

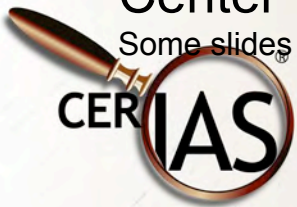
ITaP Presentation: Social Engineering

Pascal Meunier, Ph.D., M.Sc., CISSP

March 14, 2007

Some slides developed thanks to support and contributions from Symantec Corporation, support from the NSF SFS Capacity Building Program (Award Number 0113725) and the Purdue e-Enterprise Center

Some slides copyright (2004) Purdue Research Foundation. All rights reserved.



Social Engineering

- Social engineering is used to exploit human behavior to violate policies (implicit or explicit)
- I see four types, from the victim's point of view:
 - Passive
 - ❖ Unaware
 - Blissfully unaware anything is wrong
 - ❖ Not wanting to get involved
 - "Not my job"
 - Agent
 - ❖ Unaware
 - "Perfect Con"
 - ❖ Coerced (no physical threat)
 - "I shouldn't be doing this, but..."

Importance of Trust

- Common tactic: establish a trust relationship and exploit it
 - Trust starts by identification
 - but must be followed by authentication!
- Most S.E. problems are related to identification without authentication
 - "I am so and so, and ..."
 - Fake badges, uniforms
- Identification by impression and persuasion
 - Logos
 - Theater (confidence, dress, body language, tone of voice)
 - Knowledge of specific information

Attacker Goals

- Avoid providing a reason for passive victims to get involved
- Get physical or logical (e.g., remote) access
 - steal
 - read
 - plant
 - modify
- Manipulate agents towards objective
 - Reveal information
 - Perform actions

Social Engineering Exploit Vectors

- User Interfaces
 - Exploiting UI limitations
- Phone
- Email
- Letters, printed documents and signs
- Instant Messaging, Phone Texting
- Media: CDs, DVDs, USB keys, etc...
- Physical Presence
 - Body language
 - Clothes, etc...

Related concepts

- Pretexting
 - a.k.a. lies, fibs to extract information
- Phishing
 - Deceiving a user into using a fake web site
- Nigerian Scam
- Identity theft
 - Pretending to be someone else, e.g., calling support while on a trip (with no way to authenticate the call)
- Trojans
 - Deceiving a user into running a malicious program
- Physical Security
- Recon

Recon & Exposures

- Exposures give information to an attacker that helps make a social engineering attack more convincing
- Source: "Dumpster Diving"
 - Vacation or trip calendars
 - ❖ May help determine when to call support, pretending to be absent person
 - ❖ When to show up with a "package" for them, to gain (unsupervised?) access to their desk and even office computer
 - Phone or employee lists
 - ❖ "I would have called so-and-so (real names) but they are not there. Can you open the door for me?"
 - Orders
 - ❖ What may need "servicing" or "be taken for repairs"

Exposures

- Anybody can give another example of an exposure?
- Describe a common strategy for limiting exposures

Exposures

- Anybody can give another example of an exposure?
 - Exposed computer screens (e.g., shoulder surfing)
 - Vacation email auto-responders
 - Company phone directories accessible by phone
 - Technical help forums
- Describe a common strategy for limiting exposures
 - Paper shredders
 - ❖ Do you have a policy for identifying and handling sensitive printed information?

Physical Presence (Physical Security)

- Door behaviors
 - Tailing someone through a door
 - Holding the door for someone
 - Secure areas
 - ❖ Locked areas
 - ❖ Guarded areas
 - ❖ Backdoors
- Theater & Lies
 - Attacker tactics
 - Victimized behaviors and social contracts
- Physical Trojans, a.k.a. "road apples"

Example Common Scenarios

- **Passive**
 - You wave your FOB key near the detector or unlock a building door
 - You go in
 - Attacker catches the door before it finishes closing and follows
 - You don't challenge or report attacker and keep going
- **Active**
 - "Please, hold the door, I have my hands full! Thanks!"
 - Someone calls your number from the door and asks to be "buzzed in" by saying "Please let me in, I forgot my key home and it's a 45 minute drive" and if necessary "I work/live on floor X, my name is _____, don't you remember me?"

Door Behavior Experiences

- Bomb alert
- Everybody evacuated
- After building was declared clear, people were let back in
 - Needed to prove identity and business in building
- Person tried to sneak in, pretending to be with my group
- Declared to the guard, "This person isn't with us"
 - Person was stopped and interrogated
- Made me feel like a jerk
 - Security isn't always pleasant

Door Behavior Experiences

- I didn't have the keys to a room where I was going to present
- I needed to prepare
- My escort was late
- Someone saw me waiting at the door, looking distressed and all dressed up
- Opened the door for me (room had expensive equipment and communicated with a secure area)
- On another occasion I was let into a locked room simply by politely asking a receptionist
 - Was it common sense or was my story made up?

Other Experiences or Examples

- Can anybody describe another door social engineering scenario?

Social Engineering Theater

- Authority
- Specific knowledge
 - I'm here to pickup server #KA-019 for repairs
- Begging
 - Just this time, only for 10 minutes
 - I need to go to the bathroom! Now, please, it's urgent!
- Appearance
 - Clipboard
 - Uniform
 - Suit
- Impatience and annoyed stance
- Politeness

Social Attitudes of Victims

- Helpful employees and "team players"
 - So and so is not here, but I'll find the document (s)he promised you
- Ingratiation (a.k.a. "brown-nosing")
- Conformity, peer pressure
- Diffusion of responsibility, disengagement
 - Not my job
 - Laziness and conformity
 - ❖ The door is propped open? Oh who cares...
- Friendliness
 - Conflict avoidance: Should I raise a stink?

Victim Personnel

- Lack of self-confidence
 - I don't want to lose my job over this
 - What if I made a mistake and he's really here to see the VP?
- Lack of authority
- Enterprise culture
 - Lack of education about security problems
 - Ill-defined responsibilities

Willing Victims

- 70% of respondents in a 2004 study would have given their passwords in exchange for chocolate
 - 34% volunteered their passwords anyway
 - One can hope they would have simply lied to get the chocolate
 - Reference:
<http://news.bbc.co.uk/1/hi/technology/3639679.stm>
- 79% unwittingly gave away exposures
 - date of birth
 - mother's maiden name
 - RSA Security study (at same url)
- 90% gave passwords for a pen in a 2003 survey
 - <http://www.out-law.com/page-3496>

Cognitive Biases that Help Social Engineering

- Halo effect
 - Attractive, well-dressed, well-spoken people are more believable
- Ingroup bias
 - Preferential treatment given to members of own group
 - ❖ I'm just doing my job (just like you)
- Confirmation bias
 - Tendency to interpret information in a way that confirms one's preconceptions
- http://en.wikipedia.org/wiki/List_of_cognitive_biases

Social Engineering: Hierarchy/Authority

- You get a phone call from the CFO, on a trip, "I can't remember the VPN password, and I need a document now!"
- Your account will be terminated tomorrow unless you take action, as described in this attachment!
- Please help me get my money out of this crazy country!
- Oh, no, I forgot my key/badge/token!

Exploiting Human Curiosity with Media (USB Key Story)

- USB keys loaded with trojans and malware spread around parking lot
 - bait!
- Employees arriving for work picked them up
- Put them in their computers to look
- Trojan collected passwords, logins, etc... and emailed findings to attackers
- Reference:
http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1
- Could be camera memory, etc...

User Interface

- Poor user interface design may facilitate social engineering
- Example:
 - In some email programs, someone could be fooled into thinking that an attachment was a safe file, and open it. What appeared as "resume.txt" was in reality
 - ❖ "resume.txt" .exe"
 - User interface design affects the security of applications!

Exercises

- Identify a user interface limitation that may allow social engineering

Example Answers

- Identify a user interface limitation that may allow social engineering
 - Phishing email scams
 - ❖ Look-alike web sites that capture passwords

Reverse Social Engineering

- Instead of asking for information and help, you provide it initially
 - Except the given instructions are detrimental
- Of course they need help because of something the attacker did
- Alternatively, some attackers call random numbers until they find someone who asked for help

What to do

- Try to recognize possible attack situations
- Follow procedures and policies
 - Inform yourself of what they are
 - If you're in charge, do you have security procedures?
 - ❖ Did you train your employees?
- Possible examples:
 - Regular employees should take note of suspicious people inside the building
 - ❖ Ask around if anyone vouches for them
 - ❖ Don't confront them
 - Report them to security
 - Propped-open security doors must be attended by a guard

Signs That You May Be a Under Attack

- You know you shouldn't be doing this
 - But you feel compelled to do it anyways
- It feels weird, uncomfortable
- You're in a situation where you can't ask the appropriate person for confirmation
 - Or you are made to think so
- You are being rushed
- Names and titles are being used ("name dropping")
- You're afraid to offend, delay, or of being a jerk (insert epithet)

Exercise for you to do later

- Proper responses are easier to enact if practiced
- Team up in groups of 2 or 3 and make up a skit to demonstrate a social engineering technique; your "victim" will be another person in the audience who will "fall for it". Follow it up with a second version showing the correct response. Do try to obtain the most outrageous results possible (while being convincing). After the skit, explain the preparation you would have needed to conduct the attack.
 - You can get inspiration from the table of correct responses (Granger 2002):
 - ❖ <http://www.securityfocus.com/infocus/1533>

Movies

- "Catch me if You Can" (movie based on Frank Abagnale's story)
 - Amongst other things, man "steals" schoolgirls from headmistress in the school itself (!) by pretending to be a pilot recruiting hostesses
- Ace Ventura, Pet Detective
 - Ace pretends to be a delivery person in order to "dognap"

See Also

- Granger S. (2001, 2002) Security Focus "Infocus" articles on Social Engineering
- Wikipedia
[http://en.wikipedia.org/wiki/Social_engineering_\(computer_security\)](http://en.wikipedia.org/wiki/Social_engineering_(computer_security))
- CSEPS, Certified Social Engineering Prevention Specialist
- "The Art of Deception" (Kevin Mitnick)

Contributors

Jared Robinson, Alan Krassowski, Craig Ozancin, Tim Brown, Wes Higaki, Melissa Dark, Chris Clifton, Gustavo Rodriguez-Rivera

