Password Less Authentication (PLA)

Srikar Sagi
Agenda

- Why Factors - Problem Statement
- Why Factors – Motivations
- Mobile Device based Authentication
- User Registration
- User Experience
- Authentication Process
- Authentication Schematics
- Competitors to PLA
- OTP & PLA Differentiators
- References & QnA
- Appendix
Why Factors-Problem Statements

Customers
Too Many Passwords, password complexities, same passwords, sharing of passwords
Why Factors-Problems Statements

Customers
Password Changes, Reset requests & Remembering Security Questions for many sites

---

Reset Password

New Password

Confirm Password

New Question

New Answer

The password must meet the following requirements:

- Must contain at least 8 characters
- Must contain at least 1 uppercase letter
- Must contain at least 1 lowercase letter
- Must contain at least 1 digit
- Must contain at least 1 special character
- Must not contain any part of your username

- Must not repeat any of your previous 24 passwords
- Must differ from your previous password by more than the last character

---

Generate Password    Reset Password    Send Password
Why Factors-Problem Statements

Customers
Too many Tokens, Token Costs, Lost Tokens, Dispatch Costs & Lost Business Costs
Why Factors-Problem Statements

Executive Management

• Cost of -- Fraud Operations, Software Security Controls, Service Desk, Frustrated Users & Lost business

• Identity Theft 9.8% (IC3-2010) - 3rd Most Internet Crime

• PoneMon Report – 2011 - Cost of Cyber Crime Study

• The Shocking Scale of Cybercrime - Shared by Richard R. in Mobile Security Trends - LinkedIn

• State of Enterprise Security - 2010 Report by Norton
Why Factors-Motivation

SMS Bank Tokens Vulnerable

[Link to ZDNet article]

ZDNet / Security / Story

SMS bank tokens vulnerable: RSA

By Darren Pauli, ZDNet.com.au on January 18th, 2011

Mobile phone attacks will increase this year as criminals attempt to intercept SMS-based authentication tokens, according to security company RSA.

The tokens are designed to complement username and password log-in checks by requiring users to validate payments with unique numerical codes, in this instance sent by SMS.

It is becoming more popular, and the Commonwealth Bank of Australia claims to have 80 per cent of its customer base using tokens to validate third-party payments via SMS or through safer handheld token-number generators. The bank isn’t forcing customers to use it, but those who don’t will not be permitted to carry out high-risk transactions over NetBank.

(iPhone 4 image by Jorge Quinteros, CC2.0)

RSA said in a 2011 predictions report that sending tokens via SMS will make phones a target.

"The use of out-of-band authentication SMS ... as an additional layer of security adds to the vulnerabilities in the mobile channel," the company said in its report.

"A criminal can ... conduct a telephony denial-of-service attack which essentially renders a consumer's mobile device unavailable.

"SMS forwarding services are also becoming mainstream in the fraud underground and enable the [token] sent by a bank via text to a user's mobile phone to be intercepted and forwarded directly to the cyber criminal's phone."

The company said that mobile phone smishing attacks, or phishing scams sent via SMS, will also rise this year.
One Time Passwords are not Secure – Analysis
http://www.nowires.org/Papers-PDF/OTPanalysis.pdf

Why Factors-Motivation
Why Factors-Motivation

RSA Secure-ID Hardware Token Hacked

http://technorati.com/technology/it/article/rsa-hackedtime-to-panic-for-corporate/

Network security vendor RSA has announced that they have been the victim of "an extremely sophisticated cyber attack in progress being mounted against RSA". Specific details of the breach have been limited thus far, but RSA has confirmed that data taken from their network directly pertains to their SecuriID two factor authentication products.

The SecuriID system is employed by corporations and businesses all over the world as a means of securing access to sensitive business systems both on-site and from remote locations. The keys generated by the system require a user to connect using their username, a personalized PIN number, and a security token generated by SecureID devices. Each token is generated by the user when they begin a connection, and usually remains valid for about 30 seconds. This method has been a cornerstone of system access security for quite some time, but now may be at risk of breach.

If you've never seen a SecuriID device, they typically appear as a keychain sized box with a small LCD screen that allows an individual the ability to generate personal access codes on demand to connect to business systems. The breach at RSA, while not directly jeopardizing any consumer data, could lead to subsequent attacks on systems that use the device for security.

RSA chairman Arthur W. Covelli Jr. posted an open letter on the company's website detailing the steps that RSA is taking to mitigate the damage. Unfortunately, at this stage, SecuriID customers are forced to rely on their employees to take appropriate steps to safeguard their access information. It's safe to say that currently nobody knows how or when the hackers will attempt to use the stolen data, but it's likely they will try.
With passwords "broken," US rolls out Internet identity plan

At a US Chamber of Commerce event today, the federal government rolled out its vision for robust online credentials that it hopes will replace the current mess of multiple accounts and insecure passwords. The choice of the Chamber of Commerce wasn’t an accident, either; the government wants to squelch any talk of a "national Internet ID card" and emphasize that the plan will be both voluntary and led by the private sector.

The National Strategy for Trusted Identities in Cyberspace (NSTIC) hasn’t changed much since the draft plan unveiled in January, though the final version (PDF) contains an even stronger emphasis on NSTIC being a private-sector, voluntary undertaking. This point was stressed so many times in a background briefing call for reporters this morning that it’s clear the government fears a potential backlash against its efforts.

The final version of NSTIC tries to address two problems: the fact that passwords are "broken" and the fact that it’s almost impossible to prove your identity on the Internet. The future belongs to smart cards, cell phones, USB security sticks, and similar solutions—when the Department of Defense moved away from passwords to a smartcard security solution, it saw network intrusions drop by 46 percent.

The rest of the system is simple: create the baseline tools needed for online commerce to thrive. Indeed, the
Why Factors-Motivation

- Human *Psyche* for Mobile phones
- Frustrated Users – many & similar Passwords
- Human Dependency on Mobile phones
- Trust on Mobile Network’s Control Channel
- Increase in Mobile Device Capabilities
- Use of Mobile’s Geo Loc’ for Authorization Decision
- Trust on Public Key Cryptography
- Automated Mobile Signal attacks are costly (Logistics)
- Mobile Apps – Controlled by Central Release Authorities
- Mobile Phone Population crossing 5 Billion devices
- Adult(15-65)Population more than 3 Billion out of 7 Billion
- Expected – 50 Billion Internet connected Devices by 2020
Mobile Device based Authentication

Onwership Based Authentication with Mobile

For

1. Speed of Auth/Z
2. Ease of Use (UI, Registration)
3. Adaptation Flexibility & Scalability
User Registration

Account login

User Name
nikolas@facelog.com

Password
***************

Go to
My account

Log In

PLA Authentication

User Id

PIN

Request Challenge-1

New to PLA? Register
User Registration

FaceLog Payments & Identity Systems

Welcome Nikolas

-------------------I Want Password Less Authentication-------------------

Difficult to remember all your passwords?? Here is a boon for it!!! Just remember one pin and forget all your password's!!! Click on me to try!!!

Available balance in USD (primary): $1,042.90 USD
Total balance (all currencies, available and pending) converted to USD: $5,074.86 USD

<table>
<thead>
<tr>
<th>Currency</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>USD (Primary)</td>
<td>$1,042.90</td>
</tr>
<tr>
<td>CAD</td>
<td>$1,712.10 CAD</td>
</tr>
<tr>
<td>GBP</td>
<td>£604.50 GBP</td>
</tr>
<tr>
<td>EUR</td>
<td>€660.50 EUR</td>
</tr>
<tr>
<td>AUD</td>
<td>$386.10 AUD</td>
</tr>
</tbody>
</table>

See all balances

My recent activity | Payments received | Payments sent

View all of my transactions
User Registration

FaceLog Payments & Identity Systems

User Name
nikolas@facelog.com

Choose a 6 Digit PIN
(The same PIN you need to select for your mobile Application)
123789

Re-Enter Same 6 Digit PIN
(The same PIN you need to select for your mobile Application)
123789

Enter Personal Mobile Phone Number (This Mobile Proves Your Identity – Hence Keep this Phone Private to yourself)
(Eg: If your mobile Number is 9647748443 and your country is India then enter as 919647748443)
919176617699

Re-Enter Personal Mobile Phone Number (This Mobile Proves Your Identity – Hence Keep this Phone Private to yourself)
(Eg: If your mobile Number is 9647748443 and your country is India then enter as 919647748443)
919176617699

Your Download Message Code = X12-972JM123-ABC – Download the app only if you see this

I Agree All Terms & Conditions & Register me for PLA
You Got a Message from www.facelog.com to download the PLA Mobile Application from the Below Link

http://www.facelog.com/download/pla/user/msgcode=X12-972JM123-ABC

Select “YES” to Download PLA Mobile App
User Registration

Welcome to PLA Mobile App
Choose Your Action

- Register
- Authenticate
- Change PIN
User Registration

To read IMSI & ICC-ID
User Registration

Same PIN Entered on the web page
User Registration

1. PLA Mobile App
   Registration Forwarded To Server

2. MSC
   HLR
   SS7
   Operator Data Center

3. Decrypt IMSI, ICC-ID with Servier’s Pvt Key

4. UID, IMSI, ICC-ID, Mobile Number in the DB

Encrypted IMSI + ICC-ID

20
User Registration

1. Create AppID with Rand Generator (with some other Info)
2. Encrypt AppID with (PIN+IMSI+ ICC-ID) & ReEncrypt with Servier’s Pvt Key
3. Write
4. Update DB with AppID for the User
5. Encrypted App ID

PLA Registration Success

Update DB with AppID for the User

Operator Data Center

MSC
HLR
SS7
User Experience

FaceLog Payments & Identity Systems

Account login

User Name
Password

Go to
My account
Log In
Problem with login?

PLA Authentication

User Id:
****@

PIN

Request Challenge-1

Your Web Challenge
Enter This Challenge in Your Mobile App

5678
User Experience

Enter Challenge-1 to Authenticate
Welcome Nikolas
Authentication Success!

Account Type: Premier  Status: Verified

You have logged in on, 8/10/2011 12.34 pm
From IP address: 10.239.41.48
Authentication Process

Step-1  Credential Collection on **TWO distinct** Networks

Step-2  User ID is sent by User as **multipart/x-mixed-replace** Request and **Challenge-1** is received on Web Page from Server on IP Network as a multipart/x-mixed-replace Response

Step-3  Server Sends **Challenge-2** as Push/SMS Message on Mobile Phone over the air using Telecom Network (stores Challenge-1 & 2)

Step-4  User enters **Challenge-1** on Mobile App & Mobile App reads **Challenge-2** from Push/SMS, Hashes **C1+C2+IMSI+ICC-ID+AppID** and Encrypts with Server’s Public Key (Encrypted Packet)

**NOTE:** **Challenge-2** is always Opaque to user– may or may not know
Authentication Process

**Step-5**  Encrypted Packet is Sent as SMS/Push Response from Mobile Network

**Step-6**  Server reads the Push Response/SMS Message from User

**Step-7**  Server Decrypts Encrypted Packet with its Private Key

**Step-8**  Server loads \(C1+C2+IMSI+ICC-ID+AppID\) stored in the Database for that user’s request and hashes again

**Step-9**  If Hashes Match then Welcome screen is pushed to the web user as a Response to \texttt{multipart/x-mixed-replace}\n
Authentication Schematics

Login Page of www.facelog.com
Accessed with Desk/LapTop NetBook/SmartPhone

1] Enter UID
2] Get Server’s Challenge-1
Submit
Your Challenge-1 A2Z4

Send UID & Request For Login

HTTP multipart/x-mixed-replace MIME Request

Return Challenge-1
HTTP multipart/x-mixed-replace MIME Response

Return Challenge-2
To User’s Mobile Device

SSL/IP Network

TeleCom

You Received Auth Challenge – Open App

Return Challenge-2
(Any one Channel – SMS/USSD/GPRS/3G)

IMSI, ICC-ID Already Available
As part of User Registration
Login Page of www.facelog.com
Accessed with
Desk/LapTop
NetBook/SmartPhone

Waiting For Auth
Result
Submit

Internet

Decrypt Data with
Server’s Pvt Key &
Generate
Hash & Compare
Challenge

Authenticate

SSL/IP
Network

TeleCom

Challenge-1,2,
IMSI, ICC-ID &
UID From
Auth DB

MSC
HLR
SS7
Operator
Data Center

1

2

3

4

5

6

Challenge
‐
1,2,
IMSI,
ICC
‐
ID
&
UID
From
Auth
DB

Decrypt Data with
Server’s Pvt Key &
Generate
Hash & Compare
Challenge

Return Auth Result –or Main
Page/Insider Pages
(multipart/x-mixed-replace
REFRESH/Update)

Send Encrypted
Packet
(Encrypted Hash of Challenge-1 & 2
+IMSI
+ICC-ID
+AppID)

Enter Challenge-1 to
Authenticate
A2Z4

Authorization Schematics

Login Page of www.facelog.com
Accessed with
Desk/LapTop
NetBook/SmartPhone

Waiting For Auth
Result
Submit

Internet

Decrypt Data with
Server’s Pvt Key &
Generate
Hash & Compare
Challenge

Return Auth Result –or Main
Page/Insider Pages
(multipart/x-mixed-replace
REFRESH/Update)

Send Encrypted
Packet
(Encrypted Hash of Challenge-1 & 2
+IMSI
+ICC-ID
+AppID)

Enter Challenge-1 to
Authenticate
A2Z4

SSL/IP
Network

TeleCom

Challenge-1,2,
IMSI, ICC-ID &
UID From
Auth DB
**Best Channel – Real Experience for PLA**

<table>
<thead>
<tr>
<th>#</th>
<th>Connectivity Protocol / Bearer Channel</th>
<th>Dev Cost</th>
<th>OS Comp</th>
<th>Initial Testing Cost</th>
<th>Integration Cost (Between Operator &amp; Servers)</th>
<th>Connection Speed</th>
<th>Connection Type</th>
<th>Location Dependency</th>
<th>User Experience (Server Response Speed)</th>
<th>Setup Costs (H/W &amp; S/W)</th>
<th>End User Charges</th>
<th>OPS Cost</th>
<th>Support (user compliants)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SMS</td>
<td>LOW</td>
<td></td>
<td>MEDIUM</td>
<td>LOW</td>
<td>LOW</td>
<td>Store &amp; Forward</td>
<td>Yes - LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>HIGH</td>
</tr>
<tr>
<td>2</td>
<td>GPRS</td>
<td>MEDIUM</td>
<td></td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>Packet Based</td>
<td>Yes - LOW</td>
<td>SUPER</td>
<td>LOW</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
<td>MEDIUM</td>
</tr>
<tr>
<td>3</td>
<td>3G</td>
<td>HIGH</td>
<td></td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>Conn--Oriented</td>
<td>Yes - HIGH</td>
<td>SUPERATIVE</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
</tr>
<tr>
<td>4</td>
<td>USSD-USSR Over SMPP</td>
<td>LOW</td>
<td></td>
<td>HIGH</td>
<td>HIGH</td>
<td>HIGH</td>
<td>Session based (between Handset &amp; N/W)</td>
<td>Yes - HIGH</td>
<td>SUPERATIVE</td>
<td>MEDIUM</td>
<td>NIL</td>
<td>LOW</td>
<td>MEDIUM</td>
</tr>
</tbody>
</table>

Best Channel with Best User Experience

**USSR-Unstructured Supplementary Service Request (Network Initiated Push for Application Start-Up)**
Competitors to PLA

Products –

Browser ID
Solid Pass.com (All or some products)
Google PIN Check/Verification Code

Research Papers –

Secure Web Authentication with Mobile Phones by Min Wu, Simson Garfinkel, Rob Miller @ M.I.T

Secure Web Authentication with Mobile Phones by Min Wu, Simson Garfinkel, Rob Miller @ M.I.T
http://dimacs.rutgers.edu/Workshops/Tools/slides/wu.ppt

The same paper that was published in IEEE
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5951918

PLA, Browser ID, Solid Pass & Google PIN Check & the research paper by MIT Students all are based on “Ownership” based authentication model and hence they all can be directly compared for

1. Speed of Auth/Z
2. Ease of Use (UI, Registration)
3. Portability
4. Adaptation Flexibility & Scalability
5. Security Aspects
# OTP & PLA - Differentiators

<table>
<thead>
<tr>
<th><strong>OTPs</strong></th>
<th><strong>PLA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Multiple Tokens - for each &quot;Secure Banking Service“ - ICICI, HDFC, CITI</td>
<td>No need to carry multiple tokens for each &quot;Secure Banking Service&quot;</td>
</tr>
<tr>
<td>2. Remember UIDs or User Nos</td>
<td><strong>No remembering of passwords</strong> for any &quot;Secure Banking Service“ - <strong>Only remember the user ID</strong></td>
</tr>
<tr>
<td>3. Remembering respective passwords for each User IDs or User Numbers</td>
<td>Easy to add new &quot;Public Key&quot; for any &quot;Secure Banking Service“ in same mobile app.</td>
</tr>
<tr>
<td>4. Changing respective passwords for each User IDs or User Numbers in Credential life cycle</td>
<td>Application Logic shall take care of selecting which &quot;Public Key&quot; to use to encrypt Tokens for which &quot;Secure Banking Service&quot;</td>
</tr>
<tr>
<td>5. Dependent on Mobile Network (Mobile OTPs &amp; PLA Both)</td>
<td>Can be used for &quot;Authorization“ as well (Requires additional development)</td>
</tr>
<tr>
<td>6. Cost for HelpDesk/Support Calls for Login Issues/Resets, Token Issuance, Maintenance, Token Support calls</td>
<td><strong>Secure Banking Service can avoid the COSTS of</strong> Login issues on the IP Network, Password Strength/Expiry/Losses/Resets <strong>Only Mobile App Updates is unavoidable cost</strong> HelpDesk/Service Desk Calls</td>
</tr>
</tbody>
</table>
References

[1] Identity Theft 9.8% (IC3-2010) - 3rd Most Internet Crime


[3] SMS Bank Tokens Vulnerable

[4] One Time Passwords are not Secure – Analysis
   http://www.nowires.org/Papers-PDF/OTPanalysis.pdf

[5] RSA Secure-ID Hardware Token Hacked
   http://technorati.com/technology/it/article/rsa-hackedtime-to-panic-for-corporate/

[6] US Chamber of Commerce – Proposing No Passwords, Only H/W or Smart Phone based Login

[7] Response time reasons & panic of users for their lost or stolen mobiles

[8] Token Types, Costs, Comparisons & Current Implementors
   http://www.zdnetasia.com/war-of-the-tokens-62037260.htm

[9] Miscellaneous
Appendix

- POC Exploit/Failure Scenarios
- Differentiators – OTP & POC
- OTP Costs & Cons
- References
POC Exploit / Failure Scenarios

- **POC Exploit-1 - Replay SMS attack**
  Attacker can replay i.e. Capture the signal & resend it within the time frame – attacker would only help the end user of the POC

- **POC Exploit-2 - Sending Fake SMS**
  Attacker can send fake SMS on behalf the POC User – but cannot receive SMS on behalf of POC User – Courtesy “Control Channel” of Mobile Network, for a successful authentication the attacker must receive the initial Push/SMS Message

- **POC Exploit-3 - A total Compromise**
  For Successful compromise attacker must know & have: User ID, Cell Phone No, IMSI, ICC-ID, Token-1 & 2, AppID and the “Control Channel” to receive Network Message
POC Exploit / Failure Scenarios

- **POC Exploit-4- Lost/Stolen Mobiles**
  Mobile Phone is a *precious* device hence the time taken for an owner to discover loss of Mobile is *likely to be much shorter* compared to loss of tokens, which is used only while making a banking transaction.

  ----Jukka Riivari, CEO & President of Meridea


- **POC Exploit-5- Zero Protection Scenario**
  Attacker having overpowered the POC User & Mobile Subscriber, took control of Mobile device & the Desktop/Laptop/NetBook – this POC will completely fail

- **POC Failure Scenario-1- Multiple Users**
  POC cannot be used in Least Developed Countries, where Micro-Payments are rampant for Multiple Users per mobile
### OTP Costs & Cons

#### Hardware token


<table>
<thead>
<tr>
<th>Banks</th>
<th>ABN Amro, China Construction Bank, Citibank Singapore, DBS, HSBC, OCBC, UBS, UOB</th>
</tr>
</thead>
</table>
| **Pros** | - Has been around longer  
- Not dependent on the mobile phone operator network  
- Does not require any downloads or setup |
| **Cons** | - Inconvenience due to *necklace syndrome*,  
- Where customers with multiple Bank A/c with different Banks will have to carry multiple tokens  
- *Higher implementation costs.*  
- Experts estimate hardware's recurring costs to be around S$40 (US$24.50) to S$60 (US$36.74) per user per year, compared to under S$10 (US$6.12) per user per year for software-based tokens  
- Customer has to pay a replacement fee if it's lost  
- Not tamper-proof |
## OTP Costs & Cons

### Software token for mobile


<table>
<thead>
<tr>
<th>Banks</th>
<th>OCBC Singapore</th>
</tr>
</thead>
</table>
| **Pros**    | - Mobile phone is ubiquitous  
- No replacement fee; customer simply has to download the software application to his new phone |
| **Cons**    | - Dependent on the mobile operator network  
- Mobile phone can be as easily lost as hardware token, although chances of someone realizing his phone is missing are higher than it would be with the hardware token  
- Still very new & customers are less familiar with process, compared to SMS |
### OTP Costs & Cons

#### SMS Tokens


<table>
<thead>
<tr>
<th>Banks</th>
<th>Citibank Singapore &amp; Hong Kong, OCBC, Standard Chartered, UOB</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pros</strong></td>
<td>Mobile phone is ubiquitous</td>
</tr>
<tr>
<td></td>
<td>People in Asia are familiar with SMS</td>
</tr>
<tr>
<td></td>
<td>Requires no training</td>
</tr>
<tr>
<td><strong>Cons</strong></td>
<td>Dependent on the mobile operator network</td>
</tr>
<tr>
<td></td>
<td>Potential issues like lost transmission and unexpected delay during festive seasons or when one is overseas</td>
</tr>
<tr>
<td></td>
<td>Mobile phone can be as easily lost as hardware token, although the chances of someone realizing his phone is missing are higher than it would be with the hardware token</td>
</tr>
</tbody>
</table>