Defending The Enterprise Against Social Engineering Attacks

VALERIE THOMAS
PRINCIPAL SECURITY CONSULTANT,
SECURICON LLC
Introduction

- Principal Security Consultant for Securicon
- 10+ years in Infosec
- Coauthor of *Building An Information Security Awareness Program*
- Social Engineering Trainer
The first 5 days after the weekend are always the hardest.
Vulnerable?

• You patch every month
• You have firewalls and IDS
• And yet you’re still vulnerable to attack
• Attackers will go for the weakest link, which is the human
What is social engineering?

Persuading a person to provide information or perform an action to aid an attacker.
Why does it work?

- Uses psychological makeup of humans against us
- Most people want to be helpful
- Unaware of the threat
- Often provide “free information”
Technology will continue to advance, but the greatest vulnerability will always exist in the human behind the keyboard.
How can we stop it?

- Understand how attacks work
- Determine exposure
- Evaluate defenses
- Educate the workforce
- Streamline existing technology
- Have an incident response plan
Determine Exposure
Web exposure assessment

• What does your website look like to a social engineer?
  – Providing too much detail
• Are you leaking sensitive data online?
  – Forums
  – Documents
  – P2P
• Listed on hacking sites
How can I engage/register my business with Bank of America?

What is the Supplier Development Program?

Sponsorship

How to submit a proposal?

Newsroom

Where can I find a copy of a press release?

Corporate Philanthropy

To what organizations does Bank of America contribute?

Email Us

For Careers Profile Access Issues
Corporate Philanthropy Secure email
Supplier Relations and Development email
Investor Relations email

Write Us

Bank of America Investor Relations
NC1-007-56-70
100 N. Tryon St.
Charlotte, NC 28255

i_r@bankofamerica.com
Our locations

Choose a state
- Alabama
- Arizona
- Arkansas
- California
- Colorado
- Connecticut
- District of Columbia
- Florida
- Georgia
- Hawaii
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Missouri
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New York
- North Carolina
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Puerto Rico
- Rhode Island
- South Carolina
- Tennessee
- Texas
- Utah
- Virginia
- Washington
- West Virginia
- Wisconsin
### Job Number

**Keywords**

infrastructure

### Job Field

- **Core Business Services**
- **Information Technology**

**Add Job Field**

### Location

- **United States**
- **All**

**Add Location**
Required Skills:
- Multiple years in operating within a service organization
- Experience with Windows 2003/2008 Server
- Experience with Red Hat Linux and or Solaris Administration
- Experience with Installation, Configuration and tuning Of Apache Tomcat.
- Experience with Installation, Configuration and tuning Of Apache Web Servers.
- Experience with MYSQL Database is preferred.
- Solid understanding of Apache Tomcat and Apache Web Server application deployment and troubleshooting is required.
- Sound knowledge of JVM Performance Tuning.
- Working knowledge and Good understanding of Network Load Balancers. F5 and CSM Preferred.
- Experience with Wily Introscope and HP BAC/Sitescope monitoring systems.
- 5 years support/administration experience in a mix of the following technologies: VXML, XML, JSP, JAVA/J2EE, SPRING, AJAX, Service-Oriented Architecture.
• Installation & Configuration of Windows 2003 Server remotely through DRAC & iLO, troubleshooting server 2003 Active Directory and network infrastructure DNS, DHCP, IIS etc.
• Allocating DHCP Scope, DNS Entry Creation.
• Planning and Scheduling Monthly Patch deployment in all Middle East Servers.
• Provides Application and Operating system support.
• Installation and configuration of Anti-Virus Software (Symantec Antivirus), also working on anti-virus update issue.
• Resolving the Server related issues.
• Server Preparation as per requirement
• Managing WSUS (Windows System update Services) Server for patch deployment
• Monitoring the Servers using, HP Operations Manager, HP Sitescope
• Lotus Domino Monthly Maintenance in all Middle East Offices.
• Managing the Intra Mail Service (Lotus Notes)
• Maintaining the local VLAN based Networking
Hello,

I am learning Servlets and JSP. I have trouble creating an object for the static factory method I had written for database connection. And I need some suggestions and helpful tips of developing my class in object-oriented programing.

The database connection code I had written:

```java
import java.util.*;
import java.sql.*;

public class databaseConn {
  private String url;
  private Connection conn;

  public static databaseConn getInstance() {
    return new databaseConn();
  }

  private databaseConn() {
    url = "jdbc:mysql://localhost/employeedb?user=root&password=admin";
    try {
      Class.forName("com.mysql.jdbc.Driver");
      conn = DriverManager.getConnection(url);
      conn.createStatement();
    } catch( Exception e ) {
      e.printStackTrace();
    }
  }
}
```
Defense Logistics Agency

Defense Logistics Agency U.S. Soldiers watch Super Bowl 44 at Camp Ramadi, Iraq, Feb 8, 2010. This year, the Defense Logistics Agency is providing U.S. forces in Iraq and Afghanistan all the wings, pizza and chili they can handle on Super Bowl Sunday. (Photo by Spc. Christopher Wellner)

Defense Logistics Agency Wings, mozzarella sticks, pizza and potato wedges. DLA is ensuring U.S. troops in Iraq and Afghanistan get the full Super Bowl experience this Sunday ...

Defense Logistics Agency provides deployed troops Super Bowl fare

Last year’s Super Bowl rated as the most-watched event in U.S. television history. There is no doubt that American forces in Iraq and Afghanistan contributed to the ratings as football outpaces other major sports as the overall favorite.

Defense Logistics Agency DLA’s support to the Air Force has steadily increased in fiscal 2011 but DLA and Air Force leaders continue to look at ways to keep improving.

Thompson: DLA support to Air Force steadily improving
<table>
<thead>
<tr>
<th>Name</th>
<th>Add as Friend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td><img src="link" alt="Add as Friend" /></td>
</tr>
<tr>
<td>Dor</td>
<td><img src="link" alt="Add as Friend" /></td>
</tr>
<tr>
<td>Jess</td>
<td><img src="link" alt="Add as Friend" /></td>
</tr>
<tr>
<td>Abb</td>
<td><img src="link" alt="Add as Friend" /></td>
</tr>
<tr>
<td>M</td>
<td><img src="link" alt="Add as Friend" /></td>
</tr>
</tbody>
</table>
Twitter mapping
screamradius
See what people are saying about #Washington, #District of Columbia here!
July 30 @ 6:00 AM from screamradius

daxxpr
I'm @ The Pentagon(22202 Arlington) http://tmw.im/qkJ1
July 30 @ 1:44 AM from Telminhere

JFDaniels
I didn't know they flew ospreys straight down the middle.

Follow us on Twitter
 Embed in your site
 Feedback & suggestions
 FAQs
Evaluate Defenses
Most dangerous devices to your network
Evaluate your employees

- Phishing exercises
  - Target specific groups or random
  - Multiple metrics
    - Number of clicks
    - Infected document
    - Data entered (password reset)
- Fake social media campaign
  - Create profiles for ranking management
  - Post phishing links
Evaluate your employees

- Physical penetration testing
- How easily can unauthorized persons obtain building access?
- Are you throwing sensitive data away?
- Include social engineering in your penetration tests and application assessments
Evaluate your responders

• How long did it take to detect the attack?
  – Who alerted security?
• Did the security team follow the appropriate procedures
  – Do procedures exist?
• What actions were taken?
I changed all my passwords to "incorrect".

So whenever I forget, it will tell me "Your password is incorrect."

Educate The Workforce
Patch your people

• The staff is your first line of defense
• Establish a social engineering training program
  – Describe how attacks work
    • Statistics from any recent assessments
    • Emphasize the importance of their email address
  – Include Computer based training
    • How to spot phishing attacks (and what to do next)
    • Monthly drawing for those who report suspicious messages or activities
  – Guest speakers
• Remember this is a continuous process
Get the word out

• Start a security newsletter
  – Feature employees that were caught doing good
  – Include a news article about a recent attack

• Host information sessions
  – Identity theft prevention tips
  – Using social networking safely
  – Mobile device security
Streamline Existing Technology
Use Technology to your advantage

• Effective defense technologies likely already exist in your environment
• Host brainstorming sessions with your security team
  – Consider using an outside consultant as a facilitator
  – Begin with a movie or war stories to get everyone in the social engineering mindset
  – Use tabletop exercises to simulate attacks and identify technical or policy shortcomings
Use Technology to your advantage

- Proxies and firewalls
  - Block outbound traffic on non-standard ports
  - Proper segmentation
    - Accounting machines shouldn’t have access to production database clusters
- IDS
  - Signatures for internal port scanning
  - Ability to quickly add signatures for newly encountered threats
More technology

• Create login IDs that are not based on names (or anything else)
  – HN90346283
• Purchase domains that are similar to yours
  – Bankoffamerica.com
  – bankofaemmerica.com
  – bankofamerica-portal.com
• Reserve webmail addresses
  – amdin.bankofamerica@gmail.com
Putting it all together

• Each of these phases can be done independently
• No required order
• Adjust remaining phases based on results
Determine Exposure
Evaluate Defenses
Educate Workforce
Streamline Technology
Feedback

- The Social Engineering Defensive Framework (SDEF) is open to all
- White paper in development
- Community based project
- Feedback welcome
Valerie.Thomas@securicon.com
@hacktress09