



DARPA WASH

Site Visit

February 2021

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).
The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



Agenda

- mSense Application & Portal
 - Current Status & Progress
 - Wearables
- TEE Approach Updates
 - Samsung Knox
 - Stealth Updates
- Revised Roadmap
- Question & Answer Session

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

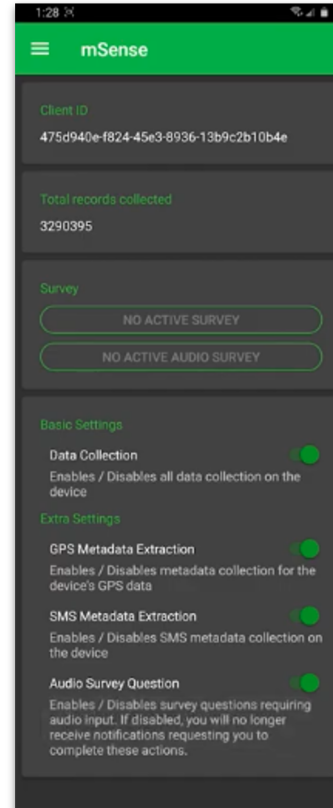
This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



Kryptowire mSense Application

- Passive Data Collection Application
 - Ground Truth Surveys
- Privacy-Preserving
 - Anonymized Collection and Communication
 - Integrated with Tozny Secure Data Storage
- Paired with Study Management Dashboard



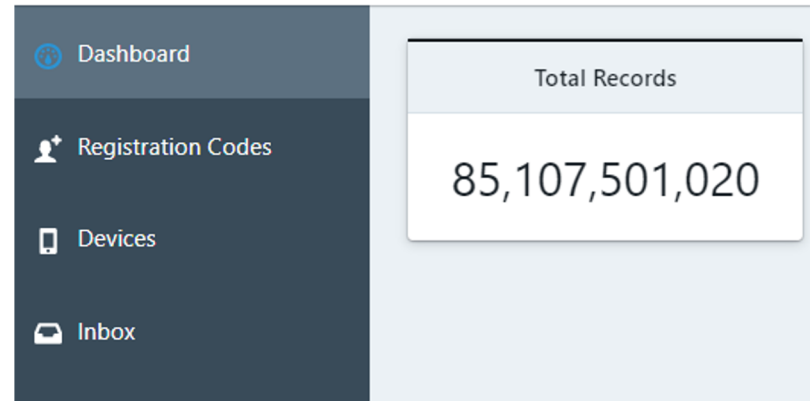
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.



Kryptowire mSense Application - Progress

- Deployment to UW cohort
 - Active data collection since spring
 - ~85 billion total records and counting
- ~6 version updates including sensing refinements, user experience, app protection, others...

Kryptowire mSense Dashboard



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



Dynamic Bad Actor data

- UW in their communication with participants often rely on if we have labeled the user a bad actor or not.
- Our labeling reflects dynamically retrieves the status of the user and labels them appropriately in the portal.

<p>Device</p> <p>BAD ACTOR</p> <p>Client ID: 19cc30e9-5bca-4b97-8561-9ee6b747f0ea Device Name: Build Version: 1.9.6-WASH Device ID: 947324609c3cc348 External UUID: 9a42d13c-520c-4f61-a0d4-98391632226f Platform: Android Registered: 11/02/2020 - 3:08:00 AM Last Upload: Invalid date Last Survey: 11/11/2020 - 2:08:14 AM</p>	<p>Surveys Completed</p> <p>15</p>	<p>Payment Owed</p> <p>\$4.26</p>	<p>Total Data Size</p> <p>0B</p>
		<p>Payment Sent</p> <p>\$0.00</p>	<p>Total Records</p>

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.



Additional Metrics

- In order to better understand user participation in the study, we're tracking completions of various surveys throughout the schedule
- We've seen that users who get to the third day of surveys are highly likely to be good actors

Total Records	Devices Registered	SID1 Completions	SID2-1 Completions	SID3-1 Completions	Final Survey Completions
85,117,254,506	8069	6064	5346	5182	2138

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



Payment history

- When responding to payment support questions, it is helpful to see how much the user has been paid
- Previously we showed the full amount, but have now added a full payment history for the user

Payment Date	Value
12/15/2020 - 3:13:59 PM	19.72
01/05/2021 - 6:16:14 PM	14.32
01/26/2021 - 4:20:43 PM	7.65

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.



UW WASH App - Progress

- Modified survey upload method
 - Source of truth is the Tozny database so methods of writing the survey records had to change
- Gyroscope and accelerometer data capture always remains active
- Updated MFCC sensing
- Updated Tozny Android SDK
- Additional telemetry events to help track down bugs
- Multiple bug fixes
- In progress - Extracting formants and other features from audio data

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).
The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



Existing SDKs' Problems

- While ResearchKit has been developed and maintained regularly by Apple, Android has been lagging behind due to lack of support
- ResearchStack project was started in 2015 with the goals to bring ResearchKit's features to Android, however, the team stopped maintaining the project since 2017.
- Currently, ResearchKit can only support a single navigation rule per step, therefore, it cannot support complicated survey structure natively.
- Existing sdks do not include parsers that could help researchers create an in-depth survey without diving deep into the code

1: [ResearchKit - Apple Developer](#)

2: [ResearchStack/ResearchStack: An SDK for building research study apps on Android. \(github.com\)](#)

Feature	ResearchKit ¹	ResearchStack ²	StudyLib
Single Choice Survey Step	✓	✓	✓
Multiple Selection Survey Step	✓	✓	✓
Slider Survey Step	✓	✓	✓
Custom Text Survey Step	✓	✗	✓
Image Choice Survey Step	✓	✗	✗
Time Picker Survey Step	✓	✗	✓
Date Picker Survey Step	✓	✓	✓
Time Range Survey Step	✓	✗	✓
Date Range Survey Step	✓	✗	✓
Scale (Slider) Survey Step	✓	✗	✓
Location Survey Step	✓	✗	✗
Audio Collection Survey Step (MFCC)	✗	✗	✓
Navigation Logic	⚠	✗	✓
Survey Parser	✗	✗	✓
Open-ended Survey Step (Multiple Selection/Single Choice)	✗	✗	✓

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



UW WASH App - StudyLib

- Support various question types
- Support open-ended questions with high flexibility
- Advanced Branching
- Apply logic based on users' responses and unlock follow-up questions or navigate to specific branches when criterias are met
- Create a survey step with just a few line of code
- Protect users' responses by communicating with parent app using secure channel

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).
The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



UW WASH App - StudyLib

Example #1:

Open-ended question with no predefined answers

Do you have children?	Yes No	Single Choice	if No, skip 14,15,16
How many children do you have?	0 1 2 3 4 5 6 7 8+	Single Choice	
How old are your children?	0-99 for each child	Custom (multiple check box with text field)	

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

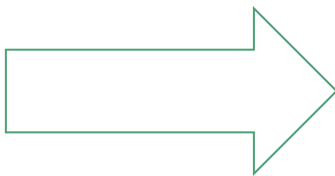
This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

UW WASH App - StudyLib

Using StudyLib SDK:



```
{
  "uuid": "f47e5ea3-354f-4599-a0f2-3251bfab7169",
  "title": "Children",
  "text": "How many children do you have?",
  "type": "single_choice",
  "lock": -1,
  "answer_options": [
    "0",
    "1",
    "2",
    "3",
    "4",
    "5",
    "6",
    "7",
    "8+"
  ],
  "optional": true
},
{
  "uuid": "79b54dbb-959f-4cfe-9d44-b8f905a8e783",
  "title": "Children",
  "text": "How old are your children?",
  "type": "multiple_choice_plus",
  "extra": 10,
  "lock": -1,
  "optional": true
},
}
```



Study Lib Demo

Children

How old are your children?

10

16

30

Check to add your own answer

Check to add your own answer

Check to add your own answer

Check to add your own answer

14

Check to add your own answer

Check to add your own answer

EXIT SKIP NEXT

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



UW WASH App - StudyLib

Example #2:

Multiple navigation rules for a question

Which of the following do you use?	Gum Chew Cigar Cigarettes Vape Other	Multiple Selection	
On average, how many cigarettes do you smoke per day?	0->99	Slider	asked if "Cigarettes" selected in Q54
[If vape is selected as answer for Q49] Where do you purchase your vape products?	Specialty Stores Online Retailer National Retailer (e.g. Wal-Mart) Gas Stations Aftermarket Dealer Other	Multiple Selection	asked if "Vape" selected in Q54

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.



Using StudyLib SDK:

- Each answer choice can unlock a question or as many questions as researchers need.
 - Each question may have multiple locks (See Example #3)

```
{
  "uuid": "49bcab7d-a7f3-4f45-8031-b8abc9f8abdc",
  "title": "",
  "text": "Which of the following do you use?",
  "type": "multiple_choice",
  "lock": -1,
  "answer_options": [
    "Gum",
    "Chew",
    "Cigar",
    "Cigarettes",
    "Vape",
    "Other"
  ],
  "rules": {
    "Cigarettes": ["d3eba718-3527-4d9c-a718-f30bdc3aa98b"],
    "Vape": ["91c37787-9b36-4e19-b084-fb1dfcb0fab4"]
  }
},
```

unlock

```
{
  "uuid": "d3eba718-3527-4d9c-a718-f30bdc3aa98b",
  "title": "",
  "text": "On average, how many cigarettes do you smoke per day?",
  "type": "slider",
  "min": 0,
  "max": 100,
  "point": -1
},
{
  "uuid": "91c37787-9b36-4e19-b084-fb1dfcb0fab4",
  "title": "",
  "text": "Where do you purchase your vape products?",
  "type": "multiple_choice",
  "answer_options": [
    "Specialty Stores",
    "Online Retailer",
    "National Retailer (e.g. Wal-Mart)",
    "Gas Stations",
    "Aftermarket Dealer",
    "Other"
  ],
  "point": -1
},
```

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



Example #3:

A question that may be asked depending on multiple other steps' responses

14		have a fever?	Yes No I don't know	Single Choice	
15		have muscle aches or pains?	Yes No I don't know	Single Choice	
16		have a cough?	Yes No I don't know	Single Choice	
17		have a stuffy nose or sniffles?	Yes No	Single Choice	
18		Are you sneezing more than usual?	Yes No	Single Choice	
19		Do you have a sore throat?	Yes No I don't know	Single Choice	
20		Do you have an ear ache?	Yes No	Single Choice	
21		Are you experiencing any shortness of breath or difficulty breathing?	Yes No	Single Choice	
22		Pick the number that describes how you felt yesterday:	1 – Worst ever 2 – Bad cold/flu symptoms 3 – Average 4 – Minor cold/flu symptoms 5 – No cold/flu symptoms	Single Choice	
23		Did you see the doctor today (in the past 24 hours)?	Yes No	Single Choice	This question appears if answering Yes to more than 2 questions above (from 14 to 21) If No, skip Q24

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

UW WASH App - StudyLib



Using StudyLib SDK:

- Assign the lock value as -2 for that question
 - Each “Yes” answer for the previous questions will increase the lock value by one
 - Question with lock value higher or equal 0 will be asked

```
{
  "uuid": "a7544603-046e-47a2-8851-555e4990b930",
  "title": "",
  "text": "Did you see the doctor today?",
  "type": "text choice",
  "style": "single",

  "lock": -2,
  "answer_options": [
    "Yes",
    "No"
  ],
  "rules": {
    "Yes": ["db2caa18-a77f-468b-b919-1ae2bcd138b9"]
  }
},
```

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.



Kryptowire mSense App - Wearables

- Sensors Collected
 - Heart Rate (via HealthKit framework)
 - Accelerometer, Altimeter, Pedometer (via CoreMotion framework)
 - Location (via CoreLocation framework)
- Standalone App
 - Enable/Disable collection for each sensor type
 - Save sensor data locally in wearable and upload directly to server
 - Background collection pending Apple's SensorKit framework updates

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Kryptowire mSense App - Wearables



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



Samsung Knox

- A defense-grade enterprise mobile security solution that's built from the chip up.
- Integrated throughout the software layers to separate data and constantly check the integrity of the device.
- Ensures only approved versions of system-critical software are loaded.
- Verify each piece of software that loads. If verification fails, Knox either records the tampering by flipping a one-time fuse called the Knox Warranty Bit, or prevents further booting.
- Devices with compromised Knox Warranty Bits cannot use certain Knox features or services, such as Knox Workspace or Samsung Pay.
- Ensures that a Samsung device is not downgraded to an earlier, vulnerable software version.

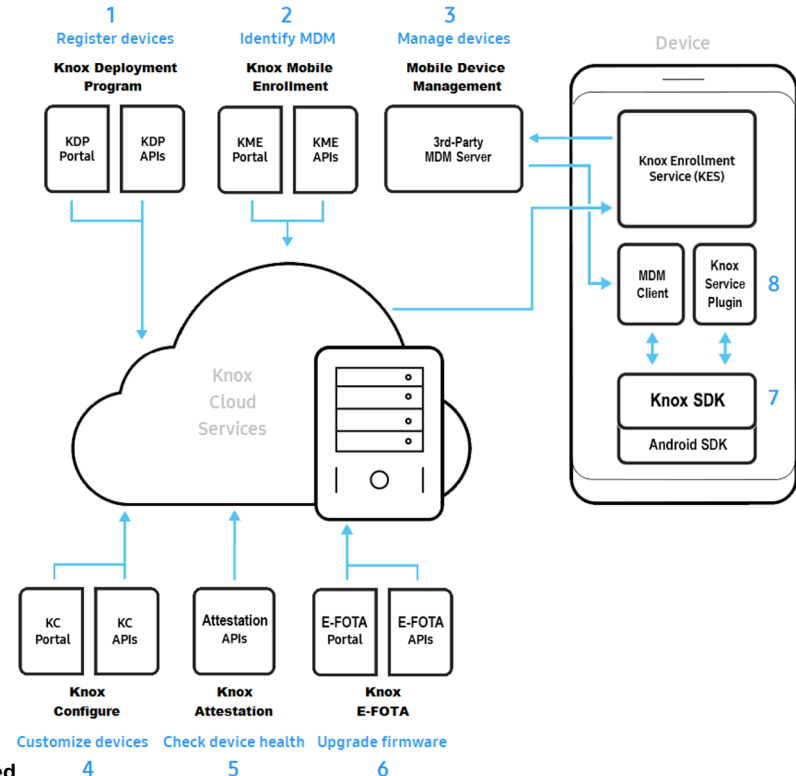
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



Samsung Knox

- Knox Deployment Program
 - Register IDs of devices purchased by enterprises.
- Knox Mobile Enrollment
 - Automatically identify MDM system that manages the device.
- Mobile Device Management
 - Automatically download the MDM client app at first boot.
- Knox Configure
 - Download Samsung Knox profiles and configurations from the cloud.
- Knox Attestation
 - Verify device integrity.
- Knox E-FOTA
 - Control device firmware updates.



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

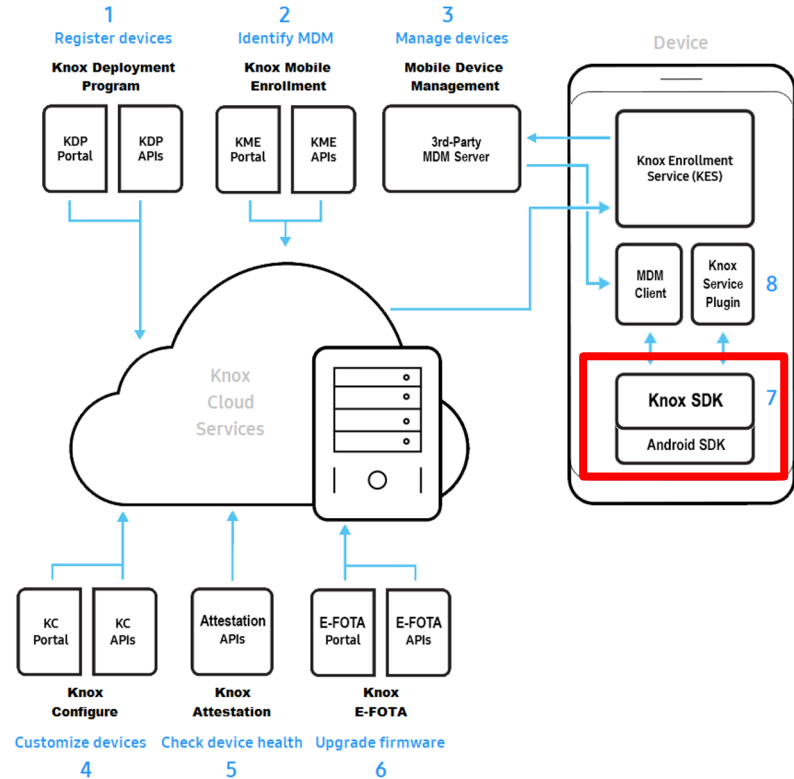
This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



Knox SDK's Highlighted Features

- Control application-related functions and restrictions.
- Manage the bluetooth, location providers, geofences, network, Wi-Fi, NFC, date and time, and browser settings
- Control device security and password settings.
- Manage certificates and keystores.



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Utilizing Samsung Knox to verify device integrity



- Knox Attestation
 - A Samsung Knox service to check device's integrity by checking whether the device is rooted or running unofficial firmware.
 - The signature of the app doing the attestation is also obtained during the process. Using the signature, the server can determine whether the app has been tampered with to prevent malicious attacks (e.g., repackaging¹ and MITM).
- Knox SDK
 - Limit and control device's functionalities remotely
- Knox E-FOTA
 - Enforcing firmware updates and prevent rollback to earlier (vulnerable) firmware versions

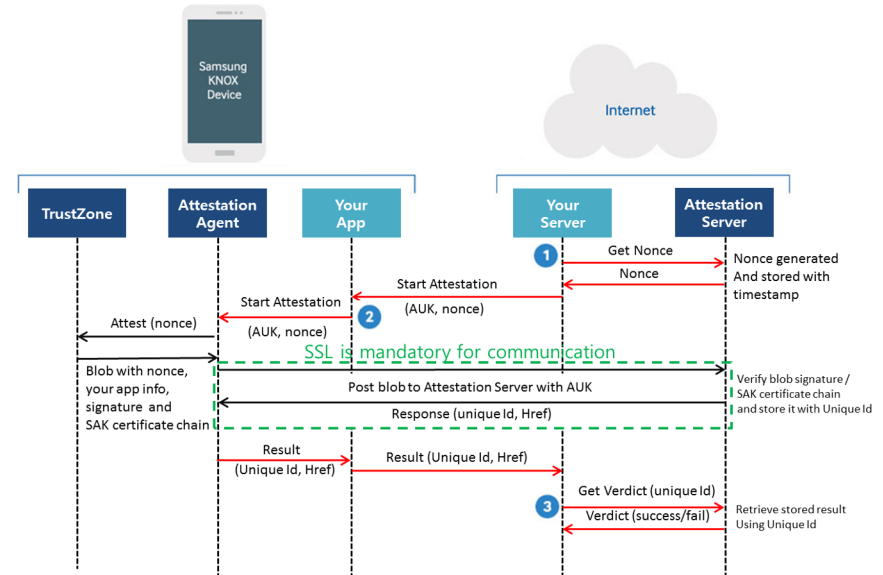
¹[Protect Android Apps Against Runtime Repackaging Attacks](#)

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.



Attestation Procedure

1. The app initiates attestation and requests a nonce from the server.
2. Upon receiving the request, the server will obtain a nonce from attestation server and send it to the app.
3. The app then starts the attestation process using the nonce.
4. Inside TrustZone (Samsung's "Secure World"), the device and app info will be transmitted to attestation server securely.
5. Upon completion of attestation, the app will receive the status of the attestation (success/failure) and let the server know attestation process has finished.
6. Finally, the server will get the verdict from attestation server and determine whether the app or user device should remain trusted.



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Utilizing Android Framework to verify device integrity



- Root detection
 - Determine if user has privileges to modify software code on the device or root access to operating system.
 - Utilizing Firebase Crashlytics' built-in root detection method and in combination with Samsung Knox SDK, a high confidence of determining root status of the device is achieved.
- User locality enforcement
 - Using Google's geocode reversing¹ functionality, the app can determine whether a user is currently running it from pre-approved locations, ZIP codes, or countries.
- Emulators detection
 - Combine various emulator detection methods to identify properties and settings most emulator existing in the markets would have
- SSL Pinning
 - Configure the app to reject all except one pre-loaded (pinned) certificate to communicate with the server
 - Compare the server certificate with the pinned certificate to make sure they match before any data transfer

¹<https://developer.android.com/reference/android/location/Geocoder>

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.



Stealth Updates

- Recently Delivered Milestone 6
 - Performed a risk-reduction benchmarking test and wrote a document on authenticating FSS Gen keys for grid-based contact tracing.
- Token-based Approach
 - Tested with single thread, could be parallelized
 - City-sized query takes around 20 seconds
 - State-sized query around 240 seconds
- Grid Approach
 - Per Phone
 - 1-yard resolution grid
 - 5 square miles
 - Updated/queried in 184 milliseconds

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.



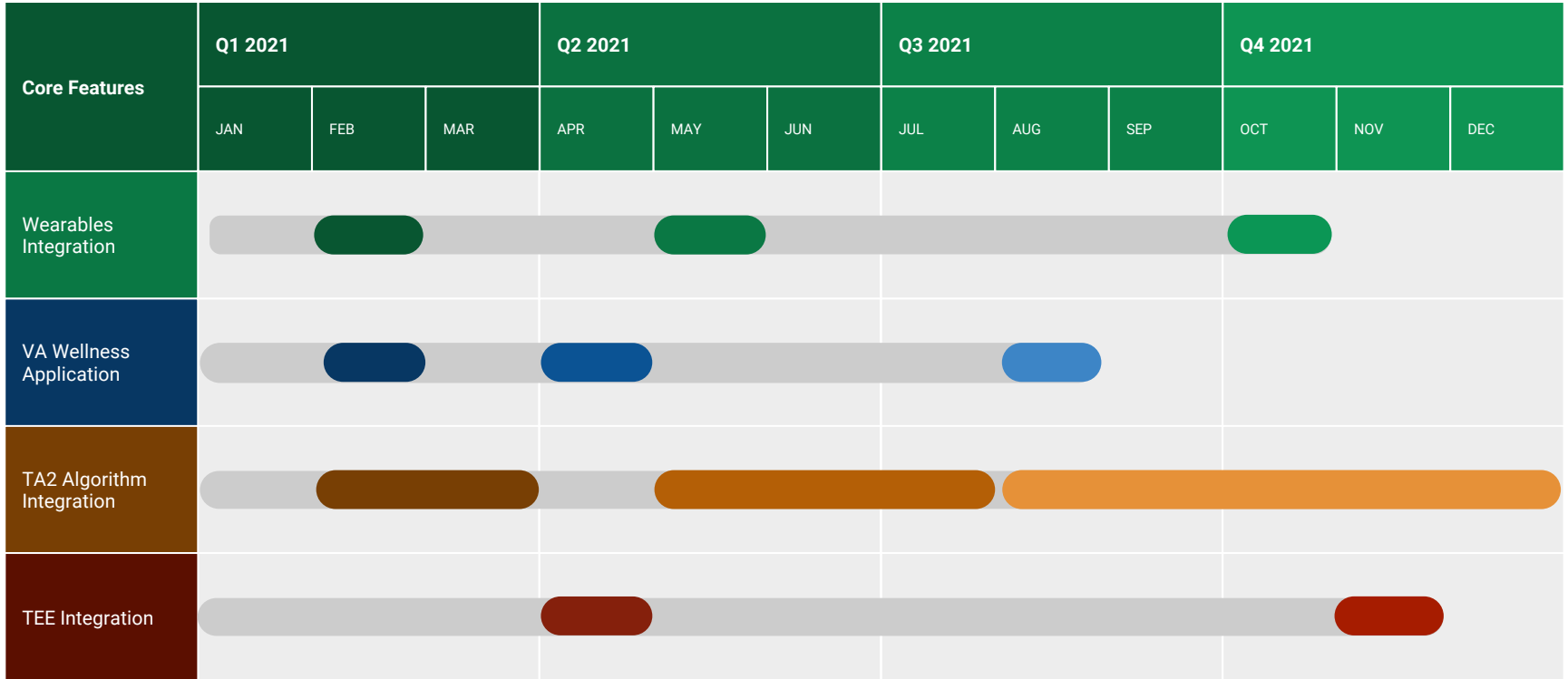
Stealth Updates

- Implementation in progress
 - Many overlaps with token based approach
- Tailoring operation to “military base sized” population
- Existing questions:
 - How to deal with a user who is in multiple areas in a single time slice
 - Validate benchmarks in real-world scenario

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).
The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Updated Roadmap



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Wearables Roadmap



February 2021

Standalone Apple Watch Application

Standalone Apple Watch Application with ability to run without the mSense App on the iOS device. Data collection will be possible with the ability to upload data directly to the backend server from the Watch.

May 2021

Fitbit Integration

Ability to integrate data from Fitbit devices into the data collection effort. Should support pulling data from Fitbit API with a user sign in and data upload to the backend server from the phone.

October 2021

Background Collection on Apple Watch

Standalone Apple Watch Application with the ability to perform background data collection and data upload directly to the backend server from the Watch. Pending approval and access granted by Apple through their new SensorKit program.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

VA Wellness Application



February 2021

Alpha Version - IN PROGRESS

Build alpha version of the VA application and publish to Apple App Store. We will target iOS first due to the larger user base, we will build an alpha version of the application that integrates with the Fitbit APIs and provides a basic user interface to show data for Sleep, Activity, and Stress.

April 2021

Beta Version

Extend alpha application to include trend information on each of the core indicators (Sleep, Activity, Stress). Include charts and notifications to highlight outliers to the trend for the user. E.g. when their sleep is worse than average, or their stress is higher.

August 2021

Launch Version

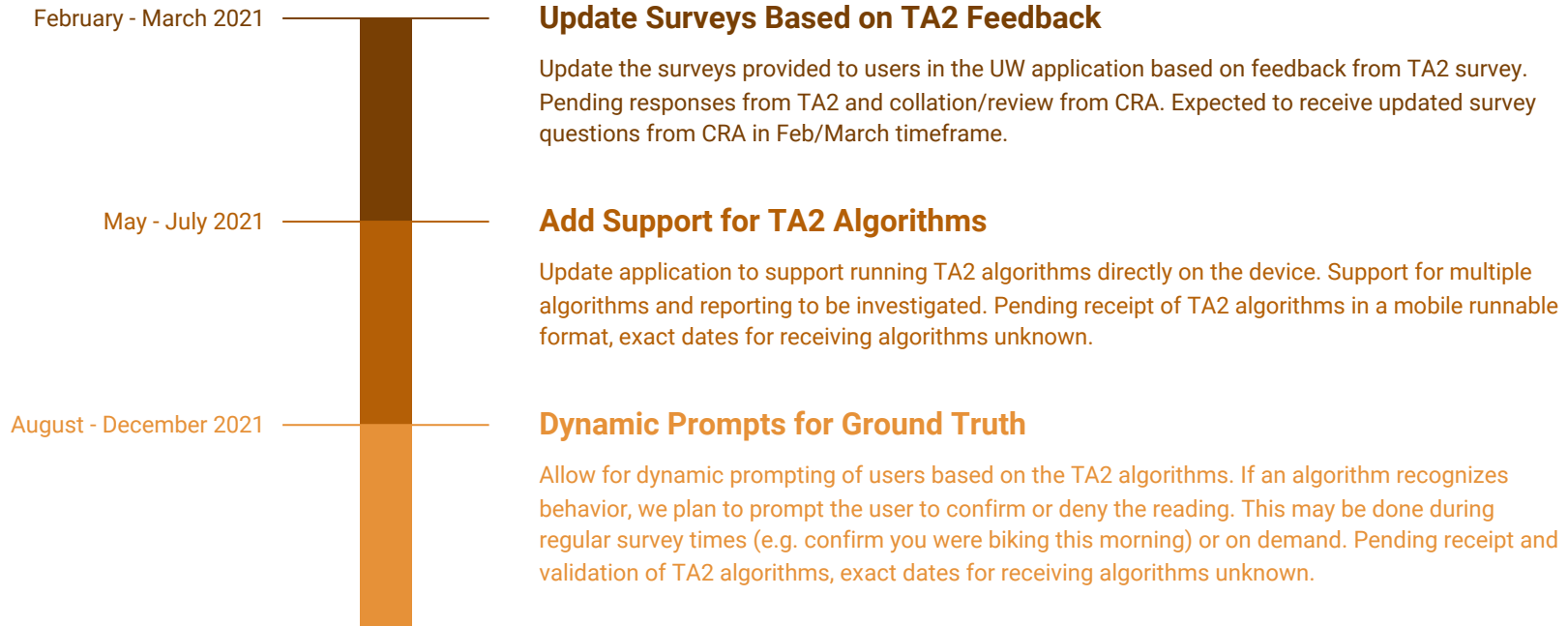
Revamp UI to use a chat-based main interface. Allow for grouping of users into defined categories (e.g. Age group, Activity level, Unit/Organization). Explore extending activity data with latest iOS libraries for sensor data collection.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

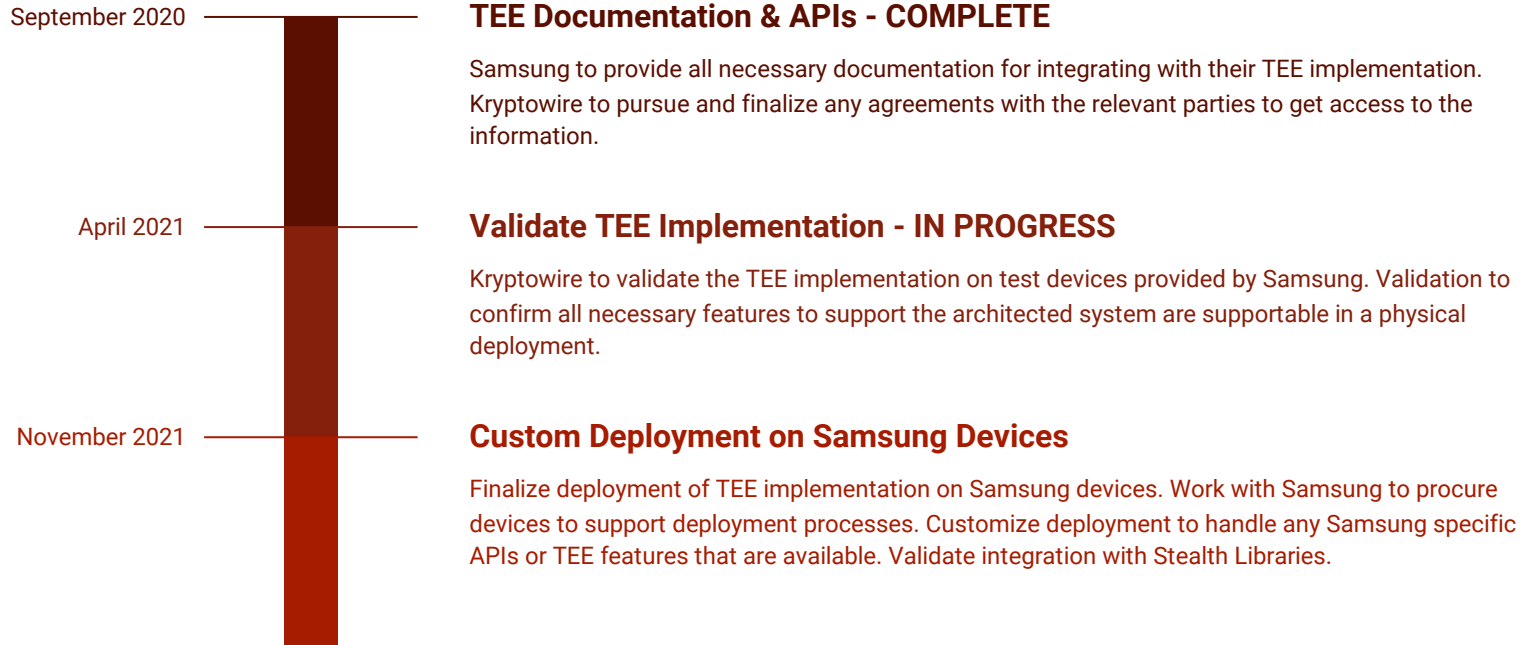
TA2 Algorithm Integration



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

TEE Roadmap



DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.



Thank you

Questions?

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

This presentation was assembled in part with funding from the Defense Advanced Research Projects Agency (DARPA).

The views, opinions and/or findings expressed are those of the author and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.