SNAP2PASS: CONSUMER-FRIENDLY CHALLENGE-RESPONSE AUTHENTICATION WITH A PHONE

BEN DODSON, DEBANGSU SENGUPTA, DAN BONEH, MONICA S. LAM
STANFORD UNIVERSITY
Outline

- Web Security Overview
- Contributions
- Snap2Pass: User-Friendly Challenge-Response
  - Demonstration
  - Analysis
- Snap2Pay: Secure and User-Friendly E-Commerce
  - Demonstration
  - Analysis
- Related Work, Conclusion
Web Security: How are we doing?

FBI Hoaxes Boost Online Fraud
By David Kravets  March 12, 2010 | 5:38 pm | Categories: Crime, Threats

Online fraud in the United States doubled to a reported $560 million in losses last year as illicit phishing expeditions by thieves.

Your Facebook Profile May Be Sold by Russian Hacker
A spammer/scammer named Kirloss is selling 1.5 million Facebook accounts for a few pennies apiece. Yours might be one of them.
Problems with Passwords

- Dictionary attacks (~ 1% choose “123456”)
- Phishing (~ 0.4% of users / year)
- Password reuse across the web (over 5 sites)

Source: Florencio and Herley,
“A Large-Scale Study of Web Password Habits” (WWW ‘07)
Can we do better?
Snap2

- Use smartphones to enhance security & **usability**
- Phones are:
  - Always with us
  - Personal / individualized
  - Powerful
    - Internet-enabled, with adequate memory and CPU, and rich sensors
Contributions

Security without loss of convenience.

- Challenge/response authentication in a snap
  - Easy to learn, fun to do
  - No extra hardware*, no change to web paradigm

- One-time-use credit cards in a snap
  - Leave no footprint
Web Authentication
(The usual way)
Web Authentication (The Snap2Pass way)
Account Creation

- Provider generates shared secret
  - Encode credentials in a QR code

```json
{"username":
...
,"key": ...
}
```
Logging In

- QR encodes challenge and communication endpoint

junction://sb/93042849
Aside: Junction

- Platform for multiparty interactions
  - Provider, browser, phone all communicate in one session
- Junction provides communication and connectivity
  - Generate and consume QR code with 1 line of code
  - Messaging in a few more
Auth Transaction

- 3 Parties involved (phone, browser, provider)
  - HMAC challenge/response between phone/provider
  - Browser must know when session has been authenticated

- Implemented as a chat transcript
  - Chatroom name is the challenge
  - All devices actively listen for messages

```
!> You have joined:
    snap2pass.com/CHALLENGE

!> phone: {username: “letmein”, response: “RESPONSE”}
!> provider: {status: “AUTH_OK”}
!> browser: /me refreshes web page
```
## Security Analysis

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Username / passwords</th>
<th>Snap2Pass</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline phishing</td>
<td>Vulnerable</td>
<td>Secure</td>
</tr>
<tr>
<td>Online phishing</td>
<td>Vulnerable</td>
<td>Loss of session</td>
</tr>
<tr>
<td>Keylogging (client malware)</td>
<td>Vulnerable</td>
<td>Secure</td>
</tr>
<tr>
<td>Loss of device / theft</td>
<td>N/A</td>
<td>Revocable account</td>
</tr>
<tr>
<td>Malware on phone</td>
<td>N/A</td>
<td>Vulnerable</td>
</tr>
<tr>
<td>Passive network attack</td>
<td>SSL required</td>
<td>Secure w/o SSL</td>
</tr>
</tbody>
</table>
Online Phishing

- A hard problem.
  - 1. Server uses geolocation to ensure browser/phone are near
  - 2. Verify sensitive transactions from phone
Extending to multiple domains

- Multiple accounts for multiple domains
  - Single app, independent accounts
    - Account creation includes domain
  - User prompt helps prevent MITM
Extending to multiple domains

- Single account, multiple domains
  - OpenID (implemented; requires username entry)
  - OpenPass (Reliant party generates challenge)
  - Public key cryptography
Usability

- Comparison of SecurID and Snap2Pass
  - How 30 users feel using this system w/ bank

![Bar chart showing comparison of security and usability between Passwords, SecurID, and Snap2Pass](chart.png)
Web Payments
(The usual way)
Problems with form-based e-commerce

- Tedious to enter billing, shipping information
- Risks associated with storing account in cloud
- Might not trust site with credit card number at all

(All are especially true for mom&pop sites)
Web Payments
(The Snap2Pay Way)
Benefits

“Should I let these guys save my credit card?”

- Reduce time spent on checkout process
  - Without requiring per-site or centralized account mgmt.
- Enhanced security
  - Phone negotiates one-time-use credit card number
- Easily ship to anyone in your address book
- Integrated receipts, tracking
Two Payment Modes

- FORMFILL provides easiest integration
  - Also allows user to modify submission
- PAYDIRECT provides enhanced security
  - Usable beyond the web, too
Direct Payments with Snap2Pay
PAYDIRECT Challenge

{ Domain: “thinkgeek.com” ,challenge: “09a762c7de4df900da65b” ,Price: “34.99 US”}
Snap2Pay: Beyond the Web
Snap2Pay: Beyond the Web
Related Work

- Phoolproof (Parno et al.)
  - Use bluetooth + custom PC software
- OTP on phone (Aloul, Zahidi)
  - Move SecurID etc. to phone
- “Seeing Is Believing” (Mccune et al.)
  - Use 2D barcodes for key exchange (unidirectional)
Conclusions

- Phones are always with us, making them personal
  - Are also connected, have decent storage, and reasonable processing power
- QR codes allow cross-device communication without modifying standard software stacks
- Result: More security for web transactions, simplified user interaction.
[Appendix]
Usability

- Comparison of SecurID and Snap2Pass
  - How 30 users feel using this system w/ bank