tiqr: a novel take on two-factor authentication

LISA 2011, Boston, MA
Overview

- Introduction

- The 2-factor landscape

- Something we all have

- tiqr

- Comparison of 2-factor AuthN technologies

- Security audit

- Questions?
Recognize this?
United Federation of Passwords
Well-known drawbacks

- The woes of username/password are well-known...

Does anybody remember these guys?

Study Reveals 75 Percent of Individuals Use Same Password for Social Networking and Email

PM's office passwords pose security risk

More than 10 per cent of passwords used in the Prime Minister's department can be easily broken in an hour by hackers
Endless patches and ‘solutions’

Current Password: ********
New Password: ********
Re-Enter New Password: ********

Passwords are like toothbrushes...
they’re best when fresh & should not be shared.

Account Security
To help keep your Facebook account as safe as possible, we can notify you when your account is accessed from a computer or mobile device that you haven’t used before.
Would you like to receive notifications for logins from new devices?
Yes ☐ No ☑

Notification methods (in addition to email):
☐ SMS (mobile text)

Submit

Computers and mobile devices currently associated with your account:

<table>
<thead>
<tr>
<th>Name</th>
<th>Time Saved</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>Le³Á Work Computer</td>
<td>Today at 1:00pm</td>
<td>Remove</td>
</tr>
<tr>
<td>Le³Á Home Computer</td>
<td>Today at 12:59pm</td>
<td>Remove</td>
</tr>
</tbody>
</table>
2-factor AuthN in one slide

+ + =

☑ ☑
The 2-factor AuthN landscape

- SMS from SURFnet - your login code is 32vj6k

---

SURFnet. We make innovation work
Drawbacks of ‘traditional’ 2-factor AuthN solutions

- Often involve additional physical tokens that users need to carry around
- May require driver software on end-user workstations
- Are proprietary in nature and incompatible with each other
- Are usually single purpose (e.g. you cannot use bank A’s token for bank B as well)
Something we all have (right?)

- (Almost) everybody owns a mobile phone
  - A 2007 study in The Netherlands showed 19 million subscribers in a country with 16.5 million people

- Most people always carry their mobile phone with them
  - A recent study by SecurEnvoy shows that one in three people notice their phone is missing in under an hour

- There are already several options:
  - SMS authentication
  - A host of ‘Apps’
  - SIM add-ons like Vasco DigiPass Nano
One Friday afternoon...

- As these things go, we started brainstorming...

- What we most dislike about almost all solutions:

  *Having to re-type complicated codes*

- So one Friday afternoon in September we started thinking...
Seeing is believing ;-)
Even cooler demo

source: http://www.dickestell.com/images/expo175.jpg
How does it work?

1. [Image of a person with a QR code]
2. [Image of a QR code]
3. [Image of a smartphone]
4. [Image of a file]
5. [Image of a computer]
6. [Image of another computer]
Design and implementation

- Fully based on Open Standards

- Uses the OCRA suite developed by the Open Authentication (OATH) initiative

- Uses the HOTP algorithm (RFC 4226)

- AES 256-bit encryption

- Uses the ZXing QR-code library by Google
  http://code.google.com/p/zxing/

- QR code patent is royalty free
## Comparison of AuthN tech.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Username/Password</td>
<td>++</td>
<td>++</td>
<td>--</td>
<td>++</td>
<td>=</td>
<td>+/-</td>
</tr>
<tr>
<td>OTP token</td>
<td>-</td>
<td>-</td>
<td>++</td>
<td>--</td>
<td>-/=</td>
<td>+</td>
</tr>
<tr>
<td>C/R token</td>
<td>-</td>
<td>-</td>
<td>++</td>
<td>--</td>
<td>-/=</td>
<td>+</td>
</tr>
<tr>
<td>PKI Token</td>
<td>--</td>
<td>--</td>
<td>++</td>
<td>--</td>
<td>=</td>
<td>+</td>
</tr>
<tr>
<td>Mobile PKI</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>?</td>
<td>+</td>
<td>++</td>
</tr>
<tr>
<td>SMS OTP</td>
<td>+</td>
<td>=</td>
<td>X</td>
<td>-</td>
<td>--</td>
<td>-</td>
</tr>
<tr>
<td>OTP Apps</td>
<td>+</td>
<td>+/=</td>
<td>+</td>
<td>+/=</td>
<td>+/=</td>
<td>=</td>
</tr>
<tr>
<td>tiqri</td>
<td>+</td>
<td>+/=</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>
Security audit

- We contracted an external auditor

- Goals of the audit were:
  - White box security testing
  - tiqr architecture and design analysis
  - Code audit

- The audit was performed earlier this year

- We got good feedback and fixed some issues

- Status now: tiqr is a secure solution

- Read the report: https://tiqr.org/audit/
tiqr roadmap

- Available on Apple’s App Store ✔
- Available on Android Market ✔
- Release as Open Source ✔
- Security & code audit ✔
- Partner with other solutions in progress
- Other mobile platforms you? we?
- Pilot with “real users” Q4 2011 - Q1 2012
Questions? Comments? Please contact me or visit https://tiqr.org/

roland.vanrijswijk@surfnet.nl
nl.linkedin.com/in/rolandvanrijswijk
@reseauxsansfil