



Honesty and Service®

Data Topics in Cyber Security

*Carl D. Willis-Ford
Chief Database Engineer
SRA International, Inc.*



*Significant Work. Extraordinary People. **SRA.***

Speaker Background

- **9 years U.S. Navy, nuclear reactor operator, fast attack submarines**
- **20+ years experience: databases, IT process, technical management**
- **B.S. Computer Science (1993)**
- **M.S. Network Security (2006)**
- **M.S. Technology Management (2008)**
- **CIO University Certificate (Federal Executive Competencies), GSA/CIOC (2008)**
- **Adjunct Faculty, George Mason University School of Management**

SQL INJECTION



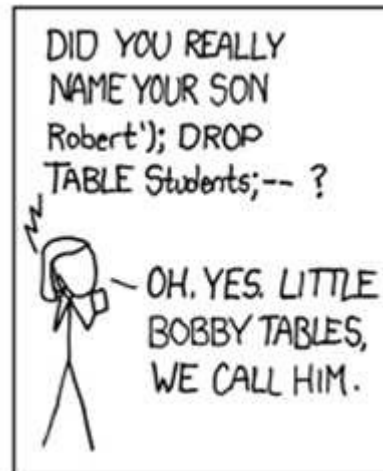
**This'll hurt you more
than it will me...**

What is SQL Injection?

- **Also known as SQL Insertion**
- **Exploits security vulnerability in database layer of application**
- **User input incorrectly filtered/not strongly typed**
- **Details covered in previous presentation**

- **rain.forest.puppy, 12/25/1998**
 - “NT Web Technology Vulnerabilities”
 - <http://www.phrack.com/issues.html?issue=54&id=8>
 - Section titled “ODBC and MS SQL server 6.5”
 - Showed that SQL Server allowed batch commands
 - In conclusion, stated “Don't assume user's input is ok for SQL queries.”
- **Chip Andrews purportedly coined the term in 2000**
 - <http://sqlsecurity.com>

Humor



<http://xkcd.com/327/>



<http://gizmodo.com/5498412/sql-injection-license-plate-hopes-to-foil-euro-traffic-cameras>

Still a Problem?

Rank	Score	ID	Name
[1]	346	CWE-79	Failure to Preserve Web Page Structure ('Cross-site Scripting')
[2]	330	CWE-89	Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')
[3]	273	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	261	CWE-352	Cross-Site Request Forgery (CSRF)
[5]	219	CWE-285	Improper Access Control (Authorization)
[6]	202	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[7]	197	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[8]	194	CWE-434	Unrestricted Upload of File with Dangerous Type
[9]	188	CWE-78	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')
[10]	188	CWE-311	Missing Encryption of Sensitive Data

Source: 2010 CWE/SANS Top 25 Most Dangerous Programming Errors: <http://cwe.mitre.org/top25/>

OWASP Top 10 Most Critical Web Application Security Risks

6th Place in 2004

2nd Place in 2007

http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

1st Place in 2010

Still a Problem?

- **2009 - 'The Analyzer' pled guilty in \$10M Bank-Hacking Case**
 - Used SQL Injection: <http://www.wired.com/threatlevel/2009/08/analyzer/>
- **2009 - Albert 'Segvec' Gonzalez charged:**
 - TJX: over 46.5M credit card details
 - Combined, over 130M credit/debit cards
 - 7-Eleven
 - Hannaford Brothers
 - Heartland Payment Systems
 - Dave & Busters
 - Boston Market
 - Used SQL Injection to place malware in system
- **Dec, 2009: Social Application 'Rock You' – data breach of over 32M user accounts**

First identified in 1998...WHY is it still a problem?

2 **CWE-89: Improper Sanitization of Special Elements used in an SQL Command ('SQL Injection')**

Summary

Weakness Prevalence	High	Consequences	Data loss, Security bypass
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

Thoughts?

SOCIAL NETWORKING

“...but we have seen that in the first half of 2009, social networking sites are the fastest growing target base for the bad guys and rank just below SQL attacks.”

<http://www.scmagazineus.com/web-hacking-attacks--thats-where-the-money-is/article/151860/>

Social Networking Sins

1. **Over-sharing company activities**
2. **Mixing personal with professional**
3. **Tweet rage**
4. **Over-connecting**
5. **Password sloth**
6. **Trigger finger (clicking everything you see)**
7. **Putting yourself/others in danger (over sharing personal info)**

http://www.csoonline.com/article/496314/Seven_Deadly_Sins_of_Social_Networking_Security

Social Networking Threats

- **Malware**
 - 6/2009 (Twitter): Guy Kawasaki-malicious link
- **Spam: hijacking accounts, send to friends list**
- **Targeted attacks: Google attackers posed as friends of employees**
(<http://www.ft.com/cms/s/2/c18091ee-09ee-11df-8b23-00144feabdc0.html>)

Social Networking Threats

- **Phishing: Twitter links to fake login pages as recently as Feb 2010.**
- **Twitter Worm:**
 - Vulnerability fixed after initial discovery in August
 - Reintroduced with service upgrade in September
 - Worm struck shortly after
- **Data leakage**

Demonstration

- <http://robmenow.com>
- <http://www.spokeo.com>

If folks don't think about this with their personal life, will they be more careful about work?

'Facebook Burglars': "In at least some of the burglaries, he told the newspaper, the suspects used social networking sites to look for homeowners who were going on vacation or saying they were out of town."

http://technolog.msnbc.msn.com/_news/2010/09/10/5086056-was-facebook-and-places-burglars-roadmap

Do you know this person?



...she wants to be your friend

The Robin Sage Experiment

- **December 2009 to January 2010**
- **Fake Facebook, Twitter, LinkedIn profiles, posing as a Cyber Threat Analyst**
- **Sent requests and established social network connections with over 300 security professionals**
 - Men and women of all ages
 - NSA, DoD, and Global 500 companies
- **Results**
 - Troops discussing locations and movement
 - Consulting opportunities from Lockheed Martin and Google
 - Given business sensitive documents for review
 - Able to determine answers to password change questions based on information provided in online conversations

<http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf>

The Main Factors of Robin Sage's Success

The main factors observed were: the ability to exploit other individuals' level of trust based

on:

- gender**
- occupation**
- education/credentials**
- friends (connections)**

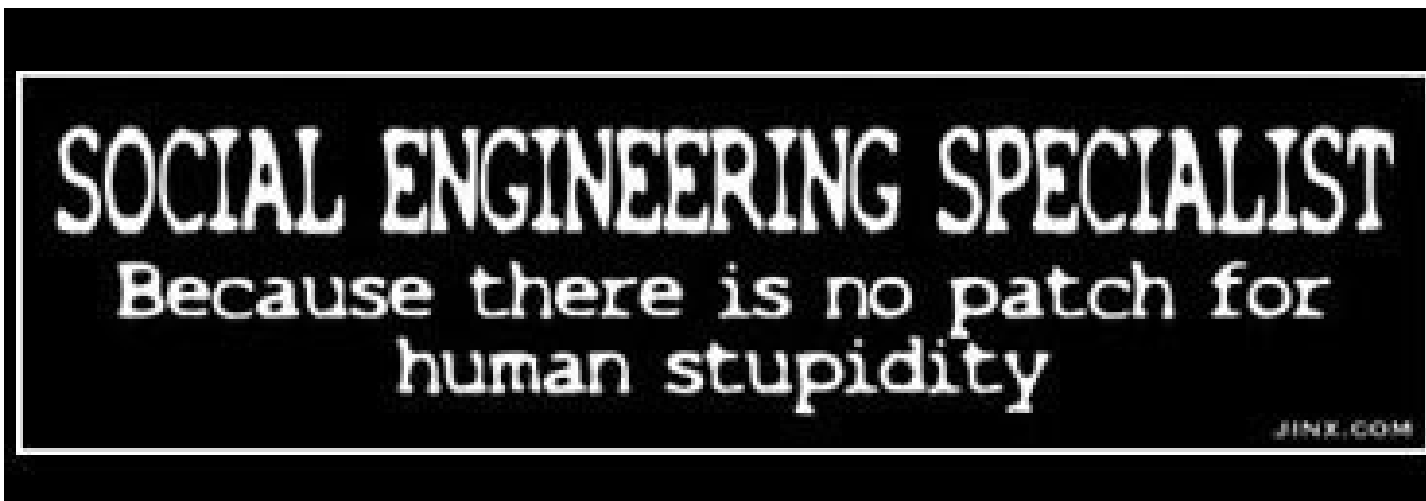
“Through this 28-day experiment, it became evident that the propagation of a false identity via social networking websites can be rampant and viral.”

Social Networking Security

The danger isn't social networking itself...

...the danger is doing it carelessly

SOCIAL ENGINEERING



<http://www.jinx.com>

A long, long time ago...(pre-2001)

- I made a simple request of a company data center: I asked the operator who handled my phone call for a copy of the previous night's database-backup tapes.
- Obliging, he sent the tapes to the receptionist's desk for me to pick up. With the tapes in hand, I could now re-create the company's databases on a server I controlled, giving me full access to the company's most-critical data.
- The astonishing part of this scenario is that I am not an employee of the company, yet I managed to get a copy of the database-backup tapes.
 - Kevin Loney, Consultant and Author

Fake Badge: Data Center Penetration

- **Consultant made up a fake company badge**
 - Electrical tape to simulate magnetic stripe
- **Tailgated into building**
- **Swiped badge at Data Center door several times**
 - Employee: “Sometimes, that thing doesn’t work”
 - Employee swipes own badge and lets consultant in
- **Consultant walks to center of room, raises his hands, and announces a surprise security audit**
 - Everyone leaves
- **Consultant uses cell phone to call executive that hired him and said “Guess where I am?”**

http://articles.techrepublic.com.com/5100-10878_11-1047991.html

Anatomy of a Hack

- **Tracking ‘Nancy’s’ MySpace and Twitter, knew she wasn’t in town.**
- **\$4 Cisco shirt from thrift store**
- **“Hi, I’m the new rep from Cisco. I’m here to see Nancy”**
- **Receptionist thought Nancy was in meeting, hacker talked his way in to waiting in cafeteria (only secured door)**
- **Dropped USB drives w/malware (places where folks forget things: bathroom sink, near coffee machine, etc.)**
- **Attacker #2 came in through smoke break door, ‘tailgating’...walked in and got first attacker from cafeteria so it looked ok on camera**
- **Installed WRT 54G router on company network, can access from parking lot**

http://www.csoonline.com/article/479038/Social_Engineering_Anatomy_of_a_Hack

Philosophy

**“Security is not mainly about software or biometrics.
First and foremost, it’s about people and policies.”**

**Richard Hunter
Senior Analyst
Gartner Group**

People & Policies

“Almost 60 percent of employees stole company data upon leaving their jobs last year. As the economy worsens and more people are laid off, more insider theft is expected to occur.”

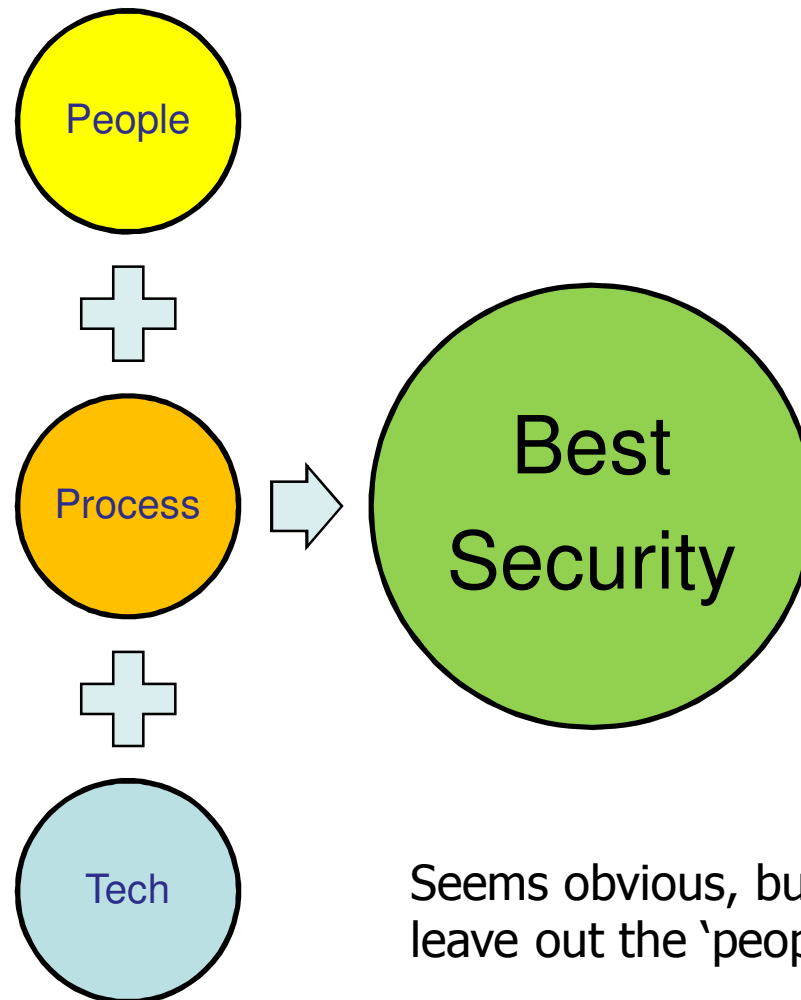
- ThomasNet Industrial News Room, February 24, 2009

Policy Alone Isn't Enough

According to a 2009 Ponemon study, information obtained from 720 IT security practitioners and 874 business managers from U.S.-based organizations reveals:

- 92% of IT security practitioners have had a laptop lost or stolen and a data breach has resulted in 71% of these cases. Only 45% were able to prove the data was encrypted.**
- 56% of business managers have disabled their laptop's encryption solution...48% admit this is in violation of their company's security policy**
- 59% of business managers sometimes or often leave their laptop with a stranger when traveling.**

The Triumvirate



Seems obvious, but many
leave out the 'people'

Classic Phishing Example

- **Original Phishing strategy (pretending to be CDW)**
 - People: None.
 - Process: Traditional, 'click on this link to login' scheme ...
 - Technology: Mass mailers, open mail relays
- **IT department strategy:**
 - People: Annual education about email-based phishing attacks
 - Process: Annual education on inspecting the provided login link to see if is legitimate
 - Technology: Spam and phishing filters

Adapted from:

<http://blog.impactalabs.com/2009/01/09/effective-malicious-hacking-another-case-for-people-process-technology-but-not-in-the-way-you-would-think/>

Smarter Phishing Example

- **Phisher's adapted strategy to overcome conventional training**
 - People: Send the email right after CDW launches a major radio ad promotion to establish context. Say "You may have heard our radio commercials..."
 - Result: User is no longer looking at Phisher as a complete stranger...trying to commercials establishes context, which leads to trust
 - Process: Inform the user that they can print some coupons for CDW at some third party website that is partnering with them for the promotion. At that site provide a coupon image that can be printed, and indicate that they can take this coupon to a store, or **click this link to login** and redeem it online right now.
 - Result: No longer asking user to 'login' from the e-mail, so doesn't relate to training.
- **Lesson: Employees with questioning attitudes are safer than those following rote policy/rules**

Lessons Learned

- **What have I learned?**
 - **Threats** are enabled by technology, but not stopped by technology alone
 - **People, Process, and Technology** must stay up-to-date and continuously adapt
 - No 'one best tool' or 'one best approach' in our business
 - **YOU** are a critical part of protecting your enterprise data, and not just through being a good DBA, but also a good corporate citizen

Suggested Sites

- **Open Web Application Security Project (OWASP)**
 - <http://www.owasp.org>
- **Imperva's SQL Injection page**
 - http://www.imperva.com/resources/glossary/sql_injection.html
- **Dark Reading - Database Security**
 - http://darkreading.com/database_security/index.jhtml
- **Databasesecurity.com**
 - <http://www.databasesecurity.com>
- **The Code Project – SQL Injection & Prevention**
 - <http://www.codeproject.com/KB/database/SqlInjectionAttacks.aspx>



Contact

Carl Willis-Ford

carl_willis-ford@sra.com

LinkedIn: Carl Willis-Ford