Behavioral Authentication for Mobile Devices

(or how to get-rid of the passwords/pins!)*

Angelos Stavrou

Kryptowire LLC & GMU

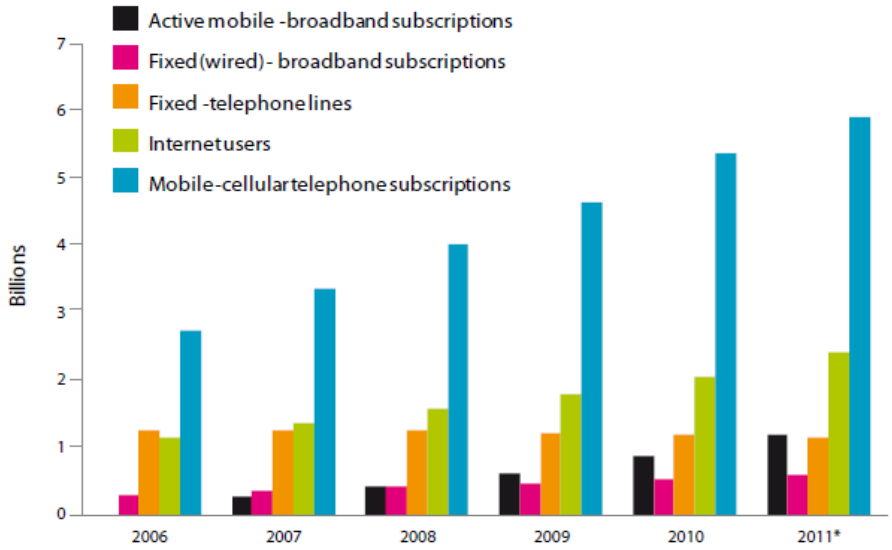
astavrou@kryptowire.com

*This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA). The views, opinions, and/or findings contained in this presentation are those of the presenter(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

kryptowire

Mobile Market Landscape

- After 125 Years, landlines surpassed by mobiles in 2002. 2006 landlines peaked at 1.3B. 2009 4.7B mobile users
- The Apple App Store, launched in 2008, reached 25 billion downloads as of March 2012 - 46 million per day
- With the growth smartphones and tablets, the app market reached roughly $5 billion worldwide in 2012
- 612M mobile phone users generating over $587Bn worth of financial transactions in 2011, $1Tr by 2016 (KPMG)



Note: * Estimate
Source: ITU World Telecommunication/ICT Indicators database

kryptowire

CIO Business Priorities

Top 10 CIO Business and Technology Priorities in 2012

Top 10 Business Priorities	Ranking	Top 10 Technology Priorities	Ranking
Increasing enterprise growth	1	Analytics and business intelligence	1
Attracting and retaining new customers	2	Mobile technologies	2
Reducing enterprise costs	3	Cloud computing (SaaS, IaaS, PaaS)	3
Creating new products and services (innovation)	4	Collaboration technologies (workflow)	4
Delivering operational results	5	Legacy modernization	5
Improving efficiency	6	IT management	6
Improving profitability (margins)	7	CRM	7
Attracting and retaining the workforce	8	ERP applications	8
Improving marketing and sales effectiveness	9	Security	9
Expanding into new markets and geographies	10	Virtualization	10

Source: Gartner Executive Programs (January 2012)

kryptowire

Traditional Device Concerns

Security Requirements

- Confidentiality
- Integrity
- Authenticity
- Availability
- Accountability
- Non Repudiation

Threats

- Eavesdropping
- Integrity
- Data Exfiltration
- Denial of Service
- Masquerading

Attacks

- Physical Attacks
- Application Attacks
- Telecommunications
- Infrastructure – App Store
- Supply Chain

Vulnerabilities

- Hardware
- Software
- OS
- Communication Protocols

kryptowire

Mobile & Smart Devices Risks

Assumptions

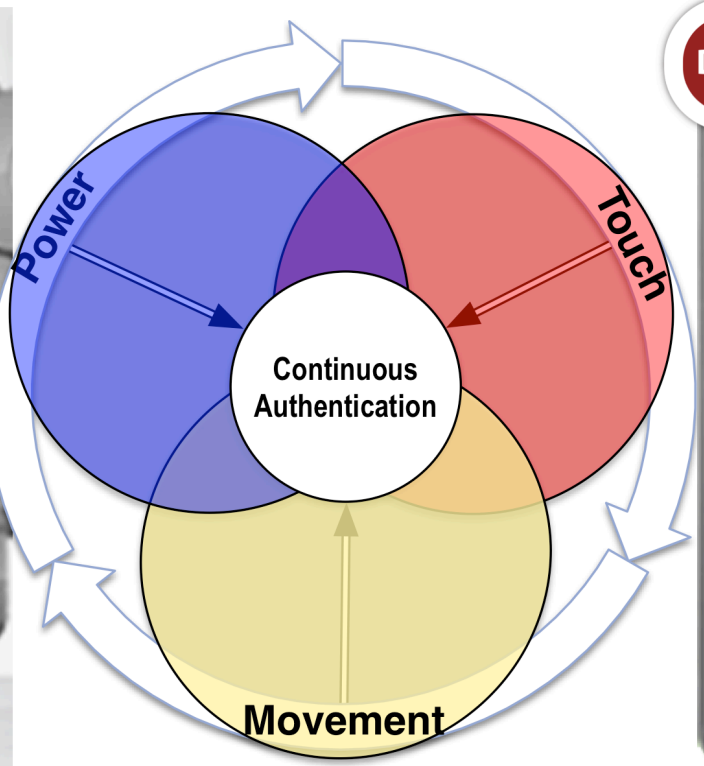
- Networked or Stand-alone Apps
- Public or Private Network
- Tethered or Untethered Synchronization
- Standard or Proprietary Protocols
- Ad Hoc Network or Base Station
- Configuration Management
- Classification Level of Data
- Connect back to DoD or IC Networks
- Interoperable with DoD or IC
- Federated or Enterprise Model

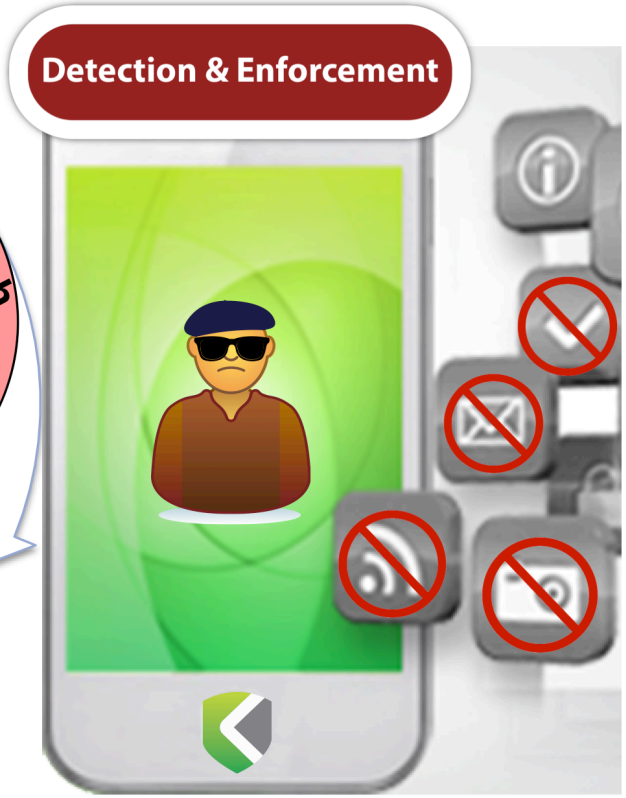
Threats

- Capture or loss of device
- Poor configuration management, administrative backdoor, automatic updates
- Eavesdropping wireless communications
- Infection from compromised PC during data synchronization
- Peer smart-phone attack or infection (via Bluetooth or WiFi)
- Attacks on Telecom Network - Base Station
- Malware - viruses, trojans, or worms spread the same way as PCs
- Location tracking
- Proper Device disposal – forensic tools
- DoS – Spam

kryptowire

Overall Approach





Capture & Profile User Activity

- ✓ Power consumption
- ✓ Touches, Gestures
- ✓ Movement (Gyroscope Accelerometer)

→ Analytics →

Authorization Based on Authentication

- ✧ Restrict Use of Apps
- ✧ Restrict Apps Access to Network
- ✧ Restrict Access to Files (View, Write)
- ✧ Restrict Use of Camera/Mic

kryptowire

Description of Mobile Biometrics

BIOMETRIC: Collect **power, touch, and movement** measurements while the user operates on mobile devices.

- Authentication Decision Engine for Authentication
  - Weights from all the biometric modalities
  - Current state of the device
  - User Activities
  - Existing profile/historical data

Biometric Identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
Power	H	H	M	H	M	H	L
Gyroscope	M	M	H	H	M	H	M
Touch-screen	H	M	M	H	M	H	L

Figure 1: Performance comparison of the proposed biometric modalities using the biometric metrics from Jain et al.

kryptowire

Project Key Objectives & Targets

Continuous active authentication for mobile devices

To achieve this, we set the following required targets:

- Profiling of Users
  - Generate accurate user profiles for energy consumption, touch, and movement in mobile devices
  - Leverage Information about the Application & Device Context
- Progressive Authentication & Safety
  - Establish a progressive permission model where a user has multiple access levels starting from non-authenticated to fully-authenticated
  - Prevent unauthorized users from disabling the collection and processing of data

kryptowire

Project Key Objectives & Targets

Continuous active authentication for mobile devices

To achieve this, we set the following required targets:

- Effectiveness & Accuracy
  - Evaluate each modality using volunteer participants both in a controlled laboratory setting and on their own by measuring the effectiveness of each biometric modality
  - Stress the system under different scenarios
- Be non-disruptive / Practical
  - Do not reduce the battery life of a device more than 5% for mobile phones and 3% for tablets. The end-goal is to reduce the impact to the battery lifetime to less than 1% for typical use cases
  - Trade-off between rate and type of measurements versus measurement precision and overall system robustness

kryptowire

Project Key Objectives & Targets

Continuous active authentication for mobile devices

To achieve this, we set the following required targets:

- Biometric Sensor Data & Profiling
  - Generate accurate user profiles for energy consumption, touch, and movement in mobile devices
  - Leverage Information about the Application & Device Context
- Current Status
  - We have successfully build the infrastructure to collect all biometric modalities
  - Create user Profiles using Application Context
    - We will show why this is vital for accuracy

kryptowire

Project Key Objectives & Targets (cont)

Continuous active authentication for mobile devices

- Effectiveness & Accuracy
  - Evaluate each modality using volunteer participants both in a controlled laboratory setting and on their own by measuring the effectiveness of each biometric modality
  - Stress the system under different scenarios
- Current Status
  - Setup Volunteer experiments (small scale, 5-10 users)
  - Collect Biometric data for following mobile applications: Chrome, Facebook, Google Maps, Camera, Listnote Speech/Text Notepad, Gmail
  - Create user Profiles using Application Context

kryptowire

Project Key Objectives & Targets

Continuous Active Authentication for mobile devices

- Progressive Authentication & Safety
  - Establish a progressive permission model where a user has multiple access levels starting from non-authenticated to fully-authenticated
  - Prevent unauthorized users from disabling the collection and processing of data
- Current Status
  - We have implemented an Android service for Policy Enforcement
    - Enforce policy device-wide or application specific
    - Can be integrated to the authentication system
    - Policy can change based on location, MDM, others
    - Restrict access to Files, Microphone, Camera, Network

kryptowire

Collecting & Analyzing Data

- We use the OS's touch driver to record measurements every microsecond
  - event_time, x_coord, y_coord, touch_area, pressure
- We use the SensorEventListener API to record accelerometer and gyroscope readings:
  - gyroscope x, y, z axes, accelerometer x, y, z axes
- We collect Power related measurements every 5 seconds:
  - Voltage, Current, Battery Charge, CPU usage, CPU frequency, Display brightness, Wi-Fi uplink bytes, Wi-Fi downlink bytes, Memory, Audio state, GPS state

kryptowire

Collecting & Analyzing Data

Touch records:

- duration, distance, direction, avg_touch_area, avg_pressure

Gyro records:

- gyroscope x, y, z axes, accelerometer x, y, z axes.

Power records

- We use the power consumed by the app in the last 5 seconds to form a time-series

kryptowire

Collecting & Analyzing Data

- We collect two sets of data per user, app, and modality (touch, gyro, power)
- One of the sets is used to establish a baseline Machine Learning model
- The other is used to test
  - We cross-test every user against every baseline (NxN tests)
  - The results of these tests are binary: 'You are the same user,' 'You are not.'

kryptowire

Training & Testing

Touch and Gyro data:

- For every record in the test set we calculate its strangeness (uniqueness), again, as the sum of distances to baseline records
- We find the place of the test record in the sample distribution of strangeness
  - If it is on the tail (determined by a confidence level), we call the record an anomaly
  - We register the fraction of anomalies in the test set as the probability of the user committing an anomaly

kryptowire

Training & Testing

Touch and Gyro data:

- We employ a method that builds a baseline of uniqueness measures for each record in the training set
- Uniqueness (strangeness) is, in our case, measured as the sum of (Euclidian) distances to the record's *k* (3) nearest neighbors (low sensitivity to changes on *k*)
- The sorted baseline of strangeness (sample distribution) measurements becomes the model

kryptowire

Methods for Touch & Gyro

- This renders a matrix that looks as follows:

Baseline				
Tested against		U1	U2	U3
	U1	0.1057	0.5999	0.4756
	U2	0.2300	0.09	0.5899
	U3	0.3334	0.456	0.1529

- Every entry represents the probability of committing an anomaly for the corresponding pair of baseline/ test sets (E.g., the probability of an anomaly for the baseline of U2 and the test of U3 is 0.456).

kryptowire

Methods for Touch & Gyro

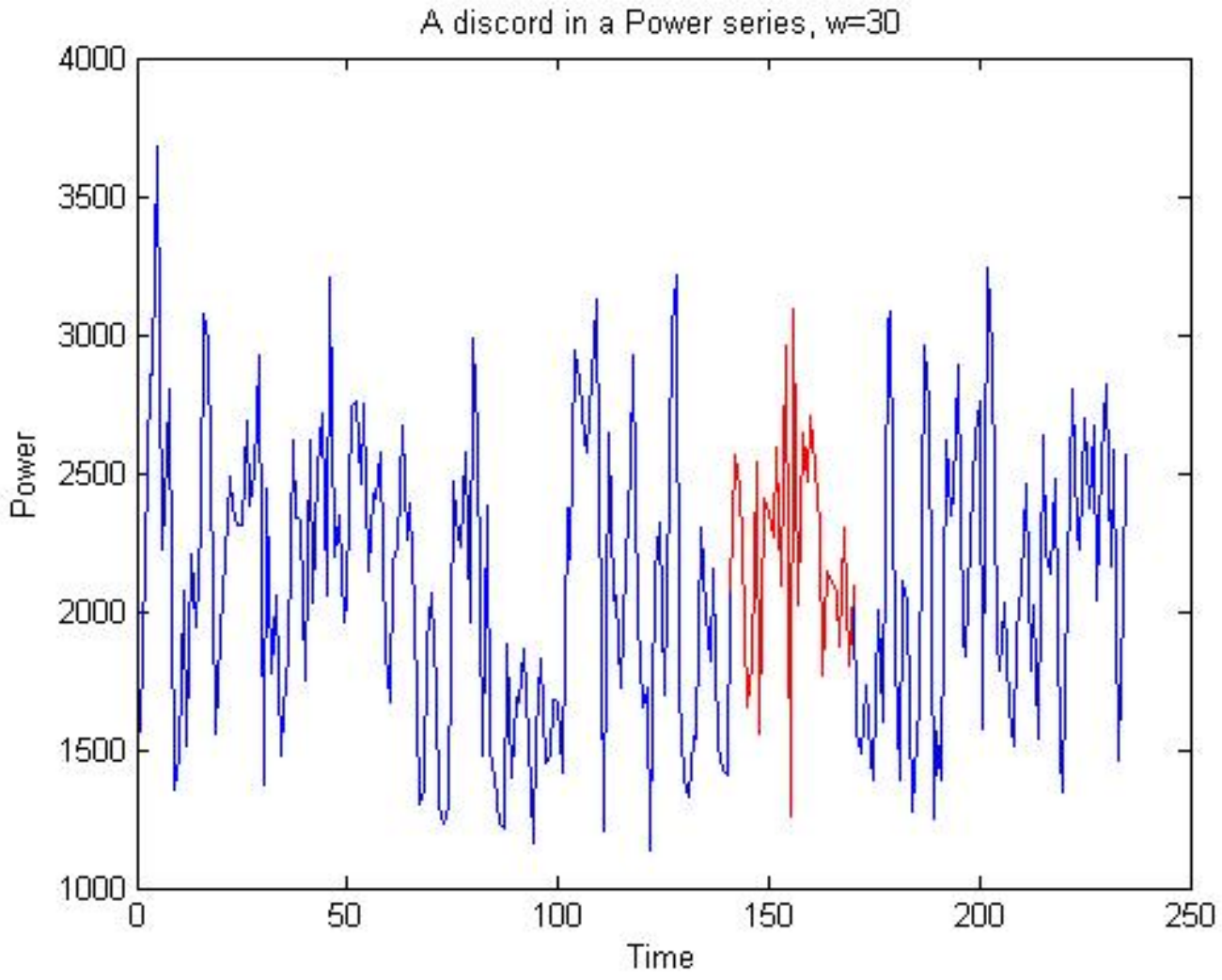
- Using this matrix, we can sweep a threshold (from 0 to 1) and diagnose as a positive every entry whose value is bigger than the threshold
  - If the positive occurs in the diagonal, it is a False Positive (the model is saying the user is not who she says she is, while the truth says otherwise).
  - If the positive occurs in the off-diagonal, it is a True Positive (the model is correctly saying this user is different than that of the baseline
- Doing this, we can compute for each value of the threshold a False Positive Rate, and a True Positive Rate, and plot the Receiving Operating Characteristic of the model for this data

kryptowire

Methods for Power

- Both the training (baseline) set and the test set are time-series
- We use a method that finds the biggest discord in a time series:
  - The biggest discord is the sub-series of size *w* whose distance to the nearest neighbor sub-series is the largest

Example of a Power discord

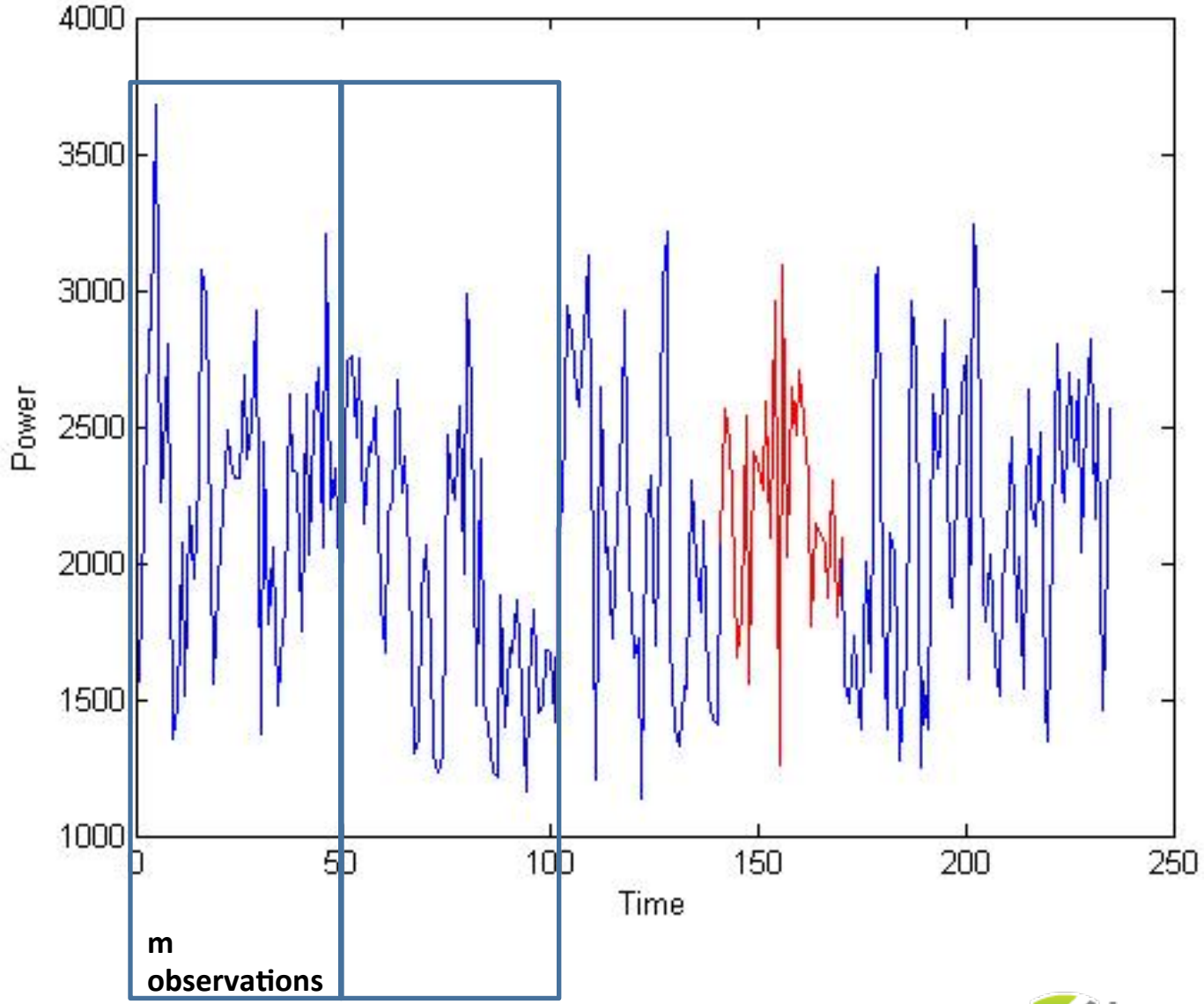


kryptowire

Method for Power

- We build a model with the distances of discords found by rolling a window of size
- We append the window to the first m observations of the power series

Methods for Power



kryptowire

Methods for Power

- We use the window of *m* observations in the baseline and append to it (rolling) windows of size Δ taken from the test set
- For each window, we also compute the distance of the biggest discord
- We are now left with two distributions of distances (baseline and test)
- We compare them using the two-sample Kolmogorov-Smirnov test
  - The test outputs a diagnosis, given a confidence level (0 if the null-hypothesis –the two distributions are the same- cannot be rejected, 1 if it can)
  - We use this diagnosis as the test result.

kryptowire

Ensemble of the Modalities

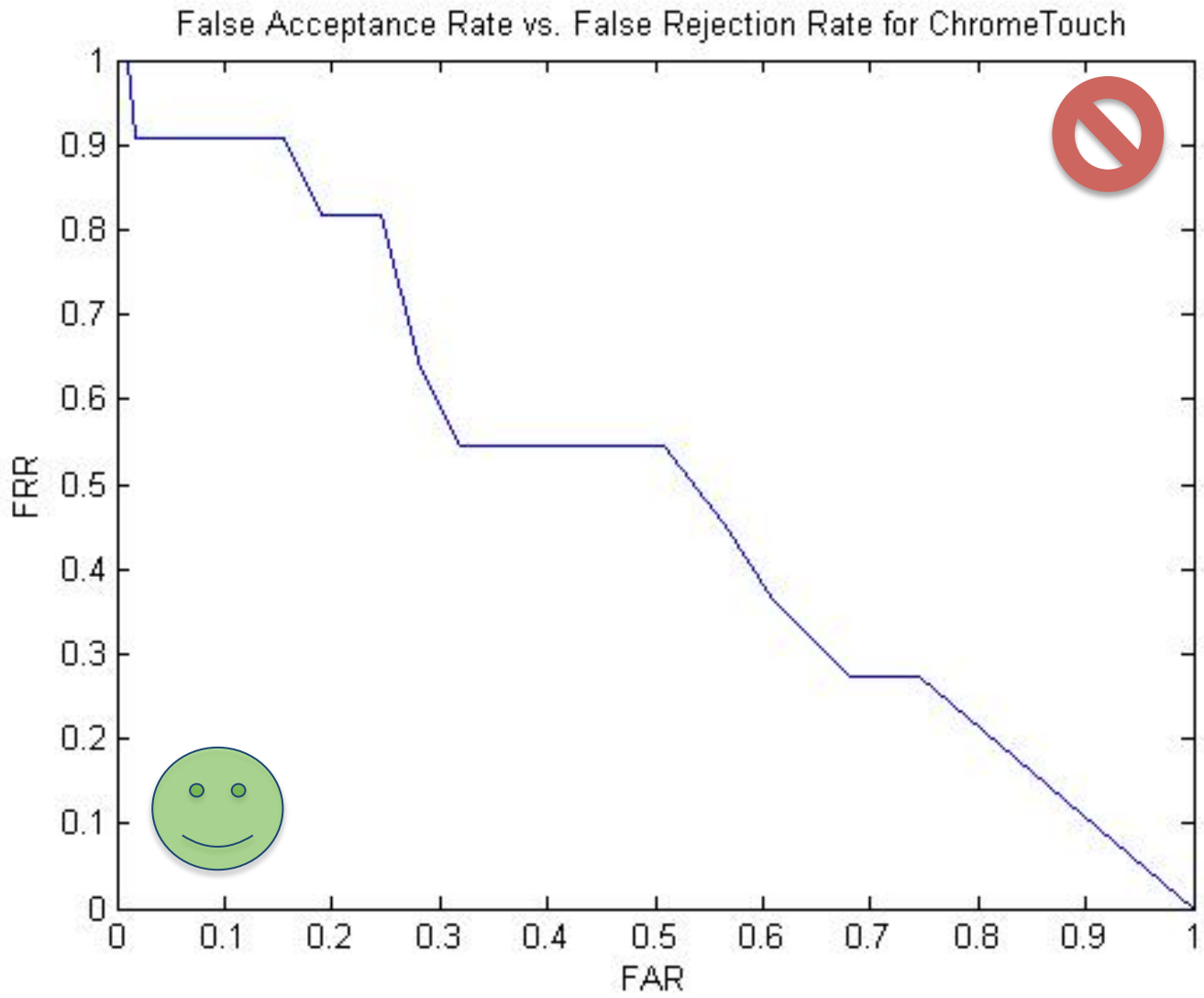
- We build an ensemble of the three methods (per app)
  - Each method votes on the test (baseline vs. test data)
  - If two or more positive votes are collected, the result is considered a positive (either a FP or a TP)
  - We build the ROC curve for the ensemble

kryptowire

Experimental Results

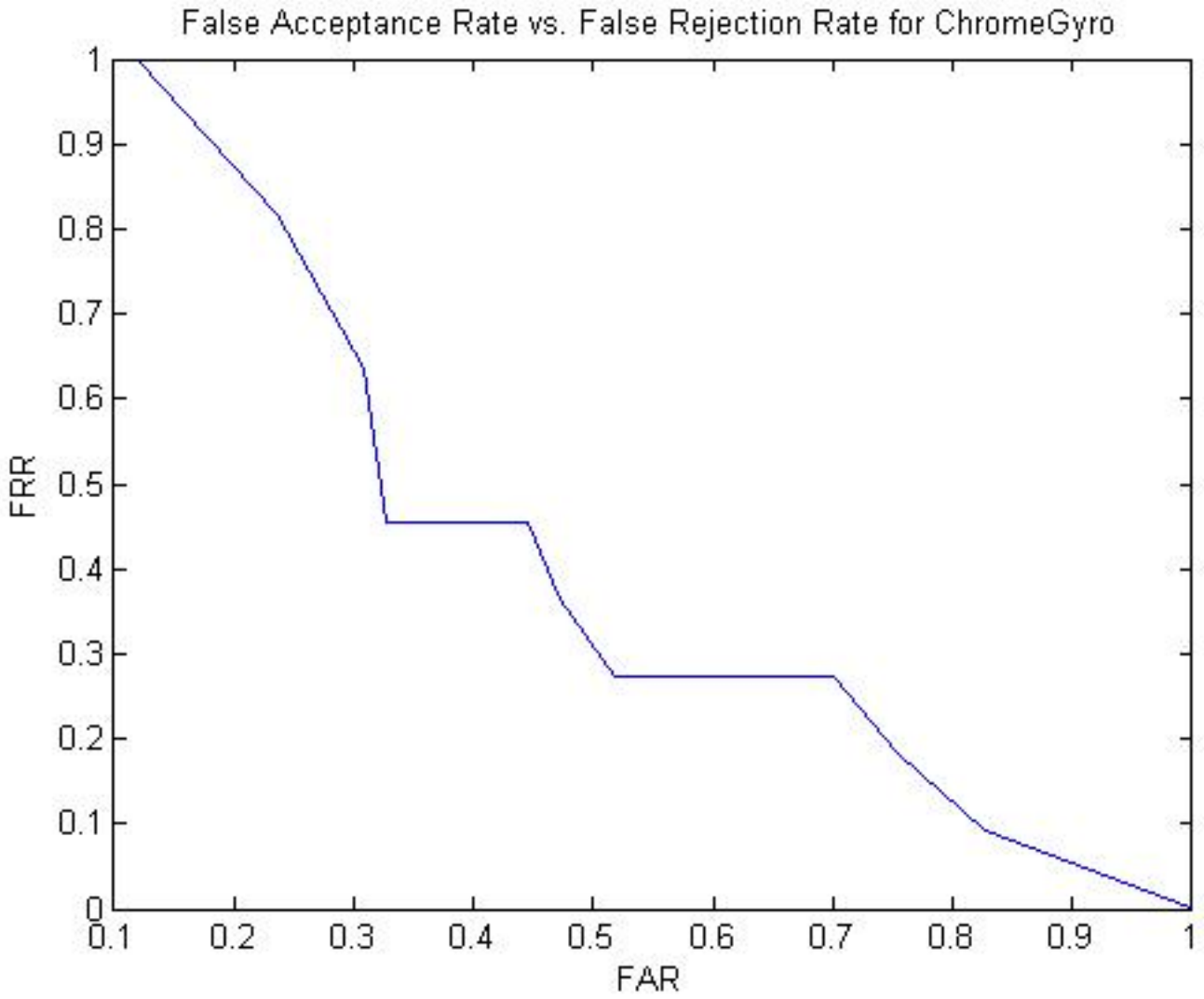
- In what follows we present:
  - ROC curves for each modality, and app (separately)
  - ROC curves for the app and modality when we ensemble the methods
- For Power discord method
  - m=50, w=30
  - Training time 20 minutes

ROC, Chrome, Touch modality

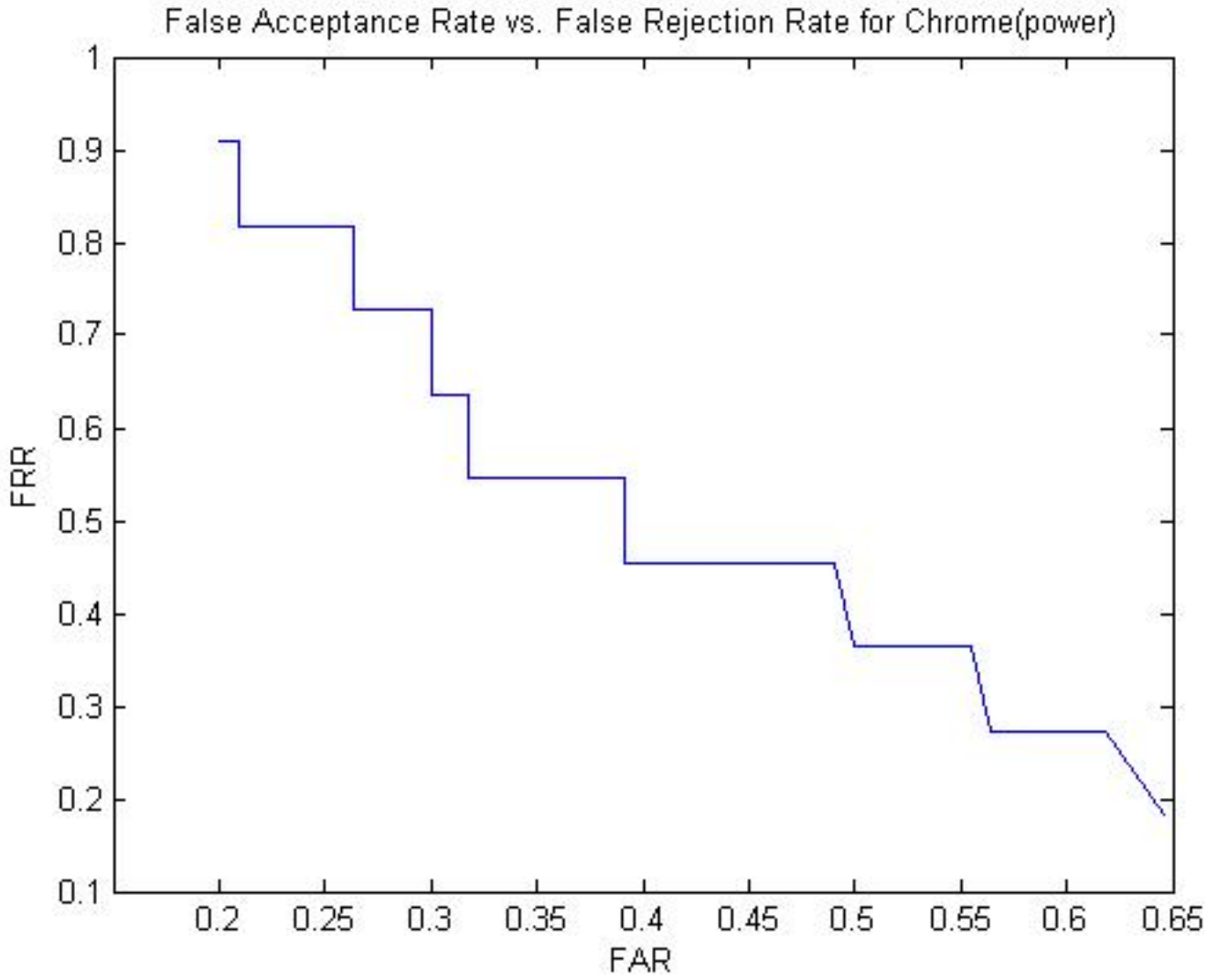


kryptowire

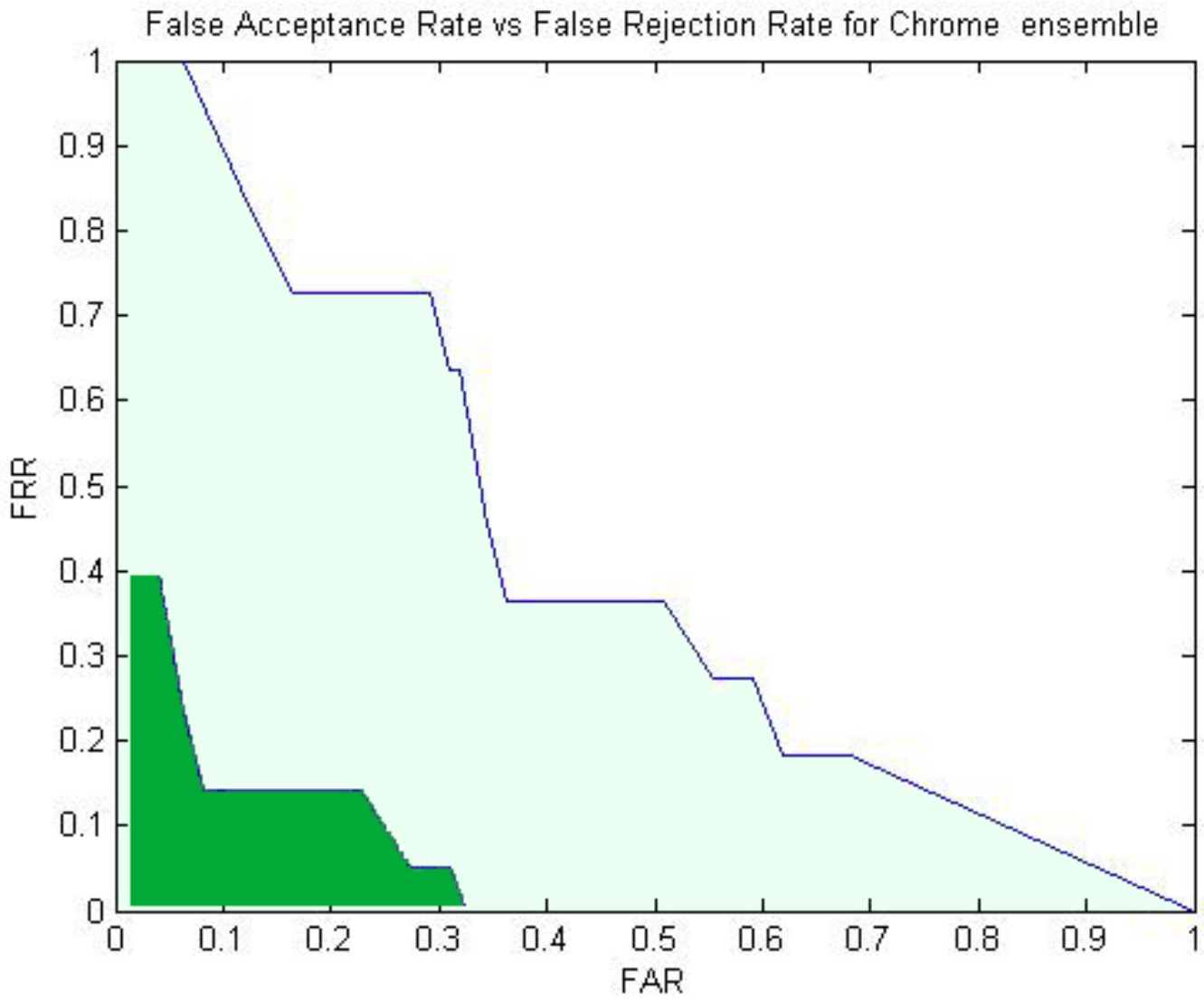
ROC, Chrome, Gyro modality



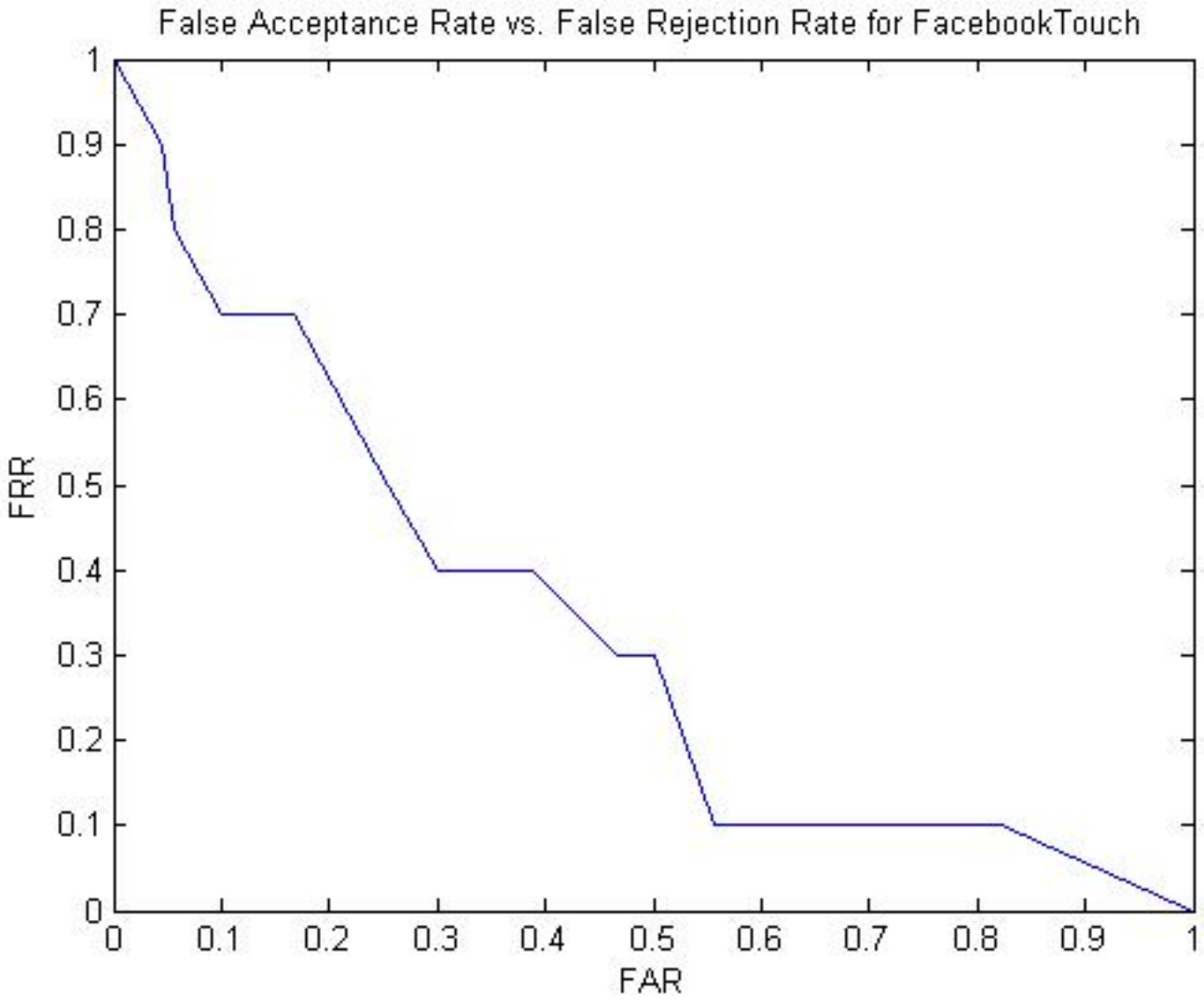
ROC, Chrome, Power modality



ROC, Chrome Ensemble

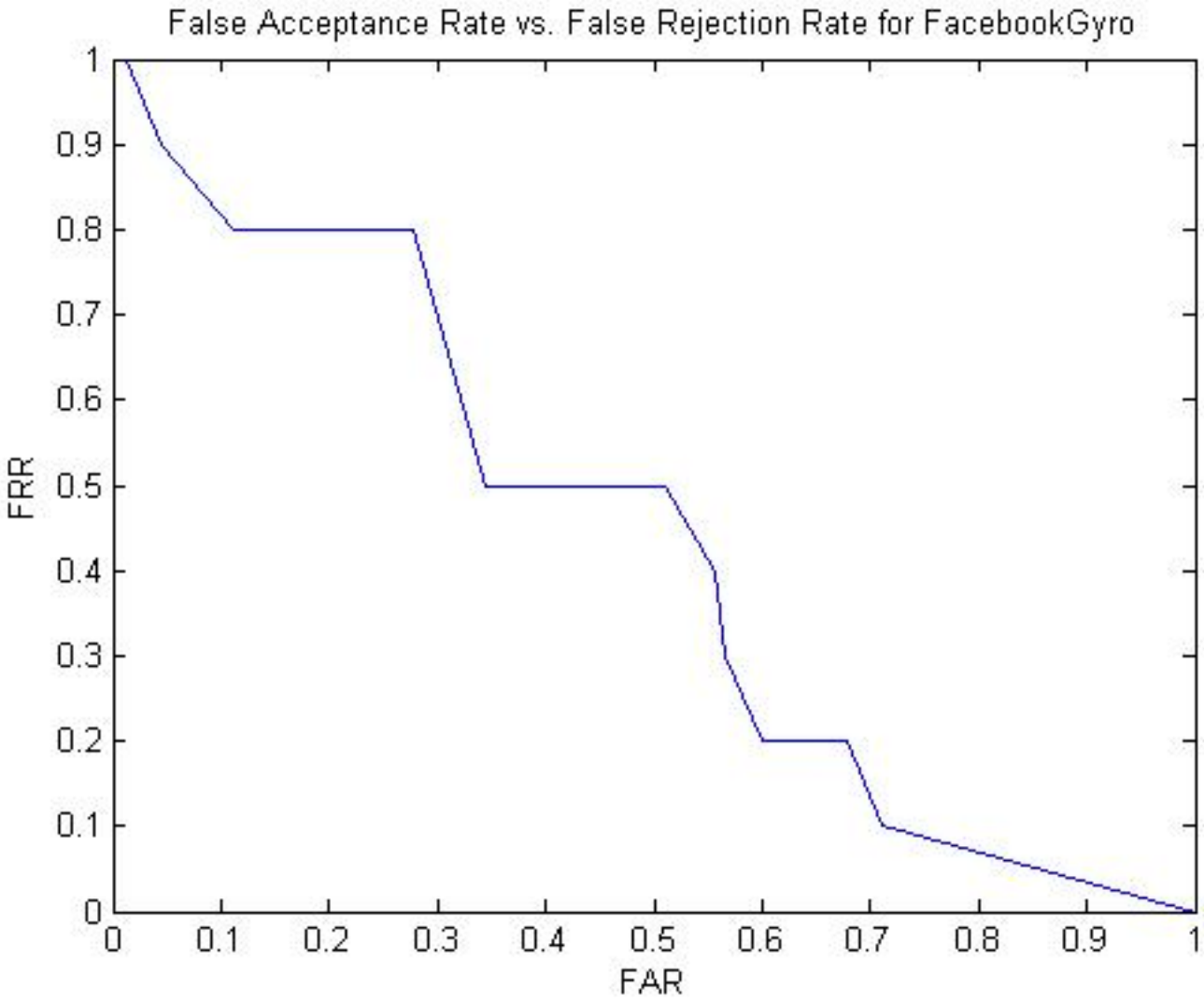


ROC, Facebook, Touch modality

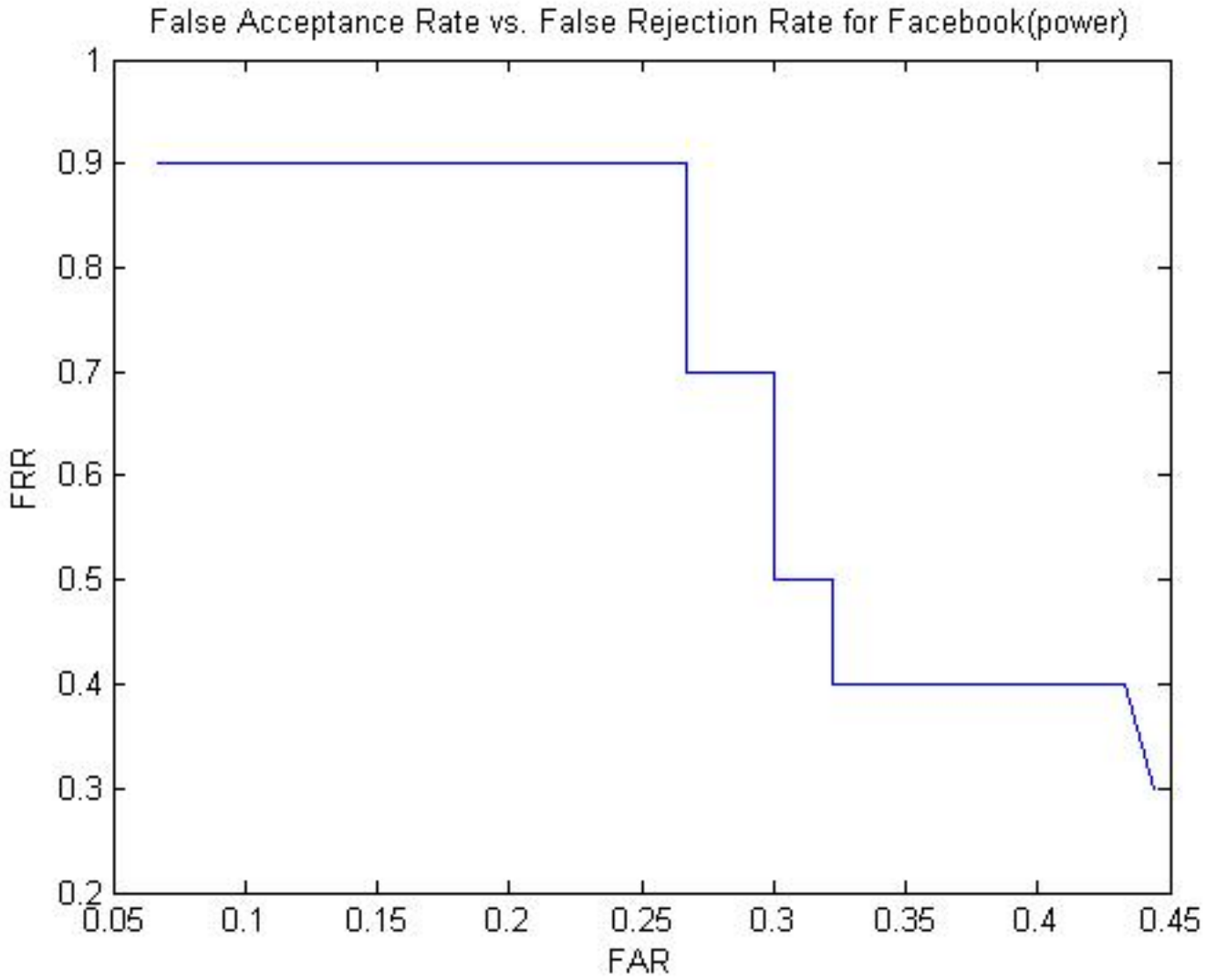


kryptowire

ROC, Facebook, Gyro modality

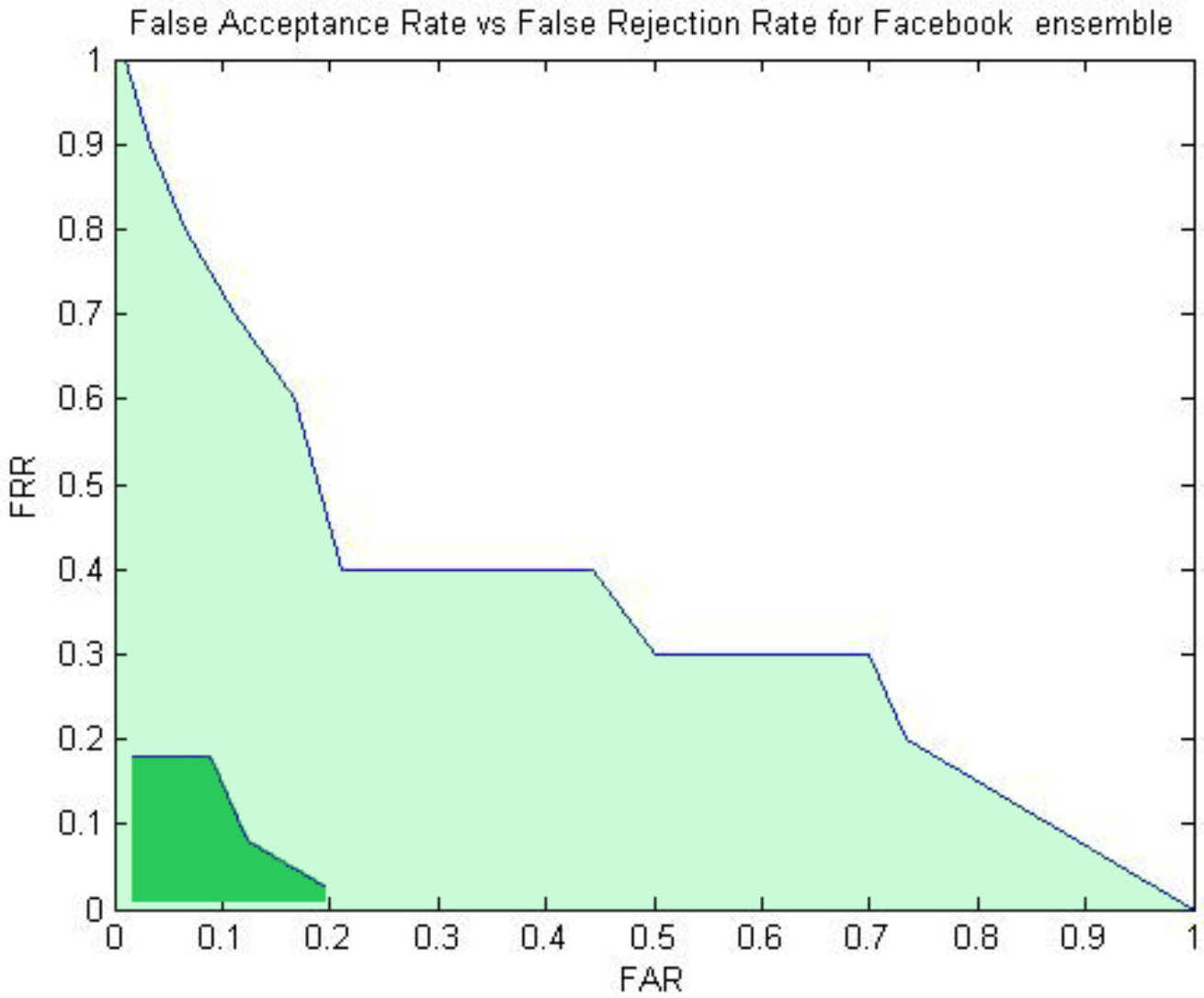


ROC, Facebook, Power modality



kryptowire

ROC, Facebook Ensemble



kryptowire

User Profiling & Testing Results

Touch/Movement vs Touch

- Touch Data show authentication can be achieved in few minutes for specific apps

- **Results depend on the Application context**
  - Apps that have completely randomized UI have false negatives!
    - Google Maps
  - Apps that have completely static UI can have false positives!
    - Camera, Microphone apps
  - Apps that have a mix of UI inputs yield the best results for Authentication
    - Chrome, Gmail, Word editors

kryptowire

User Profiling & Testing Results

Authentication Accuracy is affected by

- Duration, time and condition of training data
- How the user operates and handles the device
- Application Context
- Fusion and Penalty algorithms

- **Results depend on the Application context**
  - Apps that have completely randomized UI have false negatives!
    - Google Maps
  - Apps that have completely static UI can have false positives!
    - Camera, Microphone apps
  - Apps that have a mix of UI inputs yield the best results for Authentication
    - Chrome, Gmail, Word editors

kryptowire

User Profiling & Testing Results

Touch/Movement vs Power vs Gyro

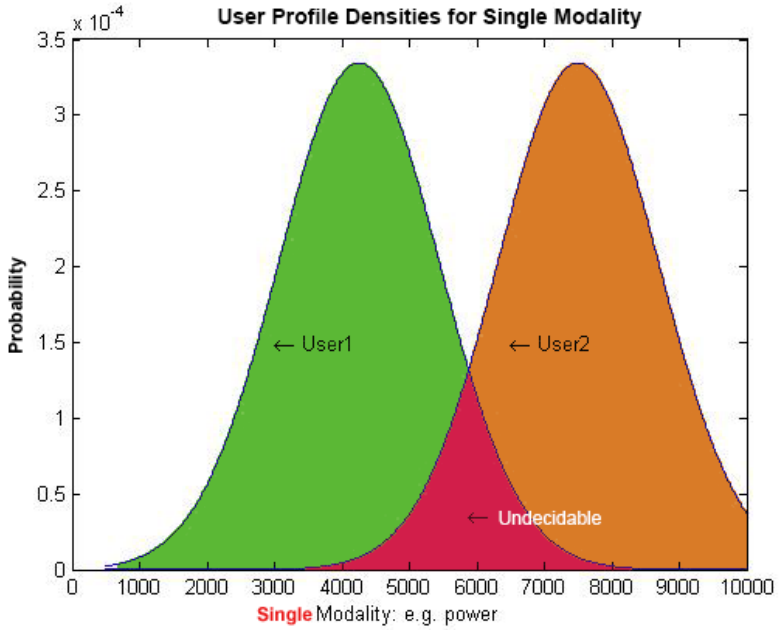
- Power Requires longer training data (>20 minutes)
  - Experiments show that for 20 minute data collection is borderline for good results, we do however get fairly good results for >20 minutes
  - Expectation that can be used as a secondary/support modality
- More and Longer Volunteer Experiments
  - We are currently running longer experiments
  - Having a more detailed model with subsystems
  - Integration of multiple modalities in progress

kryptowire

Next Steps & Conclusion

- We believe that longer training sessions will increase accuracy for **some modalities**
  - **Not all modalities are monotonically increase in terms of accuracy (Individual Gyro measurements for instance)**
- Leverage the application transitions as an additional modality
  - How much time you spend on an app is user dependent
  - Which set of apps you use and how you pass from one to the other
- Integration of Authentication and Authorization
  - Demonstrate the End-to-End Authentication to Policy/Resource Enforcement capabilities
  - Use Case studies (Email, Notes, Maps)

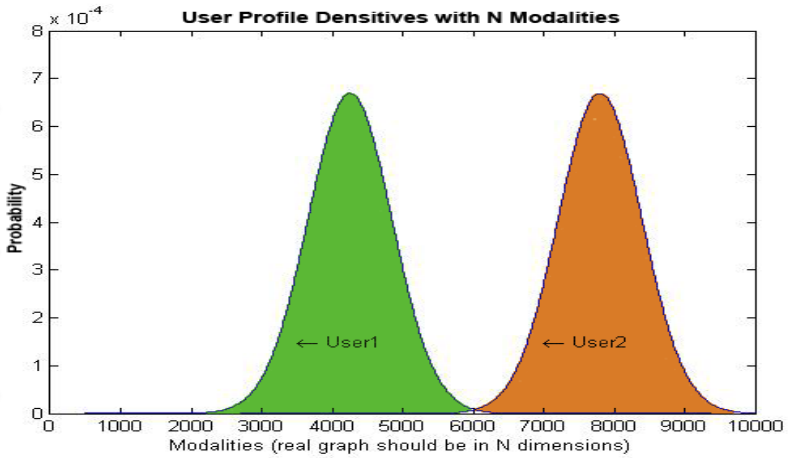
kryptowire

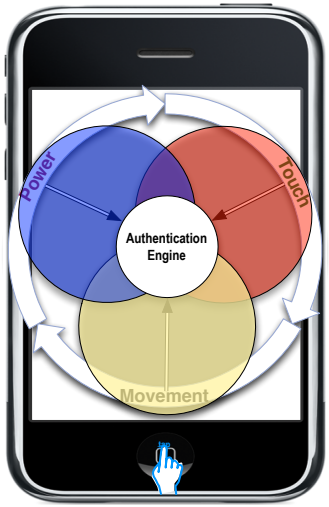


Training & Data Collection

Profile Generation

Policy Enforcement





System-wide Policy Enforcement for Critical Resources Authenticated Access

Files

Camera

Microphone

Network

Experimental Setup

Small scale experiments with 10 participants to complete four 60-minute Sessions. Devices collecting data from Mobile Phone Usage for power, touchscreen, accelerometer and gyroscope in context with the application being used

The data collection is being focused on the following mobile applications: Chrome, Facebook, Google Maps, Camera, Listnote Speech/Text Notepad, Gmail.

In additional experiments subjects are asked to perform tasks within given amount of time or are being distracted while using the device

Experiment Results

- ✓ Continuously train and separate usage between individual Mobile Users of real-time application usage **depending on the application and user characteristics**
- ✓ Without the application context, error rate increases dramatically
- ✓ Show that without multiple modalities, false positives are prohibitively high for small sliding windows of time

kryptowire

Thank you!

Questions ?

kryptowire