Hacking the Social Grid
Gullible People at 670 Million Miles Per Hour
Hacking the Social Grid:
Gullible People at 670 Million Miles Per Hour

Welcome Conference Moderator

Jorge Orchilles
Senior VP, Citi
Director, South Florida ISSA

#ISSAWebConf
Today’s Speakers

Aaron Crawford
• Social Engineer, consultant for Coalfire Labs and Founder of Squirrels in a Barrel

Ira Winkler
• President, Secure Mentem Security consultant and espionage simulator

Mark Kadrich
• CISO at SDHC, a Health Information Exchange in San Diego
Speaker Introduction

Aaron Crawford

• Founder of Squirrels in a Barrel
• Consultant at Coalfire Labs
• Founder and host of The World Championship of Social Engineering
• Over 20 years of experience
• The most proficient Red Team
• One of the most successful social engineers
• Twitter - @squirrels nabrrl
Social Media Accelerator
Social Engineering

01 Time
Are you feeling pressured or rushed? Attackers can easily use fake deadlines and other forms of time-sensitive issues to force you into a hurried and thoughtless state.

02 Familiarity
Do you trust what you know? Attackers will take advantage of the target's concord and merriment to build rapid opportunities, exploiting weaknesses.

03 Sympathy
Do you feel down into the situation? Attackers will take advantage of your emotional as well as moral obligations in order to exploit their agenda.

04 Authority
Do you fear responsibilities of those in roles above you? Attackers will utilize fear of authority and compliance to augment their protest in order to avoid resistance.

05 Awareness
Are you informed of your surroundings? Simply being alert to what is happening in your immediate environment is enough to shut down over 40% of social engineering attack vectors.

06 Opportunity
Did you know most attacks are a result of simple opportunities that manifest themselves due to oversight and misconception? Attackers do not complicate attacks instead the path of least resistance is always taken.

Common Social Engineering Attack Vectors
Footprints...
Microsoft Entity Cube

Company Email Formats

- http://email-format.com/
- https://sites.google.com/site/emails4corporations/
Metadata

[Image of a software interface showing metadata and email addresses]

- All emails found (15) - Times found
  - barrecuda.com
  - Symantec.com
  - verisign.com
  - ultimaco.com
  - appsecinc.com
  - bkwglobal.com
  - cveracode.com
  - voloch.com
  - students.uffairfax.edu
  - barbados.issa.org
  - gmp4.hbo.edu
  - gmp4.hbo.ed
  - g2-inc.com
  - parabal.com
Target Storytime

- Acme Anvil
- Large company
- Employees move freely on campus
- Designated smoking area
- Smoker area entrance
- Main entrance = guards
- How to get in?
Resistance

No Smoking
Cree.py

Current Location Details

Date: 2016-06-12 23:01:15 +0000
Location: Anaheim
From: Twitter

ANOTHER reverse sweep has sent us into the Top 4 at @MLG

Context: Anaheim as we defeat Infused 3-2! ARE YOU WATCHING? #FaZeUp https://t.co/fpjuoxtQ1
I cannot stand when people just stand in front of a building or crowded area and smoke. You might want cancer, but clearly the rest of us don't. Go somewhere else.
The Glitch

- [http://theglitch.sourceforge.net](http://theglitch.sourceforge.net)
- Only 1.4 by 0.6 inches
- USB
- Registers as HID
- Multiple payloads
- Undetectable
- Think Inside The Box!
Vape Life
Deployment

- Batteries drained dead
- Packaging
- Uniformed deployment
- Action-based models hired
- Pretext of cigarette company trying to enter vape market
- Free samples = Trojan Horse
Did it work?

SHELLS ON
SHELLS ON
SHELLS ON
SHELLS!!!!
Always – Plan B
What to do?

• Continuous Dynamic Education
• Reintroduce the human element
• Establish clear policies
• Restrict alien devices from the enterprise
• Establish gifting and free swag policies
• Continuous review and assessment of the enterprise
• Avoid static methodologies and education
• Plan from failure first
• Remember to have fun
Ira Winkler

- President at Secure Mentem
- Co-host of The Irari Report
- President at Internet Security Advisors Group
- Author of *Spies Among Us* and other books
Friending Your Life Away

Ira Winkler, CISSP

ira@securementem.com

@irawinkler

http://www.facebook.com/irawinkler
It Would be Easy to do a Presentation on Stupidity

• This is an issue that has been around long before Facebook or Twitter
• Facebook and Twitter are just more known at the moment
• Fundamentally people are people
• The younger generations are more likely to have a different version of privacy
• Current technology just allows stupidity to travel faster
• Allows for abuse faster

Responsible Use, Not No Use
Unfortunately...

• The harm might be to the individual making the mistake
  • I don’t care about this
• The harm can easily be to third parties
• This is what matters to me
• One indiscretion can affect millions
• One indiscretion can be a matter of life and death
Historical Perspective

- BBS
- IRC
  - Still in use
  - Birthplace of Anonymous
- Usenet Newsgroups
- Mailing lists
- Compuserve, AOL
- Dating sites
- Blogs
Cybercrime Enabled

• Usenet created the ability for online relationships

• This enabled cyberstalking

• People posting corporate info created a potential for computer and IP compromise

• Started making the work of criminals easier
The C4I-Pro List

• All intel experts
• Custom to put out your bio
• I thought it was strange
• Someone from China posted
• I commented that it was a bad idea to post intel backgrounds
• Was flamed about my comments being against the open nature of the group
• No show of support
Companies Are Afraid to Comment

• Companies afraid to comment about activities off company time
• Afraid to play Big Brother
• Companies didn’t create policies
• Some consultants advised companies to let all their employees comment on the Internet
• Basically, unless it’s porn, it’s OK.
Are Companies Dumber Than Employees?

• They are putting info out as quickly as the employees
• Marketing putting out information, while security is told to stay away
• It’s not just companies
• USS Briscoe (?) posted crew information after attacking al Qaeda
• Donald Trump
MySpace Started a Trend

• MySpace started adding pictures
• People started talking of plans in advance
• Wholesale release of information
• Took level of embarrassment to a whole new level
• Started employers doing research on employees
• Again, hesitant to talk to current employees
YouTube

• Became the second most popular search engine behind Google
• Videos went up destroying lives
Twitter Brought Things to a New Level

• Almost the ultimate in vanity
• People started to announce every aspect of their life
• People started to write things at will
• No consideration to context or repercussions
• Too easy to distribute pictures
• Flash crimes
Other Viral Sites

• “Dog Poop Girl”
Facebook

• Became a Killer App
• Is essentially the embodiment of everything wrong with all other social media
• Farmville Zynga started telling us how people waste their time
• What people post is scary
• It places themselves and, more important, others at risk
The Ones I Really Worry About

• FourSquare

• TriplIt

• Facebook vacation posts

• Pokemon Go
Google

• Refer to my Is Google Evil? presentation
• YouTube has your age and proclivities
• Google knows what you are thinking
• Calendar knows where you will be and who you will be with
• Latitude knows where you are
• Checkout knows what you are buying
• Gmail knows your friends
• Google Apps knows your business
LinkedIn

- LinkedIn is limited, but has specific information that can be used for social engineering purposes
  - Used by APT for targeting
  - Education, employers, coworkers, titles, interests, travel, etc.
- Beginning social networking ability with discussions, groups, etc.
- Beginning to use Facebook like ads with your info
- Can tell when someone is looking for a job by new connections and referrals
Data Aggregators

• There are a lot of services out there that can put together a profile based on Social Networking sites
• Can put together friends, family, business, interests, etc
• Maltego for example
• Icanstalku.com
• Pleaserobme.com
UGOsweeps: I am currently nearby http://maps.google.com/?q=40.7635,-73.9823333333

less then a minute ago · Map Location · View Tweet · View Picture · Reply to UGOsweeps

kerrysimon: I am currently nearby http://maps.google.com/?q=36.1146666667,-115.193666667

1 minute ago · Map Location · View Tweet · View Picture · Reply to kerrysimon

faraichideya: I am currently nearby http://maps.google.com/?q=31.9493333333,-111.866666667

4 minutes ago · Map Location · View Tweet · View Picture · Reply to faraichideya

fragileheart: I am currently nearby http://maps.google.com/?q=43.6411666667,-79.422

6 minutes ago · Map Location · View Tweet · View Picture · Reply to fragileheart
Implications of Location Posting Services

• Business locations
• Knowing where you are
• Knowing where you are not
• Do you really want the world being able to track you?
Facebook Robberies

- Documented cases include couple in Indiana, family in Arizona
- Recent criminal posting that he actually did rob a house in Oregon
- In previous case, they IDed the perpetrator as a recent Friend
- Probably many other cases but hard to track
- “Not a Harvard graduate” posting pictures of kid duct taped
- Ashton Kutcher catching Twitter hacker through FourSquare
Notable Crimes

- APT Attacks LinkedIn enabled
  - Use LinkedIn for spear phishing targeting
- Twitter Hack
  - Used Social Media to guess Yahoo! password reset question
- Sarah Palin Hack
  - Used Social Media to get answer to password reset question
- Hugh Thompson
  - Scientific American article to reset bank passwords
More Serious Issues

• Israeli Military
  • Soldier posted location of an upcoming raid

• McConnell Gubernatorial Campaign
  • Web designer tweeted that he was working on a website prior to formal announcement

• Wife of British Intelligence operative posting issues on social media
Employee Issues Go Viral

• Fedex delivery guy video
• UPS delivery guy video
• Papa John’s

Restaurant # 3070
3477 Broadway
New York, NY 10031
(212)368-7272

01/06/2012 08:10pm

InStore Order

Name: lady chinky eyes
Third Party Indiscretions

• Posting Bachelorette party photos, tagging bride, and ruined wedding

• Constant posting about other people to appear unprofessional
Other People Posting About You

You have a family request.

Darth Vader
Darth Vader listed you as his son. Would you like to confirm?
Confirm  Ignore

NOOOOOOOOOOOOOOOOOO!!!!
Business Implications

- Do I want to know about your psychological disorder?
- Can I sit down across from you professionally, when you express extreme political or social views?
- Does your company have a right to temper your behaviors that can impact your customer interactions?
- What is the implication of your off hours?
- What is your brand?
Consider If These are on Your Profile
Security People as Bad as Others

• Implications of lack of professionalism
  • More interested in fighting each other than the bad guys
  • Much more than in other fields

• Maybe even indicate psychological problems

• You would think security professionals realize that Twitter is not a closed forum and lasts forever

• Shows questionable proclivities

• Shows desire to be associated with hacker underground

• Easy to violate ethics codes
• Idiots watch whole presentation they supposedly hate – College professor and industry association board member

WOW! The first bit of truth in Ira Winkler's presentation is on 48:35. "I guess they want me to be useful for a change“

That presentation had me baffled too, painful to watch. This time I'll try to get through it. I walked out in person.

Wouldn’t a normal person not watch?
Malware Introduction

- Malicious links via Twitter, Facebook and other sites
  - Short URLs
  - Easy to post, send and IM
- Malicious ads in Facebook
  - Embeds malware, even if Facebook denies it
- Introduction to malicious websites
It is More Than Security

• Lost productivity is immense
  • Don’t get me started on Pokemon Go

• I personally lose too much time if I leave Facebook on
  • I even make a lot of money via Facebook

• IMs less time efficient than calling, but allow for non-work related calls

• Brand image can be ruined
This is Still Nothing New

• Despite the recent incidents, this is nothing new

• Yes, I gave a history of the Internet

• We need to learn from the past to see what can be successful now
Boils Down to Operational Security

- Companies frequently don’t have a social media policy
- They don’t want to interfere with their employees’ private lives
- US military even afraid to set a strong policy despite problems
- Companies afraid to even stop Facebook access
Is the Job Market That Good?

• Companies afraid that if they don’t allow Facebook and IM, they are going to lose young employees
• Do you really want an employee who cares more about social networking than their job?
• How much does social networking really help most positions?
• Again, it is OK if there is a use for it
Responsible Use, Not No Use

• Ban Social Media unless required at work
• Stress and enforce ban against discussing work related issues outside of work
• Enforce the policy as you need consistent enforcement or it is technically unenforceable
• Awareness programs that rely on employee self-interests, as they overlap with yours
• I really wish there was more to say, but the problem is that there is more a lack of will to do things right
• There are worse things than porn
Just in Case

SOCIAL MEDIA EXPLAINED

- « I need to pee »
- « I peed »
- « This is where I pee »
- « Why am I peeing ? »
- « Look at this pee ! »
- « I’m good at peeing »
- « Let’s all pee together »
ADVANCED PERSISTENT SECURITY
A CYBERWARFARE APPROACH TO IMPLEMENTING ADAPTIVE ENTERPRISE PROTECTION, DETECTION, AND REACTION STRATEGIES
Ira Winkler | Araceli Treu Gomes
For More Information

Ira Winkler, CISSP
ira@securementem.com
www.facebook.com/ira.winkler
@irawinkler
www.linkedin.com/in/irawinkler

www.irarireport.com
@irarireport.com
Speaker Introduction

Mark S. Kadrich

- CISO at SDHC a Health Information Exchange in San Diego
- CISO at 211 San Diego a Community Information Service
- Social Engineering Weasel, Author, Blogger, and all around trustworthy guy.
BDSM

- **Business Development in Social Media**
  - Corporate business models based upon scraping SM data, analyzing it, and helping you use it to model your customers
  - Same Methodology used in clinical applications
    - Identify high risk behaviors
    - Provide treatment options based on new relationships
  - Criminals ALSO develop lines of business
    - Collect data, build products
    - Anyone buy a root kit kit lately?
    - Crime is a business!
Bad Developments in Social Media

- Criminal business models based upon scraping SM data, analyzing it, and using it to identify low risk targets
- Social Applications are like tracer rounds – they work in both directions
  - Criminals luring folks out to rob them
  - Criminals luring folks out to rob their houses
  - People posting vacation pictures – write an app that looks for the words “vacation”, “flights”, “dinner”.....you DO get the point?
- At some point it really gets just too easy....
• **Bad Data in Social Media**
  • If you can’t control the data sphere flood it with false data
    • You may be able to hide briefly
    • At least you’ll know who’s watching
    • I’m actually on a beach in Spain right now....
  • How do you attribute trust or provenance to the data?
    • You trust the weather lady on TV, right?
    • You don’t need to if your targets are individuals since most people don’t lie very well. (We’re trained to lie. We just call it Corporate Branding)
Open Discussion & Q&A

- **Jorge Orchilles**  
  Director, South Florida ISSA
- **Aaron Crawford**  
  Social Engineer
- **Ira Winkler**  
  President, Secure Mentum
- **Mark Kadrich**  
  CISO at SDHC a Health Information Exchange in San Diego and CISO at 211 San Diego

To ask a question:
*Type in your question in the Chat area of your screen.*
*You may need to click on the double arrows to open this function.*
Thank you
Moderator - Jorge Orchilles
Speakers
Aaron Crawford
Ira Winkler
Mark Kadrich

Thank you Citrix for donating the Webcast service
Upcoming ISSA International Web Conference

IoT: The Information Ecosystem of the Future – And Its Issues

2-Hour Live Event: Tuesday, August 23, 2016
Start Time: 9:00 a.m. US-Pacific/ 12:00 p.m. US-Eastern/ 5:00 p.m. London
A recording of the conference and a link to the survey to get CPE credit for attending the June ISSA International Web Conference will soon be available at:

If you or your company are interested in becoming a sponsor for the monthly ISSA International Web Conferences, please visit: https://www.issa.org/?page=BecomeASponsor