Psychological Principles in Social Engineering

September 20, 2011
Introductions

- Joe Sechman, CISSP|CISA|CSSLP, Director of Attack and Penetration Testing Practice
- Robert Carr, CISSP|OSCP, Senior Manager within Attack and Penetration Testing Practice
Presentation Goal

• Increase awareness regarding social engineering techniques by examining common psychological principles and real-world examples

• *Disclaimer* we are NOT psychologists or law enforcement
What is Social Engineering?

Social engineering is the ability to manipulate people, by deception, into giving out information or performing an action.²

Psychological Principles

- Conformity (Solomon Asch)
- Obedience to Authority (Stanley Milgram)
- Ingratiation (J.S. Seiter)
- Influence/Persuasion (Robert Cialdini)
Conformity

• Conformity

• The act of matching attitudes, beliefs, and behaviors to what individuals perceive is normal of their society or social group.
Conformity

• Types

  • Informational
    • An individual seeks information from the group to come to a decision.

  • Normative
    • An individual changes their behavior in public to align with the group.
Conformity

• The Asch Experiment
  • Tested whether individuals will conform with a group.
  • All but one of the participants were confederates of the experiment.
Conformity

• The Asch Experiment

• “Vision Tests”
Conformity

• “Vision Test”

• Results

  • 18 subjects

    • 74% of subjects complied at least once.

    • 32% of responses were compliant
Conformity

- “Vision Test”
  - Further Observations
    - None of the participants complied 100%
  - Criticisms
    - Societal Views
      - What is compliant and what is polite?
Conformity Examples

• Cults

  • Jonestown Massacre
    • Led by Jim Jones
    • November 18, 1978. 913 victims

  • Heavens Gate
    • Led by Marshall Applewhite and Bonnie Nettles
    • March 26, 1997
    • Leaving human existence for alien life (Hale-Bopp)
Conformity Social Engineering Examples

- Physical
  - Tailgating a Group
- Phishing
  - Group Inclusion/Pressure Emails
    - Peer Emails to join fake/new social site or job focused site
Conformity Social Engineering Examples

• Phishing Example:

Dear Target,

There are currently 15 members of your company who have enrolled in CorporateLink.com. The following is a list of members from your company who joined CorporateLink.com today:

  Smith
  Jones
  Wright
  James

Join now:  http://malicioussite.com/join.php

CorporateLink Team
Obedience to Authority

- Milgram Experiment
  - Three participants
    - Teacher (volunteer)
    - Learner (confederate)
    - Experimenter
Obedience to Authority

• Milgram Experiment

  • The Learner is setup with an electrode attached to his arm.

  • The Teacher and Learner are in different rooms but can communicate with each other.

  • The Teacher is shown equipment that will deliver electric shock to the Learner when a wrong answer is given.
Obedience to Authority

• Milgram Experiment Results

  • Pre-test surveys predicted that 1-3/100 participants would deliver the 450 volt shock.

  • 26/40 participants delivered the 450 volt maximum shock
Obedience to Authority Examples

• The Holocaust

  • A motivating factor for the Milgram Experiment
  
  • Nazi guards viewed atrocities as “following orders” and managed completely separate, and seemingly “normal” lives
  
  • Objectification and increasingly horrendous atrocities enabled guards to become desensitized
Serial Killers

Obedience / Authority

• Business Owners Recruited Victims
  • John Wayne Gacy
  • Wayne Williams

• Abuse of Authority
  • Dennis Rader
  • Ted Bundy
Obedience to Authority SE Examples

- Social Engineering Examples
  - Hierarchy Jumping
    - Phishing
    - Phone
    - Physical
Obedience to Authority SE Examples

• Social Engineering Examples

• Phishing

Target,

Our Audit team needs you to fill out the attached questionnaire immediately. Please open the attached document, answer the four questions in the space provided and click submit.

Regards,

Internal Audit
Ingratiation

- Ingratiation
  - Becoming more likeable to a target
Ingratiation

• Seiter Ingratiation Experiment

• Food servers will receive significantly higher tips when they compliment their customers than when they do not.

• Servers complimented patrons on their order in about half of the cases.
Ingratiation

• Seiter Ingratiation Experiment

• Results

  • Complimented Patrons Left
    • 18.94% Gratuity
  • Control Patrons Left
    • 16.41% Gratuity
Ingratiation Examples

- Serial Killers
  - Employ Ingratiation to claim victims
    - Jeffrey Dahmer
    - John Wayne Gacy
  - Employ Ingratiation against investigators
    - Inquire about details of the investigation, may also draw unnecessary suspicion
      - 1996 Olympic Park Bombing
      - Dennis Rader, BTK Killer
Ingratiation Social Engineering Examples

• Physical Compliments
  • Knowledge
  • Dress
  • Age Based

• Phishing Compliments
  • Performance Based
  • Accolades of Public Material
Ingratiation Social Engineering Examples

• Phishing

Dear Target,

We noticed that you have obtained your CISSP, CISA and CSSLP. Congratulations, you must have worked very hard!

We are looking to people like you who are accomplished within industry and model mentors to help students and recent graduates looking to establish a career in information security.

Please take a few minutes to review our program as it won't require a large time investment and can help the next generation of professionals.

http://maliciouswebsite.com/mentor_program.aspx

Regards,

Security Mentor Group
Influence/Persuasion

• Cialdini
  • Weapons of Influence
    • Reciprocity
    • Commitment and Consistency
    • Social Proof
    • Authority
    • Liking
    • Scarcity
Influence/Persuasion Examples

- Scarcity
  - Home Shopping Channels
    - Offers are only available for a limited time
    - Countdown is available on the screen
    - Time frames are mentioned
      - Time left to Christmas
Influence/Persuasion Examples

- Scarcity
  - Physical
    - Late for a meeting
  - Electronic
    - Phishing
      - 24 hour deal
Influence/Persuasion Examples

• Phishing

All,

We are upgrading our email server tonight at 3 a.m. EST. To ensure that you do not get locked out of your account and that you can continue to use your mobile device, you will need to login to our OWA server as soon as possible.

https://malicious.com/owa/

Regards,

IT
Predicting Behavior

- Criminal Profilers
  - Robert Ressler
  - John Douglas
  - Roy Hazelwood
Criminal Profilers

• Pioneered the art of applying psychological principles to criminal investigations using detailed interviews with convicted serial killers

• By observing and comparing their findings, profilers were able to “get into the mind” of the serial killer and create guides to local law enforcement to track down killers

• These approaches are similar in concept to those used to understand and defend against experienced social engineering attacks
Robert Ressler

• Coined the term “serial killer”
• Key player in setting up the VICAP (Violent Criminal Apprehension Program) computer-based system
• Instrumental in organizing the original program to interview notorious serial killers
John Douglas / Roy Hazelwood

- Leading pioneers along with Robert Ressler in the field of criminal profiling

- Investigated multiple, high profile serial murder cases
  - Atlanta child murders
  - Green River Killer
  - Alaskan serial killer Robert Hansen

- Douglas was the inspiration for “Jack Crawford” in Thomas Harris novels
In Conclusion

• Fundamental psychological principles are important in both executing and defending against social engineering attacks

• Examining extreme historical atrocities and behaviors provides an understanding of psychological principles

• An understanding of these principles allows for better defenses and pretexting exercises
References

- Friend, Ronald; Rafferty Yvonne; Bramel, Dana (1990). *A puzzling misinterpretation of the Asch “conformity” study.* European Journal of Social Psychology
- Muzafar Sherif (1935). "*A study of some social factors in perception: Chapter 3.*" Archives of Psychology
Questions?

Thank you for watching our presentation. We can be reached at the following addresses:

Joe Sechman, CISSP|CSSLP|CISA  
Director  
jsechman@sunera.com

Robert Carr, MBA|CISSP|OSCP  
Sr. Manager  
rcarr@sunera.com

You can also visit us at www.sunera.com  
and our blog at security.sunera.com