University of BRISTOL

Threat Models over Space and Time:

A Case Study of E2EE Messaging Applications

Partha Das Chowdhury [1], Maria Sameen [1], Jenny Blessing [2], Nicholas Boucher [2], Joseph Gardiner [1], Tom Burrows [2], Ross Anderson [1,3], and Awais Rashid [1]

[1]University of Bristol, [2]University of Cambridge, [3]University of Edinburgh

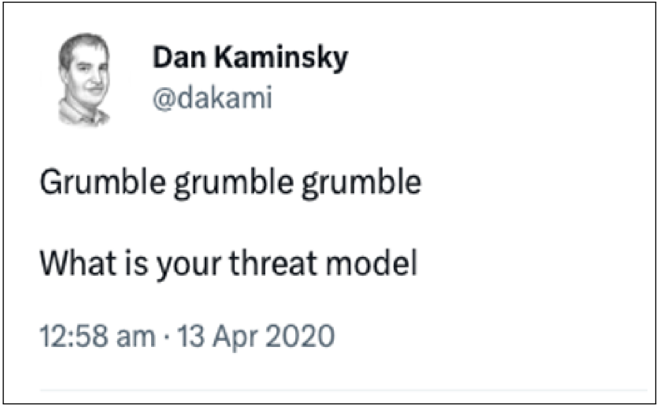
July 3, 2023

bristol.ac.uk

The Space of E2EE Communications

- There are many entities that have an interest in an instance of a communication
- They should be legitimate and indiscernible

> “Authentication is knowing where something came from, and confidentiality is knowing where it went to”
>
> *Butler Lampson*



Dan Kaminsky
@dakami

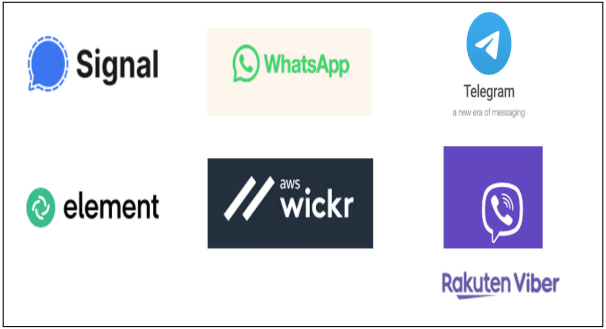
Grumble grumble grumble

What is your threat model

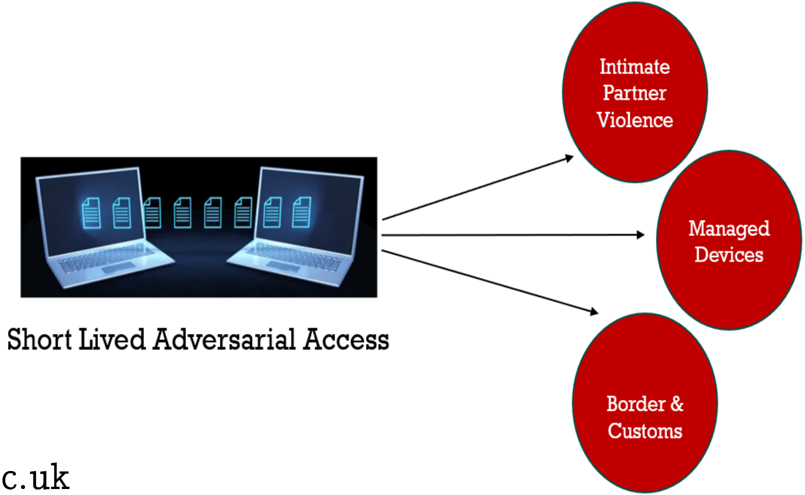
12:58 am · 13 Apr 2020

Do we do threat modelling little & often?

Desktop clients of 6 E2EE messaging applications



What is our threat model?

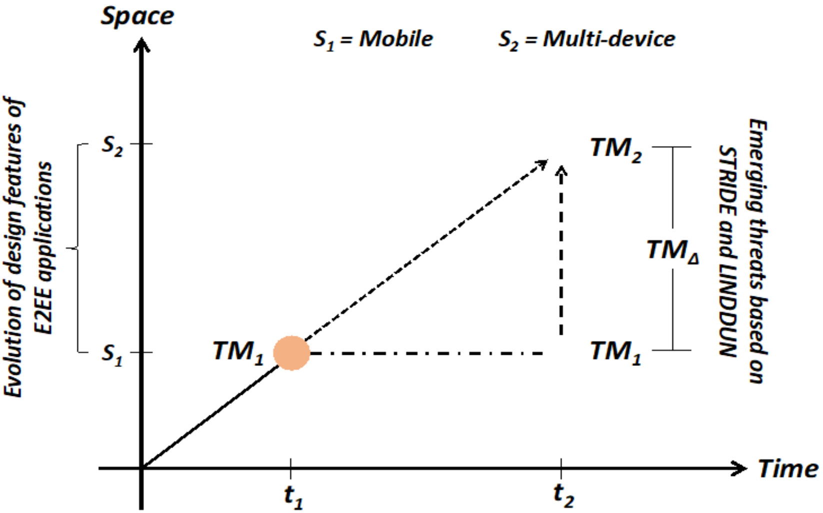


Short Lived Adversarial Access

Intimate Partner Violence

Managed Devices

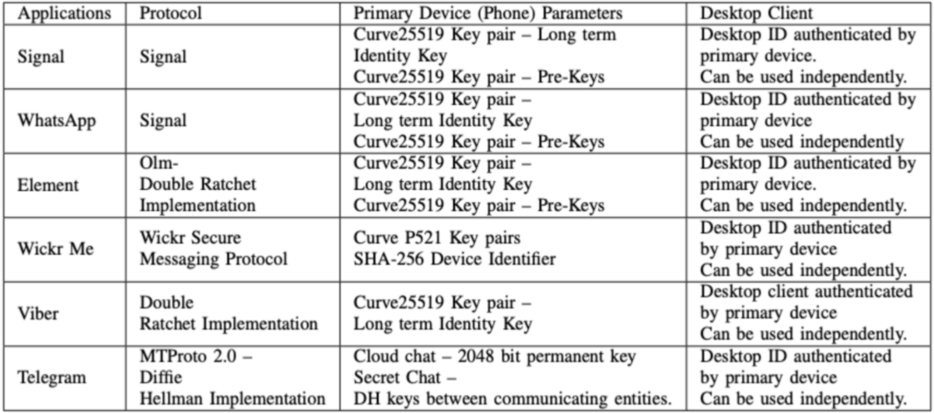
Border & Customs


Space
S1 = Mobile
S2 = Multi-device
Evolution of design features of E2EE applications
S2
S1
TM1
TM2
TMΔ
TM1
Emerging threats based on STRIDE and LINDDUN
t1
t2
Time

Background – E2EE Messaging App

- The identity key (IK) pair is the root of trust for every account in a mobile device
- Short lived keys are used for communication between entities in a communication
- The short-lived keys are signed by IK and communicated to the server
- The assumption is that apart from the legitimate owner no one else can prove possession of IK

Background – E2EE Messaging App



Applications	Protocol	Primary Device (Phone) Parameters	Desktop Client
Signal	Signal	Curve25519 Key pair – Long term Identity Key Curve25519 Key pair – Pre-Keys	Desktop ID authenticated by primary device. Can be used independently.
WhatsApp	Signal	Curve25519 Key pair – Long term Identity Key Curve25519 Key pair – Pre-Keys	Desktop ID authenticated by primary device Can be used independently
Element	Olm- Double Ratchet Implementation	Curve25519 Key pair – Long term Identity Key Curve25519 Key pair – Pre-Keys	Desktop ID authenticated by primary device. Can be used independently.
Wickr Me	Wickr Secure Messaging Protocol	Curve P521 Key pairs SHA-256 Device Identifier	Desktop ID authenticated by primary device Can be used independently.
Viber	Double Ratchet Implementation	Curve25519 Key pair – Long term Identity Key	Desktop client authenticated by primary device Can be used independently.
Telegram	MTProto 2.0 – Diffie Hellman Implementation	Cloud chat – 2048 bit permanent key Secret Chat – DH keys between communicating entities.	Desktop ID authenticated by primary device Can be used independently.

TABLE I: Properties of Popular Messaging Applications

Background – E2EE Messaging App Desktop Clients

- A standard installation of the desktop client of the mobile app
- The desktop clients generates its own root key pair
- The primary device tells the server that it is a valid desktop client
- Messaging applications are ‘uncomfortably’ silent on end point security
- They assume ratchet mechanisms will preserve forward and backward secrecy in case of breaches

Experiments

Alice

Moriarty

- Alice has a standard installation of the desktop client
- She configures the desktop client using her primary device
- Moriarty performs a standard installation of the desktop client
- He copies the state as in \library\application support\<> from Alice's machine to his own machine

Related Work

- Cremers, C., Fairoze, J., Kiesl, B. and Naska, A., 2020, October. Clone detection in secure messaging: improving post-compromise security in practice. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (pp. 1481-1495).
- Albrecht, M.R., Celi, S., Dowling, B. and Jones, D., 2023. Practically-exploitable cryptographic vulnerabilities in Matrix. Cryptology ePrint Archive

Threat Modelling

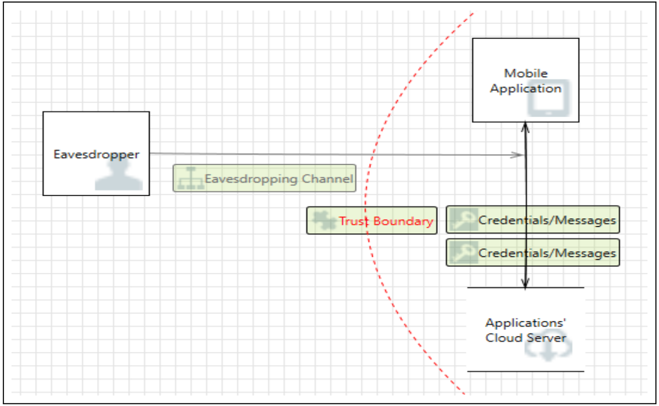
STRIDE - Security Focused

- Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege
- Threats assessed: authentication, integrity, non-repudiation, confidentiality, availability & authorization

LINDDUN - Privacy Focused

- Linkability, Identifiability, Non-repudiation, Detectability, information Disclosure, content Unawareness, Non-compliance
- Threats assessed: unlinkability, anonymity/pseudonymity, plausible deniability, undetectability/unobservability, confidentiality.

DFD (Data Flow Diagrams) for E2EE Mobile Messaging Applications



Findings

Signal

- Desktop client threat model persists with the mobile application threat model
- Access to the database decryption keys can render de-linking inconsequential

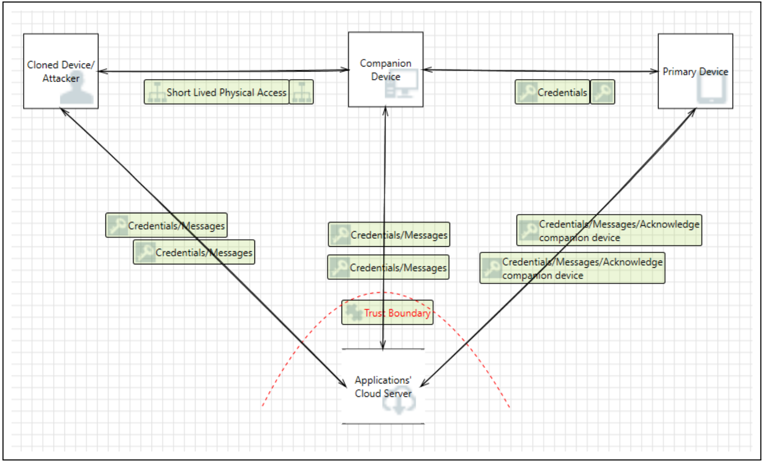
WhatsApp

- Desktop client recognizes that there can be malicious insiders
- Cloning is possible, yet improved alerts and time out does marginally better than Signal

Telegram

- Cloning is easy & persists with the eavesdropper only threat model
- There is a possibility to set time outs

DFD for Signal, WhatsApp & Telegram Desktop Applications



Viber

- Scopes threats from malicious insiders. Explicitly pins primary ID into companion devices
- Users are not responsible for detecting and recovering from threats

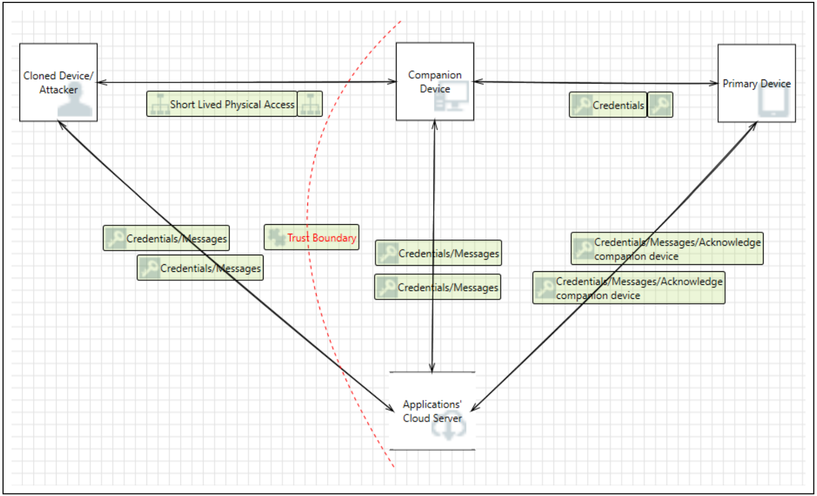
Element

- Cloning through short lived access is possible, attacker can see communicating entities
- Does not break forward secrecy

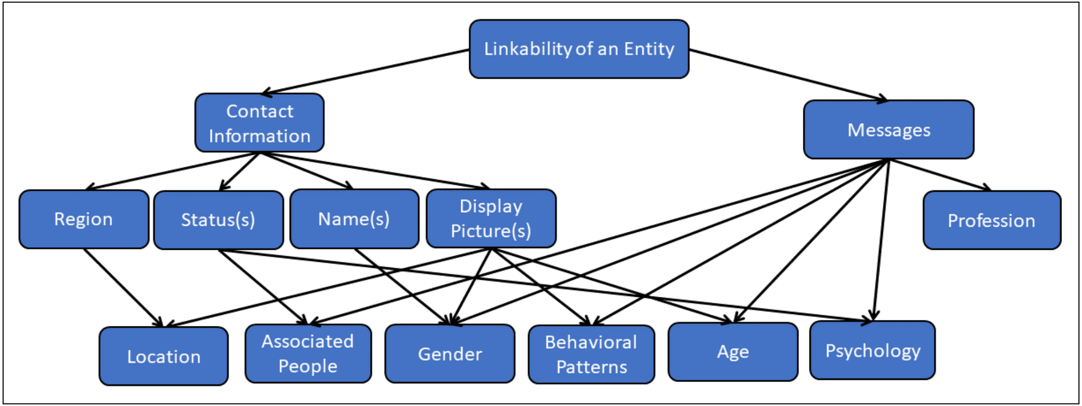
Wickr Me

- Ties a device with the cryptographic identity. Adequately scoped emergent threats
- Does not depend on the user to detect & recover from a breach

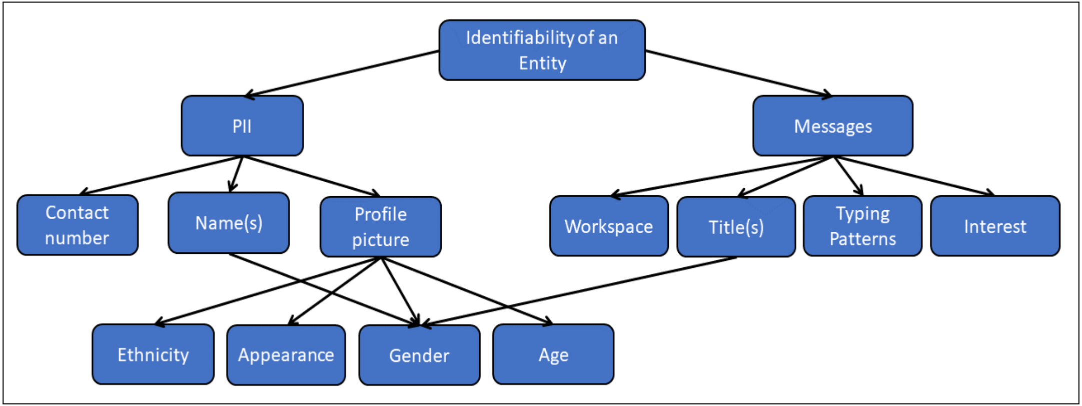
DFD for Element, WickrMe & Viber Desktop Applications



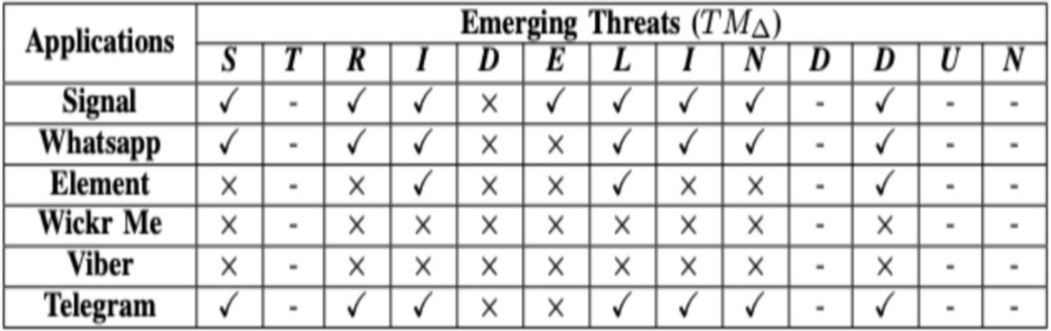
Linkability of an Entity due to cloning of a device



Identifiability of an Entity due to cloning of a device

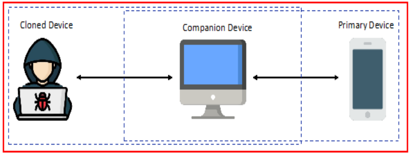


Summary of Findings

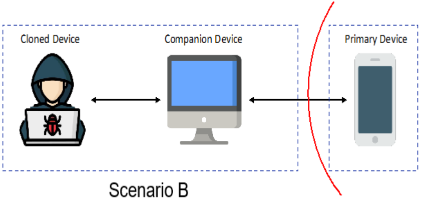


Applications	Emerging Threats (TM_Δ)												
	S	*T*	*R*	*I*	*D*	*E*	*L*	*I*	*N*	*D*	*D*	*U*	*N*
Signal	✓	-	✓	✓	×	✓	✓	✓	✓	-	✓	-	-
Whatsapp	✓	-	✓	✓	×	×	✓	✓	✓	-	✓	-	-
Element	×	-	×	✓	×	×	✓	×	×	-	✓	-	-
Wickr Me	×	-	×	×	×	×	×	×	×	-	×	-	-
Viber	×	-	×	×	×	×	×	×	×	-	×	-	-
Telegram	✓	-	✓	✓	×	×	✓	✓	✓	-	✓	-	-

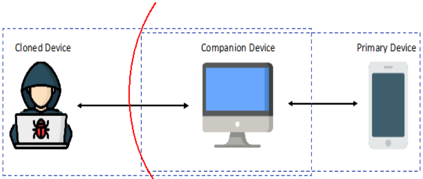
Delineation of Trust & Administrative Boundaries



Scenario A



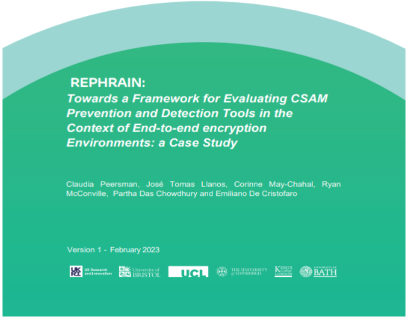
Scenario B



Scenario C

Scoping too often to protect human rights

REPHRAIN
Protecting citizens online



REPHRAIN:
Towards a Framework for Evaluating CSAM Prevention and Detection Tools in the Context of End-to-end encryption Environments: a Case Study

Claudia Peersman, José Tomas Llanos, Corinne May-Chahal, Ryan McConville, Partha Das Chowdhury and Emiliano De Cristofaro

Version 1 - February 2023

Scoping too often to protect human rights

Threats due to expanded memory scanning

- Where are they placed?
- Users are not responsible for detecting and recovering from threats.

Threats due to embedding tools within other applications

- Security & privacy permissions dependent on the goals and incentives of the embedding application
- Mandated backdoor can lead to interesting policy externalities

Engineering Secure Systems

Threat modelling across components with shared state

- Composability problem
- Administration of shared state
- Minimal sharing of state

Safe Defaults

- Users do not have fixed behavior
- How do applications adapt when the system context and user behavior change?

Conclusions

Functionality vs Security

- Some involve the user others do not
- Depends on who is your target customer perhaps

Modelling the attacker

- Modelling the attacker cannot be independent of users
- Understanding of perturbations in the trust domain due to additional features

Conclusions

Flawed Implementation

- Session handling (Signal and Element)

Usability vs Security

- Balance between usability cost and security cost
- That is why we suggest re-scoping