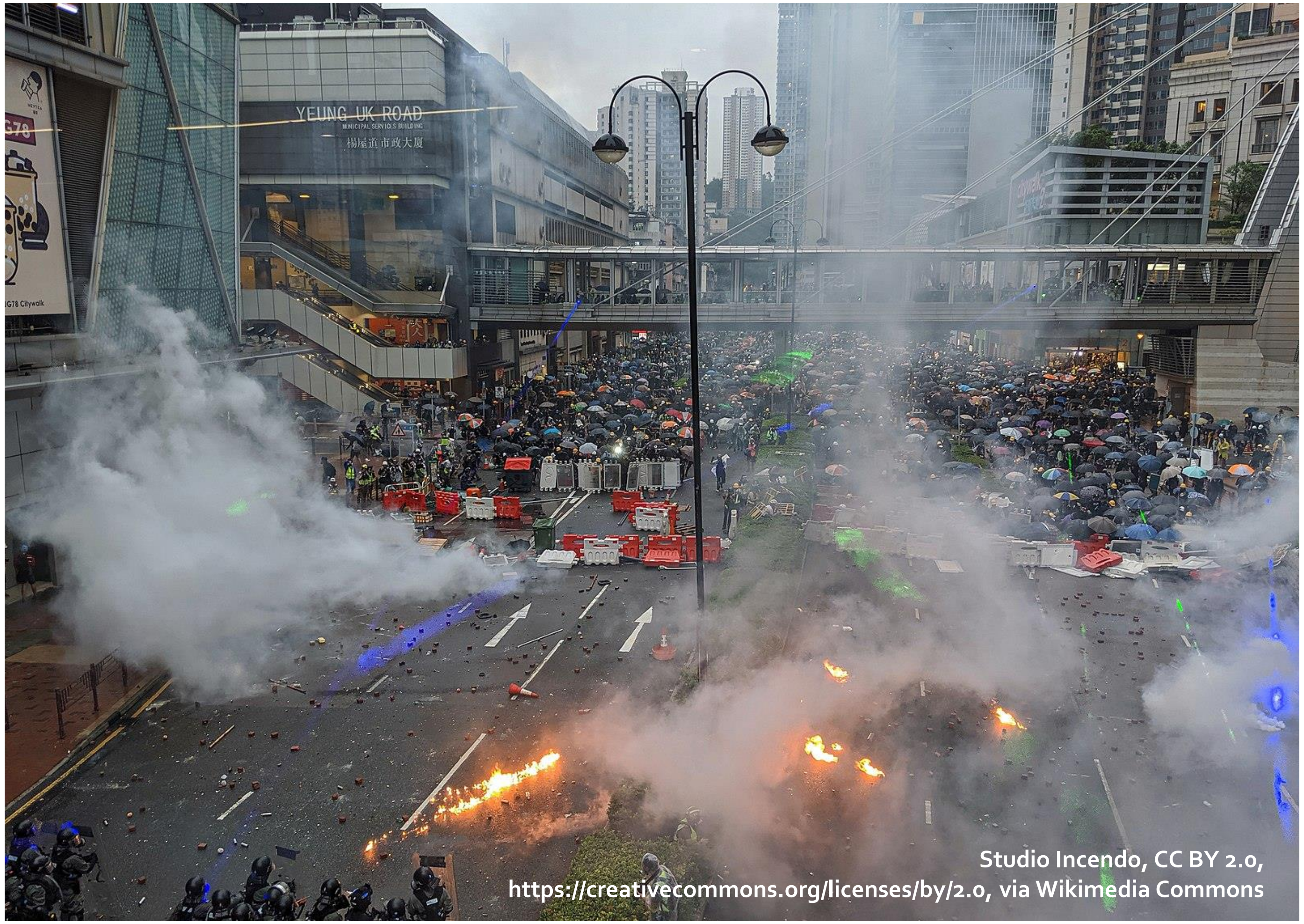
Information Security Group, Royal Holloway, University of London

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, BLM[2]



Studio Incendo, CC BY 2.0, https://creativecommons.org/licenses/by/2.0, via Wikimedia Commons

[1] H. Holbig. "Be Water, My Friend: Hong Kong's 2019 Anti-Extradition Protests." *International Journal of Sociology* 50.4 (2020): 325-337. E. Hale. "Hong Kong protesters use new flashmob strategy to avoid arrest". *The Guardian.* 13 Oct 2019.

[2] Chuang. "Welcome to the Frontlines: Beyond Violence and Nonviolence." 8 Jun 2020. Available at: https://chuangcn.org/2020/06/frontlines/ (accessed 24 Jun 2021)

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)

Participants			**Interviews**	
ID	*Experience*	*Duration*	*Medium*	*Timing*
P0	Primary	82 min	Audio	Dec 2019
P1	Primary	43 min	Audio	Dec 2019
P2	Primary	64 min	Audio	Feb 2020
P3	Primary	51 min	Video	Apr 2020
P4	Secondary	47 min	Audio	Apr 2020
P5	Secondary	39 min	Video	Jun 2020
P6	Secondary	62 min	Video	Jun 2020
P7	Primary	73 min	Audio	Jun 2020
P8	Secondary	53 min	Video	Jun 2020
P9	Primary	87 min	Audio	Jun 2020
P10	Primary	46 min	Audio	Jul 2020

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

Appropriation of consumer apps

> *“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[4]

<u>Our work suggests that</u>:

- 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

[4] E.g. R. Abu-Salma et al. "The security blanket of the chat world: An analytic evaluation and a user study of telegram." Internet Society, 2017. R. Abu-Salma et al. "Obstacles to the adoption of secure communication tools." *2017 IEEE S&P,* 2017. E. Vaziripour et al. "Action needed! helping users find and complete the authentication ceremony in signal." *SOUPS, 2018.*

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.