

Social Engineering & Low-Tech Attacks

CSH5 Chapter 19

“Social Engineering & Low-Tech Attacks”

Karthik Raman, Susan Baumes, Kevin Beets & Carl Ness



1

Copyright © 2011 M. E. Kabay. All rights reserved.

Topics

- Background & History
 - Social Engineering Methods
 - Psychology and Social Psychology of Social Engineering
 - Dangers & Impact
 - Detection
 - Response
 - Defense & Mitigation
- Spam, Phishing & Trojans
- E-mail Basics
 - Spam (not SPAM™)
 - Fighting Spam
 - Phishing
 - Trojan Code



2

CSH5 Chapter 19

CSH5 Chapter 20

Copyright © 2011 M. E. Kabay. All rights reserved.

Background & History (1)



- Trojan Horse
 - ☐ Trojan War
 - ✓ Greek mythology
 - ✓ C. 1200-1300 BCE
 - ✓ *Iliad* & *Odyssey* of Homer
 - ✓ Virgil's *Aeneid*
 - ☐ Greeks sailed to island of Tenedos
 - ✓ Pretended to abandon war
 - ✓ Left giant hollow horse with soldiers inside
 - ✓ Sinon, who convinced Trojans it was offering to Athena
 - ✓ Laocoon & Cassandra warned of danger
 - ☐ Greeks opened gates from inside, slaughtered Trojans, won war



3

Copyright © 2011 M. E. Kabay. All rights reserved.

Background & History (2)



- Definition: *obtaining information or resources using coercion or deceit*
- Manipulate trust or gullibility of people
- Often piece together information
 - ☐ Random order
 - ☐ Multiple victims / enablers
- Purposes vary but results often loss of
 - ☐ Intellectual property
 - ☐ Money
 - ☐ Business advantage
 - ☐ Credibility....



4

Copyright © 2011 M. E. Kabay. All rights reserved.

Some Notorious Social Engineers



- Frank Abagnale, Jr.
 - ☐ See *Catch Me If You Can* movie
 - ☐ Impersonated pilot, attorney, teacher...
 - ☐ Passed phony checks
 - ☐ Became expert for FBI
- Kevin Mitnick
 - ☐ Many exploits
 - ☐ See earlier lecture on *History of Computer Crime*



5

Copyright © 2011 M. E. Kabay. All rights reserved.

Social Engineering Methods



- Impersonation
- Seduction
- Low-Tech Attacks
- Network and Voice Methods
- Reverse Social Engineering



6

Copyright © 2011 M. E. Kabay. All rights reserved.

Impersonation

- Criminals wear uniforms, badges, use right terms
- Adopt confident air of entitlement
- Pretending to be HelpDesk employees
 - ❑ Employees conditioned to cooperate
 - ❑ Technical knowledge reduces questions
 - ❑ Some HelpDesks violate standards by habitually asking for passwords (BAD)
- HelpDesk employees can be victims
 - ❑ Criminals pretend to be employees
 - ❑ Often assume identity of high-ranking executives
 - ❑ Sometimes bully HelpDesk staff into violating standard operating procedures



7

Copyright © 2011 M. E. Kabay. All rights reserved.

Seduction

- Long-term strategy
 - ❑ May study victim to learn background, habits, likes, dislikes, weaknesses
- Form bond with victim
 - ❑ Apparent friendship
 - ❑ Exploit good will to ask for favors
 - ❑ May use sexual relationship as lever to develop trust
- Foot-in-the-door technique especially useful
 - ❑ Ask for tiny deviation from standards
 - ❑ Gradually increase demands



8

Copyright © 2011 M. E. Kabay. All rights reserved.

Low-Tech Attacks

- Exploit physical weaknesses in defenses
- Often support social engineering
- Examples
 - ❑ Dumpster® Diving
 - ❑ Theft
 - ❑ Leveraging Social Settings
 - ❑ Exploiting Curiosity or Naïveté
 - ❑ Bribery
 - ❑ Data Mining & Data Grinding
 - ❑ Piggybacking / Tailgating
 - ❑ Phishing & Pharming
 - ❑ Spim, Spit, & Vishing
 - ❑ Trojan Code and Viruses



9

Copyright © 2011 M. E. Kabay. All rights reserved.

Dumpster® Diving

- Dumpster® is registered trademark of *Dempster Brothers* for mobile trash receptacles
- Discarded materials are not protected by law unless on private property
- Many organizations sloppily throw away confidential info
 - ❑ Papers
 - ❑ Magnetic media
- Criminals derive value from
 - ❑ Internal organization charts
 - ❑ Memoranda
 - ❑ Vacation schedules
- Use info for industrial espionage and impersonation



10

Copyright © 2011 M. E. Kabay. All rights reserved.

Theft

- Outright theft of confidential information
 - ❑ Paper
 - ❑ CD-ROMs
 - ❑ USB flash drives and disk drives
 - ❑ Backups
 - ❑ Entire laptop computers
 - ❑ Purses, wallets, briefcases
 - ❑ Trash bags
- Information used directly or for impersonation



11

Copyright © 2011 M. E. Kabay. All rights reserved.

Leveraging Social Settings

- Employees relaxing or traveling may let down guard
- Social engineers may deliberately eavesdrop
 - ❑ Company parties
 - ❑ Clubs, trains, coffee shops
- Classic errors
 - ❑ Talking about confidential matters
 - ✓ In public amongst themselves
 - ✓ To friendly strangers
 - ✓ Loudly on mobile phones
 - ❑ Letting strangers view computer screens
 - ❑ Leaving portable computers unlocked



12

Copyright © 2011 M. E. Kabay. All rights reserved.

Exploiting Curiosity or Naïveté



- Criminals (and researchers) have left media lying around
 - ❑ CD-ROMs
 - ❑ USB flash drives
 - ❑ iPod music players
 - ❑ Music CDs
- Victims routinely insert media into company computers
- Unknowingly load malicious software; e.g.,
 - ❑ Keyloggers – capture keystrokes and send them to criminals
 - ❑ Backdoors – allow criminals to seize control of compromised computer behind firewall



13

Copyright © 2011 M. E. Kabay. All rights reserved.

Bribery



- Exchange of value in return for violation of policy
- Dangerous for social engineer
 - ❑ Obviously wrong
 - ❑ Honest employees (or one with second thoughts) will report attempt to management
 - ❑ May lead to police involvement, arrest
- Success depends in part on employee attitude
 - ❑ Disgruntled, unhappy employees better
 - ❑ Contractors
 - ❑ Those about to quit or be fired anyway
 - ❑ Criminal may probe for attitudes using negative comments



14

Copyright © 2011 M. E. Kabay. All rights reserved.

Data Mining & Data Grinding



- Search engines
 - ❑ Reveal confidential information
 - ❑ Mine information about organizations
 - ❑ Use caches for pages that have been removed
 - ❑ Web history for older versions
 - ❑ Search-engine APIs provide special tools
 - ❑ See references to “Google hacking” using any search engine
- Data grinding
 - ❑ Extracting metadata from published docs
 - ❑ Unprotected DOC & HTML files may contain valuable info (e.g., author, e-mail address,)

15

Copyright © 2011 M. E. Kabay. All rights reserved.

Network and Voice Methods



- Piggybacking / Tailgating
- Phishing & Pharming
- Spim, Spit, & Vishing
- Trojan Code and Viruses



16

Copyright © 2011 M. E. Kabay. All rights reserved.

Piggybacking / Tailgating



- Follow authorized employee into secured location
 - ❑ Using social expectations of victim
 - ❑ What is polite in normal society may be insecure an unwise for security
- Preparations
 - ❑ Dress like any other employee
 - ❑ Have excuse ready (“Forgot my card....”)
- Defenses
 - ❑ Explicitly forbid piggybacking & explain why
 - ❑ Teach employees using role-playing



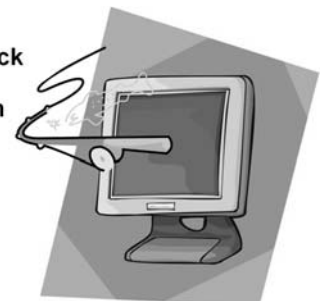
17

Copyright © 2011 M. E. Kabay. All rights reserved.

Phishing & Pharming



- Phishing
 - ❑ Sending e-mail to trick user into providing personal information
 - ❑ Try to copy official correspondence
 - ❑ Paste logos
 - ❑ Often bad grammar, spelling mistakes
- Pharming
 - ❑ Fake Websites imitate real sites (banks, stores)
 - ❑ Collect login, financial information



18

Copyright © 2011 M. E. Kabay. All rights reserved.

Spim, Spit, & Vishing

- Spim
 - ❑ Instant messaging carrying spam
 - ❑ Try to trick victim by sending link to fake Website via IM
 - ❑ Bypass normal Web/e-mail content controls
- Spit
 - ❑ Spam over Internet telephony
 - ❑ Limited controls over such spam
- Vishing
 - ❑ Voice phishing: spam using phone & e-mail
 - ❑ Trick victim into answering questions about personal information



19

Copyright © 2011 M. E. Kabay. All rights reserved.

Trojan Code and Viruses

- Discussed above in slide “Exploiting Curiosity or Naïveté”
- Attackers insert malware on victim’s computer
- Malware silently installed
- Collects or transmits confidential information
- Provides backdoor code to allow unauthorized access



20

Copyright © 2011 M. E. Kabay. All rights reserved.

Reverse Social Engineering

- Aka *knight-in-shining-armor attack*
- Social engineer creates a problem
 - ❑ E.g., a denial-of-service attack
 - ❑ Rename or move of critical file
- Arranges to seem to be only person who can solve problem
- Fixes the problem (easy if attacker caused it)
 - ❑ Gather information during solution
 - ✓ “I need to log on as you.”
 - ❑ Victim may even forget that security policy has been violated
 - ❑ Gains trust for future exploitation



21

Copyright © 2011 M. E. Kabay. All rights reserved.

Psychology & Social Psychology of Social Engineering

- Psychology of Victim
- Social Psychology
- Social Engineer Profile



22

Copyright © 2011 M. E. Kabay. All rights reserved.

Psychology of Victim

- Cognitive biases aid criminals
- Choice-supportive bias
 - ❑ Go with the flow
 - ❑ Use what works most of time
- Confirmation bias
 - ❑ Remember what fits
 - ❑ See person in janitor outfit as janitor – regardless rules
- Exposure effect
 - ❑ What is familiar is comfortable
 - ❑ Gain trust by referring to familiar topics
- Anchoring
 - ❑ Focus on one trait at a time
 - ❑ Soothing, friendly demeanor covers intrusive questions



23

Copyright © 2011 M. E. Kabay. All rights reserved.

Social Psychology

- Schema is picture of reality
 - ❑ Defines normal ways of making judgements and decisions
- Many cognitive errors
 - ❑ Fundamental attribution error: assuming that behavior indicates stable, internal attributes
 - ✓ Therefore a pleasant, friendly social engineer cannot possibly be a criminal
 - ❑ Salience: people notice outliers
 - ✓ So social engineers try to blend in
 - ❑ Conformity, compliance & obedience
 - ✓ Social engineers exert (false) authority

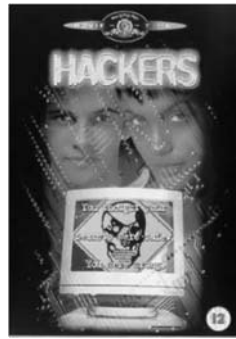
There's an entire lecture on social psychology and security later in the course.

24

Copyright © 2011 M. E. Kabay. All rights reserved.

Social Engineer Profile

- Not as in movies: may be
 - Outgoing
 - Confident
 - Well educated
 - Blend into environment (clothing, style, speech)
 - Good actor
 - Quick reactions to changing circumstances
- Dark side
 - Exploits relationships
 - Little or no empathy for victims (instrumental)
 - May be involved in criminal gangs



Especially bad stereotypes

Dangers & Impact

- Consequences
- Success Rate
- Small Businesses vs Large Organizations



Consequences

- Loss of control over internal documents
 - Advantage to competitors – loss of market share
 - Stock manipulation – SEC investigations
 - Bankrupt company
 - Possible criminal proceedings against officers
- Loss of control over customer personally identifiable information (PII)
 - Legal ramifications including \$\$\$ liability
 - Embarrassment
 - Human consequences of identity theft
- Difficulty tracking down how crime was committed
 - Destroy trust among employees



Success Rate

- Poor statistical base
 - Difficult to detect
 - Difficult to find documentation
- Anecdotal evidence from security experts
 - Social engineering works
 - Consensus that methods are often used...
 - ... and highly successful
- Organizations must prepare to defend themselves against these methods (see below)



Small Businesses vs Large Organizations

Small Businesses

- Less prepared & more vulnerable
- People know each other
- More likely to suspect and challenge strangers
- Better communication – may report suspicions quickly to people they know
- Smaller workforce to train

Large Businesses

- More fragmented: many strangers anyway
- Concern about embarrassment if stranger is executive from afar
- Bystander effect: let someone else deal with it
- Poorer communications: may never have met security officers

Detection

- People
- Audit Controls
- Technology for Detection



People (1)

- Train employees to remember details of phone calls they receive when caller asks questions
 - Gender?
 - Caller ID?
 - Noise in background?
 - Accent?
 - What questions?
 - What answers?
- Beware questions about names of managers
- No employee should ask (let alone give) password



31

Copyright © 2011 M. E. Kabay. All rights reserved.

People (2)

- Ensure that employees know they will not be punished for enforcing security policies
 - No legitimate manager would threaten them for NOT violating security rules
 - Explicitly provide script for responding to threats (“Yes, I’ll be glad to help you – please hold the line.” – and then employee notifies Security Team)
- Provide employees with notification procedure
 - Whom should they call?
 - What information is most helpful (see previous slide)?



32

Copyright © 2011 M. E. Kabay. All rights reserved.

Audit Controls

- Real-time audits of log files *may* detect social engineering attack in progress
 - But no guarantees
 - Human manipulation may have no technical exploits until later in crime
 - Actual exploit may be very fast
- Post hoc audits may be useful in reconstructing crime
 - Trace how criminal used information winkled out of employees



Winkle

33

Copyright © 2011 M. E. Kabay. All rights reserved.

Technology for Detection

- Content-blocking technology
 - E-mail
 - Web pages
- Social Engineering Defense Architecture (SEDA)
 - Voice-recognition technology
 - Provides better logging of phone calls



34

Copyright © 2011 M. E. Kabay. All rights reserved.

Response

- Integrate social engineering attacks into *computer security incident response team* processes
- Collect forensic evidence
 - In real time if possible
 - ASAP
 - Interview human victims
 - ✓ Quickly
 - ✓ Humanely – do not give impression of looking for scapegoats



35

Copyright © 2011 M. E. Kabay. All rights reserved.

Defense & Mitigation

- Training & Awareness
- Technology for Prevention
- Physical Security & Encryption



36

Copyright © 2011 M. E. Kabay. All rights reserved.

Training & Awareness

- Explain social engineering techniques to employees
 - ❑ Real case studies
 - ❑ Demonstrations
- Encourage and support challenges
 - ❑ Asking reasons for questions
 - ❑ Asking for employee identification
 - ❑ Checking for authorization for unusual requests
- Provide role-playing exercises to reduce reluctance
- Provide emergency response contact info



Technology for Prevention

- Effective antimalware tools
 - ❑ Block viruses, Trojans
 - ❑ Block dangerous Web sites
 - ❑ Block dangerous phishing spam
 - ❑ Block popups, ActiveX controls
 - ❑ Restrict types of cookies
 - ❑ Use digital certificates to authenticate internal e-mail
- Control over software installation
- Cleanse documents of hidden metadata
- Check Web for unauthorized posting of confidential documents or information



Physical Security & Encryption

- Prevent theft of confidential information
 - ❑ Lock filing cabinets
 - ❑ Shred discarded documents
 - ❑ Protect Dumpsters® against divers
- Use data encryption
 - ❑ Laptop computers
 - ❑ Peripherals such as USB drives
 - ❑ Virtual private networks for remote access

DISCUSSION