Are Mobile Devices the Answer to the Strong Authentication Problem?

SESSION ID: TECH-T08

Moderator: Alphonse (Al) Pascual
Senior Analyst, Security, Risk & Fraud
Javelin Strategy & Research

Panelists: Michael Barrett
President
The FIDO Alliance

Phillip Dunkelberger
CEO
Nok Nok Labs, Inc.

Brett McDowell
Vice President & Marketing Co-Chair
The FIDO Alliance

Nils Puhlmann
CTO
Endgame
Agenda

- The Shifting Consumer Security Paradigm
- Securing Financial Accounts & Payments
- The Impact of BYOD on Enterprise Authentication
- Predicting the Future
- Questions for the Panel
The Shifting Consumer Security Paradigm
The Consumer Security Paradigm

- In deciding on any authentication scheme we face a common conundrum:
  - How to best balance convenience, cost and effectiveness?
- For consumer applications, convenience has traditionally weighed most heavily in order to preserve the “customer relationship”.
  - As a result, passwords have remained the dominant scheme, along with other types of knowledge based authentication for most consumer-facing applications.
The Shift to Multi-Factor Authentication

- To meet growing consumer expectations for greater privacy and security, multi-factor authentication is experiencing increased adoption in consumer applications outside of the financial industry, including for use in e-commerce and social networks.

**Question:**

Are mobile devices being used effectively for multi-factor authentication in consumer applications as organizations try to balance convenience, cost, and security?
Securing Mobile Banking & Payments
Securing Mobile Banking & Payments

- Banking regulator guidance has driven the adoption of multi-factor authentication and layered security for online financial account access.
- Federal Financial Institutions Examination Council (FFIEC) authentication guidance includes:
  - *Authentication in an Internet Banking Environment* (2005)
  - *Supplement to Authentication in an Internet Banking Environment* (2011).
- Neither specifically addressed mobile banking (SMS, browser or app).
- Institutions need guidance as mobile banking suffers from a security perception problem (well deserved?).
Security Concerns Remain the Greatest Impediment to High-Value, Low-Cost Mobile Banking Adoption

Q14: You indicated you do not use mobile banking. For what reasons do you not use mobile banking? (select up to three) Select responses shown.
Confronting the Dynamics of Mobile Payments

- Mobile payments encompasses a variety of scenarios (m-commerce, mPOS, mP2P, and mobile wallets) and technology considerations (HCE, NFC, QR, SE, etc.), but lacks a central authority for guidance.

- Mobile payments suffers from the same security perception issue as mobile banking.

**Question:**

Are consumer security concerns related to mobile banking and payments justified, and what can financial institutions and payment providers do to assuage these concerns given a lack of guidance?
The Impact of BYOD on Enterprise Authentication
In a Post-BlackBerry World, Businesses Needs to Contend with Android and iOS Smartphone-Wielding Employees

2009 - July 2013, n = 1,948
Base: Consumers with smartphones.
The Impact of BYOD on Enterprise Authentication

- Mobile device management (MDM) has grown in complexity as the mobile world was taken over by Android and iOS, introducing new threats along with new authentication opportunities.
- BlackBerry devices are being displaced as enterprise facilitates the use of employee-owned devices for business purposes (a.k.a. Bring-your-own-device, or BYOD).

Question:
Have the needs of consumer and enterprise security merged, and are the authentication opportunities of BYOD worth the trouble?
Predicting the Future
The Advent of Mobile Changed Authentication

- Authentication has evolved with technology and mobile has been a major catalyst for change, facilitating:
  - Reduced costs (software tokens/one-time-passwords)
  - Greater reliability (true geolocation)
  - Increased practicality (integrated biometrics)

Question:

Which technologies on the horizon do you expect to introduce new means of authentication and how will we benefit?
Questions for the panel?