Crypto War 3 – from the DMA to Chatcontrol

Ross Anderson

Professor of Security Engineering

Cambridge and Edinburgh Universities

The Crypto Wars

- The intelligence and law-enforcement agencies have tried hard to retain information dominance:
  - Till 1993: cold-war export controls on civilian cryptography, except for devices like ATMs
  - 1993–2000: demanding access to keys (from the “Clipper” chip through CA licensing)
  - 2001–2015: demanding access to servers (“Prism”)
  - 2015–? : demanding access to devices (since people went for end-to-end encrypted messaging)
- Many themes run through the whole opera!

Academic response

- “Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications” (2015)
  - Exceptional access to all data would cause grave damage, and undermine modern security
- “Bugs in Our Pockets: The Risks of Client-side Scanning” (2021)
  - Apple proposal to scan your camera roll would be vulnerable to exploitation by the bad guys but would open the door to mass surveillance of the rest of us

Key policy issue for the EU

- Should the EU make chat and images on phones easier for law enforcement to scan, as proposed by Commissioner Johannson in the Child Sexual Abuse Regulation?
- Or should it stand up for security instead?
- Laws with similar clauses are being proposed elsewhere, e.g. Britain's Online Safety Bill
- A worldwide policy initiative coordinated by security agencies against E2EE apps...

A second front?

- The Digital Markets Act came into force Nov 2022
- Article 7 requires “gatekeeper” platforms to allow smaller platforms to interoperate, and by Mar 2024
- Article 7 was lobbied for by element.io which sells messaging systems based on Matrix to the agencies
- Possible product: interop with WhatsApp for banks who need / want to wiretap staff for compliance
- Stated goals: improve UX, cut network effects
- A similar act is stalled in the US Congress...

Implementation options

- Three paths are being discussed:
  - A common protocol (Signal variants are widely deployed; Matrix; MLS is being standardized)
  - A server-side gateway (like iMessage and SMS)
  - A client-side bridge
- Common protocols, like SMTP, fossilize – see Moxie Marlinspike's talk at CCC19
- The Mar 2024 deadline favours client-side bridging
- A server-side gateway would be hard (Facebook/ WhatsApp!) and also break end-to-end encryption

Client-side bridging

- Case 1: the client bridge is a corporate gateway
- "Dan Smith Lloyds" <+441234567890@whatsapp> is now "Dan Smith Lloyds" <dan.smith@mb.Lloyds@whatsapp>
- The gateway acts as Lloyds' compliance middlebox and logs all traffic for banking regulators
- mb.Lloyds might also be a message server, or there could be a separate Matrix server
- For corporate users, WhatsApp via Matrix now works rather like smtp email

Client-side bridging (2)

- Case 2: what about non-corporate users?
- Example: our family group uses whatsapp but our open-source friend Fabien refuses to
- If I add him as fabien@(anderson@whatsapp) will he see that our traffic is breaking his rule?
- Will the regular WhatsApp client contain code or an interface for Matrix, Telegram, Signal, Threema ... ?
- E2EE apps already a huge target; discoverable, with lots of exploit-friendly interfaces (see Pegasus exploits of WhatsApp, iMessage etc)

Naming

- How will users be identified? name@domain, or (phone#$_A$@service$_B$) at some corporate or personal gateway (phone#$_C$@service$_D$)?
- Threema uses a random ID, not phone$_E$#@threema
- Some identities change whenever you reinstall!
- How will users be discovered?
- Some users don’t want global discovery as they separate home from work, so must be opt-in
- If “only contacts of my former IDs”, too complex?

Spam and abuse

- How will services detect / block spam and abuse? WhatsApp currently uses lots of metadata
- Do you just kill a whole client gateway? If you receive some CSAM, and report it to a US tech company, they have to report to NCMEC and suspend the sender account
- Malicious CSAM has been used for years to harass journalists
- Now a DoS attack on Goldman, anyone?

The Trust Boundary

- It was bad enough when messengers expanded from phones to ancilliary desktops
- E.g. in Signal, transient desktop access can give long-term access to ratchet keys
- How many people are involved in providing key material, developing software, and blocking stuff?
- How usable will the interfaces be, for users / devs?
- DMA says maintain ‘level of security’. But policy clashes: is anonymity good or bad? Scanning?

Trusting other services

- So: will a big service be able to block connection from a small service that has anonymous users?
- If so, do we see a creeping ‘real names’ policy – perhaps leading to eIDAS / identity escrow?
- If you can’t trust the directory of a small service, can you do key transparency? You need context to tell genuine key changes from adversarial ones
- What about adversarial interop, for example by Russia against Ukraine? They already steal SMSes at scale to do account takeover (Signal, WhatsApp)

And interop’s promised benefit?

- Interop was sold to MEPs as cutting network effects
- But just look at iMessage and SMS...
- If there’s one SMS user in an iMessage group, the group bubble turns from blue to green
- This puts real pressure on youngsters to abandon Android and buy an iPhone!
- Some say: forbid such signalling by tech companies
- But then, how do I know my signal group is secure, and how does Fab know he’s not using WhatsApp?

The agencies on CSA

- “Thoughts on child safety on commodity platforms” by Ian Levy and Crispin Robinson has the agencies’ case, and is cited by Commissioner Johansson
- It proposes mechanisms like PhotoDNA to discover known illegal images (but: a list of illegal image thumbnails can’t be entrusted to devices)
- Plus ML mechanisms for detecting child nudity (but: Google false alarms on medical images)
- And NLP mechanisms to scan text before encryption / after decryption for “grooming”

Violent crime against children

- Worldwide, about 100,000 child homicides a year
- The typical perpetrator is the mother’s partner
- This is just the tip of a large iceberg of abuse, most of which is simple neglect
- Associated with multiple deprivation: poverty, slums, unstable families, alcohol/drug use, gangs...
- Richer countries have less (e.g. UK has 180-200 pa)
- Patterns of child sex abuse are not hugely different

Crimes of sexual violence against children

- Most abuse is in the family; with multiple offenders the primary abuser is very likely in the family
- Other offenders tend to be locals in a position of trust – priests, teachers, policemen, doctors...
- Tech used for surveillance and control of victims
- Revenge porn (nonconsensual intimate images)
- Offences initiated online: primarily sextortion, with minors tricked into sending images to predators
- Also, streaming video from countries like Mexico

Inhope’s indecent image pipeline

- Images found by user reporting, sent to NCMEC, which collates using PhotoDNA (image thumbnails)
- Some server-based systems (e.g. Facebook, Gmail, Hotmai) have been scanning images for years now
- About 30m hits/year to NCMEC (mostly from FB)
- 100,000 / year sent to UK police; several thousand arrests and several hundred prosecutions
- Indecent image offences peaked in 2016
- Police view now: prioritise primary offences instead

Sexting, sextortion, revenge porn

- About a third of teens flirt by sending naked images
- Under-18s are committing a crime in USA; US tech firms must report to NCMEC even if legal age locally
- Real problem: when Alice and Bob fall out, Bob may put Alice’s images online or threaten to
- About 15% of kids report some sexual victimisation
- Strict criminal liability means teachers have great difficulty dealing with sexualized bullying; there can be rapid escalation and severe side effects
- Also makes it harder to spot the serious cases

The feminist scholars’ viewpoint

- Many crimes of violence against children are linked with violence against women
- Revenge porn against women over 18 is largely ignored by tech majors and police agencies
- Growing body of scholarship links misogyny with crimes of political violence too
- The great majority of terrorists committed crimes of violence against women first
- The dangerous guy in the mosque isn’t the man who downloaded a US field army manual, but the man who beat up his sister. Local knowledge is key!

Could text scanning help?

- Our experience looking for hate speech in large corpora suggests NLP will have 5% false alarm rate
- EC said 10%, and said that with 1,000,000 grooming messages they'd cope with 100,000 false alarms
- But their arithmetic was wrong – it would be 10% of 10,000,000,000 messages per day in the EU
- Europe's 1.6 million police officers would have to check 625 messages per day each
- Or: would we be able to refine each search progressively, like with a web search?

The whole architecture's wrong

- First, subsidiarity! Measures to improve child protection must support local police, social workers, teachers and parents – not create a new central agency like Europol
- Second, learn from past mistakes! Mass surveillance doesn't help local police – see statistics around data retention directive, Sweden vs Germany vs Switzerland, 2008–10 +
- Third, human rights! Bulk intercept without warrant or suspicion has been found contrary to privacy rights by the Strasbourg and Luxemburg courts

Policy lessons

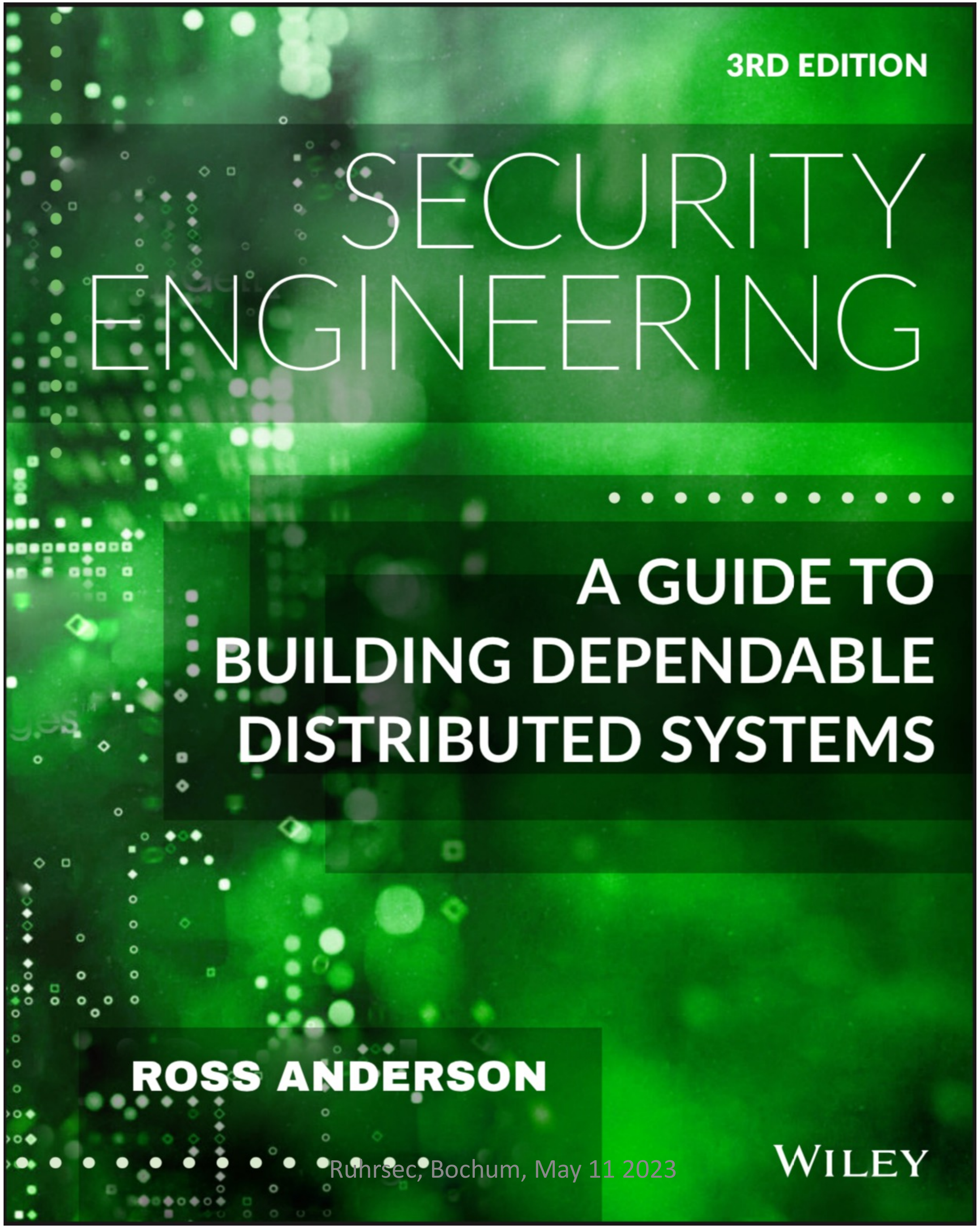
- The agencies’ claim “Large-scale growing harm is initiated online and is preventable by client scanning” is not supported by the evidence
- Crimes of sexual violence against children are real – but effective prevention means fighting poverty, more child social workers, and more police effort on family violence
- The one useful tech policy reform is better reporting, as mandated by the EU Digital Services Act. Neither interop, nor the CSA Regulation, helps

Research opportunities

- Messaging interop
- Measuring online crime and harm – the Cambridge Cybercrime Centre has lots of data for you...
- Tech-facilitated intimate partner abuse; how can we make it harder?
- What new things will come along with AI / ML?
- ....

More…

- “One Protocol to Rule them All”, arxiv:2303.14178
- “Chat Control or Child Protection”, arxiv:2210.08958
- “Bugs in our Pockets: the Risks of Client-Side Scanning”, arxiv:2110.07450
- See https://www.ross-anderson.com
- See also https://www.edri.org



3RD EDITION

SECURITY ENGINEERING

A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS

ROSS ANDERSON

WILEY