DARPA's Investments in Real World Cryptography

Dr Josh Baron
Program Manager, DARPA/I2O

Real World Cryptography 2019

9 January 2019

Cryptography at DARPA Overview

- Proceed – Computation on encrypted data
  - Fully Homomorphic Encryption, MPC
- SAFER – Safe, resilient communications over the Internet
  - Pluggable Transports, Decoy Routing, Three-Party MPC
- Brandeis – Build privacy-aware systems
  - MPC, Differential privacy, human factors
- SAFEWARE – Provably-secure software obfuscation
  - Indistinguishability Obfuscation
- RACE – Secure, distributed messaging in contested network environments
  - MPC, Obfuscated Communications
- Future?

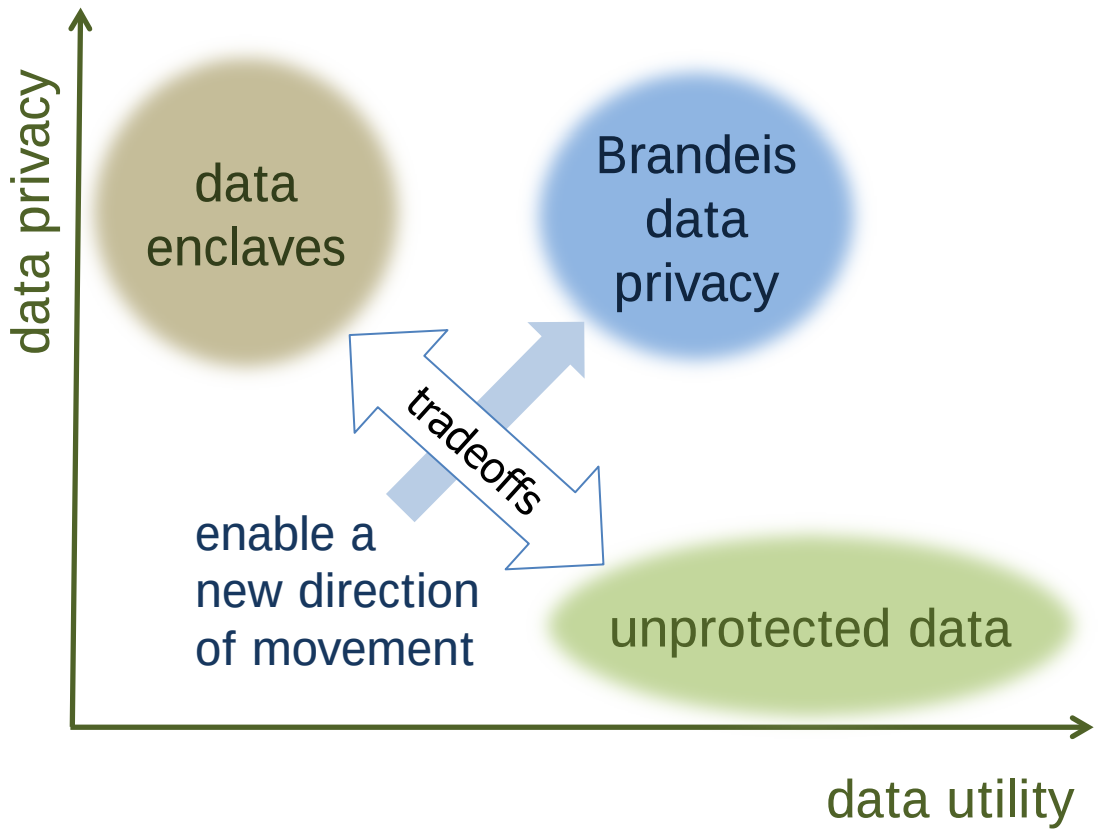
Today's Discussion

- Proceed – Computation on encrypted data
  - Fully Homomorphic Encryption, MPC
- SAFER – Safe, resilient communications over the Internet
  - Pluggable Transports, Decoy Routing, Three-Party MPC
- Brandeis – Build privacy-aware systems
  - MPC, Differential privacy, human factors
- SAFEWARE – Provably-secure software obfuscation
  - Indistinguishability Obfuscation
- RACE – Secure, distributed messaging in contested network environments
  - MPC, Obfuscated Communications
- Future?

Brandeis

Program Objective

Develop tools and techniques to enable the building of information systems where private data can be used for the intended purpose – and no other

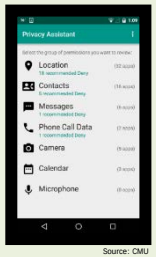


Brandeis System Concept

Data Owner

&
Devices

Human Data Interaction (TA2)

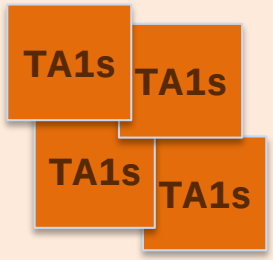


Source: CMU

Privacy Policy User Interface

(Users define and understand policy)

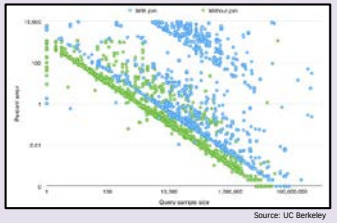
Experimental Integration Platforms (TA3)



Privacy Preserving Techniques

(Encryption, MPC, Differential Privacy)

Data Requester / User / Analyst



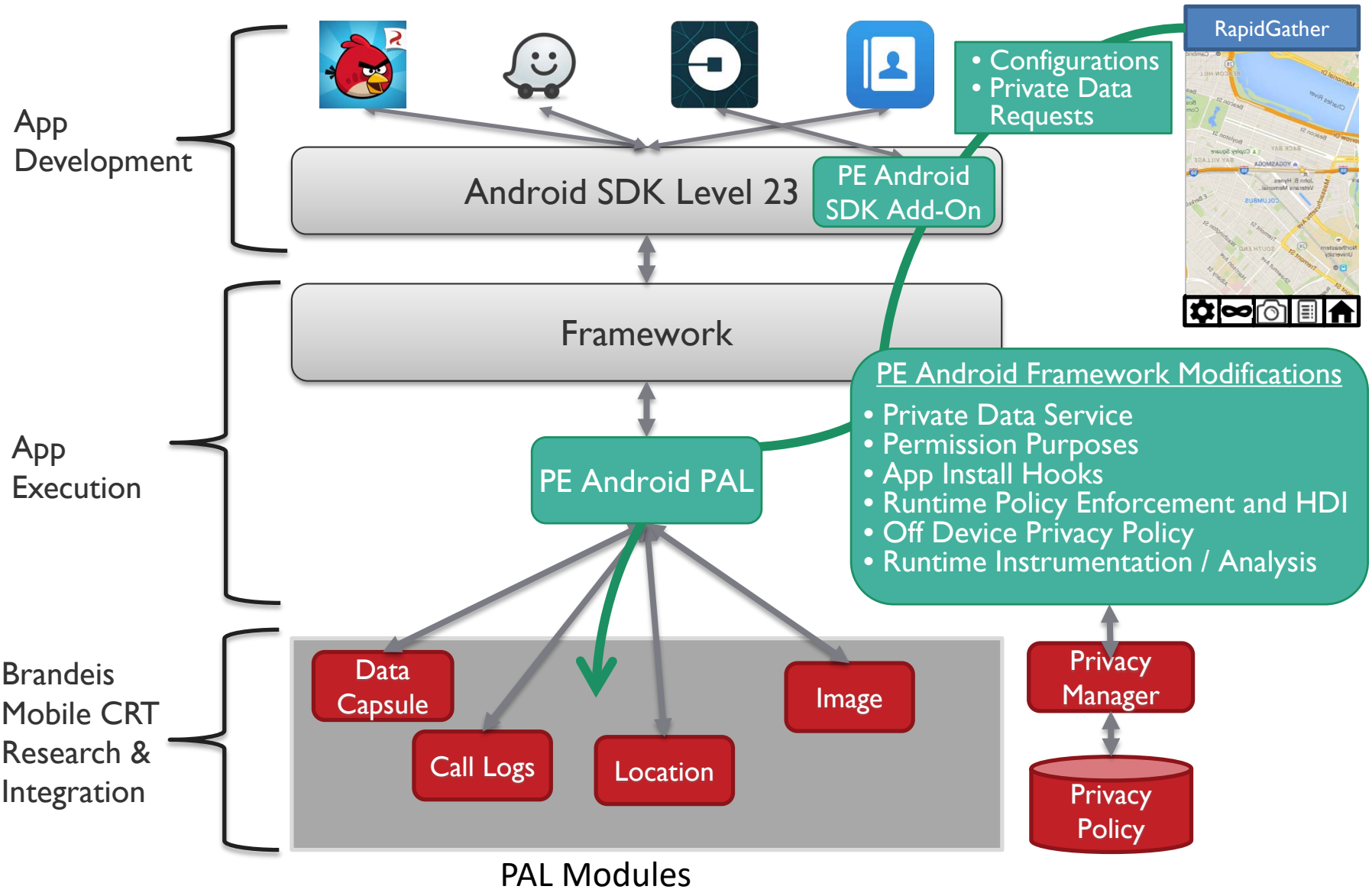
Source: UC Berkeley

Data requesters use, analyze privacy protected data

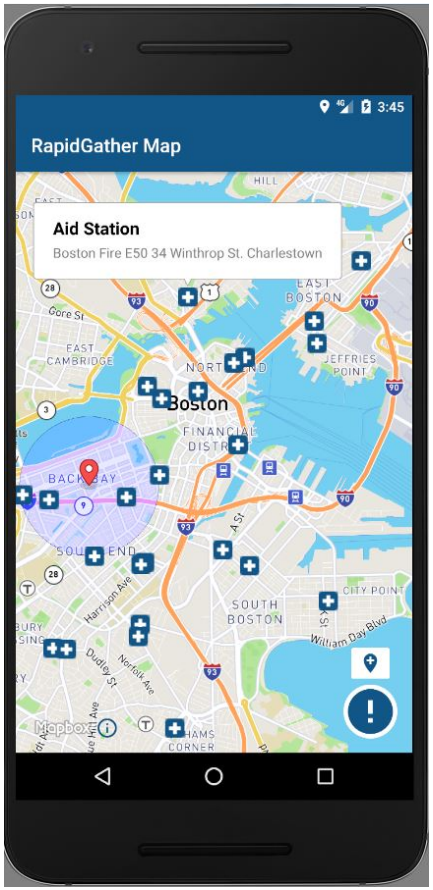
Privacy Measurement (TA4)

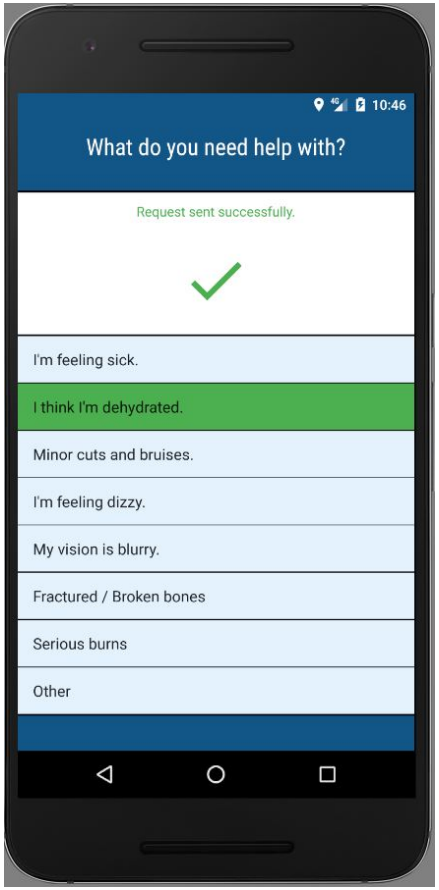
(Metrics for measuring privacy protection)

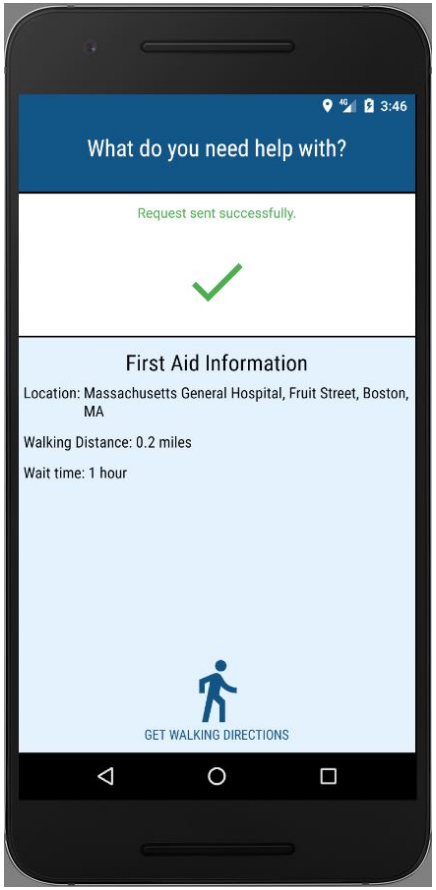
Privacy-Enhanced (PE) Android

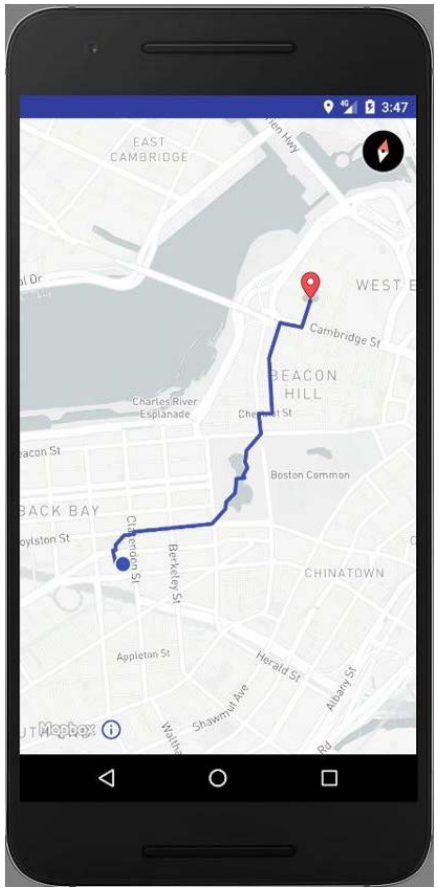


“Help Me” Application







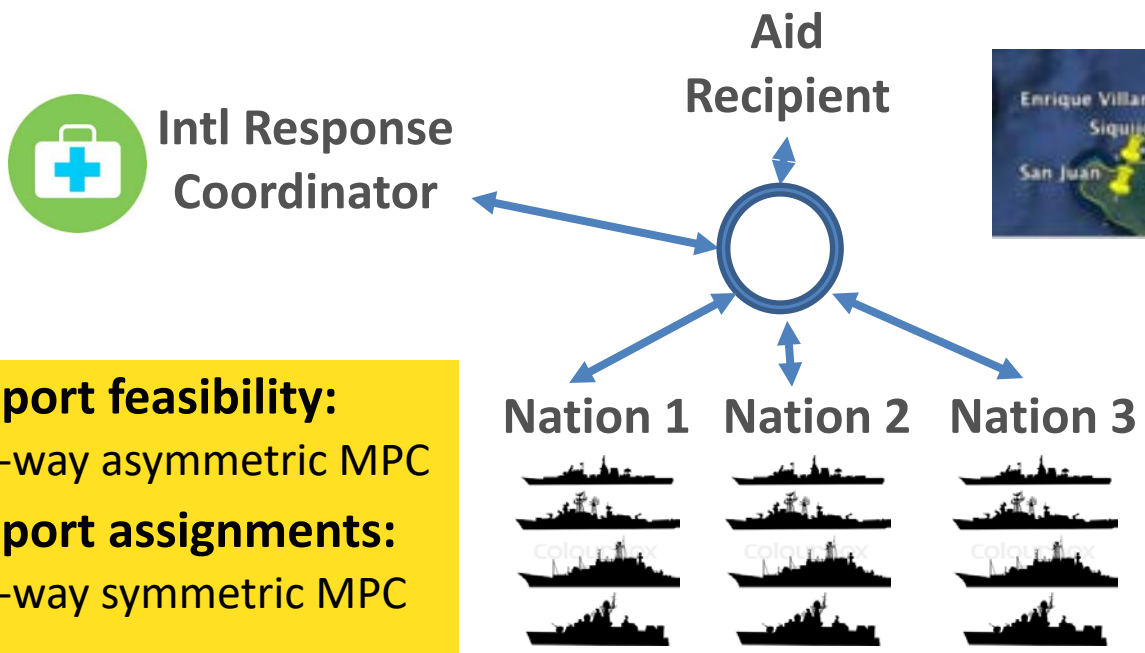


Optimized Schedule Docking

Task: Schedule the docking of S Aid Provider ships from N Nations at P ports within an Aid Recipient country by a given deadline D.

Optimization: Load-balance across ports

$$MIN\ (MAX_{Port\_j,\ Port\_k}(|\{Assigned(Ship\_i,\ Port\_j)\}| - |\{Assigned(Ship\_i,\ Port\_k)\}|))$$



10 ports

harbor-depth
offload-capability
berth-availability

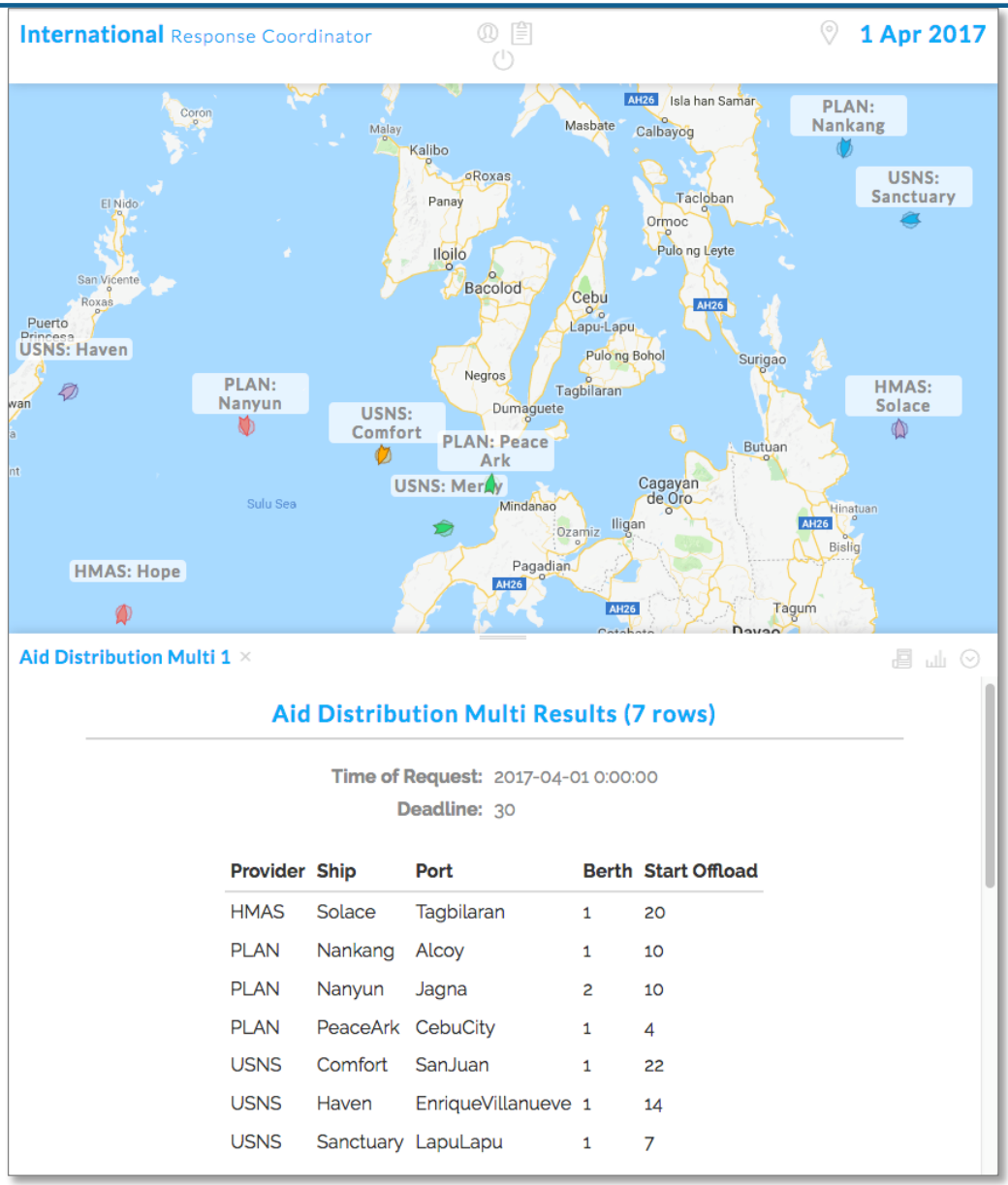
Ship-port feasibility:
- 2-way asymmetric MPC

Ship-port assignments:
- 3-way symmetric MPC

Aid Providers

ship-location
ship-maxspeed
ship-draft

Multi Ship Multi Port Aid Distribution Allocation in MPC



Provider	Ship	Port	Berth	Start Offload
HMAS	Solace	Tagbilaran	1	20
PLAN	Nankang	Alcoy	1	10
PLAN	Nanyun	Jagna	2	10
PLAN	PeaceArk	CebuCity	1	4
USNS	Comfort	SanJuan	1	22
USNS	Haven	EnriqueVillanueve	1	14
USNS	Sanctuary	LapuLapu	1	7

Privacy-Enhancing Technologies within Brandeis

- Cryptography
  - SCALE-MAMBA
  - Garbled RAM
  - Oblivious RAM
  - SGX/Sanctum
  - Functional Secret Sharing

- Differential Privacy
  - Workload Balancing
  - Composition (Ektelo)
  - Local DP
  - Open-source tools (ex: https://github.com/uber/sql-differential-privacy)

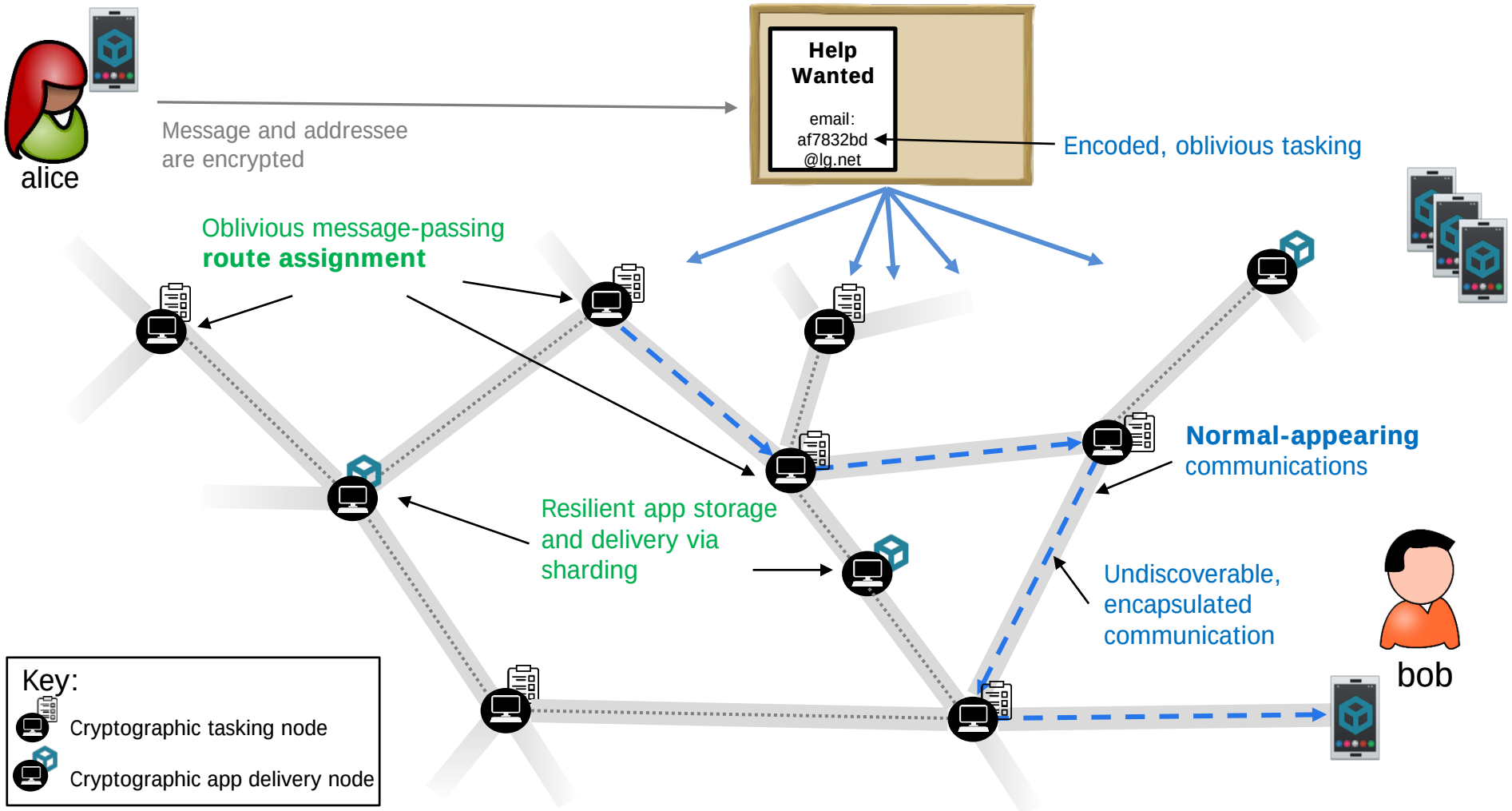
Resilient Anonymous Communication for Everyone (RACE)

RACE Goal

Use cryptography and obfuscated communications to build an anonymous, attack-resilient mobile communication system that can reside completely within a contested network environment.

RACE Approach: Avoid Large-scale Targeting

1) Cryptography: Counter service exploitation via computing on encrypted data
2) Obfuscation: Counter communication exploitation via protocol embedding



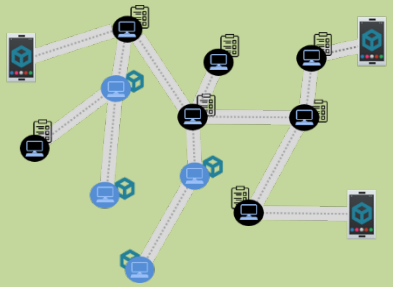
RACE Security Properties

Type	Attribute	Property
Confidentiality	user messages	Only the sender and receiver of a message can see it
	user message metadata	Confidentiality of who talks to whom and when
	unobservable communication	The fact that Alice possesses and uses the mobile application should not be inferable unless Alice's mobile device is compromised
	unobservable service node participation	The fact that Bob is running software to execute service node functionality should not be inferable unless Bob's system is compromised
Integrity	user messages	User messages cannot be changed in transit
Availability	user messages	End-to-end communication time should be one minute

RACE Program Structure

TA3: System
Distributed Messaging Operations

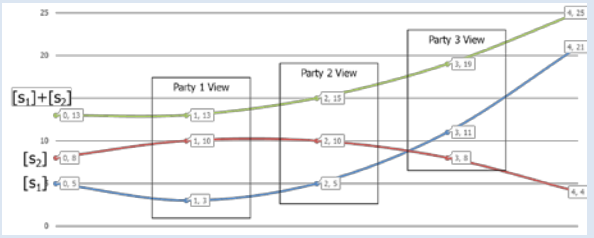
TA 3.1: Resilient App Distribution



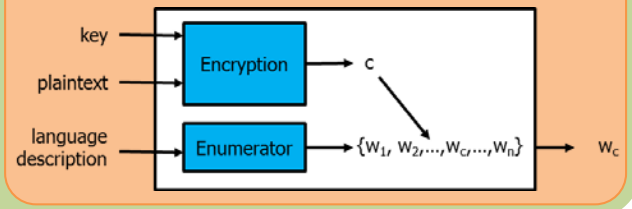
Prototype distributed tasking code

Communications toolbox

TA1: Cryptography
Resilient Distributed System Tasking



TA2: Obfuscated Communication
Countering Automated Protocol Identification



Prototype releases

Testbed and Voice of the Adversary
- Realistic network environments
- Realistic adversarial approaches
- Assess prototype systems

(Selected) RACE Metrics

	Metric	Phase 1 (18 mo)	Phase 2 (12 mo)	Phase 3 (18 mo)
Common	Nodes: users/tasking	10 / 100	100 / 1k	10k / 1k
	Crypto adversary /corruption level	Passive / 20%	Active / 10%	Active / 20%
	Crypto key infrastructure	Assumed	Not assumed	Not assumed
TA 1	msg/day / size / delay	500 / 140B / 5 min latency	5k / 140B / 1 min latency	500k / 1MB / 1 min latency
	Node refresh	Demonstrate	1/month	1/week
TA 2	Security	Quantitative/ simulated evaluation	Statistical distance proof sketch	Statistical distance full proof
	Adversary	Passive	Active link inject	Link+node inject
	Bandwidth (c-s/s-s)	100 kbps / 5 Mbps	500 kbps / 10 Mbps	500 kbps / 10 Mbps
	Channel Model	Simulation eval	Proof (passive adversary)	Proof (active adversary)
TA 3	System	Architecture	Full prototype integration	Full demo system
	Adversarial exploitation	Passive	Active node exploitation	Full spectrum exploitation
	Comm channels	Mock channel	TA 2 channel	Switch b/t channels
TA 3.1	Logical sharding	<5	Atomic functionalities	Innocuous “gadgets”
	Nodes: total/reconstruct	50/10	250/30	1000/50
	App reconstruction	10 min	5 min	5 min

Future Cryptography Programs at DARPA (?)

Zero Knowledge

- Making Mathematically Verifiable Statements Without Revealing Sensitive Information
- Question 1: What can/should I prove in ZK?
- Question 2: How efficiently can I prove it?
  - Proof *and* statement/witness efficiency
- Question 3: What are the big theoretical “heavy lifts” that need to be addressed?
  - PCPs, Interactive Proof Complexity, etc…

Consensus Protocols (Blockchain)

- ABC RFI
- What should DARPA's role be?
- Question 1: What can we actually do now that we cannot before?
  - Permissioned blockchains = old news
  - Permissionless blockchains = ?
  - Economic understandings of security + Distributed Computation Protocols = ?
- Question 2: How secure are consensus protocols really?
  - Are distributed systems truly decentralized?
    - Apostolaki et al, Oakland 2018: at the AS level, Bitcoin is highly *centralized*

www.darpa.mil

People/phone/computer icons from https://openclipart.org/ and https://github.com/KDE/breeze-icons