Building a Privacy Testbed

Partha das Chowdhury, Awais Rashid

Joint work with: Joseph Gardiner, Maria Sameen, Maysara Alhindi, Graham Peden, Winston Ellis, Anthony Mazeli and Mohammad Tahaei
(and formerly Jacob Halsey)

bristol.ac.uk
Why a Privacy Testbed?

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

Amazon's Ring logs every doorbell press and app action

By Lee Mathias, Technology desk editor

April 16, 2018

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

By David Beer, Product Management Director
Why a Privacy Testbed?

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

Checking claims about data and information storage and flows for compliance

Rigorous evaluation under experimental conditions; generating and sharing datasets.

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

bristol.ac.uk
Case in Point: E2EE Messaging Apps

Data vs. Meta-data

DST-IPs, Name & Location

Location on Map

bristol.ac.uk
Initial Scoping of Use Cases

TEST BED

- Automated Privacy Exploit Generation
- Integrate Analysis Tools
- Deployment Specs
- Dataset Outputs

User Researcher

Dashboard

Drop an App

User - End User

Data Capture

Results on Information Leakage and other properties

Report Generation

Network Information

Data Usage by App

2nd Party Information Exchange

Generating User Behavior

Deployment

Cloud Dependencies

Secure Hardware Dependencies

Deployment

User Behavior: Real vs Simulated

Compile and Check for Errors

Error Handling & Reconfiguration

Feeds

Feeds
High-level Design

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

kvm-compose

Testbed

Orchestration

Hypervisor

Server App
Client App 1
Guest OS
Emulated Smartphone 1
Emulated Smartphone N

Deployment

Networking

Network Capture

Data Logging

Analysis Framework 1
Analysis Framework 2
Analysis Framework K

Automated Analysis

Testbed Engine

bristol.ac.uk

REPHRAIN
Protecting citizens online
Implementation

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

The level of abstraction, we model the protocols/applications

Cloud Lock-in

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

App Interaction

Validate state transitions while configuring playbooks.
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

Background

User – End User

User – Researcher

Scenarios

Usability

Scenarios

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

[Website]  www.rephrain.ac.uk

[Twitter]  @REPHRAIN1

[Email]  rephrain-centre@bristol.ac.uk

We would love to hear from you. Thank you!

bristol.ac.uk