THE ROLE OF PEOPLE IN SECURITY

“Technology alone will not solve the security problem”

Reading

• Textbook Chapter 4
Objectives

• Understand
  • Basic terminology
  • Steps organizations can take to improve their security
  • Common user actions that may put an organization’s information at risk
  • Methods attackers may use to gain information about an organization
  • Ways in which users can aid security

Social Engineering

• Highly successful attack component
• The process of convincing an authorized individual to provide to an unauthorized individual
  • confidential information or
  • access controlled space or information
• The attacker uses deceptive practices to
  • Convince someone to divulge information they normally would not divulge
  • Convince someone to do something they normally wouldn’t do
• Social engineering is successful because people
  • Want to be helpful
  • Want to avoid confrontation
Example – Edward Snowden

- Reported on 2/13/14
- Colleague entered his/her password on Snowden’s computer
- Snowden captured the password
- Snowden used the colleague’s identity for access to documents (1.7M+)
- Snowden colleague (perhaps supervisor) forced out of NSA

Snowden is currently living in an undisclosed location in Moscow

Social Engineering Techniques…

- Ask a question – hoping the responder will be helpful
- Engage the target in a conversation, and attempt to be sympathetic (harsh boss, medical emergency, facing financial ruin, etc.)
- Appeal to target’s ego (praise target for work they did previously, the ask for help with a problem)
- Intimidation – threaten to call the target’s boss
- Exploit target’s biases and beliefs
…Social Engineering Techniques

- Attacker claims authority – leads to situation in which the target might fear consequences of refusal to provide info
- Consensus – attacker asserts request is common practice
- Familiarity – people do things for people they like
- Urgency – encourages shortcuts in a process
- Impersonation – attacker pretends to be someone they are not

Recent Example …

- On 1/18/2019 2:29 PM, Dr. Fotis Sotiropoulos wrote:
  - Are you available?
  - *Fotis Sotiropoulos, Ph.D*
  - Dean, College of Engineering and Applied Sciences
  - Professor of Civil Engineering
  - Stony Brook University

Message tp Polychronakis, who is a CS security expert, so he played along with the request
Recent Example …

*From:* Michalis Polychronakis <mikepo@cs.stonybrook.edu>
*Sent:* Friday, January 18, 2019 2:37 PM
*To:* Dr. Fotis Sotiropoulos
*I’m not on campus today :( Feel free to call me at 936-666-xxxx if needed.

...Recent Example ...

On 1/18/2019 3:00 PM, Dr. Fotis Sotiropoulos wrote:
*Ok. I am currently in a meeting and I dont know when the meeting
*will round off. I would have call you but phone is not allow. I
*will want you to handle something for me right away and I will
*be glad if you can do that for me asap.*
*Fotis Sotiropoulos, Ph.D*
*Dean, College of Engineering and Applied Sciences*
*Professor of Civil Engineering*
*Stony Brook University*
**Recent Example**

*From:* Michalis Polychronakis  
<mikepo@cs.stonybrook.edu>

*Sent:* Friday, January 18, 2019 3:01 PM  
*To:* Dr. Fotis Sotiropoulos
*Subject:* Re: Are you available on campus

Sure, how can I help

---

**Recent Example**

*On 1/18/2019 3:03 PM, Dr. Fotis Sotiropoulos wrote:*  
I will really be glad if you can handle this for me asap.I need  
you to help me get Apple itunes cards from the store, I will  
reimburse you back when I get back to the office.I need to send it  
to someone and it is very important. I'm still in a meeting and I need  
to get it sent right away.  
Please let me know if you can do that now?  

*Fotis Sotiropoulos, Ph.D*  
Dean, College of Engineering and Applied Sciences  
Professor of Civil Engineering  
Stony Brook University
...Recent Example...

• *From:* Michalis Polychronakis  
  <mikepo@cs.stonybrook.edu>  
• *Sent:* Friday, January 18, 2019 3:06 PM  
• *To:* Dr. Fotis Sotiropoulos  
• *Subject:* Re: Are you available on campus  
• Ummm.. OK, I think I can do it from my apple account. What amount?

...Recent Example...

• On 1/18/2019 3:09 PM, Dr. Fotis Sotiropoulos wrote:  
  Have you order for Apple itunes card before on your account?  
  I need 5 pieces of the card @ $100 denomination on each card.  
  If you want to process on your apple account, you will need to  
  purchase 1 @  
  $100 first and after the E-code has been sent to you, then you will  
  be able to purchase the remaining 4 cards as well after 5 mins  
  interval  
  *Fotis Sotiropoulos, Ph.D*  
  Dean, College of Engineering and Applied Sciences  
  Professor of Civil Engineering  
  Stony Brook University
...Recent Example

*From:* Michalis Polychronakis <mikepo@cs.stonybrook.edu>
*Sent:* Friday, January 18, 2019 3:13 PM
*To:* Dr. Fotis Sotiropoulos
*Subject:* Re: Are you available on campus

OK, got it. Can you send me the department's credit card number so that I can use it for the purchase? Or should I just call Lisa to give it to me?

More Social Engineering Techniques

- **Third party authorization** – create the appearance of a third party authorization when there is none (e.g., appearing in an office claiming to be authorized by a person who happens to be away)
- Help desk support – either a call claiming to be help desk or a call from an attacker to a help desk
- Contractors – organizations usually have outside contractors for routine chores, so attacker can gain entry by impersonating a contractor
- **Shoulder surfing** – directly observe target entering sensitive information
Obtaining Insider Information

- 1978 Stanley Mark Rifkin stole $10.2 million from the Security Pacific Bank
  - This was a social engineering attack involving the technique of obtaining insider information.
- Rifkin
  - Was a computer consultant for the bank
  - Obtained the information needed to do wire transfers
  - Impersonated a bank officer, and ordered a transfer of $10.2 million to a bogus account in a New York bank
  - Transferred that money to an account in Switzerland
  - Used the money to buy diamonds
  - Was caught after bragging
  - Served eight years in prison

Indirect Methods

- Phishing - acquiring private information by masquerading as a trustworthy entity in an electronic communication
- Pharming – misdirecting users to fake web sites made to look official
Vishing

• Use of voice technology to obtain information
  • Variation of phishing
  • Takes advantage of the trust people place in correctness of Caller ID
  • Attackers spoof calls from legitimate entities using VoIP
  • Voice messaging can ask to call a number (trap)
  • Attackers hope to obtain credit card numbers or other information for identity theft.

• Successful because
  • With caller ID, people believe they can identify who is calling them.
  • Caller ID can be spoofed.

Recognizing Phishing

• Analyze any e-mails received asking for personal information carefully
• Organizations should warn their users
  • Never send e-mails asking for personal information
  • Never request passwords
• Watch for technical or grammatical errors or a different language style
• Unusual URL address

Basis for these attacks is program-generated e-mail
Spear Phishing & Pharming

• Spear phishing
  • Modification to normal phishing attacks
  • Special targeting using specific information
  • Designed to trick user into believing message is genuine
  • Targets high-importance individuals, or “whales”

• Pharming
  • Redirects the user to a bogus website
  • Appears similar to the original
  • Convinces the user to give information

Shoulder Surfing

• Attacker directly observes sensitive information by
  • Looking over the shoulder of the user
  • Setting up a camera
  • Using binoculars

• Targeted information
  • Personal identification number (PIN) at an ATM
  • Access control entry code at a secure gate or door
  • Calling card or credit card number

• Defenses
  • Small shield to surround a keypad
Reverse Social Engineering

• The victim initiates contact with the social engineer
• Can result in increased trust
  • Trick is in convincing user to initiate contact
  • (e.g., spoofed e-mail with a “help phone number”)
  • Easier to do during times of change or confusion
    • Company merges with another
    • One or more new hires that are not familiar with the company
    • New software roll out

• Not as well known as normal social engineering.

Security Hoaxes

• Hoaxes designed to elicit user reaction
  • Asked to delete a file, or
  • Change a setting, or
  • Spread the word

• Example
  • Request to delete software modules

• Defense
  • Training and awareness
Poor Security Practices

- Users create security problems via poor practices
  - Password selections
  - Writing secrets (e.g., passwords) down
  - Leaving a session (or a secure access door) open
  - Installing unauthorized hardware/software
  - Discarding secure information (available via dumpster diving)

Password Selection …

- Users tend to pick passwords that are easy for them to remember
  - Dates
  - Names
  - +1,2,3 on changes Mary1, Mary2, Mary3
- If it’s easy for them to remember, it means that the more you know about the user, the better your chance of discovering their password
… Password Selection

- General rules for good password selection
  - Use eight or more characters in your password
  - Include a combination of upper- and lowercase letters
  - Include at least one number and one special character
  - Do not use a common word, phrase, or name, and
  - Choose a password that you can remember so that you do not need to write it down.
  - Think of a phrase, song, poem or speech that you know by heart.
    - Use the first letter of each word in the phrase.
    - Jack be nimble, jack be quick, jack jumped over the candlestick
    - Becomes Jbnjbqjj0tcs!

Dictionary Attacks

- Brute force (systematic guessing) attacks are much simpler if passwords are dictionary words
- A given language might have 10K-40K words in a dictionary
- Relatively simple to iterate through all the possible words
Piggybacking

• Following closely behind a person who has just used their own access card to gain physical access to a room or building.
  • Relies on the attacker taking advantage of an authorized user not following security procedures.
  • i.e. returning from a smoking area
• Countered by
  • Training and awareness
  • Guards
  • Man trap

Dumpster Diving

• Process of going through a target's trash
• The tactic is not unique to the computer community
  • Identity thieves, private investigators, and law enforcement personnel have done it for years to obtain information about an individual or organization
• Sensitive information should be shredded.
• Consider securing the trash receptacle.
• Consider shredding personal or sensitive information you discard in the trash.

Shredding not easily available in many offices
Installing Unauthorized Hardware and Software...

• Establish a policy that restricts users installing software and new hardware on their systems
• Common examples:
  • unauthorized communication software to allow users to connect to their machine from home
  • Installing a wireless access point so that they can access the organization’s network from many different areas
  • user has set up a backdoor into the network, circumventing all the other security mechanisms in place

...Installing Unauthorized Hardware and Software

• Another example - games
• Many organizations do not allow their users to load software or install new hardware without authorization.
• Many organizations also screen, and occasionally intercept, e-mail messages with links or attachments
  • This helps prevent users from unwittingly executing malware.
• Many organizations have their mail servers strip off executable attachments to e-mail
Physical Access by Non-Employees

- If an attacker can gain physical access, the attacker can penetrate computer systems and networks more easily
- Organizations frequently become complacent when faced with a legitimate reason to access the facility.
- Physical access provides opportunity for individuals to look for critical information carelessly left out
- Cell phones cameras a risk (e.g., no cameras in certain areas)
- Many organizations require that employees wear badges
- Important (but difficult) for employees to challenge those without badges

People as a Security Tool

- People can be an effective security mechanism
  - Policies and procedures
  - Training and awareness
  - Many eyes
  - Challenge visitors
  - Report abnormal conditions
- Make everyone responsible and involved
Security Awareness

- A security awareness program will vary depending on
  - The organization’s environment
  - The level of threat
- Initial employee training on social engineering
  - As well as periodic refresher training
- Clean Desk Policy
  - Keeping workplace clean of information to prevent disclosure to others during casual interactions
  - All information secured when not physically there to guard it

Individual User Responsibilities ...

- Lock doors
- No sensitive information in your car
- Secure storage media containing sensitive information (e.g., flash drives)
- Shred sensitive documents before discarding.
- Do not divulge sensitive information to individuals not authorized to know it
- Do not discuss sensitive information with family members
… Individual User Responsibilities

• Protect laptops that contain the organization’s information.
• Be aware of who is around you when discussing sensitive information.
• Enforce corporate access control procedures.
• Report suspected or actual violations of security policies
• Follow procedures established to enforce good password security practices

Did You Achieve the Objectives?

• Understand
  • Basic terminology
  • Steps organizations can take to improve their security
  • Common user actions that may put an organization’s information at risk
  • Methods attackers may use to gain information about an organization
  • Ways in which users can aid security