Lecture 14:

Social Engineering

Lecture Outline

• What is Social Engineering?
• Common Attack techniques
• Examples
• Threats of Social Engineering
• Countermeasures
What is System?

- Component
  - smartcard, a PC or piece of software
- Infrastructure
  - Operating system, network, etc
- Applications
- IT staff
- Internal users and management
- Customers and external users
- Environment

Anderson, 2008
What is System?

- Component
  - smartcard, a PC or piece of software
- Infrastructure
  - Operating system, network, etc.
- Applications
- IT staff
- Internal users and management
- Customers and external users
- Environment

Human being becomes the **weak link** in security

What is Social Engineering?

Manipulation of people by deception into giving out information or performing an action

I. Mann, Hacking the Human, Gower (2008)
Social Engineering Attack

An **outsider** uses **psychological tricks** on **legitimate associates** exploiting basic **human nature**

- Trust
- Fear
- Desire to Help

To gain

- Access Details to a Facility or System
- Sensitive information
- Authorization details

Getting a **password** from a person is "**easier**" than breaking into a system

How does it work?

- **Social engineers** leverage
  - Trust
  - Helpfulness
  - Easily attainable information
  - Knowledge of internal processes
  - Impersonation of authority
  - Technology

- Often use several small attacks
  - Social engineering is all about **taking advantage of others** to **gather information** and to **infiltrate** into an organization
Examples

• Act as a legitimate user
• Pretends as a vice president
• A published security vulnerability
• Posing as a systems administrator
• Call to get someone or specific information
• Use search engines to collect information about company and its associates

Survey


• **Individuals:** 853 IT and Security professionals
• **Location:** US, UK, Canada, Australia, New Zealand and Germany
• **Time:** July-August, 2011
Survey


- **Individuals:** 853 IT and Security professionals
- **Location:** US, UK, Canada, Australia, New Zealand and Germany
- **Time:** July-August, 2011
1. Pretexting

- Act of *creating* and using an *invented* scenario (pretext) to divulge target’s *sensitive information*
How to get a pizza for free?

https://www.youtube.com/watch?v=z68gZJwdAAg

2. Phishing

- Phishing techniques
  - Involves email, Websites and phone calls
  - These look highly legitimate and solicit personal information
    - the one that you use commonly
  - Include a sense of urgency
  - Asks to verify personal data
### Phishing Types

<table>
<thead>
<tr>
<th>Website/Email phishing</th>
<th>Smear phishing</th>
<th>Phone Phishing/ (Interactive Voice Response)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create <em>fake</em> email or website that resemble the original one</td>
<td>Similar except <em>highly targeted</em> and <em>directed</em> at organizations</td>
<td><em>directed</em> by phone</td>
</tr>
<tr>
<td></td>
<td><em>Legitimacy</em>, is established using information gathering</td>
<td><em>legitimate IVR commands</em> are recorded and played to customers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Asks victim to <em>renew, validate</em> his services with a bank/credit union/service. IVR directions include the entry of PI, PIN, Password, SSN</td>
</tr>
</tbody>
</table>

### Phishing – Website phishing

- Example used on the Internet, involving misuse of the name PayPal
  - www.PayPai.com
  - www.PayPa1.com

- Victim notices as it looks same, and think it is just a slight defect in the text or resolution
Another example

Another example
Another example
Pretexting + Phishing

- Attacker makes three calls pretending as 3 different users
- Attacker reveals victim’s confidential bank information
  - His *current balance* in the account
  - His *business transactions* including amount, recipient
- Sell it to other parties

[Mitnick, 2002]

Call 1

“ABC Bank, this is Kim. Do you want to open an account today?”

“Hi, Kim. I have a question. Do you guys use CreditChex?” “Yes”

“When you phone in to CreditChex, what do you call the number you give them-- is it a Merchant ID?”

A pause; she is suspicious ... whether she should answer; The caller quickly continued without missing a beat:

“Because, Kim, I'm working on a book. It deals with private investigations”

“Yes,” she replied with confidence, pleased to be helping a writer.

“So it's called a Merchant ID, right?” “Uh huh.”

“Okay, great. Because I wanted to make sure I had the lingo right. For the book. Thanks for your help. Good-bye, Kim.”
Call 2

“ABC Bank, New Accounts, this is Chris.”

“Hi, Chris. This is Alex,” the caller said.
“I’m a customer service rep. with CreditChex. We’re doing a survey to improve our services. Can you spare me a couple of minutes?”

She was glad to, and the caller went on:

“How often do you call us with an inquiry?”

She answered, and continued answering the questions

“How’s our response time?” “How long have you been with the bank?” “What Merchant ID are you currently using?” “Have you ever found inaccuracies with the information we’ve provided you?” “If you had any suggestions for improving our service”

She agreed, they chatted a bit, the caller rang off, and Christ went back to work.

Call 3

“CreditChex, this is Henry McKinsey, how can I help you?”

“Hello, Henry” Caller said he is from ABC Bank.
He gave the proper Merchant ID, then Name and Social Security # of the person he was looking for information on.

Caller took Henry in confidence. Henry read the listing from his computer screen:

“Well it is reported NSF in 1998, one time, amount of $2,066.”
NSF – Non Sufficient Funds -banking lingo for checks, written when there isn’t enough money in the account to cover them.

“Any activities since then?” attacker asked “No activities.”

“Have there been any other inquiries?”

“Let’s see. Okay, two of them, both last month. Third United Credit Union of Chicago.”
He stumbled over the next name, Schenectady Mutual Investments, and had to spell it. “That’s in New York State,” he added.
Another example
Pretexting + Phishing

- The confidential information that attacker got from bank

<table>
<thead>
<tr>
<th>First Call</th>
<th>&quot;So it's called a Merchant ID, right?&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second Call</td>
<td>“What Merchant ID are you currently using?”</td>
</tr>
<tr>
<td>Third Call</td>
<td>“Let's see. Okay, two of them, both last month. Third United Credit Union of Chicago.&quot; He stumbled over the next name, Schenectady Mutual Investments, and had to spell it. &quot;That's in New York State,&quot; he added.</td>
</tr>
</tbody>
</table>

3. Baiting / Road Apples

- Trojan horse variant that uses physical media and relies on the curiosity or greed of victim

- **Physical media - CD, floppy, USB Flash Drive**
- **Labeled to draw curiosity**
  - "Layoffs 2009 – Private and Confidential"
  - "HR Staff Reduction Plan"
  - "Confidential Organizational Changes"
- **"autorun" feature loads Trojan or virus to track keystrokes**
  - E.g., Looks for IDs and passwords
Example
Baiting / Road Apples
Stasiukonis S., Social Engineering the USB ways, 2006

• Credit union’s security assessment against social engineering

Consultants collected USB drives

Wrote Trojan to collect and email passwords, logins & machine-specific information from user’s computer

Scattered USB drives in parking lot, smoking areas, and other places

• After about 3 days:
  – 20 USB drives were planted
  – 15 were found and plugged into computers
  – Data obtained help to compromise additional systems

4. Shoulder Surfing

• Involves stealthily observing the target to obtain or deduce on confidential information

Observing password keystrokes on a keyboard
PIN entered into an ATMs, security locks, alarm keypads
Disclosure of Credit Cards or other Confidential Data
4. Shoulder Surfing

- Common happens in
  - Aircraft, airport, coffee shops, public Wi-Fi areas in hotels, other public places

Shoulder Surfing - Example

- Samantha’s background
  - College degree in business management
  - Stacked up loans to do it
  - Got a secretarial position job offer from Lambeck Manufacturing.
  - Wasn’t happy with job
  - Two months later junior product managers left
  - They hired an amateur from outside the company who has less knowledge about the industry than she did

[Mitnick, 2002]
Shoulder Surfing - Example

• Samantha’s Revenge
  – A guy from an industry trade magazine approached her to leak confidential information about a product
  – Offer her some benefits in response
  – Unintentionally, some time ago she watched a senior colleague’s (Martin Johansson) fingers while entering his passwords

Shoulder Surfing - Example

• She remembered a memo and typed up a new one from the original one. Her version read:

TO: C. Pelton,
IT dept. FROM: L. Cartright,

Development Martin Johansson will be working with a special projects team in my department. I hereby authorize him to have access to the servers used by the engineering group. Mr. Johansson’s security profile is to be updated to grant him the same access rights as a product developer.

Louis Cartright
Shoulder Surfing - Example

• Sent it as a Fax
• Three days later, she logged in onto the network with Johannson’s user name and password
• Locate the *Product specification*
• Downloaded them to USB disk
• The confidential data is on its way to the reporter

5. Tailgating

• Following an authorized person into a building – basically, riding on their coattails
  
  – *Stealthily slipping* to get physical access to premises
  – Preying on common politeness
  – When authorized individual is kind enough to hold the door open
6. Dumpster Diving

• Diving into *target’s dumpsters* in search of valuable information

What do they get?

- Confidential data
  - Confidential reports
  - Sales forecasts
  - Source code
  - Configurations
  - Internal communications
  - Post-it notes, and discarded applications

- Banking information
  - Blank credit applications
  - Salary data
  - Customer accounts

- Other technical data
  - Network diagrams
  - A phone list
  - Computer manuals
  - Employee lists
  - Discarded printouts showing internal operations and more

• Unusual for security to catch people going through trash pins
6. Dumpster Diving

- Your company’s trash may be your enemy’s treasure
- Even corporates use Dumpster-diving

Dumpster Diving - Example

- Mark Joseph Edwards in his book Internet Security with Windows NT, says:
  - *Entire reports discarded because of typos, passwords written on scraps of paper*
  - *All of which could help an intruder*…
Quid Pro Quo

• Giving something to get something in return
  “I scratch your back – you scratch my back”

• Examples:
  – Impersonation of a Help Desk
  – Gift in exchange of Information

• Surveys show that people are willing to trade private
  information for relatively low value
  – Bottle cap contests
  – Surveys themselves

Social Engineering

Risks and Countermeasures
**Attacker's Tools**

- Staff often use and respond to electronic requests
- Relative anonymity of internet
- Can damage computer resources

- Target can not see the hacker
- PBX is an attractive target
- Stealing is possible without trace

**Vulnerability Factors**

**Insufficient Security Training**
- Sabotage
- Marketing
- Providing Support

**Unawareness**
- Simplest and cheapest way
- Intimidation
- Persuasion
- Assistance

**Several Organisational Units**

**Lack of Appropriate Security Policies**

**Easy Access of Information**
- e.g., Email IDs & Phone Extension numbers of employees
Alerts

- Show inability to give valid call back number
- Make information request
- Claim of authority
- Show haste
- Unusual compliment or praise
- Show discomfort when questioned
- Drop name inadvertently
- Threaten of dire consequences if information is not provided

Social Engineering Attack

<table>
<thead>
<tr>
<th>Research on Target Company</th>
</tr>
</thead>
</table>
| Dumpster diving | Websites | Employees | Tailgating ...

![Diagram showing the process of a social engineering attack: Research on Target Company, Select Victim, Develop Relationships, Exploit Relationships.]

- Identify Frustrated Employees
- Vulnerable Employees

- Trust
- Ignorance
- Fear
- Greed
- Moral Duty

- Collect Sensitive Account Information
- Financial Information
- Current Technologies
Impacts

- Damage of goodwill
- Loss of privacy
- Economic losses
- Lawsuits and arbitrations
- Temporary or permanent closure
- Dangers of terrorism

Countermeasures

Preventing Insider Threat

- Separation of duties
- Rotation of duties
- Least Privilege
- Controlled Access
- Logging and auditing
- Legal policies
- Archive critical data
What can you do?

• Never share passwords – NEVER NEVER NEVER!!!
• Use different passwords for personal and business matters
• Don’t discuss company confidential matter in public
• Shred company confidential information
• Find CDs, USB? Don’t use them!
• Know how to spot a phish – beware of email attachments
What can you do?

• Never use a link within an email or call a phone number from within an email – look up the organization independently
• Don’t forward or respond to unsolicited email, chain letters or other hoaxes
• Screen lock your computer when you walk away
• Don’t let strangers into secure areas – let them use their badge
• Don’t share confidential information with strangers over the phone

Lecture Summary

During this lecture we considered:

• What is Social Engineering
• What are common social engineering attack techniques
  – Examples
  – Threats of Social Engineering
• What are social engineering countermeasures