University of BRISTOL

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

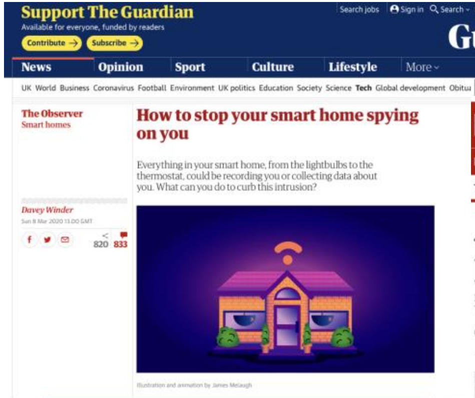
REPHRAIN
Protecting citizens online

REPHRAIN Privacy Testbed

Partha Das Chowdhury. (partha.daschowdhury@bristol.ac.uk)
Joe Gardiner (joe.gardiner@bristol.ac.uk)

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

Why a Privacy Testbed?



Support The Guardian
Available for everyone, funded by readers
Contribute → Subscribe →

Search jobs | Sign in | Search | The Guardian | UK edition

News | Opinion | Sport | Culture | Lifestyle | More

UK World Business Coronavirus Football Environment UK politics Education Society Science Tech Global development Obitua

The Observer
Smart homes

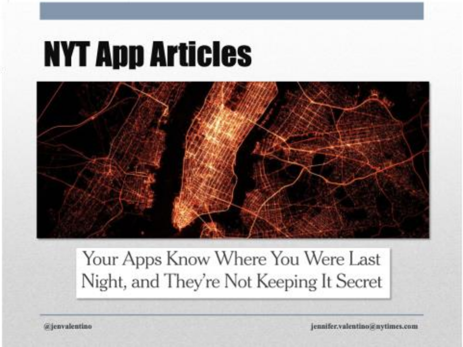
How to stop your smart home spying on you

Everything in your smart home, from the lightbulbs to the thermostat, could be recording you or collecting data about you. What can you do to curb this intrusion?

Davey Winder
Sun 8 Mar 2020 11.00 GMT

820 833

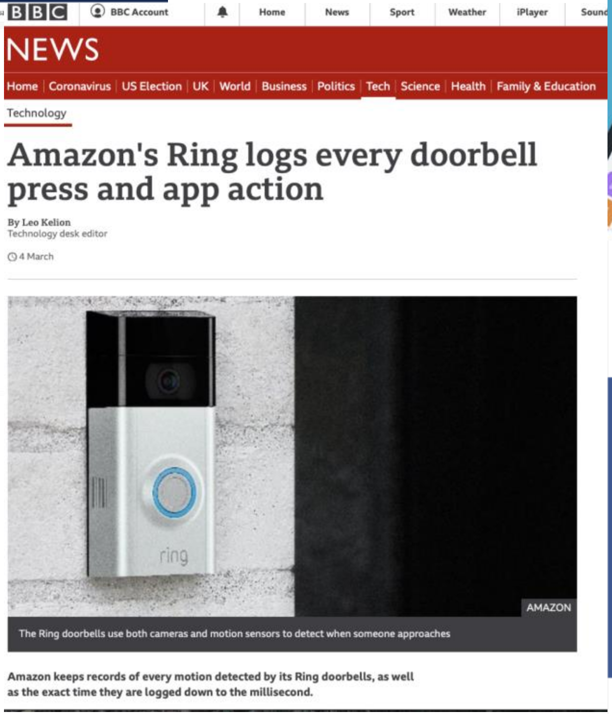
Illustration and animation by James Melaugh



NYT App Articles

Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret

@jenvalentino jennifer.valentino@nytimes.com



BBC | BBC Account | Home | News | Sport | Weather | iPlayer | Sound

NEWS

Home | Coronavirus | US Election | UK | World | Business | Politics | Tech | Science | Health | Family & Education

Technology

Amazon's Ring logs every doorbell press and app action

By Leo Kelion
Technology desk editor

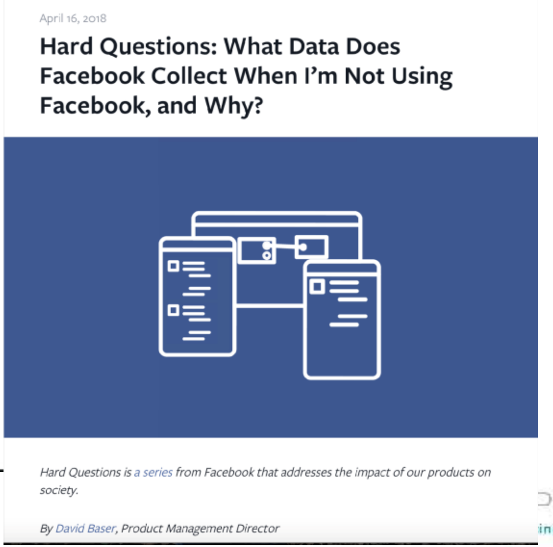
4 March

AMAZON

The Ring doorbells use both cameras and motion sensors to detect when someone approaches

Amazon keeps records of every motion detected by its Ring doorbells, as well as the exact time they are logged down to the millisecond.

NHS
E4 is in Local Covid Alert Level - Medium
Your app is active and scanning
Venue check-in
Check symptoms
NHS COVID-19



April 16, 2018

Hard Questions: What Data Does Facebook Collect When I'm Not Using Facebook, and Why?

Hard Questions is a series from Facebook that addresses the impact of our products on society.

By David Baser, Product Management Director

bristol.ac.uk

PHRAIN
ing citizens online

Why a Privacy Testbed?

App Developer

Assurance about privacy properties – regulatory compliance, care for users, behaviour of third-party libraries/APIs

Regulators

Checking claims about data and information storage and flows for compliance

Researchers/Journalists/ Citizens Rights Groups

Rigorous evaluation under experimental conditions; generating and sharing datasets.

End users

Does it do what it says on the tin? (a.k.a privacy policy, DPIA or privacy labels).

Implementation

Virtualisation

- Can deploy OS from disk image, or build as required
- Android applications emulated using Google’s Android Virtual Device (AVD)
  - Deployed inside Ubuntu Desktop VM
- Virtualisation managed by kvm-compose tool

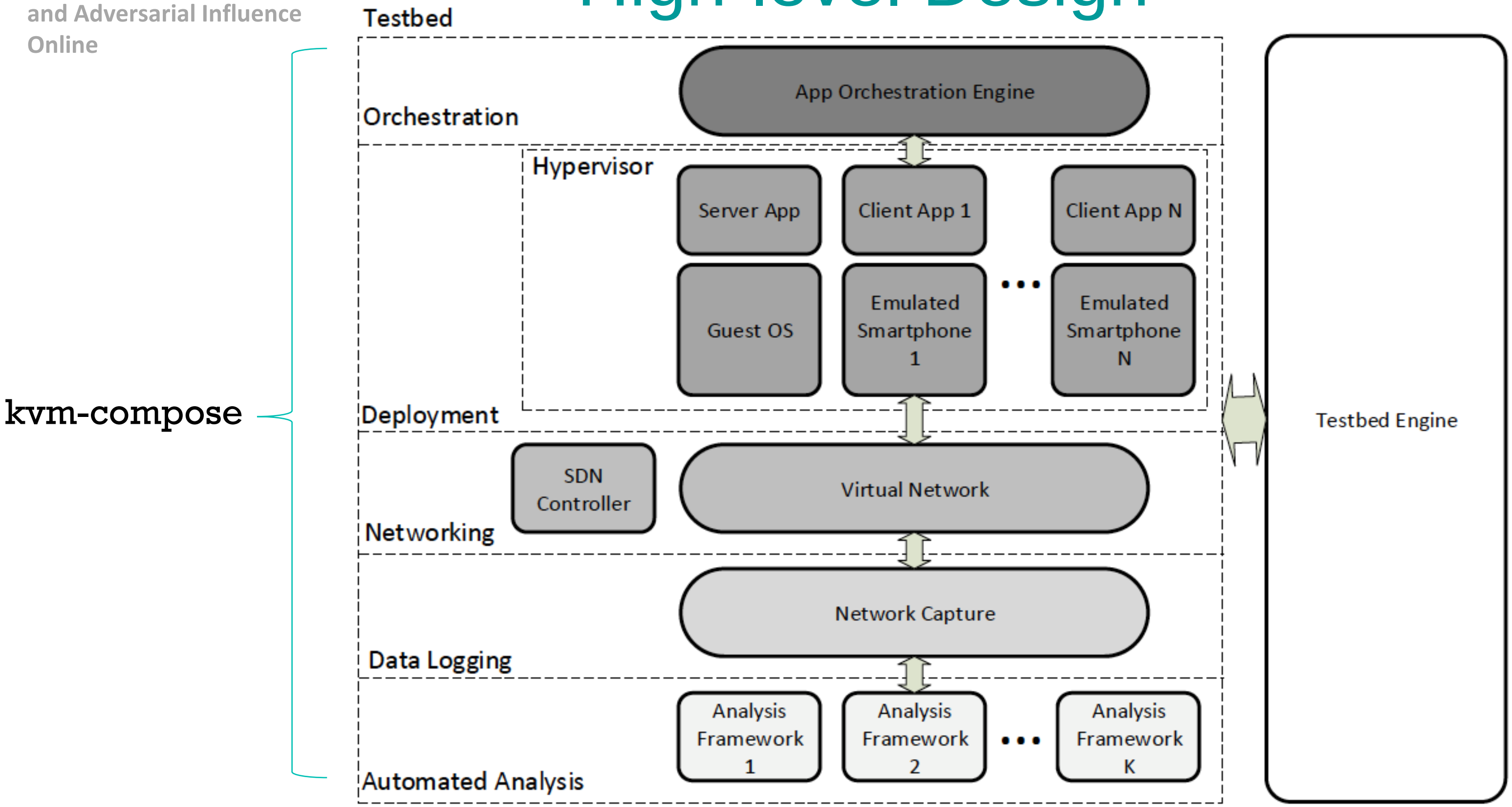
Kvm-compose

- CLI tool built by the team for Linux using RUST (and the libvirt library)
- Create custom test environments from configuration file using (up/down commands)

Networking

- Networking is provided using OpenvSwitch (OVS)
- OVS bridges can easily be linked up to an SDN controller (such as Floodlight), enabling more advanced network management.

High-level Design



Challenges and Lessons

Cloud Lock-in

The level of abstraction, we model the protocols/applications

App Interaction

Not a case of plug n play. E2EE apps require a SIM
Need for custom scripts to simulate user interaction in ADB.

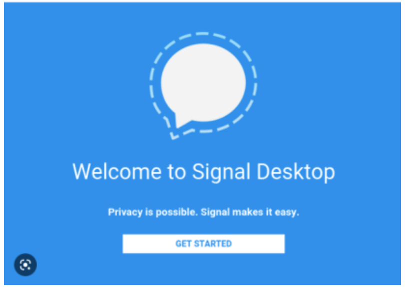
Testbed Implementation

Validate state transitions while configuring playbooks.

Signal Desktop client on the Testbed

(University of Bristol & University of Cambridge)

Pixel 3
with
Android 10
Q (API 29)

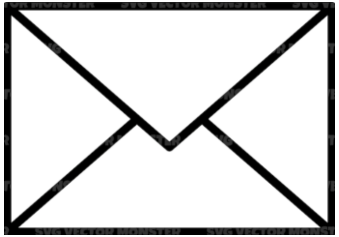


Welcome to Signal Desktop

Privacy is possible. Signal makes it easy.

GET STARTED

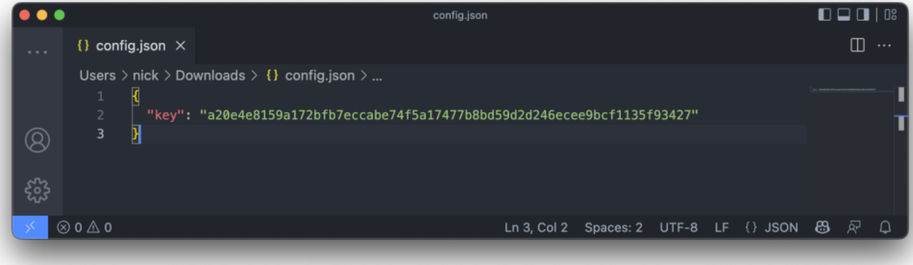
Standard
Signal
Desktop



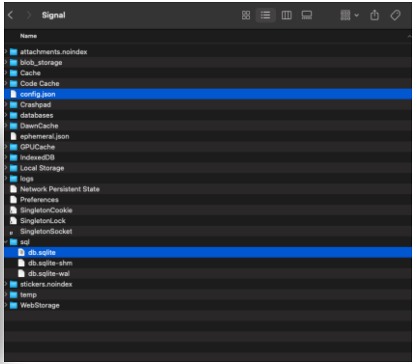
TLS-
Interceptor

National Research Centre on Privacy, Harm Reduction and Adversarial Influence Online

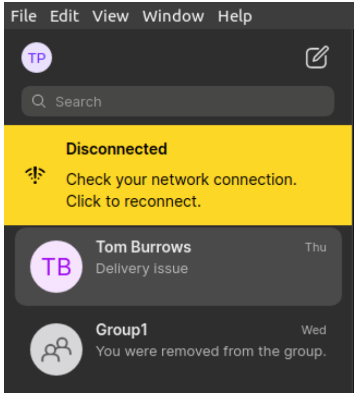
Plaintext Key



```
{
  "key": "a20e4e8159a172bfb7eccabe74f5a17477b8bd59d2d246ecee9bcf1135f93427"
}
```



```
attachments.noindex
blob_storage
Cache
Code Cache
config.json
Crashpad
databases
DawnCache
ephemeral.json
GPUCache
IndexedDB
Local Storage
logs
Network Persistent State
Preferences
SingletonCookie
SingletonLock
SingletonSocket
sql
  db.sqlite
  db.sqlite-shm
  db.sqlite-wal
stickers.noindex
temp
WebStorage
```



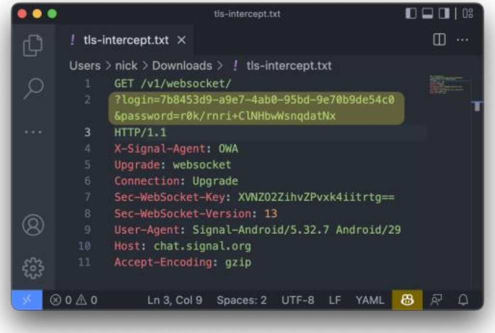
Disconnected

Check your network connection.
Click to reconnect.

Tom Burrows — Thu
Delivery issue

Group1 — Wed
You were removed from the group.

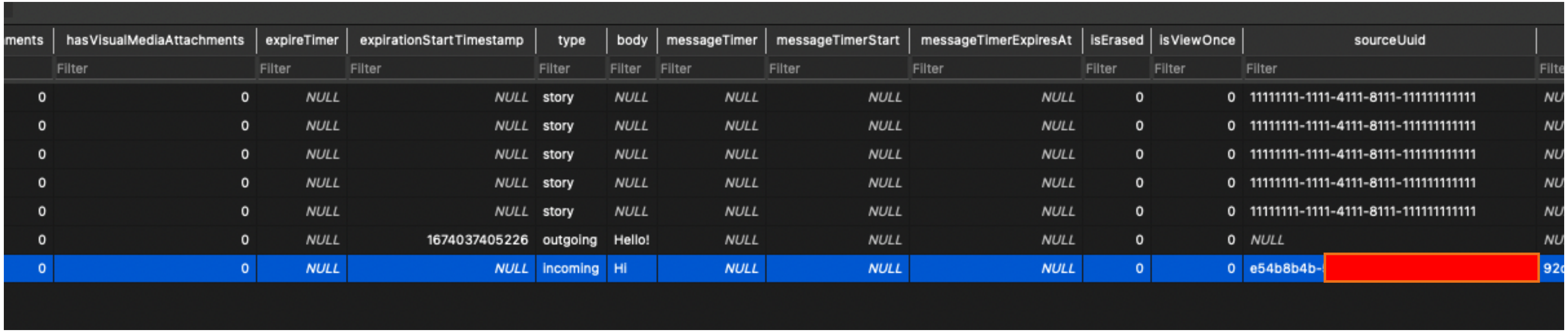
Short Lived Adversarial Access



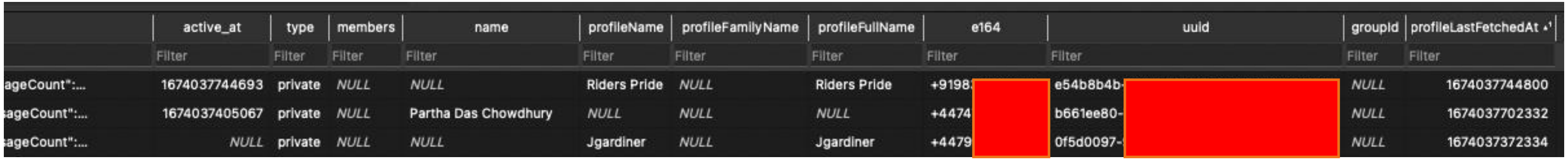
```
GET /v1/websocket/
?login=7b8453d9-a9e7-4ab0-95bd-9e70b9de54c0
&password=r0k/rnri+ClNHbwWsnqdatNx
HTTP/1.1
X-Signal-Agent: OWA
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Key: XVNZO2ZihvZPvxk4iitrtg==
Sec-WebSocket-Version: 13
User-Agent: Signal-Android/5.32.7 Android/29
Host: chat.signal.org
Accept-Encoding: gzip
```

Victim Desktop Warning

TLS-Interceptor



ments	hasVisualMediaAttachments	expireTimer	expirationStartTimestamp	type	body	messageTimer	messageTimerStart	messageTimerExpiresAt	isErased	isViewOnce	sourceUuid	Filte
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filte
0	0	NULL	NULL	story	NULL	NULL	NULL	NULL	0	0	11111111-1111-4111-8111-111111111111	NU
0	0	NULL	NULL	story	NULL	NULL	NULL	NULL	0	0	11111111-1111-4111-8111-111111111111	NU
0	0	NULL	NULL	story	NULL	NULL	NULL	NULL	0	0	11111111-1111-4111-8111-111111111111	NU
0	0	NULL	NULL	story	NULL	NULL	NULL	NULL	0	0	11111111-1111-4111-8111-111111111111	NU
0	0	NULL	NULL	story	NULL	NULL	NULL	NULL	0	0	11111111-1111-4111-8111-111111111111	NU
0	0	NULL	1674037405226	outgoing	Hello!	NULL	NULL	NULL	0	0	NULL	NU
0	0	NULL	NULL	incoming	Hi	NULL	NULL	NULL	0	0	e54b8b4b-[redacted]	92c



	active_at	type	members	name	profileName	profileFamilyName	profileFullName	e164	uuid	groupId	profileLastFetchedAt
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
ageCount":...	1674037744693	private	NULL	NULL	Riders Pride	NULL	Riders Pride	+9198[redacted]	e54b8b4b-[redacted]	NULL	1674037744800
ageCount":...	1674037405067	private	NULL	Partha Das Chowdhury	NULL	NULL	NULL	+4474[redacted]	b661ee80-[redacted]	NULL	1674037702332
ageCount":...	NULL	private	NULL	NULL	Jgardiner	NULL	Jgardiner	+4479[redacted]	0f5d0097-[redacted]	NULL	1674037372334

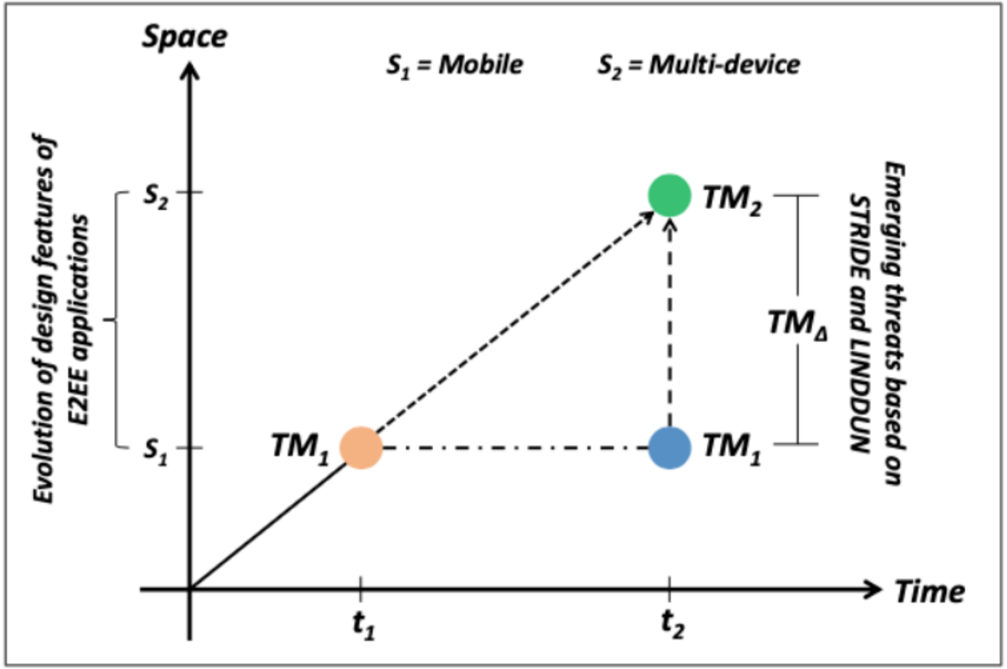
Short Lived Adversarial Access

Threat Models over Space and Time: A Case Study of E2EE Messaging Applications

Partha Das Chowdhury[*], Maria Sameen[*], Jenny Blessing[†], Nicholas Boucher[†], Joseph Gardiner[*], Tom Burrows[†], Ross Anderson[†‡], Awais Rashid[*]
[*]University of Bristol, UK {*partha.daschowdhury, maria.sameen, joe.gardiner, awais.rashid*}*@bristol.ac.uk*
[†]University of Cambridge, UK. {*jenny.blessing, nicholas.boucher, ross.anderson*}*@cl.cam.ac.uk, tom@tpmb.uk*
[‡]University of Edinburgh, UK *ross.j.anderson@ed.ac.uk*

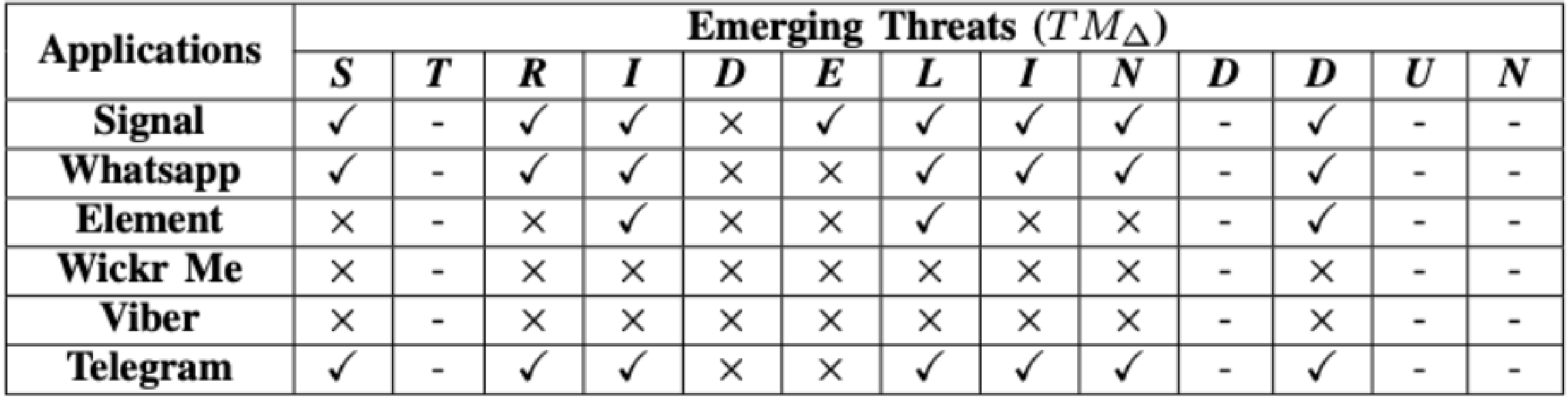
http://arxiv.org/abs/2301.05653

Motivation


Space
S_1 = Mobile
S_2 = Multi-device
Evolution of design features of E2EE applications
S_2
S_1
TM_1
TM_2
TM_Δ
TM_1
Emerging threats based on STRIDE and LINDDUN
Time
t_1
t_2

Evolution of Threat Models – Short lived (adversarial) access

Short Lived Adversarial Access



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	✓	-	✓	✓	×	×	✓	✓	✓	-	✓	-	-

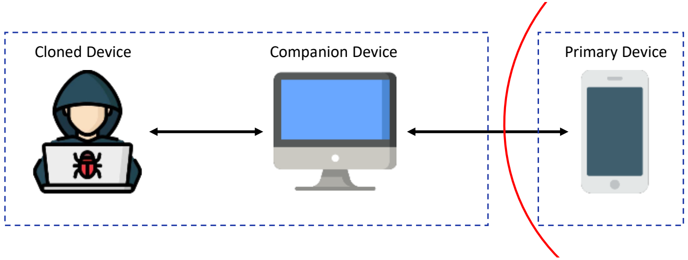
(-) -> Not tested, (x) -> Attack not possible, (✓) -> Attack possible

STRIDE:
- Spoofing
- Tampering
- Repudiation
- Information disclosure
- Denial of service (DoS)
- Elevation of privilege

LINDDUN:
- Linkability
- Identifiability
- Non-Repudiation
- Detectability
- Disclosure of Information
- Unawareness
- Non-compliance

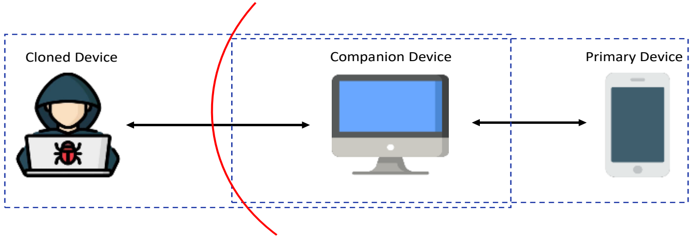
Aligning Administrative boundary & Trust Boundary

- Administrative boundary – Logical entities within which we function
- Trust boundary –The placement of security controls

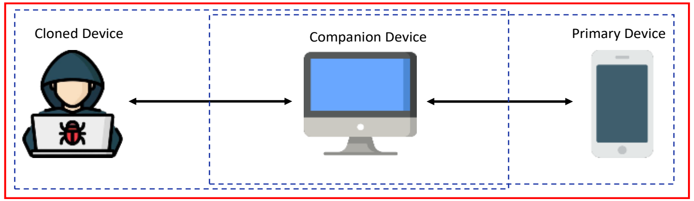


- Trust boundary includes only the device.
- Requires frequent access control even for short lived access.

Aligning Administrative boundary & Trust Boundary



- Anyone within the administrative boundary can clone desktop clients through short lived access.
- The trust boundary includes legitimate insiders who can turn malicious



- Desktop clients cannot be cloned through short lived access.
- Trust boundary incudes only desktop clients fired by the primary device.

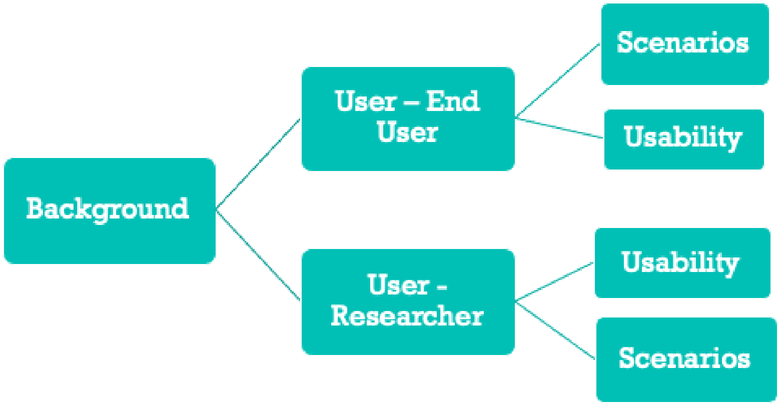
Security Engineering Lessons

- Reconciliation of security requirements across components with shared state
  - Desktop clients and primary devices share state.
  - Shared state is open to compromise in some desktop clients.
  - Model the threats of the shared components.

- Safe Defaults
  - Participants behavior change over time.
  - Threat modelling should accommodate this change in behavior and intentions.

Ongoing and Future Plans

Ongoing – Focus Groups with Wider Testbed Users



Future Implementation Priorities

- Scale up in terms of deployment of VMs
- Connecting with other test beds (e.g., IoT/LoraWAN at Edinburgh)
- Usability to the extent possible without oversimplifying the testbed.
- Integrate additional (external) analysis tools in the Testbed
- Enable the community to have a commodity privacy testbed.

National Research Centre on
Privacy, Harm Reduction
and Adversarial Influence
Online

To learn more about REPHRAIN, our future plans and how to get involved:

www.rephrain.ac.uk

@REPHRAIN1

rephrain-centre@bristol.ac.uk

REPHRAIN
Protecting citizens online

We would love to hear from you. Thank you!

E2EE Paper: http://arxiv.org/abs/2301.05653

bristol.ac.uk