Social Engineering

Bo Luo
bluo@ku.edu

Social Engineering

- Q1: What is Social Engineering?

- A:
  - The art and science of getting people to comply with your wishes.
  - An outside hacker's use of psychological tricks … in order to obtain information [needed] to gain access to the system.
  - Getting needed information …from a person rather than breaking into a system.

Social Engineering

- "You could spend a fortune purchasing technology and services...and your network infrastructure could still remain vulnerable to old-fashioned manipulation."

-Kevin Mitnick

Password Authentication

- Social engineering
  - shoulder surfing, dumpster diving, …
  - A more complicated example: 2009 Twitter Hack (a.k.a. Hacker Croll)
    - Step 1: know an email account of a Twitter employee
      - use public information to build profile of company/person
      - find an entry point
        - » an employee with a personal Gmail account
        - » answer "security question", system sends password reset link to a secondary email:******@h******.com
        - » guess it's hotmail.com
        - » guess username from public information
    - Step 2: hotmail.com account no longer active
      - register it
      - get a reset link and reset the password

Password Authentication

- Social engineering
  - Step 3: analyze old email to learn the original password
    - e.g., lost password messages from other Web services
    - restore password to original so owner doesn't notice

> *To: Lazy User*
> *From: Super Duper Web Service*
> *Subject: Thank you for signing up to Super Duper Web Service*
>
> *Dear Lazy User,*
>
> *Thank you for signing up to Super Duper Web Service. For the benefit of our support department (and anybody else who is reading this), please find your account information below:*
>
> *username: LazyUser*
> *password: funsticks*
>
> *To reset your password please follow the link to.. ahh forget it, nobody does this anyway.*
>
> *Regards,*
>
> *Super Duper Web Service*

Password Authentication

- Social engineering
  - Step 4: use the found password to log into Twitter employee's work account on Google Apps
    - download and post 310 internal Twitter documents
  - Step 5: rinse and repeat
    - use the same username/password combination and password reset features to access AT&T, Amazon, iTunes
  - Step 6: hack other accounts using "secret questions"
  - Result: Croll obtained access to Twitter's high profile executives' numerous internet accounts
- Lessons learned:
  - a mix of many mistakes!
  - a fundamental problem is identification/registration

Social Engineering

- Weakest link
  - No matter how strong your:
    - Firewalls
    - Intrusion Detection Systems
    - Cryptography
    - Anti-virus software
  - You are the weakest link in computer security!
  - People are more vulnerable than computers
  - "The weakest link in the security chain is the human element" -Kevin Mitnick

Social Engineering

- Key features:
  - Uses Psychological Methods
  - Exploits human tendency to trust
  - Goals are the Same as Hacking
- Why social engineering
  - Easier than technical hacking
  - Hard to detect and track

Social Engineers

- More like actors than hackers
- Psychologists?
- Learn to know how people feel by observing their actions
  - can alter these feelings by changing what they say and do
  - make the victim want to give them the information they need

Social Engineering Approaches

- From psychological point of view
  - Carelessness
  - Comfort Zone
  - Helpfulness
  - Fear

Careless Approach

- Victim is Careless
  - Does not implement, use, or enforce proper countermeasures
- Used for Reconnaissance
- Looking for what is laying around

Careless Approach

- Dumpster Diving/Trashing
  - Huge amount of information in the trash
  - Most of it does not seem to be a threat
  - The who, what and where of an organization
  - Knowledge of internal systems
  - Materials for greater authenticity
  - Intelligence Agencies have done this for years

Careless Approach

- Building/Password Theft
  - Requires physical access
  - Looking for passwords or other information left out in the open
  - Little more information than dumpster diving

Careless Approach

- Password Harvesting
  - Internet or mail-in sweepstakes
  - Tester for password strength
  - Based on the belief that people don't change their passwords over different accounts

Comfort Zone Approach

- Victim organization members are in a comfortable environment
  - Lower threat perception
- Get into the comfort zone
  - People are less defensive
- Usually requires the use of another approach

Comfort Zone Approach

- Impersonation
  - Could be anyone
    - Tech Support, Co-Worker, Boss, CEO, User, Maintenance Staff
  - Generally Two Goals
    - Asking for a password
    - Building access - Careless Approach

Comfort Zone Approach

- Shoulder Surfing
- Direct Theft
  - Outside workplace
  - Wallet, id badge, or purse stolen
- Smoking Zone
  - Attacker will sit out in the smoking area
  - Piggy back into the office when users go back to work

Comfort Zone Approach

- Insider Threats
  - Legitimate employee
  - Could sell or use data found by “accident”
  - Result of poor access control
  - Asking for favors from IT staff for information
    - Usually spread out over a long period of time

Helpful Approach

- People generally try to help even if they do not know who they are helping
- Usually involves being in a position of obvious need
- Attacker generally does not even ask for the help they receive

Helpful Approach

- Piggybacking
  - Attacker will trail an employee entering the building
  - More Effective:
    - Carry something large so they hold the door open for you
    - Go in when a large group of employees are going in
  - Pretend to be unable to find door key

Helpful Approach

- Troubled user
  - Calling organization numbers asking for help
  - Getting a username and asking to have a password reset

Fear Approach

- Usually draws from the other approaches
- Puts the user in a state of fear and anxiety
- Very aggressive

Fear Approach

- Conformity
  - The user is the only one who has not helped out the attacker with this request in the past
  - Personal responsibility is diffused
  - User gets justification for granting an attack.

Fear Approach

- Time Frame
  - Fictitious deadline
  - Impersonates payroll bookkeeper, proposal coordinator
  - Asks for password change
- Importance
  - Classic boss or director needs routine password reset
  - Showing up from a utility after a natural occurrence (thunderstorm, tornado, etc)

Social Engineering

- Approaches from technical point of view
  - Quid Pro Quo
  - Phishing
  - Baiting
  - Pretexting

Quid Pro Quo

- Something for Something
  - Call random numbers at a company, claiming to be from technical support.
  - Eventually, you will reach someone with a legitamite problem
  - Grateful you called them back, they will follow your instructions
  - The attacker will "help" the user, but will really have the victim type commands that will allow the attacker to install malware

Phishing

- Fraudulently obtaining private information
  - Send an email that looks like it came from a legitimate business
  - Request verification of information and warn of some consequence if not provided
  - Usually contains link to a fraudulent web page that looks legitimate
  - User gives information to the social engineer
  - Ex: Ebay Scam

Phishing

- Spear phishing
  - Specific phishing
  - Ex: email that makes claims using your name
- Vishing
  - Phone phishing
  - Rogue interactive voice system
  - Ex:call bank to verify information

Phishing

Warning: This message has had one or more attachments removed
Warning: (Fraud report.zip, Fraudreport.exe).
Warning: Please read the "ITTC-Attachment-Warning.txt" attachment(s) for more information.

One new alert was received on monday 11/14/2011.

We have detected a new personal loan application submited from non-associated location. I have attached a loan application received from Bank of Hawaii. Please see details in report below to verify or approve the request.

FRAUD PREVENTOION DEPARTMENT

EQUIFAX
Equifax Credit Information Services, Inc
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

Phishing

Thank you for subm ha itting your information for potential empl ijw oyment opport qt unities.
We look forward to reviewing your appl gms ication,
but can not do so until you comp zuu lete our internal application.

The pay range for available posi cel tions range from $35.77 per hour to $57.62 per hour.
Prior to begin able to be consi bog dered, you will first need you to formally apply.
Please go here to be pze gin the process:

www.url5.tk/69s <http://url5.tk/69s>

Also, the following perks are pote pe ntially ava qdd ilable:

- Pa rc id Time Off
- Hea uf lth Benefits Package
- Hig zj her than average salaries
- Tuition Reim jhq bursement
- Exte bp nsive 401(k)program

Phishing

Your Federal Tax Payment ID: 05472767 has been rejected.
Return Reason Code R21 - The identification number used in the Company Identification Field is not valid.

Please, check the information and refer to Code R21 to get details about
your company payment in transaction contacts section:

MailScanner has detected a possible fraud attempt from "astola.com.au" claiming to be http://eftps.gov/R21
<http://astola.com.au/le4ojw/index.html>

In other way forward information to your accountant adviser. EFTPS:
The Electronic Federal Tax Payment System
PLEASE NOTE: Your tax payment is due regardless of EFTPS online availability.
In case of an emergency, you can always make your tax payment by calling the EFTPS.

Phishing

Warning: This message has had one or more attachments removed
Warning: (USPSreport.exe, USPS report.zip).
Warning: Please read the "ITTC-Attachment-Warning.txt" attachment(s) for more information.

Hello!

Unfortunately we failed to deliver the postal package you have sent on the 19th of September in time because the recipient's address is erroneous.

Please print out the shipment label attached and collect the package at our office.

United States Postal Service

Phishing

Warning: This message has had one or more attachments removed
Warning: (report485770.pdf.exe, report 485770.pdf.zip).
Warning: Please read the "ITTC-Attachment-Warning.txt" attachment(s) for more information.

The ACH transfer (ID: 59284589058169), recently initiated from your bank account, was canceled by The Electronic Payments Association (NACHA).

Please download the attachment(transfer report pdf).

If you have any questions please contact us at info@nacha.org.
Thank you for using http://www.nacha.org.

Patrick Wilson
Department of Risk Management,
Insurance & Loss Prevention.
NACHA

3450 Sunrise Valley dr.

Phishing

DO NOT REPLY TO THIS EMAIL! IT IS AUTOMATICALLY GENERATED!

It has been 446 days since you changed your ITTC password. This is the current ITTC Password Policy:

Passwords must conform to the following guidelines:

* Must be different than the user's login name
* Must be at least seven characters
* Must include a digit (0-9), and at least one upper and one lower case character (a-z, A-Z)
* Must use a special character (for example, ! @ # 0 ^ &)
* You cannot change your password to your existing password
* Your password must be changed every 6 months
* You cannot share your password with anyone!

To change your password:

* Go to http://password.ittc.ku.edu

If you have any problems or concerns, please email help@ittc.ku.edu

Baiting

- Real world Trojan horse
  - Uses physical media
  - Relies on greed/curiosity of victim
  - Attacker leaves a malware infected cd or usb drive in a location sure to be found
  - Attacker puts a legitimate or curious lable to gain interest
    - Ex: "Company Earnings 2009" left at company elevator
    - Curious employee/Good samaritan uses
    - User inserts media and unknowingly installs malware

Pretexting

- Invented Scenario
  - Prior Research/Setup used to establish legitimacy
    - Give information that a user would normally not divulge
  - This technique is used to impersonate
    - Authority etc.
    - Using prepared answers to victims questions
    - Other gathered information
  - Ex: Law Enforcement
    - Threat of alleged infraction to detain suspect and hold for questioning

Controls against Social Engineers

- User Education and Training
- Identifying Areas of Risk
  - Tactics correspond to Area
- Strong, Enforced, and Tested Security Policy

User Education and Training

- Security Orientation for new employees
- Yearly security training for all employees
- Weekly newsletters, videos, brochures, games and booklets detailing incidents and how they could have been prevented
- Signs, posters, coffee mugs, pens, pencils, mouse pads, screen savers, etc with security slogans (I.e. “Loose lips sink ships”).

Areas of Risk

- Certain areas have certain risks
- What are the risks for these areas?
  - Help Desk, Building entrance, Office, Mail Room, Machine room/Phone Closet, Dumpsters, Intranet/Internet, Overall

Security Policy

- Management should know the importance of protecting against social engineering attacks
- Specific enough that employees should not have to make judgment calls
- Include procedure for responding to an attack