Deception 2.0
Social networks for information operations

Christophe DEVAUX
c christophe.devaux(at)sogeti.com

Arnauld MASCRET
arnauld.mascret(at)sogeti.com

Fred RAYNAL
frederic.raynal(at)sogeti.com
What is this talk about?

**Goal**
- *Recruit* someone from a target company

**How-to**
- Profile the company
- Profile groups of interest
- Profile a few individual targets
Warning

- This fiction is a fiction. We gathered the events to create a story, but this remains a fiction. However, characters, techniques and events are real.
- We will not talk about penetration testing: it is an option, it can be used here, but we assume you know what it is.
Contents

1. Overviews

2. From science to solutions: the company

3. From science to solutions: groups

4. From science to solutions: one guy
1. Overviews
   - Deception
     - Information gathering
     - Info op

2. From science to solutions: the company

3. From science to solutions: groups

4. From science to solutions: one guy
Illusions

- Operation Fortitude: code name during WW2 to persuade the Germans that the invasion was going to take place in the North of France and Norway
- Guilty spamming: accuse many men to cheat and reveal the secret if they do not pay a ransom to a paypal account
- Copyright violation: fake ICPP Foundation (icpp-online.com) in Europe, Kenzero trojan acting for Romancing Inc. in Japan
Basic rules to gather information

Common mistakes

- Know exactly what you are looking for
- Google is not the only way to get information on the Internet
- Internet is not the only way to get information
Cover your footprints

2 ways to get information

- **Direct**: you go straight to the one who has the needed information
  - The attacker can be detected while he collects information, or after
  - You get the most accurate information

- **Indirect**: either someone gets the info for you, or you don’t get near the target
  - Information can be less accurate
  - Harder to detect the attacker
Know exactly what you are looking for

Ask yourself the right questions

- What information do you really need?
- Who can have this information?
- Are there ways to deduce this information from other elements?

Making pizza in California

Q: how many pizzas a day can be cooked and frozen in this factory?

- $A_0$: count the doughs... but this requires to go to the factory :(
- $A_1$: estimate the amount of boxes in the delivery truck, and count the number of trucks a day
- $A_2$: go to the firemen, ask for the plan of the factory, deduce the capacity of the factory
Google in not the only way to get information on the Internet

<table>
<thead>
<tr>
<th>Think outside Google</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human: spock.com, theyrule.net, namebase.org, . . .</td>
</tr>
<tr>
<td>Network: netcraft.com, webhosting.info, ripe.net, allwhois.com,. . .</td>
</tr>
<tr>
<td>Misc.: opensecrets.org, sourcewatch.org, wikileaks.org, . . .</td>
</tr>
</tbody>
</table>
Internet is not the only way to get information

Technical hacking is not the only way

- Ask people, they are usually helpful
- Check old press coverage
- Dumpster diving, to get your hand on internal documents
Focus in this talk: LinkedIn & Facebook

A business oriented social network: LinkedIn
- Over 65 million members
- Focused in North America, but spreading worldwide
- Many employees from Fortune 500 companies are using LinkedIn

A friendly social network: Facebook
- 350 millions active users
- Half of them log in every day
- +40% users in less than 6 months
- Nearly 58% of the users are between 18 and 34 year old

\[http://www.checkfacebook.com/\]
Contents

1. Overviews
   - Deception
   - Information gathering
   - Info op

2. From science to solutions: the company

3. From science to solutions: groups

4. From science to solutions: one guy
Putting everything together

How things work (most of the time)

- Spot a target
- Attack this target
  - Environment: learn as much as you can
  - Intrusion: get to the target
  - Reliability: if needed, ensure a long term access to your target
- Analyze what you learnt from your target
- Go back to stage 1
Our (fake) operation

A 3 stage operation

- The company: find general information about the target, learn about the physical locations, the business, ...
- Interesting groups: depending on what you want to learn/do, get into some groups of people
- Individuals: target some people in the groups, profile them, then recruit them

Goal

- Long term pwnage of a company
- Every information about work with DoD is valuable
Contents

1. Overviews

2. From science to solutions: the company

3. From science to solutions: groups

4. From science to solutions: one guy

Know your enemy: who is he?
Know your enemy: what’s his business?
Goals of stage 1

Goal

- Find *places* (real or virtual) where to get information
- Learn about the target
Contents

1. Overviews

2. From science to solutions: the company
   - Know your enemy: who is he?
   - Know your enemy: what’s his business?

3. From science to solutions: groups

4. From science to solutions: one guy
Introduction

SAIC, Inc. provides scientific, engineering, systems integration, and technical services and solutions to the United States military, to agencies of the U.S. Department of Defense, to the intelligence community, to the U.S. Department of Homeland Security, and to other civil U.S. Government agencies.

Some figures (2008)

- Employees: around 45,000
- In 2009, they were number 9 contractor
- State business: US$6.6 billion
- General business: US$8.7 billion
- 5 years growth: +13.7%
History

SAIC over time

1969 - Created in San Diego by J. Robert Beyster, Ph.D.
1996 - Buys *Network Solution Inc*
2001 - US$122 million contract with the FBI: *Virtual Case File system*
2003 - New CEO: Kenneth C. Dahlberg
2004 - Handles security at the Athens Olympic games
2006 - Capital is opened to outsiders
Growth / People

Employees

- From science to solutions: the company
- From science to solutions: groups
- From science to solutions: one guy

Conclusion

Know your enemy: who is he?
Know your enemy: what's his business?
Annual sales

Growth / Money

Growth / Money

Deception 2.0
Contents

1. Overview

2. From science to solutions: the company
   - Know your enemy: who is he?
   - Know your enemy: what’s his business?

3. From science to solutions: groups

4. From science to solutions: one guy
Follow the money

What to look for?
- Business: customers, providers, nature of business, ...
- Who’s in charge?

How to look for it?
- Direct: what the target says itself, either on communication or legal issues
- Indirect: what customers, providers, the press say about the target
Auto-promotion

A company is often proud of its success:

http://www.saic.com/contractcenter/viewcon.html
## Business intelligence: lessons from the past

### Search Results for Jan 01, 1996 - Sep 26, 2009

<table>
<thead>
<tr>
<th>2000</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 pages</td>
<td>4 pages</td>
<td>4 pages</td>
<td>6 pages</td>
<td>27 pages</td>
<td>6 pages</td>
<td>14 pages</td>
<td>6 pages</td>
<td>4 pages</td>
<td>0 pages</td>
</tr>
</tbody>
</table>
Who are the customers?

What do we already know?
- Government agencies are important customers

Indirect information
- **Central Contractor Registration (CCR)**
  
  [https://www.bpn.gov/CCRSearch/Search.aspx](https://www.bpn.gov/CCRSearch/Search.aspx)
  ⇒ 227 records (March 25, 2010)

- USASpending: Where Americans Can See Where Their Money Goes (And not only the Americans)
  
  [http://www.usaspending.gov](http://www.usaspending.gov)
  ⇒ public contracts since 2000, statistics, ...
Emerging market: Iraq

Independent journalists

The Center for Public Integrity
http://www.publicintegrity.org

7 contracts for SAIC in Iraq

<table>
<thead>
<tr>
<th>Contract</th>
<th>Type of service</th>
</tr>
</thead>
<tbody>
<tr>
<td>DASW01-03-F-0500</td>
<td>Energy Expert</td>
</tr>
<tr>
<td>DASW01-03-F-0508</td>
<td>Technical Support for ORHA</td>
</tr>
<tr>
<td>DASW01-03-F-0512</td>
<td>Subject Matter Expert for ORHA</td>
</tr>
<tr>
<td>DASW01-03-F-0516</td>
<td>Expert Intelligence Analysis</td>
</tr>
<tr>
<td>DASW01-03-F-0533</td>
<td><strong>Free Media Program</strong></td>
</tr>
<tr>
<td>DASW01-03-F-0536</td>
<td>Iraq Expert Governmental Infrastructure</td>
</tr>
<tr>
<td>DASW01-03-F-0537</td>
<td>Three Experts Provide Advice for ORHA</td>
</tr>
</tbody>
</table>
Free Media Program: what is in the contracts?

Federal Funding Accountability and Transparency Act (FFATA)

- Contract number: PIID:DASW0103F0533
- Search on FFATA gives 4 results
- Each of these results has the same topic: *administrative management and general management consulting services*
- Supposed cost is US$ 15 million
- In the end, 82 millions...

<table>
<thead>
<tr>
<th>Date</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 27, 2003</td>
<td>$15,000,113</td>
</tr>
<tr>
<td>June 04, 2003</td>
<td>$3,127,660</td>
</tr>
<tr>
<td>July 03, 2003</td>
<td>$12,915,670</td>
</tr>
<tr>
<td>July 03, 2003</td>
<td>$51,307,114</td>
</tr>
</tbody>
</table>
Free Media Program: what does SAIC say?

Direct information: embarrassed silences

- Nothing on SAIC’s website...
Free Media Program: when the customer is dissatisfied...

Indirect information: what does the customer say?

- March 18, 2004: Report written by the general inspection at DoD

A modification issued to the contract with an effective date of July 18, 2003, was not signed until September 30, 2003. The value of the contract is $82.3 million through December 31, 2003. According to DCC-W contracting officials, the contract will not be renewed in December.

http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB219/
Free Media Program: ... the customer changes his provider

Indirect information: competitor

- January 9, 2004: statement by Harris Corporation

Harris Corporation

... today announced that it has been awarded a one-year, $96 million contract by The Defense Contracting Command-Washington (DCC-W), on behalf of the Coalition Provisional Authority (CPA) currently governing Iraq, for developing an existing but antiquated media network into a modern media organization for the Iraqi people.

What did we learn?

Know your enemy: the company
- What kind of business it does (customers & providers)
- Where the offices are
- How the company is structured
- ...

What’s next
- Find interesting groups/places
- Infiltrate them to learn more from the inside
- Use your general knowledge of the company
1. Overviews

2. From science to solutions: the company

3. From science to solutions: groups

4. From science to solutions: one guy
Goals of stage 2

Goal
- Find where is the information you want and/or who has it
- Study this target’s environment
- Gather less open information

Where to start with LinkedIn?
- List employees of the targeted company
- Then, find their groups
  - Area of influence of the company
  - Employees center of interests
Check the relevance

Get available information about the target

- To get the number of employees:
  - Check the company's official page on LinkedIn: **45,000**
- To get the number of employees on LinkedIn:
  - Use the advanced search field "current company": **17,635**

1 employee out of 3 uses LinkedIn
What groups do target’s employees belong to?

Very few information available if you are not in the group

- The number of members
  - But no data about who they are
- The owner
- The managers
- The members in your network

Tips

Possibly, find some members using the owner/manager profile

- People recommending/recommended
- Profiles also viewed
List employees in targeted corp

Search by current company

- 100 results by default (max. 700 with Pro account)
- Profiles are private (anonymized)
- Anonymized profile doesn’t show groups

Objectives

- Get as many employees as possible out of the 17,635
- Find a way to get the groups
Bypassing search limits

Search by current company

- Add filters using first name
- With a 2,900 first names dictionary, thanks Wikipedia ;)
  - With a free account: 8,707 employees
  - With a Pro account: 11,558 employees
- Total: 11,558 employees
De-anonymizing a profile

How to get the last name?

- Open the targeted profile
- Check the list of profiles also viewed
- For each profile, find a link to the targeted profile
  - Profile also viewed
  - People recommending/recommended

Specific information

- Groups: need a de-anonymized profile, even with an advanced account
- List of contacts: need to be a direct relation
De-anonymizing a profile

Using “profiles also viewed” features

People

Private
Chief Technology Officer at WhiteHat Security, Inc.
San Francisco Bay Area | Information Technology and Services

Current
- Chief Technology Officer at WhiteHat Security, Inc.

Past
- Information Security Officer at Yahoo!
- Systems Administrator at Amgen

Recommendations
5 people have recommended this user

Connections
500+ connections

Viewers of this profile also viewed...
Bill Pennington
SVP of Services at WhiteHat Security

Jeff Moss
Director of Black Hat, Founder of DEF CON, Member of Homeland Security Advisory Council

Dave Atlee
Owner, Immunity, Inc.

Trey Ford
Product Manager, SaaS Business Unit at McAfee

Viewers of this profile also viewed...
Dave Atlee
Owner, Immunity, Inc.

Jay Boate
Senior Security Analyst and Owner, InGuardians, Inc.

Jeremiah Grossman
Chief Technology Officer at WhiteHat Security, Inc.
Get the groups of a user

3 options

- Using an advanced account and a de-anonymized profile
- Using an account which shares a group with the target
  - Sharing a group de-anonymize a profile automatically
- Be in the target’s relations
Finding hidden contacts

Retrieving hidden contacts of a target

**Condition**: target is a level 1 relation

- Open a random profile
- If it is a level 2 relation:
  - there is a shared relation between the profile and me
  - Check if the shared relation is the target

Choosing *random* profile: try to guess who is a relation

- Select profiles from (shared) groups
- Select recommending / recommended people
- Select "also viewed" people
Finding hidden contacts

With a direct access to a profile

Bob Marley
Researcher in Computer Security
Paris Area, France | Computer & Network Security

How you're connected to Bob

You

Jimmy Hendrix

Bob Marley

You and this LinkedIn user don't know anyone in common

You can only view the profiles of users within your network. However, as you add connections, you may discover people you know in common.

Add Connections
Some facts

**Results**

- 45,000 employees
- 17,635 on LinkedIn
- We get 8,707 profiles and not just 100
- To get them, we used a 2,900 first names dictionary
- About 60% of the profiles can be de-anonymized
Conclusion

How to improve the tools efficiency

- Use dedicated accounts for collect
  - With many relations
  - In many different groups (bigger groups are preferred)
- Use *trashable* accounts for the generic collect
  - No captcha when creating a new account
  - No need to confirm the email address
  - Create a new account each time one is banned
Overviews

From science to solutions: the company
From science to solutions: groups
From science to solutions: one guy
Conclusion

A new hype

Contents

1. Overviews
2. From science to solutions: the company
3. From science to solutions: groups
   • A new hype
4. From science to solutions: one guy
Mixing virtual and real life

A good way to learn a lot

- Spot places where employees from the target gather or pass by
  - Airports, stations, bars, restaurants, ...
- Listen to their conversations
- Listen to their communications

⇒ Need to find another place to attack
Mixing virtual and real life

A good way to learn a lot

- Spot places where employees from the target gather or pass by
- Listen to their conversations
  - Put (micro)phones in chairs and so on
  - ... but it looks too much like old school James Bond
- Listen to their communications
⇒ Need to find another place to attack
Mixing virtual and real life

A good way to learn a lot

- Spot places where employees from the target gather or pass by
- Listen to their conversations
- Listen to their communications
  - Provide a free Access Point
  - And sniff everything
  - ... but websites are more and more secure, with SSL :(

⇒ Need to find another place to attack
Gathering information thanks to the iPhone

**iPhone: a new hype**

- Many people have one
- They install many applications, especially *social networks*
- Facebook, LinkedIn, Twitter, etc., all are on the AppStore (for free)

And... what about security? :)
Gathering information thanks to the iPhone

**Facebook application**
- Authentication uses HTTPS
- ... but only authentication :)
  ⇒ Cookies can be sniffed and replayed

**What can we do?**
- We are limited to the Facebook API
- We can’t install any Facebook application using it :(  
- But we can spy on user’s wall, friends, discussions, pictures, ...
- Cookie is valid as the user did not deliberately disconnect from the iPhone application
  - Cookies lifetime is set to one year :)
Goals of stage 3

Goal

- Profile the human target
- Find ways to get close to him
A star is born: Ed Horch

NSA Player Information: Ed Horch

Given name(s): Ed
Surname(s): Horch
Home: NJ, United States

Click to submit a photo

NSA = National Scrabble Association . . ;)

Deception 2.0
Contents

1. Overviews
2. From science to solutions: the company
3. From science to solutions: groups
4. From science to solutions: one guy
   - Direct information
   - Indirect information
   - Scrabble eggs
A star is born: **Ed Horch**

**Ed Horch**
System Administrator at SAIC  
Greater New York City Area

- **Current**
  - ClearCase and Unix/Linux System Administrator at SAIC

- **Past**
  - Member, Board of Trustees at Unitarian Universalist Congregation of Somerset Hills
  - Software Engineer at Leapstone
  - Software Engineer at Hewlett-Packard

- **Education**
  - Rutgers, The State University of New Jersey-New Brunswick
  - University of Alabama in Huntsville
  - Washington University in St. Louis

- **Recommended**
  - 1 person has recommended Ed

- **Connections**
  - 89 connections

- **Industry**
  - Computer Software

- **Websites**
  - My Website
  - My Blog

**Ed Horch’s Summary**
Software Engineer, System Administrator and Configuration Management Specialist with over 25 years of experience in all phases of Unix-based software development within global corporate settings. Expertise in software Deception 2.0

**Public profile powered by:** LinkedIn
Create a public profile: [Sign In](#) or [Join Now](#)

**View Ed Horch’s full profile:**
- See who you and Ed Horch know in common
- Get introduced to Ed Horch
- Contact Ed Horch directly

**Name Search:**
Search for people you know from over 60 million professionals already on LinkedIn.

First Name:  
Last Name:  
(example: Jeff Weiner)  
Search
Ed 2.0

Direct results found in less than 5 minutes

- General information
- His personal website: http://www.horch.org/
- His blog: http://edhorch.livejournal.com/
- His Twitter: http://twitter.com/edhorch
- His Facebook: http://www.facebook.com/edhorch
- His LinkedIn: http://www.linkedin.com/in/edhorch
Direct results found in less than 5 minutes

- **General information**
  - Whois/phone book: address, phone & fax number
  - DomainTools.com to search for other sites with EH92257
  - Watch the house with Google Maps Street
  - Main email: edhorch.org

- **His personal website:** [http://www.horch.org/](http://www.horch.org/)
- **His blog:** [http://edhorch.livejournal.com/](http://edhorch.livejournal.com/)
- **His Twitter:** [http://twitter.com/edhorch](http://twitter.com/edhorch)
- **His Facebook:** [http://www.facebook.com/edhorch](http://www.facebook.com/edhorch)
- **His LinkedIn:** [http://www.linkedin.com/in/edhorch](http://www.linkedin.com/in/edhorch)
Ed 2.0

Direct results found in less than 5 minutes

- General information
- His personal website: http://www.horch.org/
  - His resume, which does not mention SAIC
  - His wife and children (including pictures and story)
- His blog: http://edhorch.livejournal.com/
- His Twitter: http://twitter.com/edhorch
- His Facebook: http://www.facebook.com/edhorch
- His LinkedIn: http://www.linkedin.com/in/edhorch
Ed 2.0

Direct results found in less than 5 minutes

- General information
- His personal website: http://www.horch.org/
- His blog: http://edhorch.livejournal.com/
  - His day-to-day mood
  - His political involvement, including his support for Obama’s health reform
  - His hobbies: Scrabble and his Ford Fusion
  - His life, from his Grandma’s cancer to names of the systems he administrates at SAIC
- His Twitter: http://twitter.com/edhorch
- His Facebook: http://www.facebook.com/edhorch
- His LinkedIn: http://www.linkedin.com/in/edhorch
Direct results found in less than 5 minutes

- General information
- His personal website: http://www.horch.org/
- His blog: http://edhorch.livejournal.com/
- His Twitter: http://twitter.com/edhorch
  - His connections: 49 following, 45 followers, 9 listed
  - His comments on a live Scrabble tournament
  - Good quotes: *Tell me Hiro never used his time-stopping power just to get more sleep.*
  - He has a gmail account
- His Facebook: http://www.facebook.com/edhorch
- His LinkedIn: http://www.linkedin.com/in/edhorch
Ed 2.0

Direct results found in less than 5 minutes

- General information
- His personal website: http://www.horch.org/
- His blog: http://edhorch.livejournal.com/
- His Twitter: http://twitter.com/edhorch
- His Facebook: http://www.facebook.com/edhorch
  - Member of SAIC and Ford Fusion networks
  - More connections: 360 friends
- His LinkedIn: http://www.linkedin.com/in/edhorch
Direct results found in less than 5 minutes

- General information
- His personal website: http://www.horch.org/
- His blog: http://edhorch.livejournal.com/
- His Twitter: http://twitter.com/edhorch
- His Facebook: http://www.facebook.com/edhorch
- His LinkedIn: http://www.linkedin.com/in/edhorch
  - 89 hidden connections and 1 recommendation
  - Trace all his career and education
  - Groups: LOPSA, Hyperreal, UUCSH, RHPS
  - Interests: ClearCase, Unix, Linux, System Administration
His wife, Karen Reilly-Horch

Also very 2.0

- Member of many social networks and sites: Facebook, LinkedIn, Twitter, Amazon wishlist, ...
- Career: chemistry, then sysadmin, then full time mom since October 21, 2005, then part time sysadmin again
- Comes from the same university as her husband
- Participates in many health care related forums
Contents

1. Overviews
2. From science to solutions: the company
3. From science to solutions: groups
4. From science to solutions: one guy
   - Direct information
   - Indirect information
   - Scrabble eggs

Deception 2.0
Tax Records Search - Web Listings

⇒ local tax, account number, surface, value, ...

http://tax1.co.monmouth.nj.us/cgi-bin/prc6.cgi?
menu=index&ms_user=foo&passwd=bar&district=0801
Somerset County Clerk Web Site

⇒ All the 4 loans he subscribed . . .

MORTGAGE

THIS MORTGAGE ("Security Instrument") is given on May 30, 1997
The mortgagor is Edward Burnett Horch, Husband and Eileen Michelle Reilly-
Horch, Wife
American Federal Mortgage Corporation, which is organized and existing
under the laws of
1952 Route 22 East, Bound Brook, NJ 08805

TWO HUNDRED SEVEN THOUSAND DOLLARS AND 00/100 Dollars (U.S.
207,000.00) This debt is evidenced by Borrower’s note dated the same date as this Security
Instrument ("Note"), which provides for monthly payments, with the full debt, if not paid earlier, due and payable on
June 1, 2027 This Security Instrument secures to Lender (a) the repayment of the debt

("Borrower") Borrower owes Lender the principal sum of

("Lender")
Family house

http://earth.google.com/
Facebook to collect information

General configuration

- Relevant information can not be reached from the public page
- The wall is protected
- Connections can be viewed by anyone
- No advanced account
Applications in Facebook

How they work

- The user must register the application into his profile
- but an authorization is **required** to use it
- Grants access to private information
API Facebook: AJAX

Access user’s information
- All user’s information (name, location, ...)
- Everything published on the wall
- Access to the gallery

Access to connections
- List of friends
- Information about friends
- Messages published by friends
AJAX = JavaScript

JavaScript is mandatory to use Facebook

JavaScript library
- OS fingerprinting, browser (and plugins) detection
- IP Scanner on private network

Other information
- Connection date and frequency
- Browser history ⇒ Spear Phishing
Ed + Facebook = Scrabble egg

Scrabble spreading

- Create (fake) users who install our Scrabble application, send advertisement to real users too
- Lure Ed to install our application
- Targeted attack on Ed
  - Use Ed as a trojan horse
Ed + Facebook = Scrabble egg

Scrabble spreading

- Create (fake) users who install our Scrabble application, send advertisement to real users too
- Lure Ed to install our application
- Targeted attack on Ed
  - Learn from Ed’s behavior, OS, browsers, . . .
  - Select the proper exploits to own all Ed’s hosts
  - Total secrecy: the attack is launched only against Ed, for a short period of time :)  
- Use Ed as a trojan horse
Scrabble Egg architecture

Target

Trapped Application

Attacker

Server (hidden)
Contents

1. Overviews
2. From science to solutions: the company
3. From science to solutions: groups
4. From science to solutions: one guy
Conclusion

Such an operation is:

- Illegal: of course, but that does not mean some people don’t do it for living
  - Raytheon hiring Cyber Warrior and media sanitizer
- Non reversible: once an intruder is in the network, he cannot be removed
  - Ask hosting company Network Solutions, massively owned 2 times in the past few days
- Long: consider 3-6 months at least for such an operation
- Happening every day...
Last words

- Information is precious
- Technical hacking is not the only way of attacking
- Offensive is not always illegal