


# Social Engineering for Penetration Testers



Sharon Conheady

# Alternative names for this talk

- ✓ Buffer overflows are really hard, lying is easy+
- ✓ If you can't go through the firewall, go through the secretary+
- ✓ Too attack and surely take it, attack where they do not defend+

# A Definition



*efforts to influence popular attitudes and social behaviour on a large scale, whether by governments or private groups*

- Wikipedia definition



PICK-UPS  
"GOOD TIME" GIRLS  
PROSTITUTES  
**SPREAD SYPHILIS AND GONORRHEA**

You can't beat the Axis if you get VD

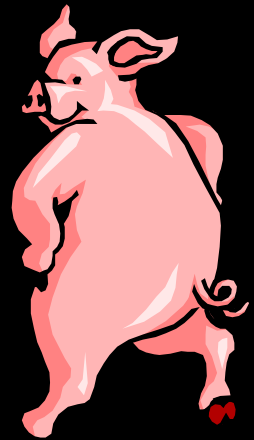
**CHANGE**  
WE CAN BELIEVE IN



- ✓ *Bush Down to 8 Friends on Myspace*
- ✓ *Jesus Christ to Star in Next Series of Batman*
- ✓ *Bush Claims He Has Supernatural Abilities*
- ✓ *Donald Trump missing, feared kidnapped*
- ✓ *What Annoyed Us About The Olympic Opening Ceremony*
- ✓ *Fox News Admits Grievous Error*
- ✓ *New Economic Stimulus Package Includes Goat*
- ✓ ***Preliminary US Presidential election polls results here***

# Swine Flu Social Engineering

- ✓ First US swine flu victims!
- ✓ US swine flu statistics
- ✓ Salma Hayek caught swine flu!
- ✓ Swine flu worldwide!
- ✓ Swine flu in Hollywood!
- ✓ Swine flu in USA
- ✓ Madonna caught swine flu!



# What is Social Engineering?

*techniques hackers use to deceive a trusted computer user within a company into revealing sensitive information, or trick an unsuspecting mark into performing actions that create a security hole for them to slip through*

- Kevin Mitnick



# Why social engineering works


- ✓ People want to help
  - ✓ Customer service focussed society (e.g. call centres)
- ✓ Greed
  - ✓ Passwords for chocolate
- ✓ Tendency to trust
- ✓ Complacency
  - ✓ It's easier to give people information to get rid of them
- ✓ Fear (of getting into trouble for not doing their job)
- ✓ People don't like confrontations
  - ✓ The yes rule

# Remote v\$ On Site v\$ Real World



- ✓ Remote
  - ✓ Email
  - ✓ Fax
  - ✓ Telephone
- ✓ On site
  - ✓ Extreme social engineering
  - ✓ Very effective but may be easier to get caught
- ✓ Next generation: real world attacks
  - ✓ Traffic ticket incident, February 2009

# Different types of attacks

- 
- ✓ Mumble attack
  - ✓ Reverse social engineering
  - ✓ Road apples
  - ✓ 10 attack
  - ✓ Phishing
  - ✓ Remote v's On Site v& Real World

# Is Social Engineering a real problem?

October 29, 2007

## Online raiders fool banks into handing over customers' details

Adam Fresco, Crime Correspondent

A gang of online bank robbers that has taken at least ten people and stolen hundreds of thousands of pounds is being hunted by an anti-fraud unit.

The gang hacked into private bank accounts and stole details to order new debit and credit cards which they used to buy expensive jewellery, electronic goods and other items.

The gang managed to get enough information to have £60,000 transferred from his mortgage repayment current account, which it then spent.

Barclays Bank managed to intercept much of the money but is believed to have stopped at least £500,000 being transferred to clients. But officers from the Dedicated Cheque Fraud Unit say that there may be many more victims.

### RELATED LINKS

- Government to police virtual worlds
- Online criminals target Facebook

Detective Constable Harrington said his favourite method, known as "account take over", in which the thieves got enough private information to convince a bank that they were the customer and then ordered a new card and PIN.

## Thief woos bank staff with chocolates - then steals diamonds worth £14m

By Stephen Castle in Brussels  
Sunday, 18 March 2007

A thief has evaded one of the world's most expensive hi-tech security systems to steal diamonds - than his victim's staff: personal details.

In what may be the conman burglar in Antwerp's diamond district, posing as a bank frequenter, he won their confidence to one diamond.

Now, embarrassed, wondering how to get away with a false Argentinian passport.

## Comcast hackers come forward

10/06/2008

hackers who successfully shut down the internet for hours have

admitted that they had said they were 'hacking themselves into'.

the age of shutting down a million

Print Email

## Boy tries to talk his way onto plane again

★★★★★ (No Ratings Yet)

Posted on: May 29th, 2008 by John Morgan

Last year, a 10-year old boy succeeded in boarding a flight to Texas with nothing but his wits and his smart mouth as a passport. On Tuesday, he tried it again, but was caught and stopped at the boarding gate, according to authorities.

Security tapes at Seattle-Tacoma International Airport show Semaj Booker successfully going through airport security before 05:00. The checkpoint and metal detector were operated by the Transport Security Administration.

At 03:00, Semaj's mother reported him missing to police in Tacoma.

Police are looking into how the boy was able to get so far in the airport through security without showing a boarding pass, according to the Northwest region spokesperson for the TSA in Salt Lake City, Dwayne Baird.

Semaj attempted to board a flight to Sacramento, California, operated by Southwest Airlines but was detained before he could do so, according to a statement from Perry Cooper, a spokesperson from the airport.

In January last year, Semaj successfully lied himself a seat on a flight operated by Southwest Airlines, claiming that his mother was in the boarding area. He changed planes in Phoenix and landed in San Antonio before he was caught. Days earlier, the boy stole and crashed a car.

# A Social Engineering attack on Twitter




" One of the admins has a yahoo account, i've reset the password by answering to the secret question. Then, in the mailbox, i have found his/her twitter password. I've used social engineering only, no exploit, no xss vulnerability, no backdoor, np sql injection."

- Hacker Croll, April 2009

# Why perform a social engineering test?

- ✓ To test the effectiveness of physical security controls
- ✓ To test the level of (and even improve) security awareness among staff
- ✓ To give your staff practice at identifying the techniques that social engineers may use and at learning how to deal with social engineering situations
- ✓ To provide valuable recommendations on both security awareness and physical security
- ✓ Often combined with a technical penetration test

# The stages of the attack

- 
1. Target identification
  2. Reconnaissance
  3. Creating your scenario
  4. Going in for the attack
  5. Getting out again
  6. (Writing the report)

# Before you start

*Community Chest*

**GET OUT  
OF JAIL, FREE**



**THIS CARD MAY BE KEPT UNTIL NEEDED OR SOLD**



# Reconnaissance (1)



## ” Passive information gathering

- ✓ Search engines
- ✓ Social networking sites
- ✓ Company website / Annual reports
- ✓ Job ads / Employee resumes
- ✓ Online developers forums
- ✓ Whois records
- ✓ Maltego
- ✓ Etc

# Reconnaissance (2)



## ” Physical reconnaissance

- ✓ Google Maps
- ✓ Where are the security guards?
- ✓ Do smokers congregate in a certain area outside?
- ✓ Where are the CCTV cameras?
- ✓ Watch staff movements. What time do employees go in / leave the office? What time do staff have lunch?
- ✓ Do staff wear and/or show passes? Can you copy them?
- ✓ Any unusual ways in? Fire escapes / garages /etc.

# Creating Your Scenario

- ✓ Think about how sophisticated your attack needs to be
- ✓ More security focused organisations, eg, banks, will require a more complex attack
- ✓ Use props
  - ” mobile phones, recording devices, ID cards, cups of coffee, folders/documents to deliver...
  - ” costumes: security jackets, hard hats, cleaners overalls, clipboard, suit, courier, pest control...



# The Times Top Ten Real-Life Spy Gadgets

1. Poison-tipped umbrella
2. Dart gun
3. Compass buttons
4. Exploding briefcase
5. Exploding rats
6. Cigarette-case gun
7. HOLLOWED-OUT lighter
8. Wallet document camera
9. Microphone in an olive
10. Rock bug

*the ultimate spy accessory*



# Creating Your Scenario

- ✓ Think about how sophisticated your attack needs to be
- ✓ More security focused organisations, eg, banks, will require a more complex attack
- ✓ Use props
  - ” mobile phones, recording devices, ID cards, cups of coffee, folders/documents to deliver...
  - ” costumes: security jackets, hard hats, cleaners overalls, clipboard, suit, courier, pest control...



# Sample scenarios - phone

- ✓ Internal IT support
- ✓ Freelance IT journalist
- ✓ Recruitment agent
- ✓ Charity worker
- ✓ ISP abuse team member



# Sample scenarios . on site

- ✓ Tailgate (not really a scenario but often works . try carrying two cups of coffee)
- ✓ Employee / Temp
- ✓ Delivery guy
- ✓ Girlfriend/boyfriend
- ✓ Workman / engineer
- ✓ Fire warden
- ✓ Cleaner/security/main tenance
- ✓ **Do not impersonate real people or organisations!**

# Going in for the attack

- ✓ Use your scenario to get in
- ✓ Gain access to network
- ✓ Prove you were there
  - ✓ Trophy gathering . physical and electronic
  - ✓ Leave a token
  - ✓ Take photos
  - ✓ Make some internal phone calls
- ✓ Have an exit strategy




# Reporting



- ✓ Tell the story
- ✓ Standard pen test report with methods used, vulnerabilities, recommendations
- ✓ Use photos and other evidence
- ✓ Don't name individuals

# A few tips

- 
- ✓ Use a false name, but use your own first name.
  - ✓ Consider using a surname that sounds like your own
  - ✓ Be a woman (preferably a foreign one)
  - ✓ Flirt / use flattery
  - ✓ Offer an incentive
  - ✓ Get a job

# Secrets of Success



✓ Balance of Power

✓ Time Travel . or how to be an effective liar

Hello Bob,

I hope you don't mind me emailing you. I found your graduate profile on your company website and got your email address from reception.

I am a final year student studying Computer Science, Linguistics & French at Trinity College Dublin. I am currently looking for a job for when I finish university. I am very interested in your company's Graduate Development Programme. It looks like it has lots of variety and would be good experience for someone coming from an IT background who is looking to get into the financial side of things. Although I aim to have a career in finance, I am concerned about starting this with a degree in computer science. I was wondering what your opinion on this move may be, or if you know of any other graduates who may have done something similar who I could talk to.

The closing date for graduate applications is next Wednesday 23rd December, so I am trying to do all my research and get the application in as soon as possible. I would appreciate any views you have on this matter.

Thanking you in advance,

Sharon Conheady

Hi Sharon,

I am very impressed with your guile in getting my email address. I am more than happy to receive your email.

You should not be at all concerned with whether your degree course is not relevant for the job. We pride ourselves on not being a Degree Snob organisation. A lot of my fellow grads have come from backgrounds such as Physics, Classics, History etc so we aren't concerned with that. I think the fact you do computer science is a benefit, because you will have developed analytical and logic skills which are very important. Also your linguistics background demonstrates communicative skills. You will need to try and get this across in the application form.

If you need any other help on the application form feel free to ask - you can call me or you can email me. There will be an area on the form asking where you heard about the job - if you put my name down it will show that you've taken time and initiative to talk to me, and its something I would certainly mention to the Grad HR Team.

As I said if you have any other questions feel free to ask.

Bob

Hi Bob,

Thanks for replying. It is good to hear that your company does not insist on having a finance or a business degree. I know some of the banks do, and that has put me off.

I am actually in London tomorrow and Wednesday for a last minute interview, so I was wondering if it might be possible to come in for a quick 15 minute visit and see the kind of thing you do in your company and maybe go through some of my answers on the application form.

Do you think I could meet you or someone from Graduate Recruitment to do this?

Thanks again for all your help - it is very much appreciated.

Sharon

Yeah - if you need directions just let me know.

I will let Reception know you are coming so just report to reception and they will give you a pass.

# What can go wrong?

- ✓ You are recognised
- ✓ Balance of power backfires
- ✓ Overcompensate by giving too much detail
- ✓ Laws you might break
  - Trespass, Deception, Breaking and Entering, Going equipped, Theft, Vandalism, Impersonating a government official, etc

=> BE PREPARED!



# How to prevent social engineering attacks

- ✓ Education & Awareness
- ✓ Social engineering testing
- ✓ Security policy
- ✓ Vet your staff
- ✓ Get your staff involved
- ✓ Don't trust anyone!

# Questions



Social Engineering for Penetration Testers

Sharon Conheady

[sharon@conheady.co.uk](mailto:sharon@conheady.co.uk)