Towards a more Secure Online Banking Experience

Nick Owen
October 2009
@wikidsystems
nowen@wikidsystems.com
Where are we going? And why are we in this hand-basket?
Authentication

Evil Princess Duck Bot

Sweet Chicky Chirpalot
Session Authentication

- Static Passwords
- Machine authentication
  - Spoof-able
- Two-factor authentication
  - Tokens
  - SMS
Mutual/Host Authentication

• Image-based
  – Subject to MITM attacks
  – Highly annoying
  – Fall back to 20 questions

• Programmatic SSL cert validation
  – Similar to SSH
Transaction Authentication

- One-time passwords
- Call-back system
- SMS
- Digital Signing
What's the current situation?
Zeus!
Defeating Zeus

• Anti-fraud measures
• Transaction authentication via call-back, SMS or other cryptographically distinct method
Are we done yet?

- Call-back
  - Scaleability, calls per second?
  - Costs
  - Metasploit VoiP war-dialer

- Attacks on SMS
  - Paris Hilton's secret question
  - Nokia 1100 phones
Open Source A5/1 Rainbow Tables!
Throw this in the mix

Mobile Banking!

The BlackBerry® Mobile Banking application from Bank of America has our ATM and banking center Locator, which will find the nearest locations with a simple touch of a button, no address input required. Added convenience whether you're traveling or just driving around town and need to get your money quickly.

The App will also give one-touch access to:

- Check available balances
- Pay bills
- Transfer funds

Read the rest of this entry »
How can this be a good thing?

- Chance to deploy a client
- Defeat of A5/1 means public key encryption
- Most mobile users will also be PC users
- Confirm transactions made in one on the other
- Extremely difficult to break real two-channel banking
If the problem is...

• Stolen passwords
  – The answer is strong session authentication
If the problem is...

- MITM attacks
  - The answer is strong mutual https authentication
If the problem is

- Malware
  - The answer is transaction authentication via a second channel
But those are not the problems

- The problem is a determined, persistent, motivated attacker
- So, what's needed is a forward-thinking, security-focused, responsive, banking software industry
Why aren't we here already?

- Banks don't want to develop software
- Marketing over security
- Banks fear support costs of online banking
- Duopoly in Personal Financial Software
- Monopoly in Aggregation
How about: Bankforge.net?

- Open source site for OFX applications
- Supported by the banks. Bounties? Prizes?
- Plenty of FI organizations that could promote/manage such a site
- Minimal support costs
- Increase competition for Aggregation & Personal Finance software
Financial Aggregation

Aggregator

OFX over SSL

Public Key Encryption
Two-factor Authentication
Transaction Authentication

Personal Finance Software
Principles

• Rely on well-tested security principles
• Don't rely on the security of 3rd parties
• Maximize the user's understanding of what's going on
• Use public key encryption!
Browser Improvements

- Site-specific browser
- Content Security Policies
UI Tweaks

- Transaction Mode!

- You could do this with client side asymmetric encryption
Open Financial Exchange (OFX) is a unified specification for the electronic exchange of financial data between financial institutions, businesses and consumers via the Internet. OFX is not a financial institution.

For more information or questions about OFX, please email us at ofxinfo@ofx.net
©2007 Open Financial Exchange, All Rights Reserved
OFX?

For more information or questions about OFX, please email us at ofx@openfinancialexchange.com

©2007 Open Financial Exchange, All Rights Reserved
OFX on Sourceforge

“Hello Li.

I'm sorry nobody has responded; that probably means nobody is able to help you. As you might have figured out already, the community for the OFX protocol is kind of narrow. It probably has to do with the lack of interest from the banks in fostering such a community.”
Can we have ATM-esque Security?
Summary

- Banks need to implement transaction authentication via a 2\textsuperscript{nd} channel ASAP
- Be careful relying on 3\textsuperscript{rd} parties
- Use cryptography! Wisely...
- Involve the user
- Banks need to support the OFX community
Thanks!

Nick Owen
October 2009
@wikidsystems
nowen@wikidsystems.com