Active Authentication: Search Behavior and Decoy Technology The RUU Project (Are You You?)

Salvatore J Stolfo and Jonathan Voris
Allure Security Technology, Inc.
Malek Ben Salem
Accenture

Active Authentication PI Meeting

October 2014

This research was developed with funding from the Defense Advanced Research Projects Agency (DARPA).

Allure Security Technology - Agenda

- Desktop
  - RUU Sensor Status
- Mobile
  - Decoy Apps
  - mRUU Status

Allure Security Technology - Stolfo Decoy/RUU Patents

- 2 Patents Issued to Columbia University and Exclusively Licensed to Allure Security Technology
  - US 8528091 B2 – September 3, 2013
  - US 8769684 B2 – July 1, 2014
- 1 Notice of Allowance

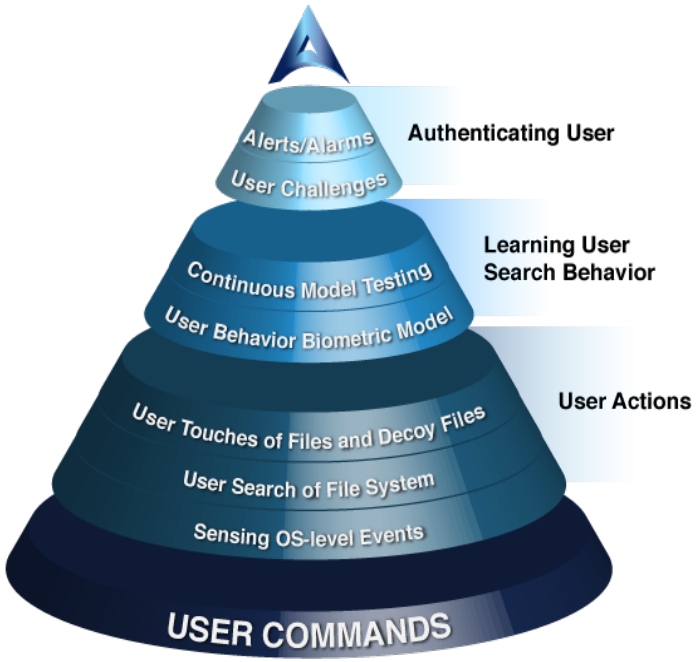
Phase 2

Desktop

RUU Sensor Overview and Prior Results

OS and file activity profiles combined with decoy touches

Active Authentication Methodology



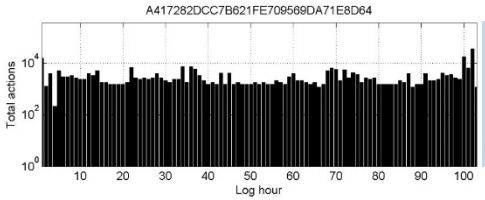
Experiment Results

- ✓ **68%** detection at 1% FP rate
- ✓ **73%** detection at 2% FP rate
- ✓ **95%** chance of detecting a malicious session within 15 minutes with one false positive per 40 hour work week

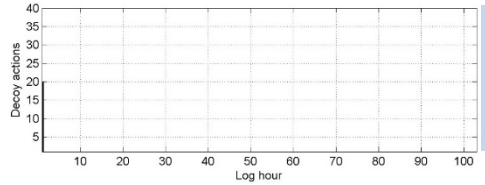
Experiment

160 user participated in long term study of legitimate user activity for one week on average

Action Profile of a Legitimate User

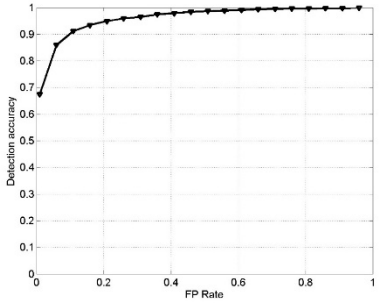


Number of total actions



Number of decoy touch actions

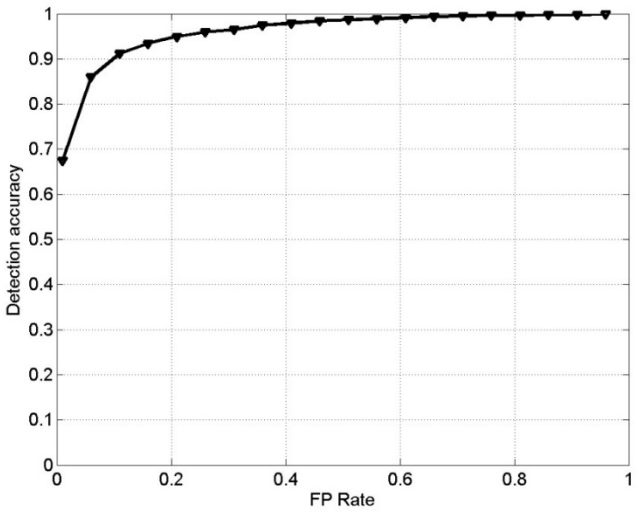
22 users participated in 15 minute simulated masquerader study



Masquerader Detection ROC Curve

RUU Detection Accuracy

OS and file activity profiles combined with decoy touches



Time until detection (TTD) given evaluation frequency for a 40-hour work week.

Frequency	Total Samples	FP Req.	Acc.	Evals	TTD
1m	2400	0.042%	49.55%	5	5m
2m	1200	0.083%	50.29%	5	10m
3m	800	0.125%	51.46%	5	15m
4m	600	0.167%	53.11%	4	16m
5m	480	0.208%	54.00%	4	20m

- Evaluation interval: 3 minutes
- Active authentication corresponds to Bernoulli trial: Probability that masquerader evades detection in 5 consecutive evaluations is less than 5%.
- **Detection within 15 minutes with 95% confidence**

Experiment

Overall Average Attacker Detection Across All Users

160 Users

1 week average capture period

Experiment Results

- 73% detection accuracy at 2% false positive rate
- Constraint: 1 FP per 40 hour work week
  - Fifteen minutes until detection with 95% confidence

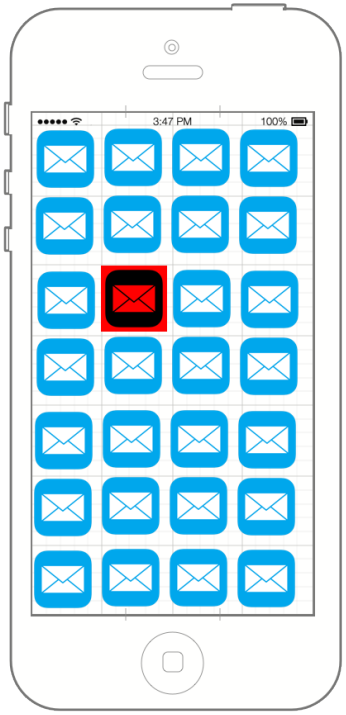
mRUU

Mobile

Decoy Apps – Notional View of Decoy App Concept

Integration of User App Behavior Model and Decoy Apps

Decoy Apps



27x **Decoy Mail App**

1x **The Real App**

User Study

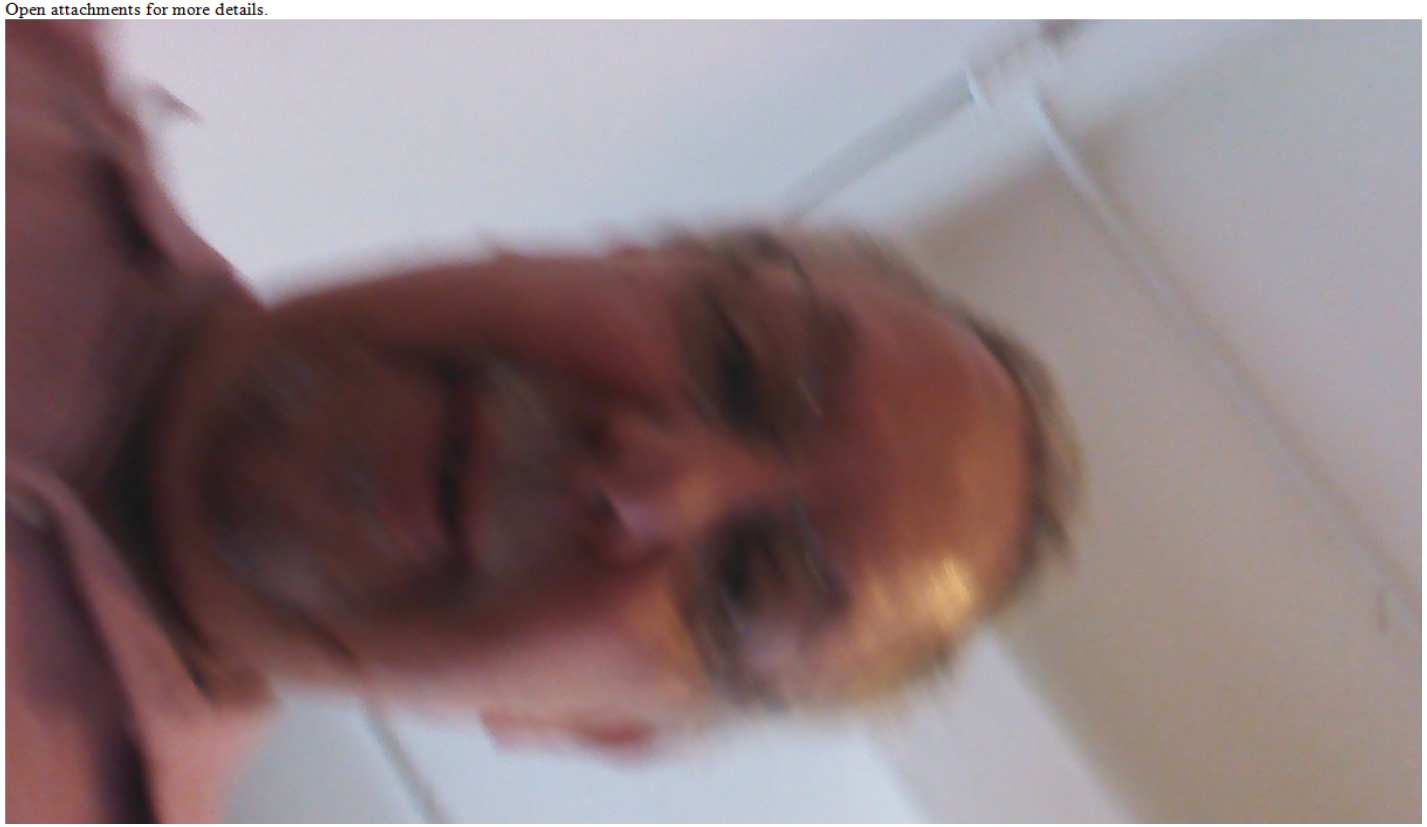
- IRB-approved Pilot study performed with preliminary Activity Collector
  - Users gathered from Accenture and Columbia University
  - Used to inform modeling approach
- Full scale user study in July-August 2014
  - 53 Accenture users

mRUU Mitigation Strategy
Experimentation

Sample Beacon Email Alert

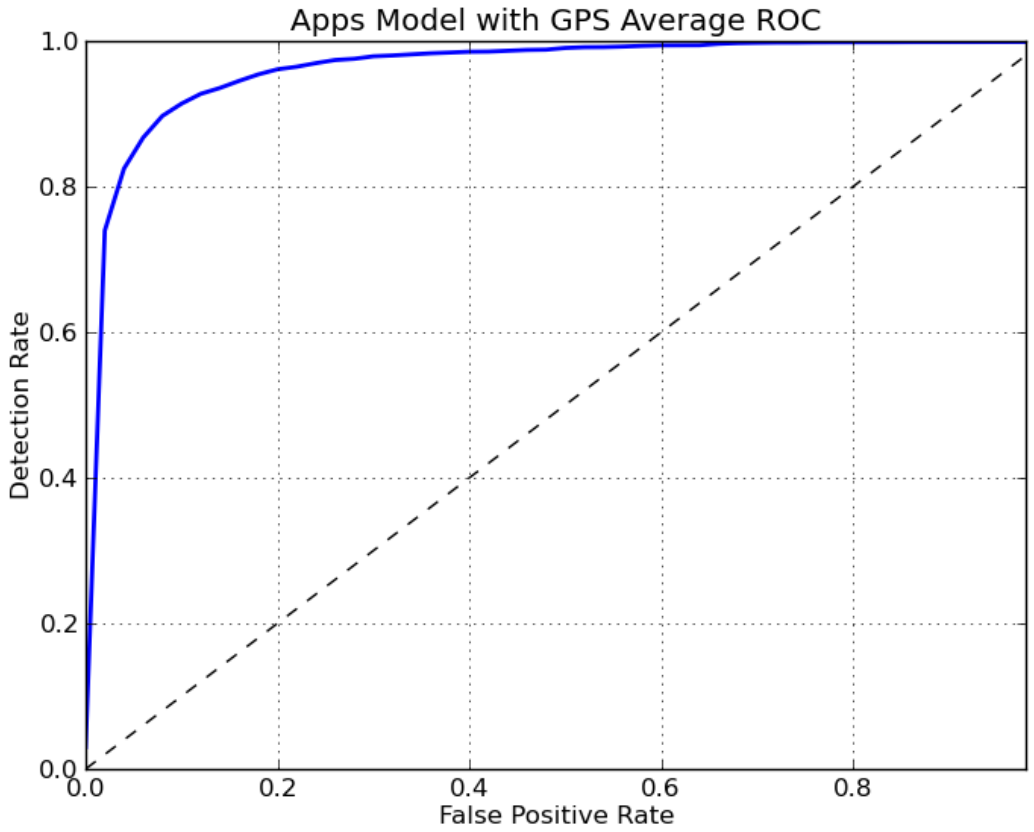
From: rapd.cn@gmail.com
Subject: Beacon Activated
Date: June 16, 2014 at 11:27:37 AM EDT
To: sal@alluresecurity.com

Somebody at /172.18.0.215 has accessed your beaconized application.
Open attachments for more details.



User Study Results

- 10 minute TTD with a operational FP rate of 1 per day



Application Usage Model ROC Curve

Thank you!