Computer Security

02r. Assignment 1 Review

Paul Krzyzanowski
Rutgers University
Spring 2017
Question 1

Briefly, what is social engineering?

• “Social engineering is an art of deceiving, to obtain information by pretending to be someone that s/he is not.”
  – See top of section 2 of the Chelleth paper, page 180

• Any of various forms of social deception
Question 1 [Social Engineering Discussion]

• Social engineering is the top attack technique for computers
  – Beats out exploits by hardware and software vulnerabilities

• Outsiders want to become insiders to get access to what they need
  – They use social engineering to get insiders to help them

• Phishing emails are the most common way to get account information from insiders

• Social engineering is often a first step to other attacks
  – Account compromise
  – Client-side attacks & compromising personal devices
  – Physical intrusion
  – Destruction

Define each of these concisely
(a) What is *policy*? 
(b) What is *mechanism*? 
(c) What is *assurance*?

• What is policy?  
  – A definition of what you’re supposed to achieve

• What is mechanism?  
  – The ciphers, access controls, hardware tamper-resistance and other machinery that you assemble in order to implement the policy

• What is assurance?  
  – “the amount of reliance you can place on each particular mechanism.
Question 3

What is meant by *security theater*?

- Measures designed to produce a feeling of security rather than the reality
  - Term created by *Bruce Schneier* in his book *Beyond Fear*

- A common example is airport security
  - Extra security measures, such as removing shoes, or confiscating liquids do essentially nothing to increase security … but ended up costing huge $$$
Question 3 [Security Theater Discussion]

• A few more examples
  – Entering some buildings
    • A guard will ask to see your drivers license – even though they have no idea who you are and don’t record the license
  – Fingerprint scanning
    • Gives some people the illusion of high security when it really isn’t
  – Photo ID badges (rather than access cards)
  – Photo ID on credit cards (demonstrated to be completely ineffective)
  – Security guards at a stadium focused on checking for beer or food in bags
    • May blindly ignore real threats (like guns)
  – Thinking your system is safe because you installed an anti-virus program
  – Drug stores scanning your license when you buy Sudafed
    (I assume meth labs have better ways of getting Pseudoephedrine Hydrochloride)

• While security theater makes some (stupid) people feel better
  – There are real costs
  – There are consequences: if people don’t fly because it’s more of a pain, they can drive, which is a lot more deadly
  – By focusing security inspections in a few areas, the bad guys can more easily hide things in areas that are not inspected
Question 4

Why does the FDIC recommend that bank employees take periodic vacations?

To give someone else a chance to take over and ensure that there is no ongoing fraud by a specific employee.

- It is “one element of an institution’s overall internal control system.” During the employee’s time away, “their duties and responsibilities should be assumed by other employees.”
  - FDIC Vacation Policies letter

- “So other people at the firm can check out their ‘book’ of trades and comb them for irregularities, fraudulent trades, and in general to clear away any webs of financial deceit.”
  - Marketplace article
Question 4 [Vacation Policy Discussion]

• Often, ongoing fraud requires continuous presence of the perpetrator
  – Manipulate records
  – Respond to questions

• Think about Ponzi schemes (e.g., Bernie Madoff)
  – Take money from people
  – Pretend to invest it & produce “good” returns, thus attracting more investors
  – Use money from new investors to pay off old ones if necessary & keep extra money for yourself
  – Create fake trading records and forged accounting statements
  – In the Bernie Madoff case, people suspected that was too much for him to do on his own:
    • James Ratley, president of the Association of Certified Fraud Examiners said, “In order for him to have done this by himself, he would have had to have been at work night and day, no vacation and no time off. He would have had to nurture the Ponzi scheme daily. What happened when he was gone? Who handled it when somebody called in while he was on vacation and said, ‘I need access to money?’”

https://en.wikipedia.org/wiki/Participants_in_the_Madoff_investment_scandal

“Perpetration of an embezzlement of any substantial size usually requires the constant presence of the embezzler in order to manipulate records, respond to inquiries from customers or other employees, and otherwise prevent detection. It is important for examiners and bank management to recognize that the benefits of this policy may be substantially, if not totally, eroded if the duties performed by an absent individual are not assumed by someone else.”

– FDIC Vacation Policies letter
What is the purpose of the “learning” phase in Ken Thompson’s compiler example?

To program a compiler to “know” what a pattern means

- In his simple example, the first version of the compiler is hard-coded to translate ‘\v’ to 11 (the ASCII code for vertical tab)
- After that, the compiler “knows” that \v expands to 11, so the value can be removed and the code can simply replace the pattern “\v” with the value of \v, which is now “magically” known to the compiler as 11.
Question 5 [Thompson Discussion]

What was Ken Thompson’s hack?

a) Modify the C compiler to recognize a line of code in the source code to the UNIX `login` command (login.c)

b) Have the compiler output code to allow `login` to accept a known password as well as the user’s real password

c) Modify the C compiler to insert this hacked code into the C compiler when the C compiler is compiled

d) You can now remove the malware code from the C compiler and have clean, bug-free source for the C compiler
   • But when you compile it with the C compiler from (c), it will add the malware into the code and generate a hacked compiler
   • That compiler works fine except
     – Whenever `login.c` is compiled, it will add code to detect an extra known password
     – Whenever the C compiler is compiled, it will add two chunks of code: (1) to detect the pattern in `login.c` and generate malware for that program and (2) to detect the compilation of the C compiler itself and modify the resulting binary to hack future compilations of `login` or the C compiler
The end