Social Engineering

Dr. Talal Alkharobi

Why do we care?

- Humans are potentially the **least** secure link in any secure system

"You are the weakest link..."

Social Engineering Definitions

3

- Management of human beings in accordance with their place and function in society—applied social science. *Webster*
- Manipulation of human beings to obtain information or confidence pertaining to the security of networked computer systems (with malicious intent)
- Cracking techniques that rely on weaknesses in peopleware rather than software
- **Wetware/Peopleware**—Human beings (programmers, operators, administrators) attached to a computer system, as opposed to

Social engineering Why?

4

- It is much easier to trick someone into giving his/her password for a system than to spend the effort to hack in.
- The white hat hacker Archangel (nicknamed "The Greatest Social Engineer of All Time") has demonstrated social engineering techniques to gain everything like
  - Passwords
  - Pizza
  - Automobiles
  - Airline tickets.

5

Social Engineering Methods

- Offering help if a problem occurs
- Sending free software or patch to install
- Using false pop-up window asking for log-in
- Capturing victim keystrokes
- Leaving floppy/CD/Flash sitting around with malicious code
- Using insider lingo to gain trust
- Offering a prize for registering web
- Dropping document or file at company mail room
- Modifying fax machine heading to appear from normal location

6

Social Engineering Methods

- Asking for a file to be transferred to an apparently internal location
- Getting voice mailbox set up for callbacks, making attacker seem internal
- Pretending to be
  - fellow employee
  - employee of vendor
  - authority figure
  - new employee requesting help
  - vendor offering patch, etc.

7

Warning Signs of an Attack

- Refusal to give callback number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of noncompliance
- Shows discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting

8

Common Targets of Attacks

- Unaware of info value—receptionist
- Special privileges—help desk tech support
- Manufacturer/vendor—vendors
- Specific departments—accounting, HR

9

Factors Making Companies Vulnerable

- Large number of employees
- Multiple facilities
- Info on employee whereabouts left in voice mail messages
- Phone extension info made available
- Lack of security training
- Lack of data classification system
- No incident reporting/response plan

10

Social Engineering Techniques Pretexting

- The act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone.
- It's more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information (e.g., for impersonation: date of birth, Social Security Number, last bill amount) to establish legitimacy in the mind of the target.

11

Social Engineering Techniques Pretexting

- This technique is often used to trick a business into disclosing customer information, and is used by private investigators to obtain telephone records, utility records, banking records and other information directly from junior company service representatives.
- The information can then be used to establish even greater legitimacy under tougher questioning with a manager (e.g., to make account changes, get specific balances, etc).

12

Social Engineering Techniques Pretexting

- Pretexting can also be used to impersonate co-workers, police, bank, tax authorities or insurance investigators — or any other individual who could have perceived authority or right-to-know in the mind of the target.
- The pretexter must simply prepare answers to questions that might be asked by the target.
- In some cases all that is needed is a voice of the right gender, an earnest tone and an ability to think on one's feet.

13

Social Engineering Techniques Phishing

- Phishing applies to email appearing to come from a legitimate business — a bank, or credit card company — requesting "verification" of information and warning of some dire consequence if it is not done.
- The letter usually contains a link to a fradulent web page that looks legitimate — with company logos and content — and has a form requesting everything from a home address to an ATM card's PIN.

14

Social Engineering Techniques IVR/phone phishing

- This technique uses a rogue Interactive Voice Response (IVR) system to recreate a legitimate sounding copy of a bank or other institution's IVR system.
- The victim is prompted (typically via a phishing email) to call in to the "bank" (via a provided toll free number) and verify information.
- A typical system will continually reject logins ensuring the victim enters PINs or passwords multiple times.
- More advanced systems will even transfer the victim to the attacker posing as a customer

15

Social Engineering Techniques Trojan Horses

- To take advantage of curiosity or greed to deliver malware.
- Trojan horse can arrive as an email attachment promising anything from a "cool" screen saver, an important anti-virus or system upgrade.
- The recipient is expected to give in to the need to see the program and open the attachment.
- In addition, many users will blindly click on any attachments they receive that seem even mildly legitimate.

Dr. Talal Alkharobi

16

Social Engineering Techniques Road apple

- A road apple is a real-world variation of a Trojan Horse that uses physical media and relies on the curiosity of the victim.
- The attacker leaves a malware infected floppy disc, CD ROM or USB key in a location sure to be found (bathroom, elevator, sidewalk), gives it a legitimate looking and curiosity piquing label - and simply waits.
- Example: Get corporate logo off target's web site, make a disk label using logo and write "Executive Salary Summary Q1 2006" on the front.

Dr. Talal Alkharobi

17

Social Engineering Techniques

Quid pro quo (Something for something)

- An attacker calls random numbers at a company claiming to be calling back from technical support.
- Eventually they will hit someone with a legitimate problem, grateful that someone is calling back to help them.
- The attacker will "help" solve the problem and in the process have the user type commands that give the attacker access and/or launch malware.
- In a 2003 information security survey, 90% of office workers outside of their building gave away their password in answer to a survey question in