Authentication in a networked world

Joseph Bonneau
Gates Scholars Internal Symposium
May 2, 2012
Finding #1

People choose banking PINs poorly
‘Pin number’ burglar used victims’ cards

He struck as couple slept

GARRY WILLEY

A JUDGE laid down a pin number warning after he heard how a couple fell victim to a “cunning” career crook.

Serial offender Paul Miller - whose grim record carries 167 previous convictions - crept into the victim’s North Tyneside home while they slept.

His haul included cash, laptops, a handbag and driving licence.

But Miller, 31, also pocketed two Barclays cards, Newcastle Crown Court heard. And within hours he was plundering £1,000 from an ATM on nearby Wallsend High Street when he guessed right the owner had used her date of birth as a pin. Jailing Miller for four and a half years, Judge Roger Thorn said: “If anybody is still using their date of birth as a pin they should learn a lesson from this case.

“You knew that by using the driving licence you could get the date of birth and having identified that you took a chance that the holder was using it as a pin. You were right.”

The dead-of-night raid last summer has left the victims feeling paranoid in their own home, the court heard.

Miller, of Wilberforce Street, Wallsend, denied burglary and fraud but was convicted by a jury.

He slipped inside the house when he realised the front door was unlocked, prowling through rooms and rounding up property while the couple slept.

Miller was later captured on CCTV using the cards to withdraw batches of cash from the same ATM. A pre-sentence report said Miller - a heroin addict who first took drugs when he was 12 - posed a risk of harm through potential confrontations with homeowners. His record includes offences of arson and robbery as well as 32 previous burglaries - nine targeting homes.
Finding #2

People choose passwords poorly
Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
To be or not to be, that is the question.

1 quadrillion variations ≈ 50 bits?

Want to create a really strong password? Ask Hamlet.

Or Macbeth. Or Othello. Or even take a lyric from your favourite song. The more unusual the better. Try thinking of a memorable line like, 'To be, or not to be, that is the question' and then use numbers, symbols and mixed letters to recreate it:

2bon2b1t1q is a password with quadrillions of variations. Which is a lot.

In short, strong passwords can keep you safe online, which is good to know.

To find out more on how to be safer on the Internet go to google.co.uk/goodtoknow
Finding #3

Motivation doesn't really matter
Finding #4

Bad passwords are universal
123456 123456
123456789 111111
password 000000
iloveyou 123456789
princess 123123
1234567 111222tianya
rockyou 5201314
iloveyou 123321
12345678 12345678
abc123 123
nicole 123
babygirl 123
monday 666666
lovely 7758521
jessica 888888
babygirl 1314520
babygirl 1234567
babygirl wangyut2
babygirl woaini
babygirl 11111111
babygirl a123456
babygirl 111222
babygirl 112233
babygirl 654321
babygirl 654321
babygirl 100200
babygirl 123654
babygirl 123123123
babygirl 123123123
RockYou:

- 123456
- 12345
- 123456789
- password
- iloveyou
- princess
- 1234567
- rockyou
- 12345678
- abc123
- nicole
- daniel
- babygirl
- monkey
- lovely
- jessica
- 654321
- michael
- ashley
- qwerty
- 111111
- iloveu
- 000000
- michelle
- tigger

CSDN:

- 123456
- 111111
- 000000
- 123456789
- 123123
- 111222tianya
- 5201314
- 123321
- 12345678
- 123
- 666666
- 7758521
- 888888
- 1314520
- 1234567
- wangyut2
- woaini
- 11111111
- a123456
- 111222
- 112233
- 654321
- 100200
- 123654
- 123123123
Challenge #1

human-machine authentication
trusted hardware?
fingerprint
biometrics
fingerprint biometrics

Matsumoto et al. 2002
iris
biometrics
iris biometrics
iris biometrics
other biometrics
Challenge #2

the Internet identity layer
(machine-machine)
Today's Internet identity layer
Tomorrow's Internet identity layer
Today's approximation
Who controls your identity?

the state or fact of remaining the same

...we may replace past names associated with your Google Account so that you are represented consistently across all our services.
Challenge #3

machine-human authentication
Secure Connection Failed

www.vedetta.com uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

Or you can add an exception...
This certificate has been verified for the following usages:
SSL Server Certificate

Issued To
- Common Name (CN): accounts.google.com
- Organization (O): Google Inc
- Organizational Unit (OU): <Not Part Of Certificate>


Issued By
- Common Name (CN): Thawte SGC CA
- Organization (O): Thawte Consulting (Pty) Ltd.
- Organizational Unit (OU): <Not Part Of Certificate>

Validity Period
- Issued On: 7/21/11
- Expires On: 7/19/13

Fingerprints
- SHA-256 Fingerprint: BE 4E ED C4 E0 7D 2B 36 81 02 24 A4 CF 9A 9E F5 4D 08 4B 31 E4 8F 5D CB 6A 67 4D 79 DD 8B 3F 55 3D 66
- SHA-1 Fingerprint: E6 96 99 69 49 A7 17 FD D8 AF B6 B1 3A 40 39 EA 6A 73 34 44

Certificate Hierarchy
- Built-in Object Token: Verisign Class 3 Public Primary Certification Authority
  - Thawte SGC CA
    - accounts.google.com

Certificate Fields
- Built-in Object Token: Verisign Class 3 Public Primary Certification Authority
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm

Field Value

Export...
Whom do you trust by default?

Certificate Manager

<table>
<thead>
<tr>
<th>Authorities</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your Certificates</td>
<td>Servers</td>
</tr>
<tr>
<td>You have certificates on file that identify these certificate authorities:</td>
<td></td>
</tr>
<tr>
<td>• Baltimore</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Baltimore CyberTrust Root</td>
</tr>
<tr>
<td></td>
<td>Buyypass AS-983163327</td>
</tr>
<tr>
<td></td>
<td>Buyypass Class 2 CA 1</td>
</tr>
<tr>
<td></td>
<td>Buyypass Class 3 CA 1</td>
</tr>
<tr>
<td></td>
<td>(c) 2005 TÜRKTRUST Bilgi İlişşim ve Bilişim Güvenliği Hizmetleri A.Ş.</td>
</tr>
<tr>
<td></td>
<td>TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı</td>
</tr>
<tr>
<td></td>
<td>certSIGN</td>
</tr>
<tr>
<td></td>
<td>certSIGN ROOT CA</td>
</tr>
<tr>
<td></td>
<td>Chungwha Telecom Co., Ltd.</td>
</tr>
<tr>
<td></td>
<td>ePKI Root Certification Authority</td>
</tr>
<tr>
<td></td>
<td>CNNIC</td>
</tr>
<tr>
<td></td>
<td>CNNIC ROOT</td>
</tr>
<tr>
<td></td>
<td>Comodo CA Limited</td>
</tr>
<tr>
<td>AAA Certificate Services</td>
<td></td>
</tr>
<tr>
<td>View...</td>
<td>Edit...</td>
</tr>
</tbody>
</table>
Whom do you trust by default?

Certificate Manager

You have certificates on file that identify these certificate authorities:

- Baltimore CyberTrust Root
- Buypass AS-983163327
  - Buypass Class 2 CA 1
  - Buypass Class 3 CA 1
- (c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.
  - TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı
- certSIGN
  - certSIGN ROOT CA
- Chungwa Telecom Co., Ltd.
  - ePKI Root Certification Authority
- CNNIC
  - CNNIC ROOT
- Comodo CA Limited

AAA Certificate Services

View...  Edit...  Import...  Export...  Delete...
Whom do you trust by default?

Certificate Manager

<table>
<thead>
<tr>
<th>Your Certificates</th>
<th>Servers</th>
<th>Authorities</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baltimore CyberTrust Root</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buypass AS-983163327</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buypass Class 2 CA 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Buypass Class 3 CA 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(c) 2005 TÜRKTRUST Bilgi İletişim ve Bilişim Güvenliği Hizmetleri A.Ş.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TÜRKTRUST Elektronik Sertifika Hizmet Sağlayıcısı</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>certSIGN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>certSIGN ROOT CA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chungwha Telecom Co., Ltd.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ePKI Root Certification Authority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNNIC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNNIC ROOT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Comodo CA Limited</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AAA Certificate Services</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

View...  Edit...  Import...  Export...  Delete...
Better models

Is this the key everybody else sees?

Is this the key you gave me at first?
Computers are useless
They can only give you answers

Pablo Picasso, 1968
Thank you all 😊

Guessing human-chosen secrets

Joseph Bonneau

University of Cambridge
Churchill College

April 2012

This dissertation is submitted for the degree of Doctor of Philosophy