REPHRAIN PETs Testbed: Use Cases, Design Considerations and Current Progress

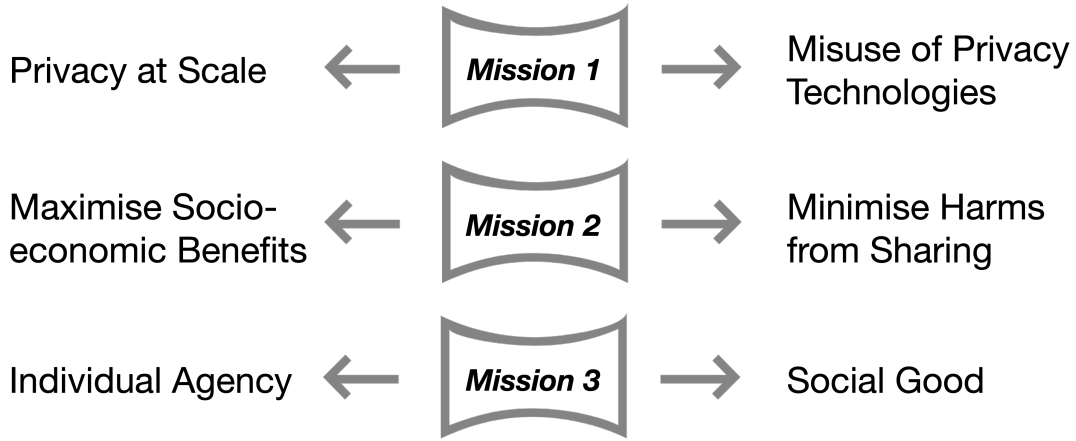
Joe Gardiner

REPHRIAN Project Meeting November 2021

University of BRISTOL
Bristol Cyber Security Group

Background – REPHRAIN Toolbox

- REPHRAIN toolbox
  - Datasets
  - Benchmarks
  - Reference Scenarios
  - Methods, Tools and Prototypes
  - PETs testbed
- Goal of this work is to design & build the PETs testbed
- Testbed will be both centrally hosted primary instance, and available to download for individual deployment



UK Research and Innovation
University of BRISTOL
UCL
UNIVERSITY OF BATH
THE UNIVERSITY of EDINBURGH
KING'S College LONDON

This Talk

- Use cases for privacy enhancing technologies (PETs) testbed
- Design considerations
- Prototype implementation


NHS
Test and Trace
B4 is in Local Covid Alert Level - Medium
Your app is active and scanning
Venue check-in
Check symptoms
NHS
COVID-19


Use GENER8
to control and be
rewarded from your
data
★★★★★
Rated 4.7 out of 5 stars

Use Cases

Intended Users

- Application Developers
  - Testing of apps/libraries as part of development
- Privacy Professionals
  - Auditing of existing applications
- Security Researchers

Use Case 1

- Developer Alpha produces an app using multiple third party libraries
- Wants to see if libraries are collecting unnecessary data from users
- Testbed launches multiple instances of Android and IoS devices with app installed
  - Testbed can simulate user interaction with app
- Testbed collects all network traffic from apps to internet, presents report to Alpha
  - Traffic contents, destinations etc
- Testbed can map collected data to a privacy-evaluation framework (e.g. Privacy by Design, LINDDUN)
- Testbed can apply automated analysis (e.g. Exodus, LibRadar)

https://www.linddun.org

Use Case 2

- Developer Beta develops a privacy preserving P2P file sharing application
- Wants to measure resilience against attacks such as Sybil or partitioning
- Launches large number of instances in P2P topology
- Makes subset of instances “malicious” to perform the attack
- Performs attacks, and measures impact on privacy and performance

Use Case 3

- Privacy Engineer Gamma wants to learn about and test modern PETs, e.g. homomorphic encryption, secure multi-party computation and differential privacy
- Testbed used to run and evaluate these technologies before use in final product
  - Can launch instances and simulate “users”

Specific Use Case Examples

- Contact Tracing Application
- Privacy Preserving Browsers

Contact Tracing Application

- Covid-19 tracing application built on Google Apple Exposure Notification (GAEN) framework.
- Developer uses *ExposureNotificationClient* to implement tracing functionality, including transmission and receiving of close contact information
- Application should not reveal any PII when exchanging close contact information or when at rest
- Instances of application and centralised control server launched into testbed
- Perform evaluation over data, e.g. attempt to de-anonymise client side data

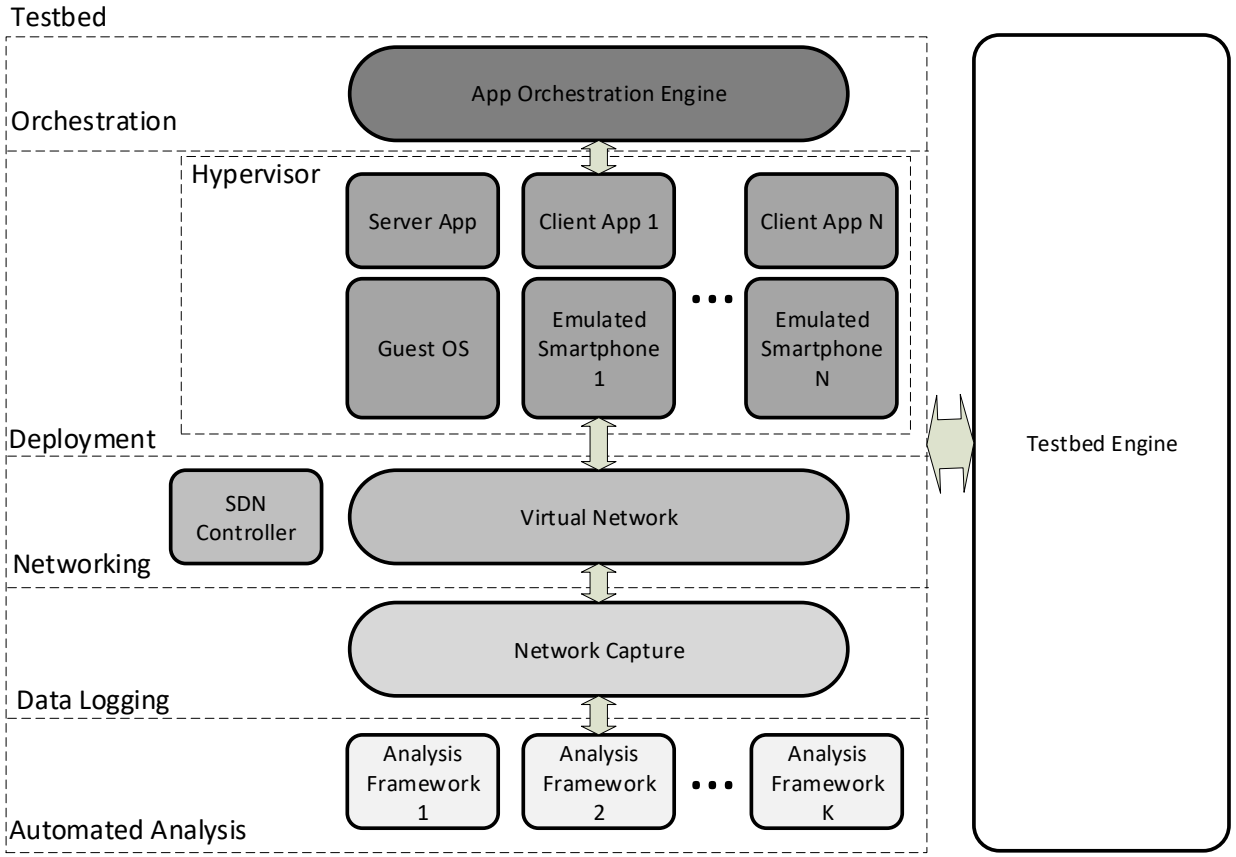
Privacy Preserving Browsers

- Browsers such as the Tor Browser and Brave use the Tor anonymity network.
- Available for both Android and iOS
- For iOS browsers use WebKit framework, which can override some anonymity features, leaving iOS users potentially vulnerable
- Testbed used to do a comparative study of privacy browsers on anonymous networks.
  - E.g. leakages that may occur due to use of WebKit framework

Testbed Design Considerations

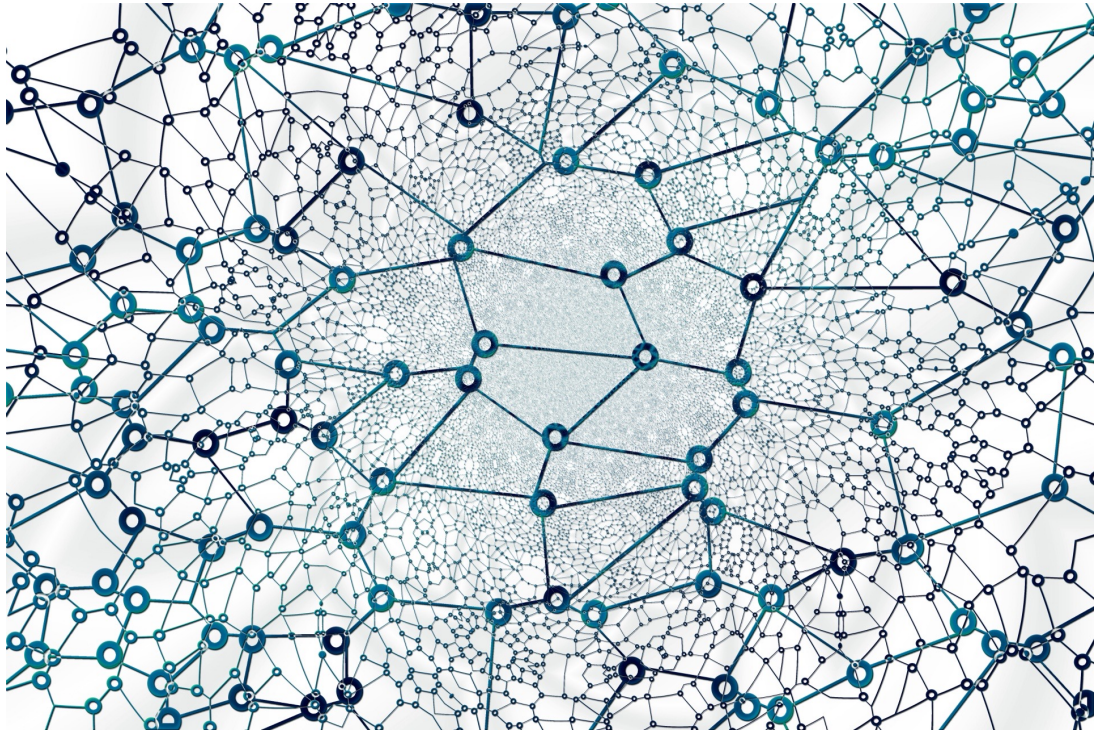
Key Functionalities

- Deployment
- Orchestration
- Data Logging



Deployment

- Testbed should allow for easy deployment of services and hosts
  - Potentially thousands
- Support for both traditional hosts, as well as emulated smartphone OSs
- Testbed should provide a virtual network
  - Use of SDN for orchestration

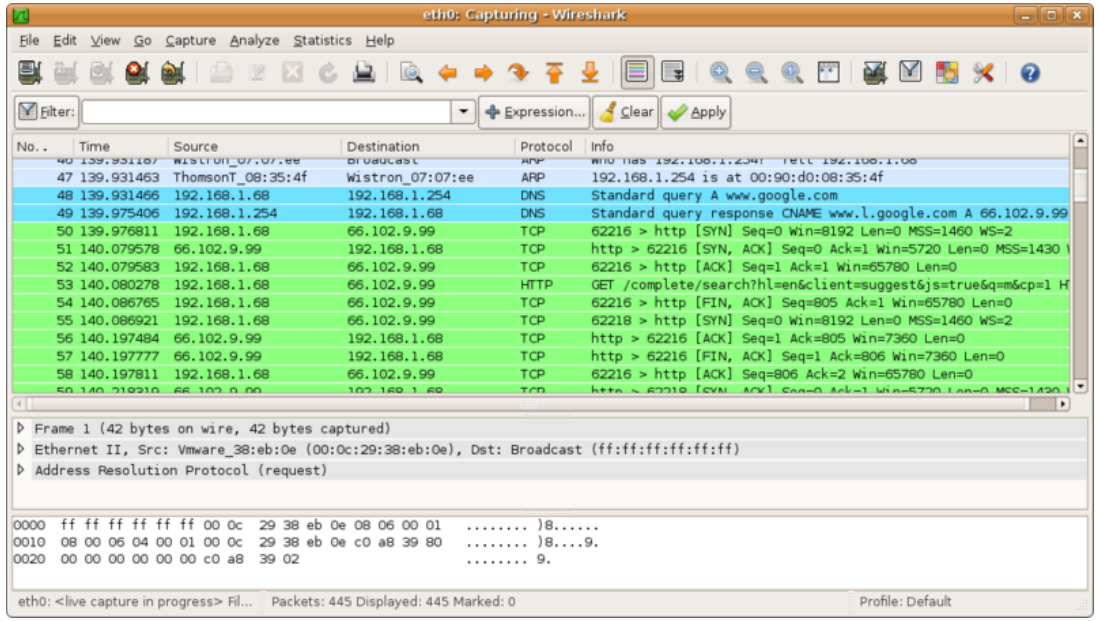


Orchestration

- Testbed should allow for automated control of applications
- Simulated user interaction, simulated sensor values
- Replaying of network traffic captures

Data Logging

- Testbed should capture sufficient data for analysis
- Potential sources:
  - Network captures
  - Memory captures
  - Screen captures



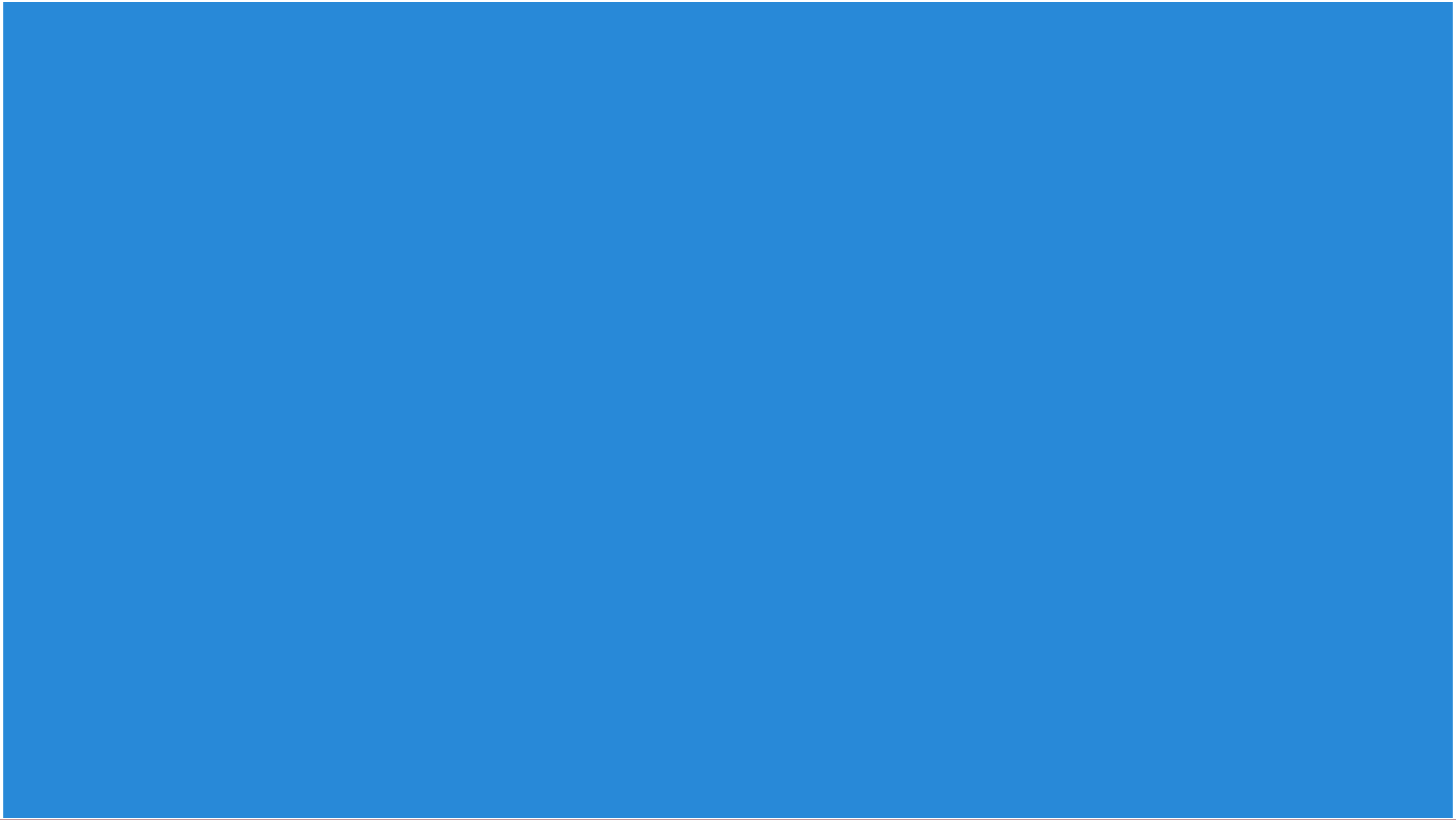
Further Design Elements

- Application Agnostic
  - Testbed should support multiple application types and architectures
- Extensibility
  - Testbed should be scalable.
  - Multiple instances of testbed should be joinable to increase virtualisation capability
- Automated Analysis
  - Testbed should have automated privacy analysis tools to be easily applied to use cases with minimal knowledge
- Modularity
  - New features (such as new analysis tool) can be added to testbed with ease

Prototype

- 3rd Year project student, Jacob Halsey
  - Supervisors: Awais Rashid, Joe Gardiner
- Tasked with building prototype testbed for REPHRAIN
- Project completion May 21
- Built kvm-compose tool:
  - Virtual machines (including installed software) and virtual network specified in config file
  - Software-defined networking
  - Currently supports network data capture
  - Two deployed applications
    - Swiss Covid-19
    - Signal Framework

Demo – Swiss Covid-19 App



Future

- App interaction automation - automating the process of simulating apps, in particular user interactions, to enable larger scale testing without intervention
- Conduct tests and make any necessary ease of use improvements for running deployments with a very large number of virtual machines.
- Add support for more complex captures such as memory dumps.
- Introduce privacy frameworks
- Hired 5 CDT student developers to build going forward.

Publications

- “A Privacy Testbed for IT Professionals: Use Cases and Design Considerations” J. Gardiner, M. Tahaei, J. Halsey, T. Elahi, A Rashid; 7th Workshop on Security Information Workers (WSIW 2021) (Extended Abstract)
- “Building a Privacy Testbed: Use Cases and Design Considerations” J. Gardiner, P. D. Chowdhury, J. Halsey, M. Tahaei, T. Elahi and A. Rashid; 4th International Workshop on SECurity and Privacy Requirements Engineering (SECPRE 2021) (Short Paper)

Conclusion

- We are aiming to build a testbed to assist IT professionals in evaluating privacy behaviour of applications
- Testbed currently in prototyping stage
  - Deployment of emulated Android VMs and OpenVSwitch virtual network, with support for network traffic capture
  - Two test applications:
    - Swiss Covid-19 track and trace application
    - Signal framework
- Keen to hear opinions and thoughts on how testbed platform can be better suited to needs and requirements of IT professionals and researchers

Questions?

Thank You!

Testbed Team:
Awais Rashid
Tariq Elahi
Joe Gardiner
Mohammad Tahaei
Partha Das Chowdhury

CDT Developers:
Graham Peden (Networking)
Maysara Alhindi (Orchestration)
Winston Ellis (Orchestration)
Maria Sameen (Modelling)
Anthony Mazeli (Documentation)

Joe Gardiner: joe.gardiner@bristol.ac.uk