CryptoParty London 19 June 2018

First Contact Problem. Tips for setting up meetings with confidential sources, without leaving an electronic data trail.

CryptoParty London
19 June 2018
https://cryptoparty.in/london
@SpyBlog

First Contact Problem

- Highly resourced investigators or those with direct personal access to you, may be able to track back and identify your previous contacts, once their suspicions have been aroused about you, or any of the other participants, in a private / secret meeting.

First Contact Problem

- Most online tools and services provide oodles of metadata, location data, log files, financial records etc, even those that are End to End strongly Encrypted
  - https://mascherari.press/the-first-contact-problem-getting-to-securedrop/
  - https://twitter.com/normative/status/1005103155531657216

First Contact Problem

Julian Sanchez @normative · Jun 8

That doesn't just mean "Use Signal" (though that's a good start). It means anticipating the compromise of an endpoint device, not retaining messages longer than necessary for the story, and setting your own messages to disappear in the event your source's device is seized.

3 10 93

Julian Sanchez @normative · Jun 8

It means making encrypted messaging a default. A journo friend once proudly told me he'd started using Signal, but "only for sensitive conversations." I had to break it to him that this wasn't a whole lot better than plaintext for leak investigations.

2 13 66

Julian Sanchez @normative · Jun 8

If secure comms isn't your default, and suddenly you tell a source it's time to switch to Signal right around the time you're reporting a story based on their sensitive information, how exactly do you think that looks to an investigator?

1 21 85

First Contact Problem

Julian Sanchez @normative · Jun 8

It also means thinking about metadata. Encrypting content isn't enough if investigators have a clear data trail that shows you talking to one of the small number of people with access to the information you're reporting.

2 16 66

Julian Sanchez @normative · Jun 8

Most critically, this is an ethical obligation at the INSTITUTIONAL level. It is not the source's job to be Ed Snowden. But it's also ridiculous to assume a bunch of 25 year old reporters can figure out secure comms on their own because they're "tech savvy" about social media.

2 32 129

Julian Sanchez @normative · Jun 8

That's like assuming the teenage kid next door can program in assembly language because he's really good at Overwatch. Reporters should not be left to figure this crap out on their own, and it shouldn't be something they start thinking about only when they get a sensitive source.

3 12 84

First Contact Problem

Julian Sanchez @normative · Jun 8

If a reporter is communicating with a source who wants to convey sensitive information, and at that point the reporter starts wondering "OK, how do we do secure comms?" congratulations, you've already fucked it up.

2 19 82

Julian Sanchez @normative · Jun 8

Also this! Do not assume your internal comms are sacrosanct! All your fancy cloak and dagger isn't worth a damn if you're blabbing to your editor in a logged Slack chat about what you're reporting.

> **Dave Maass** 🗞️ **@ #IRE18** @maassive
> I'd add that the focus shouldn't be limited to communications between reporters and sources, but also between reporters and editors.

2 19 78

Julian Sanchez @normative · Jun 8

Not mentioning your source's name isn't good enough if you leave enough info for investigators to piece together a timeline in combination with other data. Did you say where you met? They can check cell logs and see that your source was there.

1 8 41

First Contact Problem

Julian Sanchez @normative · Jun 8

Good reporters need to attack their own process. You're a dedicated investigator with subpoena power. How do you backtrack to identify your source? Think hard about this, often. Then close off those paths.

1 20 77

Julian Sanchez @normative · Jun 8

This last one is maybe the most critical thing that conscientious reporters who are trying to do secure comms don't do enough. You need to take an attacker perspective constantly. Ask "how do I break this?" until you come up empty.

3 11 65

Julian Sanchez @normative · Jun 8

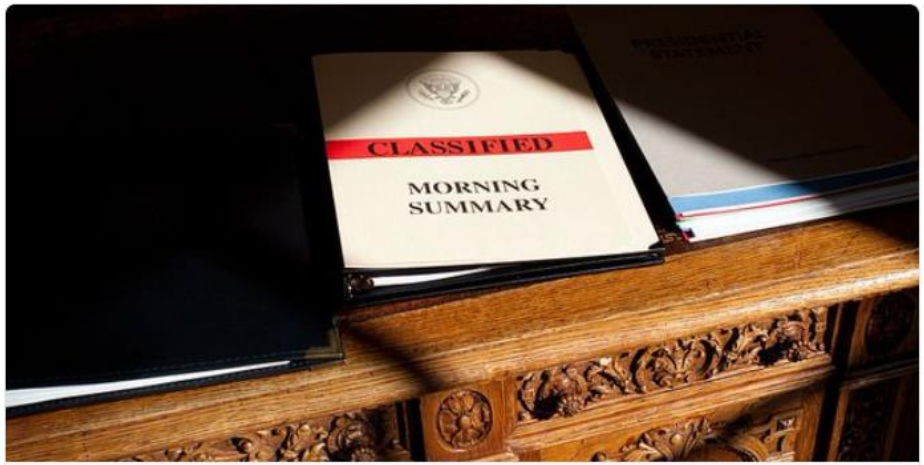
That means, incidentally, that the reporter — or, better, the person in charge of security training, which every news organization should be doing regularly — needs to know enough about the investigative process to think like the attacker & identify the common attack surfaces.

3 12 64

First Contact Problem

Julian Sanchez @normative · Jun 8

You have a SecureDrop portal to enable sources to reach out anonymously? Great. Is it on its own subdomain? Whoops, that's going to show up in your source's DNS log.



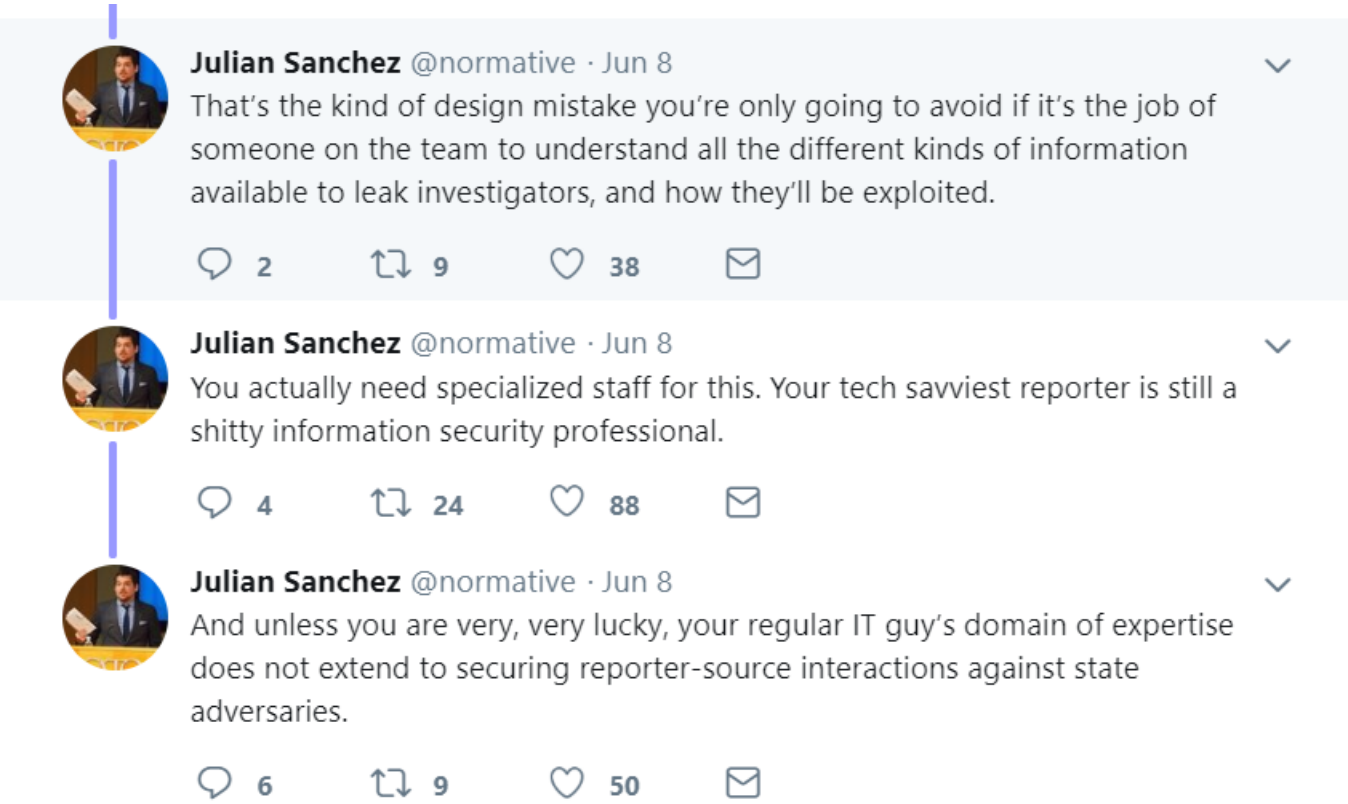
The First Contact Problem: Getting to SecureDrop

When a source wants to leak information, they must first become aware of their options & take steps to protect their operational security. However th...

mascherari.press

2 28 68

First Contact Problem



First Contact Problem

- There is no ideal solution to this, but here are a few tips
- Would appreciate your experiences and feedback,

Meeting types

- How many participants ?
  - One on one,
  - One to Many
  - Many to Many ?
- Do you know the other participant(s) by sight ?

What sort of participants ?

- State - known faces embassy based spies trying to meet contacts in Moscow etc. e.g. Ryan Foley
- State - illegal undeclared non-diplomatic cover meeting a contact or servicing a deaddrop
- Couriers with **pizzini** written notes from imprisoned on the run mafia dons
  - https://en.wikipedia.org/wiki/Pizzino
- Journalists trying to meet confidential sources or whistleblowers
- Lovers in illicit affair or with disapproving family or parents
- Celebrities avoiding paparazzi and investigative journalists and private detectives

What sort of participants ?

- Customers meeting their drug dealers
- Punters and sex workers
- Political activists meeting co-campaigners or co-conspirators
- Mergers and Acquisitions teams about to launch a company takeover or sale with financial market implications

Threat Models

- real time threats- physical surveillance teams
- real time & afterwards log files – CCTV
- taxi drivers, shopkeepers, restaurant staff etc. = witnesses - #Hunted rude people / bad tippers / extra generous tippers are remembered
- after the meeting forensic evidence e.g. google maps tile images on phone or computer, messages on a phone etc.

Hostile actors

- Counter Intelligence Agencies e.g. MI5 Security Service & @GCHQ
- Anti Terrorism Police @metpliceuk
- Serious Organised Crime police
- Political Police – “domestic extremism” #spycops
- Private Sector Corporate spies – often ex employees of above categories

Hostile Actors

- Market Speculators and Commercial Rivals
- Rival political parties or campaigns (external)
- Rival factions within your own party / campaign (leadership challenge ?)
- Jealousy & control freaks – current partners, disapproving parents
- Jealousy and control freaks – ex partners now stalkers
- Hackers for the lulz, because they can

Compartments

- Do not store the contact details and meeting locations of one confidential contact on a shared device with that of other contacts.
- Use separate burner devices, different encrypted containers with different pass phrases
- Hopefully an investigation of one source or contact will not also compromise your other sources or contacts

Signals to meet, safe, abort

- Spy Tradecraft - open / closed curtains, presence or absence of chalk marks etc. on a non suspicious regular route e.g walking the dog, going to the local shops
- Social Media, but is it anonymous or private ?

Signals to meet, safe, abort

- Encrypted Messengers e.g. **Signal** rather than Email but remember to set Disappearing Messages
- N.B. lots of Security Updates this month !
- **Get the latest versions of Signal Messenger, (iOS, Android and Desktop), GnupG, Enigmail, Tor Browser and Tails !**

Signals to meet, safe, abort

- Duress Codes – N.B. the absence of something can itself be a failsafe signal (but they have often failed in the past)
- https://en.wikipedia.org/wiki/Duress_code
- Canary tokens & Warrant Canaries

Finding the meeting location address

- Google Maps
  - Access via **Tor**
  - ideally via Tails else clear browser caches & run secure delete e.g. Eraser
- TomTom style in car GPS navigation
  - Route info log file forensics
- Don’t search for or program your home / work location or the exact location of the meeting, only to a nearby landmark e.g. travel stop or pub

Finding the meeting location address

- Only use a disposable **burner smartphone** if you are using Google Maps etc.
- Don’t switch on the burner smartphone anywhere near home / work location
- Use a paper map or A-Z of London etc. but do **not** mark the meeting location with an X !

Travel to / from the meeting

- Ideally use public transport . Pay cash. No Uber !
- If driving or via taxi, don’t drive exactly to the meeting location, walk the last few blocks
- In London use a paper Zone 6 travel card even if you are only travelling in Zones 1 and 2
- Prepaid **swapped** unregistered Oyster Card on buses
- Don’t be rude or otherwise memorable to anyone to and from the meeting
- Try to avoid CCTV (very hard) – a hat or cap with a brim, may hide your face from above some of the time

Mobile Phones

- Do you take your normal smart phone to the meeting or not ?
- Leave it switched on, but locked at home / office , plausibly charging
  - metadata implies you are still there i.e. not tracking you to the meeting
  - But is it safe from Evil Maid or other tampering ?
- Turn off WiFi and BlueTooth and NFC

Mobile Phones

- If you do take your normal phone, switch it off and remove the battery
- If the battery is sealed e.g. Apple iPhone
  - switch it off
  - Put it in a Faraday Cage bag or wrap it with multiple layers of cheap aluminium foil to block signals

Mobile Phones

- If you do take a burner SmartPhone (or Tablet or Laptop Computer) to the meeting
  - Tape over the camera(s)
  - **Mic-Lock** audio plug to disable the microphones – more against ambient noise detection and built in Google Voice Search etc. than speech quality malware bugging

Mobile Phones

- https://mic-lock.com/

Meeting Agenda, Notes,

- One group of terrorist plotters in UK, suspecting, correctly, that they were under surveillance, alternately typed their comments and replies silently into a Microsoft Word Document on a laptop computer.
- They forgot about Microsoft Word backup files and these “chats” were forensically recovered after they were arrested

Meeting Agenda, Notes,

- #Hunted fugitives Mella and Sandra were tracked to Scotland, when one of their relatives was “searched” and had a note of the their phone number and location in his pocket litter.
- Destroy e.g. burn any paper notes taken before or during a meeting

Meeting Agenda, Notes,

- N.B. impressions on paper underneath the top sheet of the note itself often recoverable via the old soft lead pencil over the impressions or by graphite powder and electrostatic charge in a forensics lab (ESDA) or iodine vapour deposit technique – highlights disturbed paper fibres
- Use soft felt tip pen rather than hard ballpoint pen or pencil, single sheet on hard glass or plastic surface
- N.B. bleed through of the felt tip pen ink and / or solvent through to the next page. This was used as a secret ink method of communication by MI6 - Berol fibre tipped pen and a chemical developer

Covert Recording of Meetings

- Political opponents or investigative journalists may use covert recording devices, mobile phone apps or hidden CCTV cameras to gather embarrassing evidence of your secret meeting in a sting operation
- Don’t be shy about showing that you switched off your phone and have nothing hidden in your bag and ask to see theirs, if you are meeting dodgy people for the first (or second) time.

Surveillance Detection

- If you have been followed by a human surveillance team, they may be in earshot / video range of your private meeting
- If in a café or restaurant, suddenly get up as if to pay the bill, but go to the toilet instead and see if anyone else suddenly jumps up to follow
- Check for familiar looking faces at different locations on your route to / from the meeting
- Do a Bluetooth scan for familiar devices names / MAC address e.g. earpeices appearing at different locations
  - Using e.g. an Android Bluetooth scanning App
  - https://play.google.com/store/apps/details?id=com.bluemotionlabs.bluescan&hl=en_GB
- Read "The Surveillance Zone" by Ami Toben
  - https://twitter.com/amitoben/status/871706640625659907

Many to Many Meeting

- Use a **GPG digital signature** on a call for a private meeting or rally or demonstration.
- Reduces the risk of Authorities or rival factions or campaigns sending out spoofed meeting invitations (happened in Egypt anti government demos)

Many to Many Meeting

- Avoid Eventbrite or other online convenience tools (ticket bar codes, attendee list, maps) etc.
- Probably ok for public events with more than 100 people expected to attend, as there will be informers / Covert Human Intelligence Agents if targeted.
- Early UK Cryptoparty London notes re Fire Safety number of attendees

Expenses & Travel Receipts

- If you are claiming back meeting expenses from your employer, you may have to be creative with the expenses claim form accounting to protect your sources
- Pay cash not with a credit card, debit card, contactless mobile phone payment etc.
- In London use a paper Travel Card or a swapped prepaid Oyster travel card
- Destroy paper tickets & receipts after the meeting

Moscow Rules

- Moscow Rules – rightly paranoid spy tradecraft in heavily surveilled Cold War Moscow (or now London)
  - https://en.wikipedia.org/wiki/The_Moscow_rules

Moscow Rules

- Assume nothing.
- Never go against your gut.
- Everyone is potentially under opposition control.
- Do not look back; you are never completely alone.
- Go with the flow, blend in.
- Vary your pattern and stay within your cover.
- Lull them into a sense of complacency.
- Do not harass the opposition.
- Pick the time and place for action.
- Keep your options open.

Moscow Rules

- Ryan Fogle
- https://p10.secure.hostingprod.com/@spyblog.org.uk/ssl/spyblog/2013/05/15/ryan-fogle-alleged-us-spy-in-moscow---unprofessional-tradecraft.html

Moscow Rules

Questions ?

Anonymity SwapShop

- Also the regular Anonymity SwapShop - bring along spare social media accounts, SIM Cards, Oyster Cards, burner phones etc. to swap or barter with other people, so as to muddy your data trails.

- See me afterwards