CS 5410 - Computer and Network Security: Social Engineering

Professor Patrick Traynor
Fall 2017
Announcements

- Assignment #2 due at 5pm
- Project Proposals due in class on Wednesday (9/20).
  - Practice selling these to each other…
- Class on Wednesday/Friday will be online
Social Engineering

- Exploiting human psychology or processes to obtain information or access
  - Bad guys
  - Advertisers
  - Governments
  - Friends
  - Academic advisors ...

- The art of manipulation.
Exploiting Human Nature

- People ...
  - are trusting
  - respect (perceived or real) authority
  - are socially conscious, e.g., personal space
  - are subject to flattery/criticism
  - are subject to intimidation
  - have unfounded fears and biases
  - are sometimes driven by cultural prejudices
  - can be lonely
  - don't think clearly around attractive/influential people
  - want easy answers/solutions
  - want solutions/answers that agree with existing beliefs
Social engineering is about lying.
FUD (Fear Uncertainty Doubt)

- Playing to fears to get you to do something that you would not do in other circumstances
  - allow privacy invasion
  - purchase dubious products
  - provide information
    - 3am call from your bank...
- In our field, be especially aware of the “four horsemen”
  - terrorists, pedophiles, drug dealers, and organized crime
Lying

- Telling a lie is a mental process that
  - requires *creativity*
  - may *involve stress*
  - manifest in *visual or auditory queues*

**Consequence**: detecting lying (and thus dealing with social engineering) is the practice of combating the lies.
Lie detectors (Polygraphs)

- Lie detectors physiological “tells” when presented with questions or information
  - breathing
  - heart rate
  - blood pressure
  - electro-dermal activity (sweatiness)
- Used in crime investigations, job interview (e.g., NSA)
- Systems are beatable with training, National Academy of Science Study (2003) indicates that they are better than a guess, but not really accurate ...
  - "a level slightly greater than chance, yet short of perfection"
- Spies could pretty effectively beat the system
Detecting Lying

• **Look at the Physical**: Look for visual queues of discomfort, lack of eye contact, or fidgety
  • Trained/practiced liars will be good at controlling this

• **Be skeptical of the improbable**: something far-fetched is likely not to be true (Occam’s Razor)
  • Hint: you don’t win lotteries you don’t enter

• **Detect Incomplete information**: watch for resistance to provide clarification or evidence (or stalling ...)

• **Don’t be flipped**: a good liar will sometimes attempt to put you on the defensive
  • “We need to check/validate your identity to proceed ..”

• **Changing the subject**: ignoring requests for validation
How to lie successfully

1. Know what the lie is before you say it.
2. Repeat the lie many times to yourself (or in a mirror) such that you don’t have to think of how to say it. Try to think of it as being “the truth”.
3. Prepare answers to follow on questions.
4. Be aware of your body language.
5. Relax ... breath, sit/stand normally.
Social Engineering

• Question: how do we use good lying skills to exploit users ....?
Pretexting

- Pretexting is the art of setting up a scenario wherein the victim’s behavior is...
  - totally acceptable under the perceived events
  - exploitable by the bad guys
- **Goal**: get the victim to disclose something they should not, or to permit the adversary to perform something they shouldn’t

- For example, let’s learn *how to rob a bank*...
How to rob a bank ...
January 16, 2008

On Wednesday, a man dressed as an armored truck employee with the company AT Systems* walked into a BB&T bank in Wheaton about 11 a.m., was handed more than $500,000 in cash and walked out, a source familiar with the case said.

It wasn't until the actual AT Systems employees arrived at the bank, at 11501 Georgia Ave., the next day that bank officials realized they'd been had.

*AT Systems was an armored truck company (now GARDA)
Stop (in the name of the law)!
... in the digital domain.

- The game becomes easier for the attacker because there is not physical context ...
Email Scams

• E-mail has been historically a vehicle for lots of social engineering
  • Nigerian Finance Minister
  • Lottery
  • Useless or overpriced goods (male enhancement, teeth whitener)
  • “help desk” requests

• Note: often just online versions of existing cons
Phishing

• **Definition:** falsely claiming to be from authority in hopes of extracting private information

• **Game:** make you think you are in one place you trust (your local bank), whereas you are in another (the bad guys computer)
  - DNS games (e.g., www.hotmail.bob.com)
  - Misleading URLs (e.g., bin encoding)
  - Forging address bar (e.g., JavaScript)
  - Fraudulent Instant messages

• **Spear Phishing**
  - Extract personal information for user
  - Use that information to appear to be more legitimate.
    - E.g., if they know your boss’s name ...
  - Can be used to setup pretexting

*Can you tell the difference?*
Baiting

- Create “lure” object and let the victim come to you.

- Examples:
  - Leave an infected thumb drive in Starbucks with a auto-run executable that infects the hard drive.
  - Latest PC game on file sharing networks.
  - Link to porn movie (.mov), actually an executable on website
    - Then get google to point to it.
Dumpster Diving

• You can learn a lot by going through somebody’s trash ...
  • Who are your friends
  • Who are your co-workers/boss
  • What projects you are working on
  • What your company plans are
  • Where/what you eat
  • Your address, phone number, URL, email address
  • What credit cards you have
  • ....

• ... the basis for a really good social engineering attack.
Enterprise Security Policy

- Policies dictate how the organization operates and how it does not operate

- Reasonable (but often painful) policies include:
  - Passwords *should never be given out to anybody* over email or phone
  - Nobody should enter the building without verified company credentials
  - Nobody external to the enterprise should ever be allowed to roam the building unescorted
  - No external person should ever be left alone in a company office
  - Only employees should be allowed on company networks/computers

- Company policy should be documented and enforced
  - Education for employees, consequences if no followed

- Policy should include incidence response plans for when these breaks occur
... its all about education

- The key to preventing social engineering is making everyone sensitive to the threat
  - talk about how people will exploit you
  - be knowledgeable about what is sensitive
  - follow the organizational policy
  - if something does not feel right, it isn’t
  - never assume anything you get from forgeable source (e.g., mail, phone, unknown person) is true/real

- Reporting
  - all attempts at social engineering should be reported within the organization, and the proper procedures for dealing with it very clearly articulated
  - reports should be widely disseminated and discussed