QUANTIFIED SELF
A Path to Self-Enlightenment or Just a Security Nightmare?

Candid Wüest
THREAT RESEARCHER

Thanks To: Mario Ballano & Hon Lau
WHAT IS QUANTIFIED SELF?

Recording everything about your life

Sports & Recreation

Intenet Of Things

Wearable Tech

Health

Business

Culture

Symantec
WHERE THE BITS FIT IN

More moving parts = more risks
UNINTENTIONAL DATA LEAKS

The secret life of mobile apps...

MAX DOMAINS CONTACTED
14

AVG DOMAINS CONTACTED
5

APP ANALYTICS
AD NETWORKS
APP PROVIDER
OS PROVIDER
SOCIAL MEDIA
APP FRAMEWORKS
CRM/MARKETING
UTILITY API
VERIFY THE DEFAULT SETTINGS!

Example: Fitbit once had the “sexual activity” visible to all by default.
From the analyzed apps
52% had no privacy policy

Apple.com

It is personal identifiable information, but not as we know it
“Apps that access HealthKit are required to have a privacy policy,...”
Jawbone: Who’s asleep during San Francisco earthquake 2014?

![Graph showing percentage of Jawbone users awake in different places during the earthquake.](image-url)
Larger proportion of the top 100 health apps leaked activity data through HTTP
Some apps accepted self-signed certificates or don’t check revocation lists

POST http://api.*****.com/Mobile/Functions.ashx?action=RegisterUser
  FName: ken
  LName: west
  GoalWeight: 68
  Email: kenwest@this.tld
  Password: P@SSw0rd

GET http://****.***/api/createUser?
  username=KenWest
  email=kenwest@this.tld
  password=P@SSw0rd

POST http://*****.*****.net/cgi-bin/account
  password: 8EEFB875DB938CEC08299BE7AA709EE0
  action: create
  email: kenwest@this.tld
  preflang: de_CH

No need to crack simply pass the hash
HTTP GET /api/getUser/877

[No authentication needed]

Name
Email
Password
Birthday
Photo
Nike_pwd
Fitbit_token
Withings_token
Google_uid
Facebook_access_token

Ideal for spammers
Email, context and
Social media accounts

Symantec.
blackhat®
EUROPE 2014
Dear User,
You have 1 new private message. Please go to …

Dear User,
You have 1 new SPAM message. Please click here…
POSSIBLE IMPACT

Account hijack
- The problem of password reuse
- Costs: Sign the user up for premium services, commitments, ...
- Change the privacy settings

Spam
- Enumerate user data to send spam with context
- Create dummy accounts & use profile page as spam landing pages
- Use social media accounts to find friends and spam them
Who said you have to run yourself? Dog-sitters?
POSSIBLE IMPACT Cont.

Loss of privacy
- Reveal personal details: Identity theft, profiling, extortion, ...
- Reveal Location: Stalking, burglar, kidnapping, corporate misuse, ...

Loss of integrity
- Modify/inject data: Gain rewards, high scores, frustrate other people ;-
- Delete the account and history
- Brick the device through firmware updates
BLUETOOTH LOW ENERGY

aka Bluetooth SMART and BTLE part of BT 4.0 (2010)

Different from classic Bluetooth
Does frequency hopping but can still be sniffed
Pairing has been broken (Mike Ryan)

”Bluetooth Smart (low energy) technology supports a feature that reduces the ability to track a Bluetooth device over a period of time by changing the address on a frequent basis.”

Bluetooth.org
SCANNING WITH A BLUEBERRY PI

TOTAL PRICE

$75

4GB SD Card
$5

Battery pack
$28

Raspberry pi
$35

Bluetooth 4.0 USB dongle
$7

OUR BLUETOOTH TRACKER
The phone may reveal the real name associated with the device. 30 from 563 devices had something like a person’s name:
- Rita :))
- Darren!
- Franks phone
- Erica
- Dawson
- Alieen's mobile!!:)
- Garret rip xxx
- Big hairy bollo
SCAN RESULTS FOR BLACKHAT EU 2014

203 BTLE devices and 21 wearable fitness trackers seen
SOME WANT THE DATA TO BE SEEN
SELF-TRACKING CAN BE RISKY FOR USERS

Your digital footprint will be everywhere!

- 20% Login credentials in clear text
- 14 Domains contacted by apps
- 52% Do not have a privacy policy
WHAT CAN USERS DO?

- Turn off Bluetooth if not required
- Keep device/software/OS updated
- Don’t reuse username/passwords
- Use strong passwords
- Look for a privacy policy
- Excessive information gathering
- Screen lock
- Device encryption
- Security software
<table>
<thead>
<tr>
<th><strong>BLOG</strong></th>
<th><a href="http://bit.ly/1pgGefW">http://bit.ly/1pgGefW</a></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WHITEPAPER</strong></td>
<td><a href="http://bit.ly/1nGB4vw">http://bit.ly/1nGB4vw</a></td>
</tr>
<tr>
<td><strong>TWITTER</strong></td>
<td>@threatintel</td>
</tr>
<tr>
<td><strong>WEB</strong></td>
<td><a href="http://www.symantec.com">http://www.symantec.com</a></td>
</tr>
</tbody>
</table>