DECOY APPLICATIONS FOR CONTINUOUS AUTHENTICATION ON MOBILE DEVICES

WAY Workshop
July 9th, 2014

Malek Ben Salem
Accenture Technology Labs

Jonathan Voris and Salvatore J. Stolfo
Allure Security Technology

This material is based on work supported by the Defense Advanced Research Projects Agency (DARPA) through the Active Authentication II Program with contract award number FA8750-13-C-0259. The views expressed are those of the author(s) and do not reflect the official policy or position of the Department of Defense or the U.S. Government. Approved for Public Release, Distribution Unlimited.

Problem Statement

- Mobile devices carry a lot of sensitive information.
- Their small size, light weight, and ubiquity makes them easily stolen.
- Authentication on these devices is vulnerable to smudge attacks [1].

The Cloud Security Alliance rates data loss from lost or stolen mobile devices as the single largest threat to mobile computing [5].

- Security solution requirements in a mobile context
  - Resource efficiency
  - Usability
  - Low deployment costs
  - Compatibility with a variety of platforms

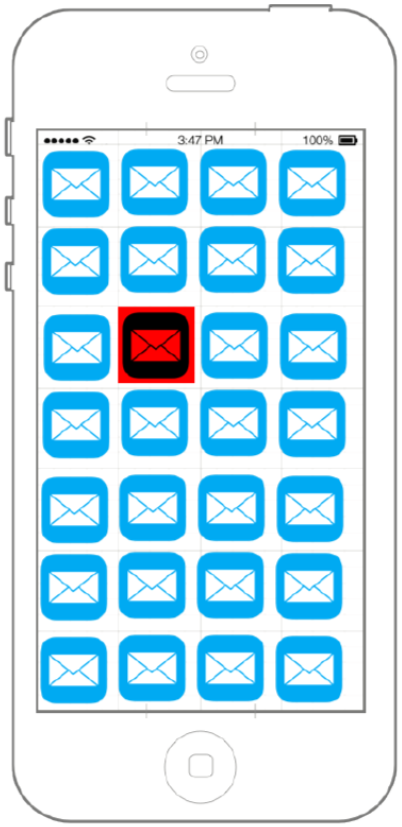
CONTINUOUS AUTHENTICATION USING DECOY APPS

- **Proposed approach:** Monitor access to decoy apps and use it to (de-) authenticate users once the user is logged in
  - Honeyfiles have been shown to be very effective at detecting masquerade activities on desktops [2].

- **Decoy apps**
  - Authentic-looking apps that hold fake but enticing information to the adversary.
  - Their only function is to act as bait to the masquerader.

- **Threat model**
  - Adversary is logged-in to device.
  - Adversary may know that decoy apps are loaded on device, but would lack the user's knowledge of which apps are real or decoys.

A Notional Decoy App Screen Layout



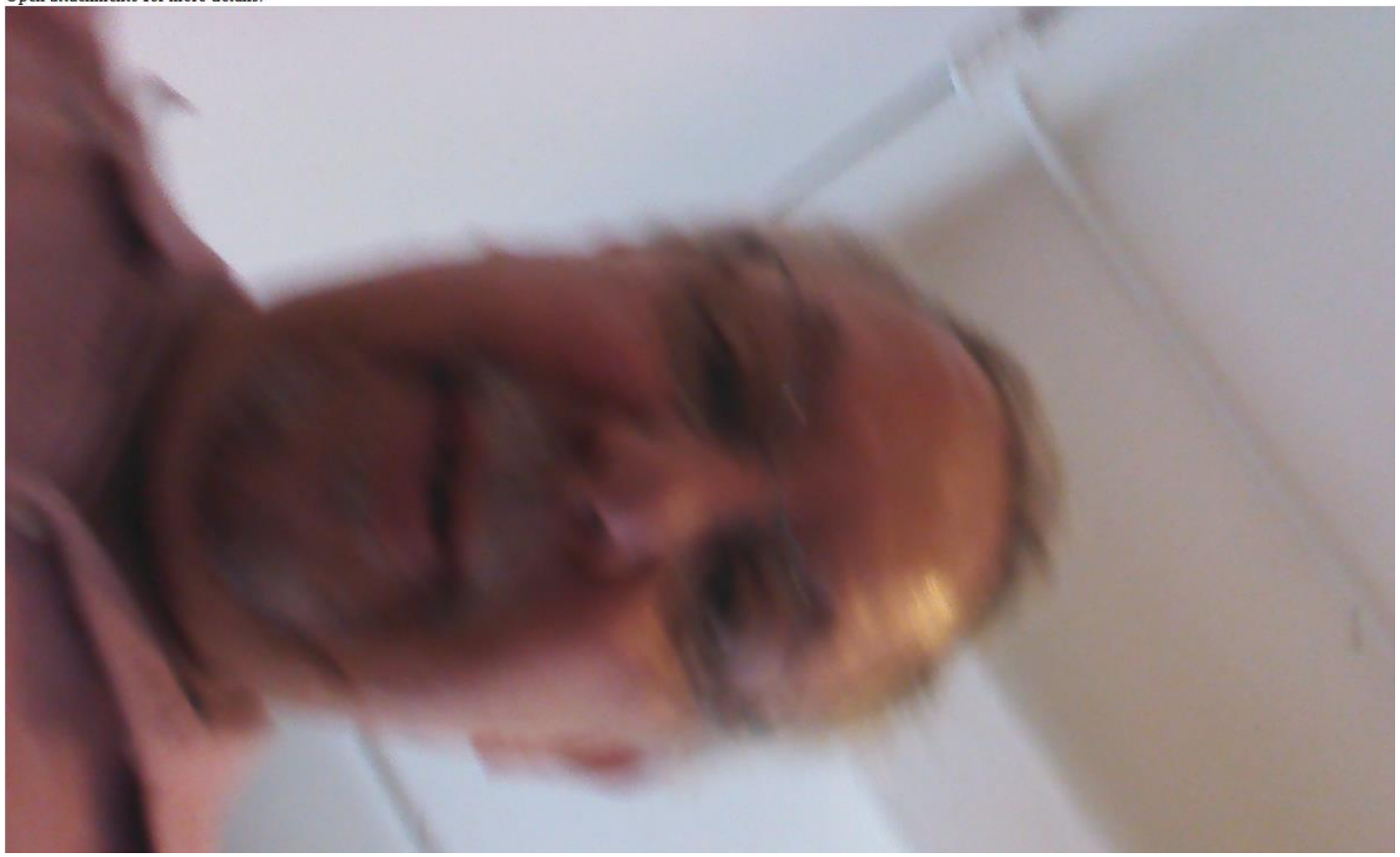
27x Decoy Mail App

1x The Real App

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.



Decoy App Generation and Installation

Manual

- Program specific fake applications which contain spurious data and issue alerts when accessed.
- Example: Decoy e-mail or banking applications could be planted on a device and seeded with realistic but inauthentic transaction information.
- Pros/Cons:
  - Produces believable applications
  - Time consuming if many varied decoys are needed.

Automated

- Transform seldom used applications into decoys by injecting existing programs with beaconing functionality
- If an organization utilizes device client security monitoring software, another option is to leverage this platform to “tag” applications as decoys.
- Pros/Cons:
  - These techniques scale much more easily
  - Require additional effort in terms of application monitoring and analysis.
  - Variability of decoy apps and their fake information is critical.

Usability

- Ease of deployment
  - Centralized or decentralized
- Expected low error rate
- Mitigation strategies
  - Mitigation strategies play a prominent role in further reducing errors:
    - E.g. challenging the user when a decoy app is touched
    - Incorporating other modalities for authentication as a challenge
      - Image or voice verification
      - Swiping a digital pattern image using a mouse or touchscreen.
- Mobile users' attitude towards security
  - Users constantly reminded about security
    - E.g. phone locks after a few minutes of no user activity.
    - Getting alerts from credit card companies for suspicious transactions.

Even if an authentic user gets alerted by error, this will remind the user that they are protected and that their security protection works.

Costs of Decoy Apps

- Costs of infrastructure
  - May be deployed to a range of devices with minimal user interaction or administrator involvement with a distribution service.
  - No consistent upkeep and monitoring required
    - Easily monitored for access
    - Contents can be periodically refreshed with little transmission overhead.
- Resource Costs
  - Little computational power and battery power: no work aside from triggering an alarm.
  - Small footprint:
    - A typical Android app consumes several megabytes only of storage capacity.
    - A limited number of highly attractive and conspicuous decoy apps will be needed to detect an attacker's intrusion

Conclusion

- Decoy applications
  - Are a natural (de-) authentication solution for mobile platforms when a phone is lost or stolen.
  - Are easily integrated with other mobile security mechanisms.
  - Incur little monitoring overhead.
  - Are generating efficiently and flexibly
  - Are lightweight and resource-friendly
- Future work:
  - Assess the efficacy of decoy applications (error rates measured in a IRB-approved user study)
  - Identify best practices for decoy application design, placement, and distribution.
  - Evaluate various mitigation strategies

References

[1] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. In Proceedings of the 4th USENIX Conference on Offensive Technologies, WOOT'10, pp. 1--7, Berkeley, CA, USA, 2010. USENIX Association.

[2] M. Ben-Salem and S. J. Stolfo. Decoy document deployment for effective masquerade attack detection. In Proceedings of the Eighth Conference on Detection of Intrusions and Malware & Vulnerability Assessment, DIMVA '11, pp. 35--54, Heidelberg, July 2011. Springer.

[3] B. M. Bowen, M. Ben-Salem, S. Hershkop, A. D. Keromytis, and S. J. Stolfo. Designing host and network sensors to mitigate the insider threat. IEEE Security & Privacy, 7(6):1--1, 2009.

[4] Cisco Systems. Cisco Visual Networking Index: Global Mobile Data Trac Forecast Update, 2013-2018. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html, 2014.

[5] D. Hubbard, C. Garlati, F. Kasprzykowski, D. Lingenfelter, J.-M. Brook, A. Decker, E. Fisher, A. Lum, S. Michalove, G. Sanchidrian, S. Wilke, A. Alva, L. J. Santos, K. Scoboria, E. Scoboria, and J. Yeoh. Top Threats to Mobile Security, 2012.

[6] Mary Meeker and Liang Wu. 2013 Internet Trends: http://www.kpcb.com/insights/2013-internet-trends, 2013.