

CSE 484 / CSE M 584 (Winter 2013)

Social Engineering & Physical Security

Tadayoshi Kohno

Thanks to Vitaly Shmatikov, Dan Boneh, Dieter Gollmann, Dan Halperin, John Manferdelli, John Mitchell, Bennet Yee, and many others for sample slides and materials ...

Goals for Today

- ◆ Social Engineering
- ◆ Physical Security

Social Engineering

Social Engineering

- ◆ Art or science of skillfully maneuvering human beings to take action in some aspect of their lives
 - From **Social Engineering: The Art of Human Hacking** by Christopher Hadnagy
 - (Also see: **The Art of Deception: Controlling the Human Element of Security** by Kevin Mitnick and William Simon)
- ◆ Used by
 - Hackers
 - Penetration testers
 - Spies
 - Identity thieves
 - Disgruntled employees
 - Scam artists
 - Executive recruiters
 - Salespeople
 - Governments
 - Doctors, psychologists, and lawyers

Information Gathering

◆ “No information is irrelevant”

◆ Example:

- Know that company executive collects stamps (see forum post related to stamp collecting)
- Call executive, mention recently inherited a stamp collection
- Send follow-up email, with a link (behind which is malware)
- Information used: email address, phone number, information about interest in stamps

Information to Collect

◆ About a company

- The company itself
- Procedures within the company (e.g., procedures for breaks)

◆ About individuals

Elicitation

- ◆ To bring or draw out, or to arrive at a conclusion by logic. Alternately, it is defined as a stimulation that calls up a particular class of behaviors
 - Being able to use elicitation means you can fashion questions that draw people out and stimulate them to take a path of behavior you want.
 - (From Social Engineering: The Art of Human Hacking by Christopher Hadnagy)
- ◆ NSA definition: “the subtle extraction of information during an apparently normal and innocent conversation.”

Why Elicitation Works

- ◆ Most people have the desire to be polite, especially to strangers
- ◆ Professionals want to appear well informed and intelligent
- ◆ If people are praised, they will often talk more and divulge more.
- ◆ Most people would not lie for the sake of lying
- ◆ Most people respond kindly to people who appear concerned about them.

Example

- ◆ Them: I'm the CEO...
- ◆ You: Wow, you're the person with the big bucks.... What do you do?
- ◆ Them: We make X, Y and ..
- ◆ You: Oh, you're the company that makes Z. I *love* Z! I read that it reached record sales
- ◆ Them: Yeah, did you know ...
- ◆
- ◆ You: You know, this is an odd question, but my boss asked me to look into new RFID security systems for our doors. I suspect you might know something about that, given your position...

Strategies

- ◆ Appeal to Someone's Ego
- ◆ Express a Mutual Interest
- ◆ Make a Deliberately False Statement
- ◆ Volunteer Information
- ◆ Assume Knowledge
- ◆ Use the Effect of Alcohol

Pretexting

- ◆ The background story, dress, grooming, personality, and attitude that make up the character you will be. Everything you would imagine that person to be.
 - Another definition: creating an invented scenario to persuade a targeted victim to release information or perform some action.
 - (From Social Engineering: The Art of Human Hacking by Christopher Hadnagy)

Principles and Planning

- ◆ The more research you do, the better chance of success
- ◆ Involving your own personal interests will increase success
- ◆ Practice dialects or expressions
- ◆ Phone can be easier than in person
- ◆ The simpler the pretext, the better the chance of success
- ◆ The pretext should appear spontaneous
- ◆ Provide a logical conclusion or follow-through for the target

Now on to physical security

- ◆ Relate **physical security** to **computer security**
 - Locks, safes, etc
- ◆ Why?
 - More similar than you might think!!
 - Lots to learn:
 - Computer security issues are often very abstract; hard to relate to
 - But physical security issues are often easier to understand
 - Hypothesis:
 - Thinking about the “physical world” in new (security) ways will help you further develop the “security mindset”
 - You can then apply this mindset to computer systems, ...
 - Plus, communities can learn from each other

Not Online

- ◆ The following slides will not be online
- ◆ But if you're interested in the subject, we recommend
 - Blaze, "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks"
 - Blaze, "Safecracking for the Computer Scientist"
 - Tool, "Guide to Lock Picking"
 - Tobias, "Opening Locks by Bumping in Five Seconds or Less"