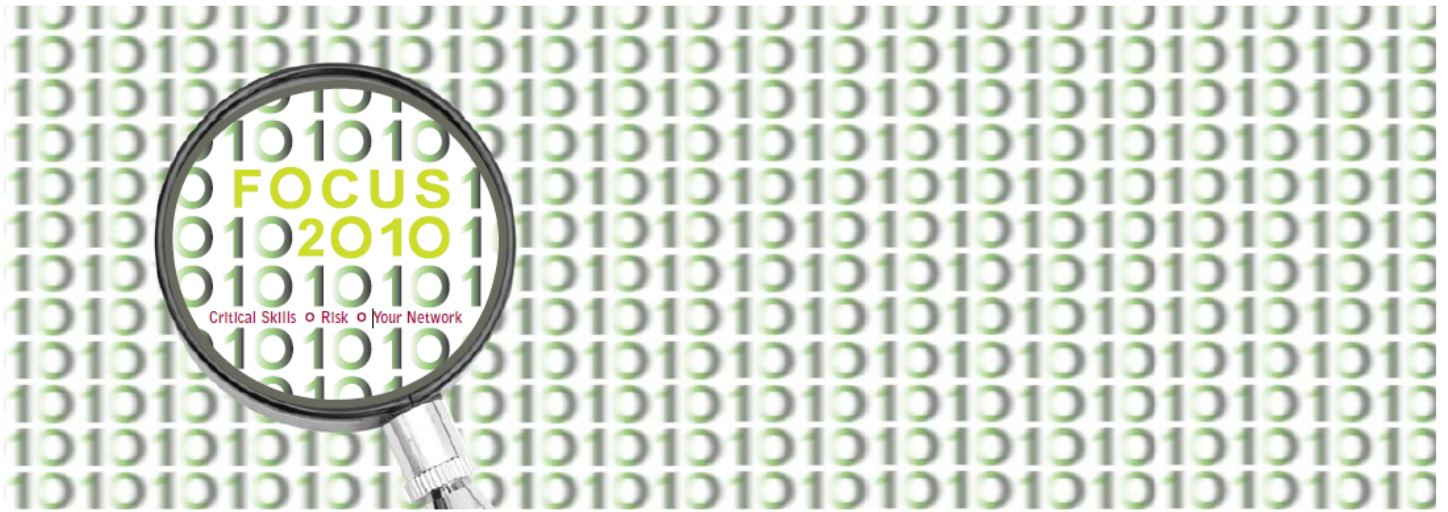


10th Annual SF ISACA Fall Conference
October 4 – 6, 2010



C13: Current Threats and Countermeasures – 2010

Lou Spahn, Accuvant, Inc.

Threats and Countermeasures

Human Factor and Physical Security

Lou Spahn— Accuvant LABS
Senior Security Consultant



Agenda

- **Social Engineering**
 - Phone Based
 - Email/Web (Phishing)
 - Physical

- **Physical Security**
 - Lock picking for the lazy/efficient
 - RFID and Prox Card Hacking/Cloning

- **Conclusion**



In the News Lately

- **Project Aurora**
 - Google
 - Adobe
 - Juniper Networks

- **NCUA**
 - Bogus CD Rom on latest phishing and “vishing” attacks

- **Center For Disease Control**
 - H1N1 Phishing Scam



Social Engineering – Phone Based

- **Working the Phones**
 - This has always been an issue and is nothing new.

 - How do you authenticate the user on the other end?

 - **Targeting:**
 - Sensitive Information
 - Usernames and Passwords
 - Account information
 - Patient Records



Social Engineering – Phone Based

- Attacks can be performed in either a “cold-call” or “target aware” manner.
- Cold-calling - Simply calling up the other end with no information and a limited back story.
 - “Hi this is Bob Smith.....”
- Target Aware – Information is gathered about the target and the victim account you want to compromise before calls are made. Usually followed with a back story.
 - “Hi this is Bob Smith of 1313 Mocking Bird Lane, My computer just crashed and”



Social Engineering – Phone Based

- Examples – IT / Admin Helpdesk:

Goal	Variations	Scenarios
Obtain Login Information to gain unauthorized access to a client environment	Can be performed with limited information (cold calling) or with client provided information (organization information or specific application information)	<ul style="list-style-type: none"> • Pretends to be a member of IT or helpdesk organization that needs to reset a password. • Calls IT or Helpdesk organization pretending to be an employee with an expired or locked out account. • Pretends to be part of a Beta application launch group and needs credentials for create account.



Social Engineering – Phone Based

- Examples – Customer Facing Call Center:

Goal	Variations	Scenarios
Obtain or change client information from call center or helpdesk support organization	Can be performed with limited information (cold calling) or with client provided information (organization information or specific application information)	<ul style="list-style-type: none"> • Angry client mad at company or phone support staff. • Hostile relationship (divorce or breakup) and not allowed access to papers or account information. • Hostile situation where there is no access to a local branch, such as in another country. • Just moved and does not have access to account information. • Computer crashed and does not have access to account information. • Needs electronic copies of account statement sent (email or fax) for loan/mortgage/car background checks. • Spouse calling on behalf of sick or hospitalized family member who has the account. • Account locked out – failed online login process and need to re-enable the account. • Missing last months statement and need a new copy sent. • Errors in current statement and need account information confirmed and/or information resent.



Social Engineering – Phone Based

- How do you authenticate someone?
 - Passwords
 - Personal Information
 - Employee ID
 - Pre-determined Security Questions
- What not to use – Don't ever rely on the phone number displayed unless you know for sure your PBX is tracking the ANI number.



SE – Phone Based

Dean's Story



SE – Phone Based

Target: ABC Corp Global Support. This is [name].

Attacker: Hi, my name is John Smith, and I am an employee of ABC Corp. I need to work from home tonight and need to find out how I am supposed to connect back to the network from home. Can you help me figure out how to get my laptop set up?

Target: Didn't they have all that set up on your laptop when they issued it to you? They usually have all that set up in advance. That's the way it was for me.

Attacker: No, I don't think it has been set up for me yet. What am I looking for?

Target: I'm not exactly the right person to call for these types of questions, but I can see if I can help you.

Attacker: Whom should I call to get this information?

Target: You can call the helpdesk at 212-555-1212 or email them at helpdesk@ABC Corp.com.

Attacker: Okay, thanks, but while I have you on the phone, can I ask you a few questions about your setup since you already have it working?

Target: I can do my best to help you. What they did for me was give me some VPN software that I use to connect to San Jose. It's the Nortel Contivity client that I have.

Attacker: Oh, I see. The Nortel Contivity client. So, you just install this VPN software and then you can get in?



SE – Phone Based

Target: Well, no, you have to configure the proper settings first.

Attacker: Do you know what the settings are?

Target: Yes, you just put in 'connect.ABCCorp.com' into the Destination field, and then your normal username and password that you use on the network.

Attacker: Oh, okay. I can't really remember what my username is because it is saved on my computer and I never have to type it in. Isn't it just your first initial and then your last name for your username?

Target: Yes, that is what my username is.

Attacker: Okay thanks. So, by the way, I have on my laptop a logon screen that they had pre-configured on my computer. I'm not sure what this is. Maybe this is part of the VPN connection. It's a screen that asks me for my username and password. Is there any chance you can pull up the same thing on your end to see if this is what I use to connect my VPN?

Target: Um... I suppose I could do this for you.

Attacker: Oh, great. That would be super helpful. I get there by opening a web browser and typing in an address. Can you open a browser and type in this address and see if you get the same thing?

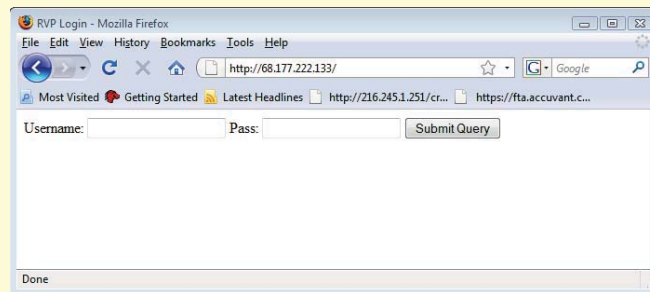
Target: Sure, I suppose I can have a quick look.



SE – Phone Based

Attacker: Okay, open your web browser, and type in this address; <http://68.177.222.133/>.

Target: Okay, I did this. I am getting a logon screen.



Attacker: Is this the logon screen you use for the VPN connection?

Target: No, I have not seen this logon screen before.

Attacker: What happens when you put your username and password in?



SE – Phone Based

Target: Hang on and I will try it... Hmm, that's weird, it just pulled up Google.

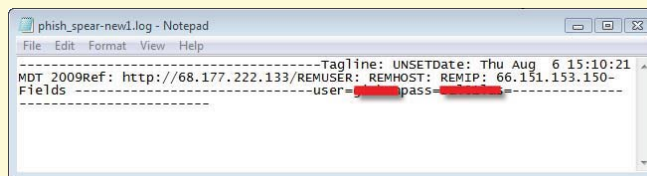
Attacker: Hmm. Oh Well. I guess that is not the VPN. I'm thinking I had better call the helpdesk and stop bothering you about this.

Target: Yeah, sorry I could not help you more; they can get you sorted out at the helpdesk though.

Attacker: That's okay. You have been very helpful indeed. I appreciate your help.

Target: Okay. No problem. Good luck.

Attacker: Okay, thanks. Bye.



```
phish_spear-new1.log - Notepad
File Edit Format View Help
-----Tagline: UNSETDate: Thu Aug 6 15:10:21
MDT 2009Ref: http://68.177.222.133/REMUSER: REMHOST: REMIP: 66.151.153.150-
Fields -----user = [REDACTED] pass = [REDACTED]
```



Social Engineering – Email/Web (Phishing)

- Many people have seen the direct emails – You've won \$1 million, or the dead relative in some random country
- Many people have seen the pop-up ads and other annoying junk on websites.
- Surprising that their guard is up if you just try one of these attacks, but in the last 2 years most successful attacks combine the 2 methods
- Accuvant averages 65% success rate with these types of attacks.



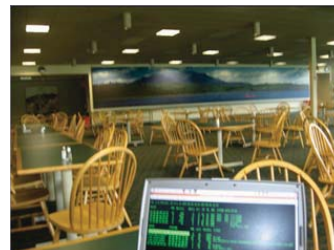
Social Engineering – Physical

- Once Physical Access is Obtained...It's Game Over!
- What type of systems do we put into place to prevent attackers from getting in?
 - Proxy Card Systems
 - Locks
 - Man Traps
 - Human Guards
- What does it take to defeat most of these systems?



Social Engineering – Physical

- A – Clipboard / Tool bag / ID Badge , a story, and a smile!



Social Engineering – Physical

Physical Security 102

True Story



Social Engineering – Physical

Dressing the part



Social Engineering – Physical

Act like you belong there



Social Engineering – Physical

Check all doors of the facility



Social Engineering – Physical

Watch out for the security guards



Social Engineering – Physical

Try to discreetly get proof of your access



Social Engineering – Physical

Finally, remember to smile and wave as you leave



Social Engineering

So what's the cure for all of this?

1. Employee security awareness training
3. Solutions to detect when an event has happened
5. Procedures for incident response
7. Communication between the employees, helpdesk, and security



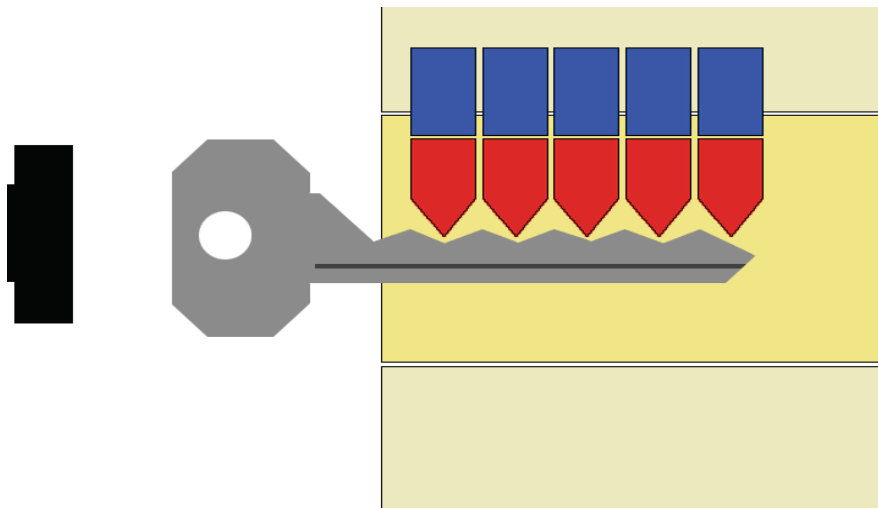
Physical Security Attacks – Key Bumping

Once Physical Access is Obtained...It's Game Over

- Bumping Technique –
 - Specialized keys
 - Newton's cradle principle
 - Related to pick gun lock picking method



Key Bumping

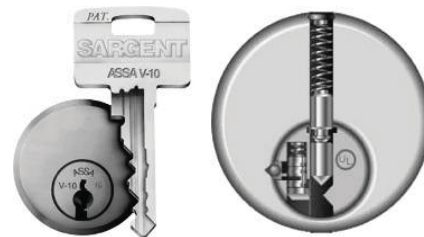


Demonstration

Key Bump

Key Bumping Threat

- High Level of Risk
 - Inexpensive
 - Inconspicuous
 - EASY
 - Few locks offer protection
 - Especially in the USA
 - Sidebars
 - Trap Pins
 - Shadow Drilling
 - Insurance problems



Key Bumping Countermeasures

- **With regard to keys:**

- How long has it been since the establishment was rekeyed?
- Can all keys be accounted for?
- Do past employees or service providers still have a key?

- **With regard to locks:**

- Determine the value/risk of assets being protected?
- By smart
- Don't be cheap
- Don't just buy the most expensive?



RFID

- RFID has been in use for a while but now is being put into "everything"
- Uses include retail, manufacturing, animal identification, to access control
- Attack Vectors:
 - Asset Tracking / Data Modification
 - SQL Injection (just like web apps)
 - Cloning



Demonstration

The Clone

RFID Defense Strategies

- **Follow the Basics:**
 - As with all RF know your footprint and placements.
 - Follow the technology - upgrade when needed
- **Avoiding Being a Victim**
 - If you can't upgrade to a newer technology (such as I-Class) change out the entry panels with ones that use TAG+Passcode.



Conclusions

Remember

The weakest security link in any organization is to have uneducated employees

and

Once access is obtained the game is over



Questions?

