Keith Watson

Security Services using Telephony

Overview

- User’s Pain
- Opportunity
- Definitions
- Competitors
- Similar Solutions
- Gaps

User’s Pain

- Users have many online accounts
  - Use a common password everywhere
  - Use a easily guessed password
  - Use a short password
  - Can’t remember the password, and reset it
- Tools to manage passwords, difficult to use
- Most new web services require a new account
  - Login with Facebook option, violates privacy

Opportunity

- 322.9 million wireless subscribers in the US
  - 102.4% wireless penetration
- 100 million SMS users

Two-Factor Authentication

- Multi-factor authentication increases confidence in the identity of the entity requesting access
  - Something you know
  - Something you have
  - Something you are
- A password alone (SYK) is weak
- Additional factors increase confidence

One-time Password

- A password used only once
- Based on some pre-configured, shared secret
- Dynamic
  - Based on the current time
  - Will repeat, but expire
- Static
  - Based on a counter
  - Will increment

Competitors

- PhoneFactor
- Authentify
- PhoneConfirm
- TeleSign
- AuthFactor (Rails plugin)

- All are proprietary products
- Some have SDKs or plugins

Similar services

- Facebook One-time password
  - SMS delivery, 20 min window
- Google Two-Step Verification
  - TOTP-based, app, SMS delivery, 30 sec window

- Facebook mechanism is secret
- Google uses open standard, no API though

What’s missing?

- Engineer and security architect focus
  - Solve business problems efficiently/effectively
- Open source library
- Pay for what you use service
- Configurability
  - PIN, no PIN, SMS send, SMS receive, call out, call in, escalation path, voice print
  - registration via phone, confirmation via web
- Authentication, verification, approval, notification, AND two-man rule options

Proposing a solution

- Defining Requirements
  - User stories
- Risk Assessment
- Initial Design
- Threat Modeling
- Revised Design
- Incremental Implementation
  - Implement feature, test, present, repeat
- Test

Requirements

- Build on standards?
- Proprietary solution?
- Customer requirements

Risk Assessment

- What are the risks?
- Is there sensitive data?
- Where is the sensitive data?
- Is at risk in transit, at rest, or both?
- What is the likelihood that sensitive data can be exposed?
- What is the impact if sensitive data is exposed?

Initial Design

- To address customer requirements and the identified risks, propose a design

Threat Modeling

- Based on the initial design, use threat modeling to determine weaknesses and vulnerabilities in the proposed design

Revised Design

- Based on the threat model, how can we revise the design to address threats?

Implementation

- Go build it… I’ll wait…

Test

- How would you test the implementation?
- What testing techniques would you use?