TUTORIAL

USABLE SECURITY POLICIES + USER TRAINING: THE BEST METHOD TO COUNTER SOCIAL ENGINEERING ATTACKS

Rebecca Long
Eastern Washington University
Cheney, Washington USA

OVERVIEW

- Introduction
  - Problem
- Background
  - Definition of social engineering
  - Social engineering cycle
- Solutions
  - Security Policies
  - User Training
- Counter-Measures
- Summary

INTRODUCTION

SECURE-SYSTEM

- A secure system…
  - Part of wider socio-technical system
  - Includes both human and technical components
- Fully secure system is ultimate goal
  - Must protect system, private data, physical campus where system is located
- Use many methods to protect and secure system
  - Security technology
  - Security policies
  - User training

PROBLEM

- Hackers will always find the easiest way to break into a system
  - Users are the weakest part of a secure-system
- Human-Factor of Security
  - Easily exploited and constantly overlooked
  - Often responsible for failure of security systems
- ***Social Engineering*** is a serious problem to any secure-system
  - Directly takes advantage of system users and the human-element

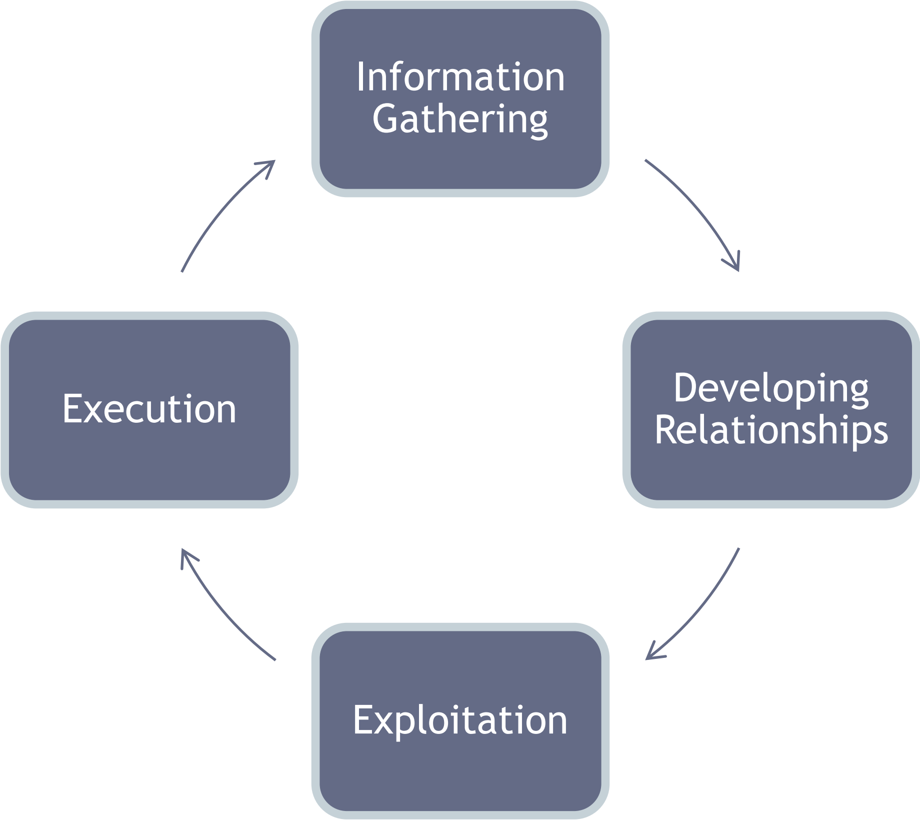
BACKGROUND

DEFINITION

- Social engineering:
  - "… exploitation of psychological triggers and cognitive biases as a means to gain unauthorized access to information or information systems"
  - "… the art and science of getting people to comply with your wishes"
  - "… uses influence and persuasion to deceive people … to take advantage of people to obtain information with or without the use of technology"
- Social engineers use tricks and manipulation to gain trust of system users

SOCIAL ENGINEERING CYCLE

- Typical cycle used by a social engineer:



INFORMATION GATHERING

- Social engineer performs background research to learn about attack target
  - Makes it easier to trick users

Techniques Used to Gather Information	
Asking for favors	Photography
Cold calling	Phishing
Contriving situations	Reverse social engineering
Dumpster diving	Simple requests
Forensic analysis	Shoulder surfing
Giving out free software	Theft
Impersonation	Trojans

DEVELOPING RELATIONSHIPS

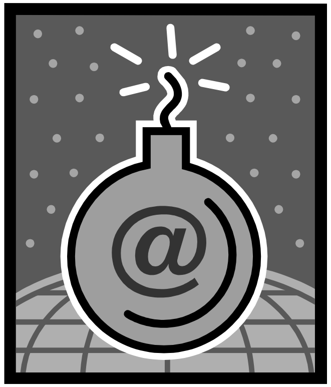
- Once enough information has been gathered, the social engineer can develop relationships with key users
  - Builds trust with user
  - To be exploited in next step

EXPLOITATION

- Once the trust between the social engineer and a user has been established, the social engineer will exploit the new relationship
  - Gain further information
  - Have the user perform an act to help the social engineer carry out their attack
    - Example:
      - Ask for remote access from user (dial-up, VPN, etc.)
      - Have user install a Trojan on a system computer

EXECUTION

- This stage of the cycle the social engineer finishes their attack
  - Example:
    - Remote in to system with access gained in previous step and perform whatever attack you wish
    - Use installed Trojan to gain access to critical system files and data



HOW TO ADDRESS SOCIAL ENGINEERING PROBLEM

SECURE WHOLE SYSTEM

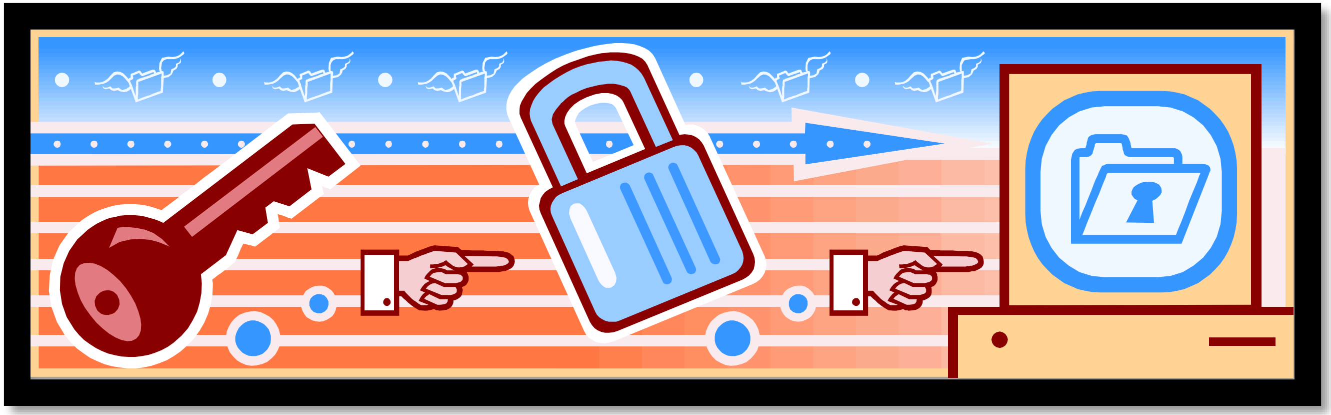
- Secure system via multiple methods
  - Technological security
  - Physical security
  - Security policies
  - User training
- Security policies work to regulate the system and users of system
  - How to use security technology
  - Minimize risk of social engineering attacks
- User training
  - Explanation of security policies
  - Give understanding of importance
  - How to recognize a social engineering attack

SECURITY POLICIES

- Security policies must be user-friendly, otherwise:
  - Users will not know how to follow
  - Users will have a difficult time trying to follow
  - Users may decide against following a policy if it seems to unreasonable

SECURITY POLICIES

- Policies must cover:
  - The technology used in the secure-system
  - How to properly dispose of documents
  - How to handle email and phone calls
  - What information can be given to public
  - Who is allowed on work campus



SECURITY POLICIES

- Policies must directly address social engineering
  - Give users procedures and directions on what to do in case of a social engineering attack
  - Have policies in place to help minimize the risk of an attack:
    - Explanation of what information is confidential and what is public
    - Users cannot give out confidential information
    - PIN setup for each user to use with Help Desk

USER TRAINING

- Training on security policies:
  - What the security policies are
  - How to correctly follow the policies
- Training must explain importance of policies
  - Users who understand purpose of policies are more likely to follow them
- Training should motivate users to actively participate in security
  - Explain it is not just the IT Department or the security guards responsibility to help protect system

USER TRAINING

- Extra training needs to be given to users specifically on social engineering
  - Explain what social engineering is
  - How social engineering attacks are carried out
  - Give examples of social engineering attacks and possible techniques
  - Explain which security policies help minimize a social engineering attack
  - How to recognize an attack
  - What to do if one happens

SOCIAL ENGINEERING COUNTER-MEASURES

PREVENTING SOCIAL ENGINEERING

- While there **is no way to 100% prevent** a social engineering attack
- The following tactics should be considered when creating security policies and user training on social engineering
  - Taken from Sarah Granger, SecurityFocus

COUNTER-MEASURE TACTICS

Area of Risk	Tactic	Counter-Measure
Building entrance	Unauthorized physical access	Tight badge security, employee training, and security officers present
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas, shred important data, erase magnetic media
General Psychological	Impersonation & persuasion	Give users continual awareness and training

COUNTER-MEASURE TACTICS

Area of Risk	Tactic	Counter-Measure
Intranet and Internet	Creation & insertion of mock software on intranet and Internet to steal passwords	Continual awareness of system and network change, training on password use
Machine Room and Phone Closet	Attempt to gain access, remove equipment, attach a protocol analyzer to grab confidential data	Keep phone closets, server rooms, etc. locked at all times and keep updated inventory on equipment
Mail Room	Insertion of forged documents	Lock and monitor mail room
Office	Shoulder surfing	Don’t type passwords with anyone present

COUNTER-MEASURE TACTICS

Area of Risk	Tactic	Counter-Measure
Office	Wandering halls looking for open offices	Require all guests to be escorted
Phone and PBX	Stealing phone toll access	Control overseas and long-distance calls, refuse transfers
Phone (Help Desk)	Impersonation and persuasion	Train employees / help desk to never give out passwords or other confidential info by phone
Phone (Help Desk)	Impersonation on help desk calls	All employees should be assigned a PIN specific to help desk support

SUMMARY

- Social and technological factors must be addressed when creating a secure-system
- Human-element of security is weakest link of any secure-system
  - Makes it vulnerable to social engineering attacks
- Specific security policies and user training must address human-element and social engineering
  - Must be user friendly
  - Must motivate users to follow policies
  - Must teach users why they are important

THANK YOU
有難うございます

QUESTIONS?