Beyond files forensic
OWADEV cloud based forensic

Elie Bursztein  Stanford University
Ivan Fontarensky  Cassidian
Matthieu Martin  Stanford University
Jean Michel Picod  Cassidian
The world is moving to the cloud
2.7 millions photos are uploaded to Facebook every 20 minutes
100 millions new files are saved on Dropbox every day
Data are moving to multiple services

- Hard drive
- Cloud
- Emails
- Hotmail
- Contacts
- LinkedIn
- Photos
- Facebook

Beyond files recovery: OWADE cloud based forensic

http://owade.org
Impact on the forensic field

- There are more data which are harder to reach
- Dealing with cloud data force us to reinvent forensic
Let’s do cloud forensics
What is **cloud forensics**?
Facebook credentials as a use case

Getting Facebook credentials require to bypass 4 layer of encryption
Show you how to \textbf{bypass the encryption layers} and get the data you want
Introducing OWADE

• Dedicated to cloud forensics

• Decrypt / recovers
  • DPAPI secrets
  • Browsers history and websites credentials
  • Instant messaging creds
  • Wifi data

• Free and open-source

http://owade.org
OWADE Overview
Outline

• File base forensics refresher
• The Windows crypto eco-system
• Wifi data and Geo-location
• Recovering browser data
• Recovering instant messaging data
• Acquiring cloud-data
• Demo
File based forensic refresher
Not all files are born equal

<table>
<thead>
<tr>
<th>Type of file</th>
<th>how to recover it</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>copy</td>
</tr>
<tr>
<td>In the trash</td>
<td>undelete utility</td>
</tr>
<tr>
<td>Deleted</td>
<td>file carving</td>
</tr>
<tr>
<td>Wiped</td>
<td>call the NSA :)</td>
</tr>
</tbody>
</table>
• Hardware information
• Softwares installed with version and serials
• Windows credentials (encrypted)
Windows crypto
Many software use Windows Crypto APIs
The Windows crypto eco-system

Crypto API → DPAPI → Credential Manager

SAM → DPAPI
Basic cryptographic blocks

- Cipher: 3DES, AES
- Hash functions: SHA-1, SHA256, HMAC
- PKI: public keys and certificates (X.509)
The Security Account Manager (SAM)

- Store Windows user credentials
- located in the registry
- Encrypted with the SYSKEY
- Password are hashed
Windows Password Hashing functions

- Two hash functions used
  - LM hash function (NT, 2K, XP, VISTA) weak
  - NTLM (XP, Vista, 7)
- Password are not salted
LM hash weakness

- Use only upper-case
- Hash password in chunk of 7 characters

Password key-space: $69^{7}$ (at most)
Rainbow Tables

- Pre-compute all the possible passwords
- Time-Memory trade-off
- Rainbow tables of all the LM hash are available
How OWADE Works

• Extract Usernames and password hashes

• LM hashes available?
  • use John/Rainbow tables to get the pass in uppercase
  • use NTLM hashes to find the password cases

• Try to crack the NTLM using John/Rainbow table
If the password is too strong we can’t recover it
but we can still decrypt DPAPI secret (sometime)
The Data Protection API

- Ensure that encrypted data can’t be decrypted without knowing the user Windows password

- Blackbox crypto API for developers:
  - Encrypt data ➞ DPAPI blob
  - Decrypt DPAPI blob ➞ data
DPAPI derivation scheme

User → SHA1(password) → pre-key → master-key

master-key → blob key → DPAPI blob
master-key → blob key → DPAPI blob
master-key → blob key → DPAPI blob
Beyond files recovery: OWADE cloud based forensic

DPAPI blob

Master-key GUID

DPAPI blob

Master key

Cipher + key

User

SHA1(password)

Software

IV + Salt

Additional entropy
• If we can’t crack the password we need its SHA1

• This SHA1 is stored in the hibernate file

• OWADE use Moonsol to recover it
• If we can’t crack the password we need its SHA1
• This SHA1 is stored in the hibernate file
• OWADE use Moonsol to recover it
DPAPI additional entropy

• Software can supply an additional entropy
  • Act as a “key” (need for decryption)
  • Force us to understand how it is generate for each software
  • Can be used to tie data to a specific machine (i.e Netbios name)
Credential Manager

- Built on top of DPAPI
- Handle transparently the encryption and storage of sensitive data
- Used by Windows, Live Messenger, Remote desktop...
# Credstore type of credentials

<table>
<thead>
<tr>
<th>Type of credential</th>
<th>Encryption</th>
<th>Example of application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic password</td>
<td>DPAPI + fixed string</td>
<td>Live messenger HTTP auth (IE)</td>
</tr>
<tr>
<td>Domain password</td>
<td>in clear</td>
<td>Netbios</td>
</tr>
<tr>
<td>Domain certificate</td>
<td>hash of certificate</td>
<td>Certificate</td>
</tr>
<tr>
<td>Domain visible password</td>
<td>DPAPI + fixed string</td>
<td>Remote access .NET passport</td>
</tr>
</tbody>
</table>
WiFi data
• Info stored for each access point
  • Mac address (BSSID)
  • Password (encrypted)
  • Last time of access
• Wifi data are stored in
  • Registry (XP)
  • XML file and Registry (Vista/7)
Decrypting WiFi password

- Encrypted with DPAPI
- Access point shared among users
  - Encrypted with the System account
  - But the system account has no password...

What is my DPAPI key ???
Decrypting WiFi password

- Use a LSASecret as DPAPI key
- Recovered with Windows Credentials
Where are you?

• We’ve recovered access point keys but where are they?

Also found by Sami Kemvar
Where are you?

- We’ve recovered access point keys but where are they?

There is an app for that!

Also found by Sami Kemvar
Location-Aware Browsing

Firefox can tell websites where you’re located so you can find info that’s more relevant and more useful. It’s about making the Web smarter – and is done in a way that totally respects your privacy. Give it a try!

Frequently Asked Questions

+ What is Location-Aware Browsing?

+ How does it work?

+ How accurate are the locations?

+ What information is being sent, and to whom? How is my privacy protected?

+ Am I being tracked as I browse the web?
HTML5 Geo-location protocol

Location-Aware Browsing

Firefox can tell you where you are and you can find information that is useful. It's about privacy. Give it a try.

Frequently Asked Questions

- What is Location-Aware Browsing?
- How does it work?
- How accurate are the locations?
HTML5 Geo-location protocol
Google Wi-Fi Data Collection Angers European Officials

Brennon Slattery, PC World  May 17, 2010 7:08 am

European officials are still miffed over Google's "accidental" Wi-Fi data collection and seek an in-depth investigation that may lead to harsh penalties for the search engine giant.

It was revealed that Google's Street View cars were collecting more than images and coordinates for its sophisticated GPS site. As much as 600GB of data from Wi-Fi networks -- in more than 30 countries -- has been snagged in Google's fishnet.
Nothing is ever easy

- Google started to restrict queries in June :( 
- Fortunately for us there are other API :)
Geo-location API restrictions

Requires 2 MAC close from each other

The MAC and IP location need to be “close”

None

see [http://elie.im/blog/](http://elie.im/blog/) for more information
Browsers
Firefox > 3.4

- **Passwords**
  - location: `signons.sqlite`
  - encryption: **3DES + Master password**

- **History**
  - URLs: `places.sqlite`
  - Forms fields: `formhistory.sqlite`
Decrypting Firefox password

User → pass → user key: HMAC-SHA1 (salt, pass) → salt

-> encrypted key

master key: 3DES (userkey, enckey)

-> encrypted pass

Site password: 3DES (master key, enc pass)
Every form field is recorded

<table>
<thead>
<tr>
<th>id</th>
<th>fieldname</th>
<th>value</th>
<th>timesUsed</th>
<th>firstUsed</th>
<th>lastUsed</th>
<th>quid</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1 email</td>
<td><a href="mailto:testblackhat@devnull.com">testblackhat@devnull.com</a></td>
<td>1</td>
<td>1311823018543000</td>
<td>1311823018543000</td>
<td>CTw24359TYySue.76</td>
</tr>
<tr>
<td>2</td>
<td>2 enterAddressFullName</td>
<td>Allan Smith</td>
<td>1</td>
<td>1311823235859000</td>
<td>1311823235859000</td>
<td>FXpcwWuRqStomB+</td>
</tr>
<tr>
<td>3</td>
<td>3 enterAddressAddressLine1</td>
<td>42 my street</td>
<td>1</td>
<td>1311823235861000</td>
<td>1311823235861000</td>
<td>EFP3mGQES8rz76r</td>
</tr>
<tr>
<td>4</td>
<td>4 enterAddressCity</td>
<td>San Francisco</td>
<td>1</td>
<td>1311823235861000</td>
<td>1311823235861000</td>
<td>/infoGVLyT4onGoI Q</td>
</tr>
<tr>
<td>5</td>
<td>5 enterAddressStateOrRegion</td>
<td>CA</td>
<td>1</td>
<td>1311823235861000</td>
<td>1311823235861000</td>
<td>n8kFwyr6S3uaStsz2</td>
</tr>
<tr>
<td>6</td>
<td>6 enterAddressPostalCode</td>
<td>94302</td>
<td></td>
<td>1311823235862000</td>
<td>1311823235862000</td>
<td>etH8zZGQ26+2mnjC</td>
</tr>
<tr>
<td>7</td>
<td>7 enterAddressPhoneNumber</td>
<td>666-666-666</td>
<td></td>
<td>1311823235862000</td>
<td>1311823235862000</td>
<td>H01M4N7ITGUbOC</td>
</tr>
<tr>
<td>8</td>
<td>8 enterAddressAddressLine1</td>
<td>my street</td>
<td></td>
<td>13118232359915000</td>
<td>13118232359915000</td>
<td>h8bLVLgTFug1eDV</td>
</tr>
<tr>
<td>9</td>
<td>9 searchbar-History</td>
<td></td>
<td>1</td>
<td>1311823282115000</td>
<td>1311823282115000</td>
<td>joN8cylT2SsydQDN</td>
</tr>
</tbody>
</table>
Configuring a Linksys?
Again the key is recorded

![SQLite Database Browser](image)
Form history leak a lot of information

- Shipping address
- Wifi key
- Credit card information
- Email
- Search history
Preventing field recording

To tell the browser to not record a field use the tag

```html
autocomplete="off"
```
• Passwords
  • location: registry
• encryption: DPAPI + URL as salt
• History
  • URLs: Index.dat
  • Forms fields:
Decrypting Internet Explorer passwords

Registry → SHA1 (URL) → Site password → Registry

URL List

URL (dpapi entropy)
• Passwords
  • location: login data (sqlite)
  • encryption: DPAPI

• History
  • URLs: History (sqlite)
  • Forms fields: Web data (sqlite)
• Passwords
  • location: keychain.plist
  • encryption: DPAPI + fixed string as entropy
• History
• URLs: History.plist (Property list format)
• Forms fields: Form Value.plist
Browsers takeaway

• Internet Explorer is the most secure.
  • If you don’t know the URL you can’t recover the pass
• Firefox is the worst
  • Passwords encryption not tied to the Windows pass
  • Login are encrypted in signons.sqlite not in formhistory.sqlite
Private mode

- Most bugs are fixed
- Requires to be creative
  - SSL OCSP requests
  - File carving
- Potential techniques
  - Analyze the hibernate file

See: [http://ly.tl/p16](http://ly.tl/p16) for more information on private mode
Instant messaging
• Encryption custom
• Difficulty extreme
• Location registry + config.xml
Decrypting Skype passwords

1. Registry
2. DPAPI Blob
3. pre-key
4. AES key: SHA1(pre-key)
5. encrypted credential
6. MD5(login\nskyper\npassword)
7. config.xml

Login
pass cracking
Beyond files recovery: OWADE cloud based forensic

E. Bursztein, I. Fontarensky, J.M. Picod, M. Martin

http://owade.org

Google Talk

- Encryption
  DPAPI + custom (salt)
- Difficulty
  Hard
- Location
  registry
Salt derivation algorithm overview

String: 0xBA0DA71D → Windows account name

Registry

computer Netbios name

Registry

DPAPI Blob

Registry

Key
Microsoft Messenger

- **Encryption**
  - DPAPI or Credstore

- **Difficulty**
  - Medium

- **Location**
  - Version dependent
## Windows Messenger by version

<table>
<thead>
<tr>
<th>Version</th>
<th>Storage</th>
<th>encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Registry</td>
<td>Base64 encoded</td>
</tr>
<tr>
<td>6</td>
<td>Credstore</td>
<td>Credstore</td>
</tr>
<tr>
<td>7</td>
<td>Registry x2</td>
<td>DPAPI x 2</td>
</tr>
<tr>
<td>Live</td>
<td>Credstore</td>
<td>Credstore</td>
</tr>
</tbody>
</table>
- Encryption
  - DES
  - key: `substr(login . "dummykey", 8)`
- Difficulty
  - easy
- Location
  - `config.xml`
- **Encryption**
  - XOR
  - key: 9
- **Difficulty**
  - trivial
- **Location**
  - user.config
- **Encryption**
  - **Base 64 + XOR**
    - key: fixed string

- **Difficulty**
  - trivial

- **Location**
  - `user.config`
• Encryption
  Clear aka encryt-what?

• Difficulty
  none

• Location
  account.xml
Beyond files recovery: OWADE cloud based forensic

E. Bursztein, I. Fontarensky, J.M. Picod, M. Martin

http://owade.org

- Encryption
  - Custom

- Difficulty
difficult (offline)

- Location
registry
**Paltalk encryption algorithm**

- VolumeSerial Number: 01234567
- Paltalk account name: myusername
- encrypted password: \(y'y'y'z\) \(y'y'y'z\) \(y'y'y'z\)
- \(c_i: y'y'y'z_i - asciiCode(S-BOX_{n,i})\)

Key:

- Registry
- Registry
Messenger take away

- If the Skype password is strong you can’t recover it
- Gtalk and Paltalk are the only ones to use computer information
- 3rd party software are the least secure
Conclusion

• People moving to the cloud means more data that is harder to get
• Forensics needs to evolve to cope with this
• OWADE is the first tool dedicated to cloud forensic
  • Decrypt the 4 major browsers data
  • Decrypt Instant messaging credentials
  • Open-source
Download OWADE
http://owade.org

Follow-us on Twitter
@elie, @owade

Donate to OWADE to support it!