Social Engineering

Human Factors in Information Security

Masters Seminar on Computer Security Threats and Counter Measures, University of Fribourg, 2007

Manuel Studer
Email: manuel.studer@unifr.ch

Content

- Introduction
- Social Engineering Attack Pattern
- Example of Reverse Social Engineering
- Psychological Triggers
- Multilayered Defense
- Conclusion

Introduction

- What we know so far:

Intrusion Detection

Firewalls

RSA

Asymmetric Encryption

Triple DES

Symmetric Encryption

PGP

WPA

Proxies

VPN

Unix Salt

Introduction

- What we know so far:

Intrusion Detection

RSA

Triple [illegible]

PGP

Proxies

VPN

Fi[illegible]

[illegible]ymmetric Encryption

Symmetric Encryption

WPA

Unix Salt

Weakest link in information security: HUMAN

Introduction

- Aim of this presentation is to understand following relation:

Computer Security $\subset$ Information Security

Definition

- Definition of “Social Engineering”:

  “... is the art and science of getting people to comply to your wishes.” (Harl's Talk at Access All Areas III, 1997)

  “... getting people to do things they wouldn’t ordinarily do for a stranger.” (Kevin D. Mitnick, “Art of Deception”, 2002)

Social Engineers

- Probably most successful "social engineer" so far:

Kevin D. Mitnick (born 1963)

- Convicted for breaking into the computer systems of Fujitsu, Motorola, Nokia, and Sun Microsystems. ⇒ 4 years prison
- Now founder of security firm: "Mitnick Security Consulting".

Social Engineers

- Who is Kevin D. Mitnick NOT?

- A particularly knowledgeable computer programmer.
- "... a malicious hacker." (cite Kevin D. Mitnick, "The Art of Deception", 2002)

Social Engineering Methods

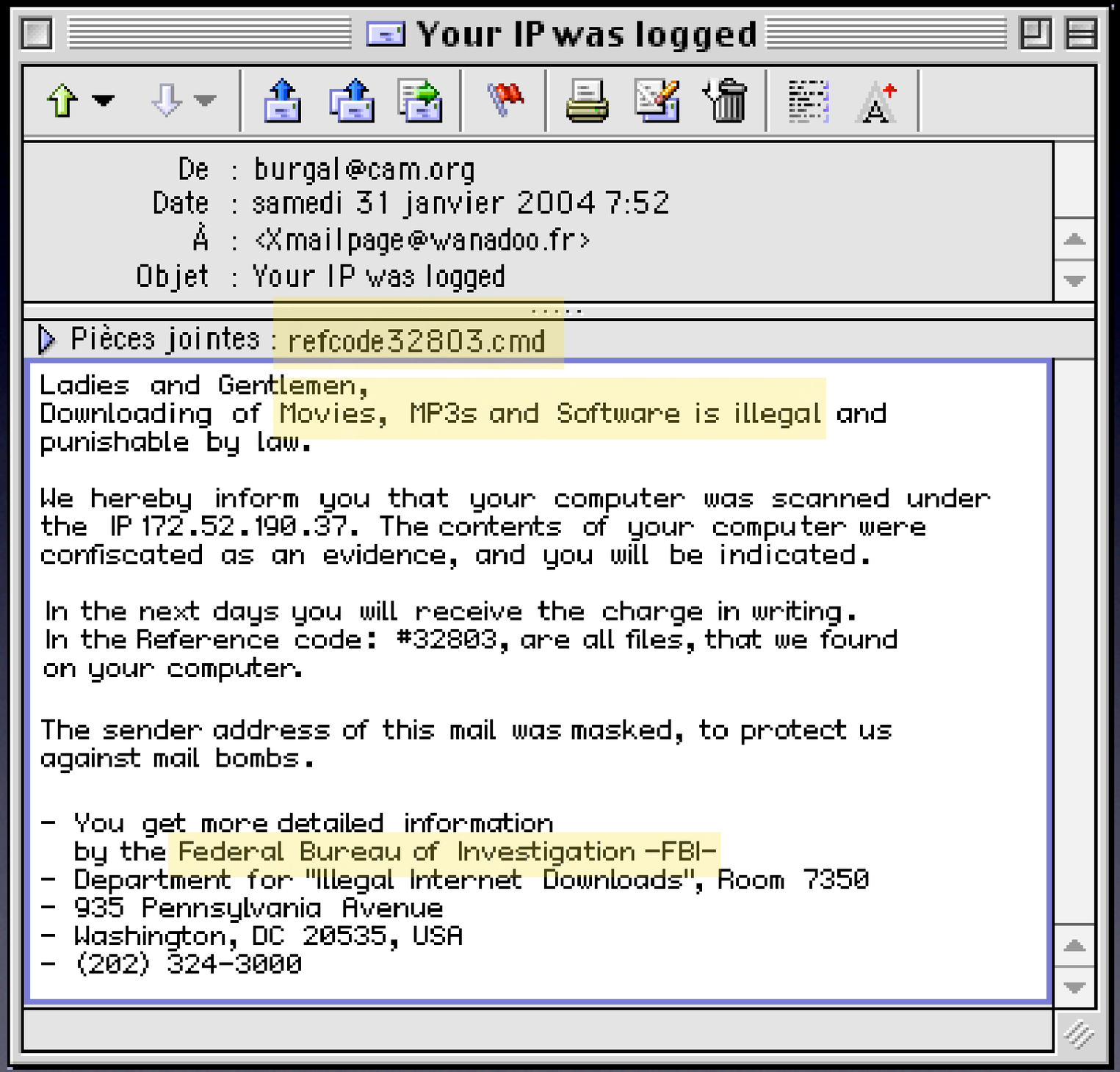
- Human based attack

  Any medium that provides one-to-one connection, e.g. face-to-face, telephone, electronic mail.

- Computer based attack

  Trick somebody into supplying valuable information, e.g. pop-ups, phishing.

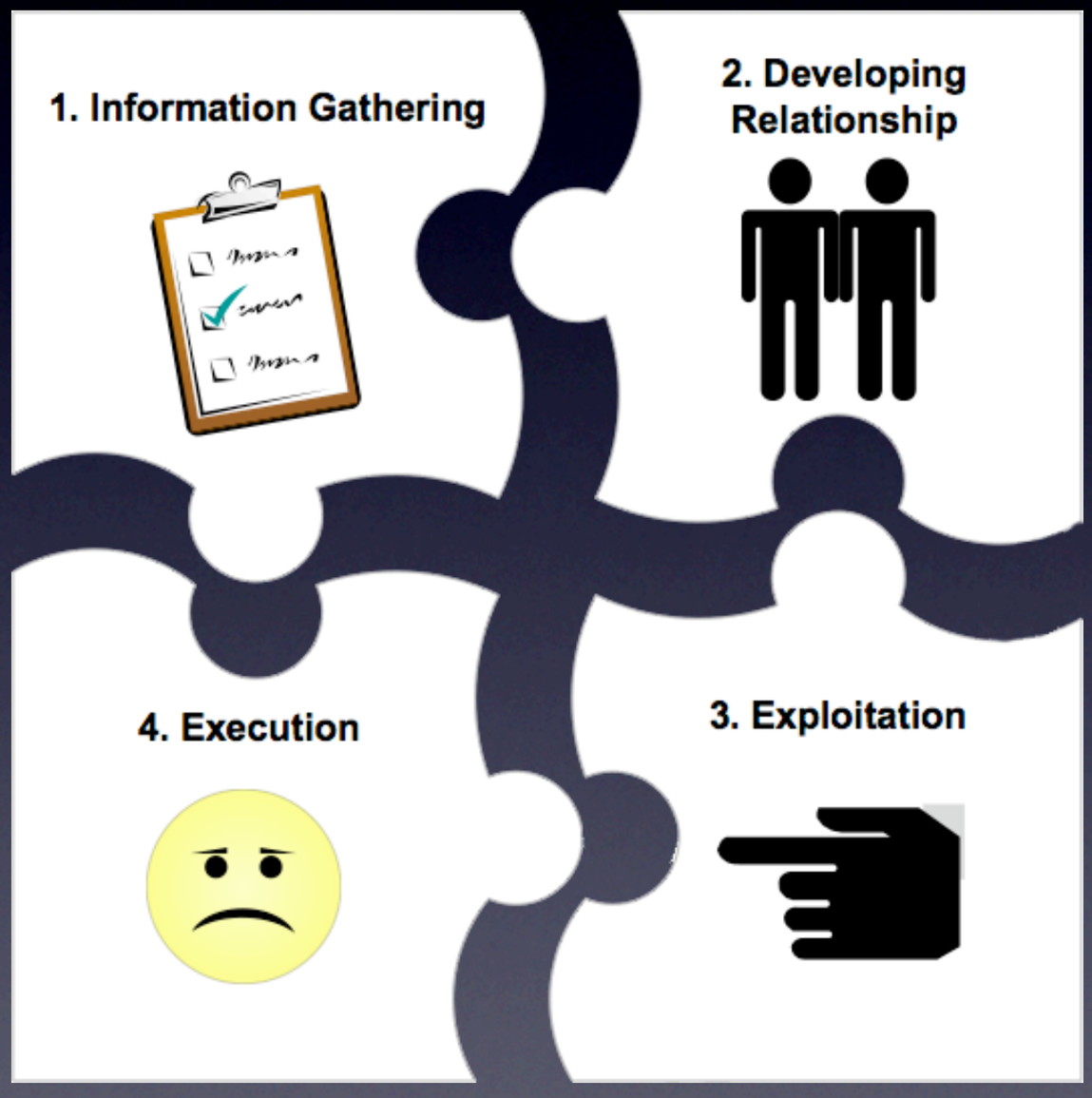
Sober Virus


Your IP was logged
De : burgal@cam.org
Date : samedi 31 janvier 2004 7:52
Á : <Xmailpage@wanadoo.fr>
Objet : Your IP was logged
Pièces jointes : refcode32803.cmd
Ladies and Gentlemen,
Downloading of Movies, MP3s and Software is illegal and
punishable by law.
We hereby inform you that your computer was scanned under
the IP 172.52.190.37. The contents of your computer were
confiscated as an evidence, and you will be indicated.
In the next days you will receive the charge in writing.
In the Reference code: #32803, are all files, that we found
on your computer.
The sender address of this mail was masked, to protect us
against mail bombs.
- You get more detailed information
by the Federal Bureau of Investigation -FBI-
- Department for "Illegal Internet Downloads", Room 7350
- 935 Pennsylvania Avenue
- Washington, DC 20535, USA
- (202) 324-3000

Social Engineering

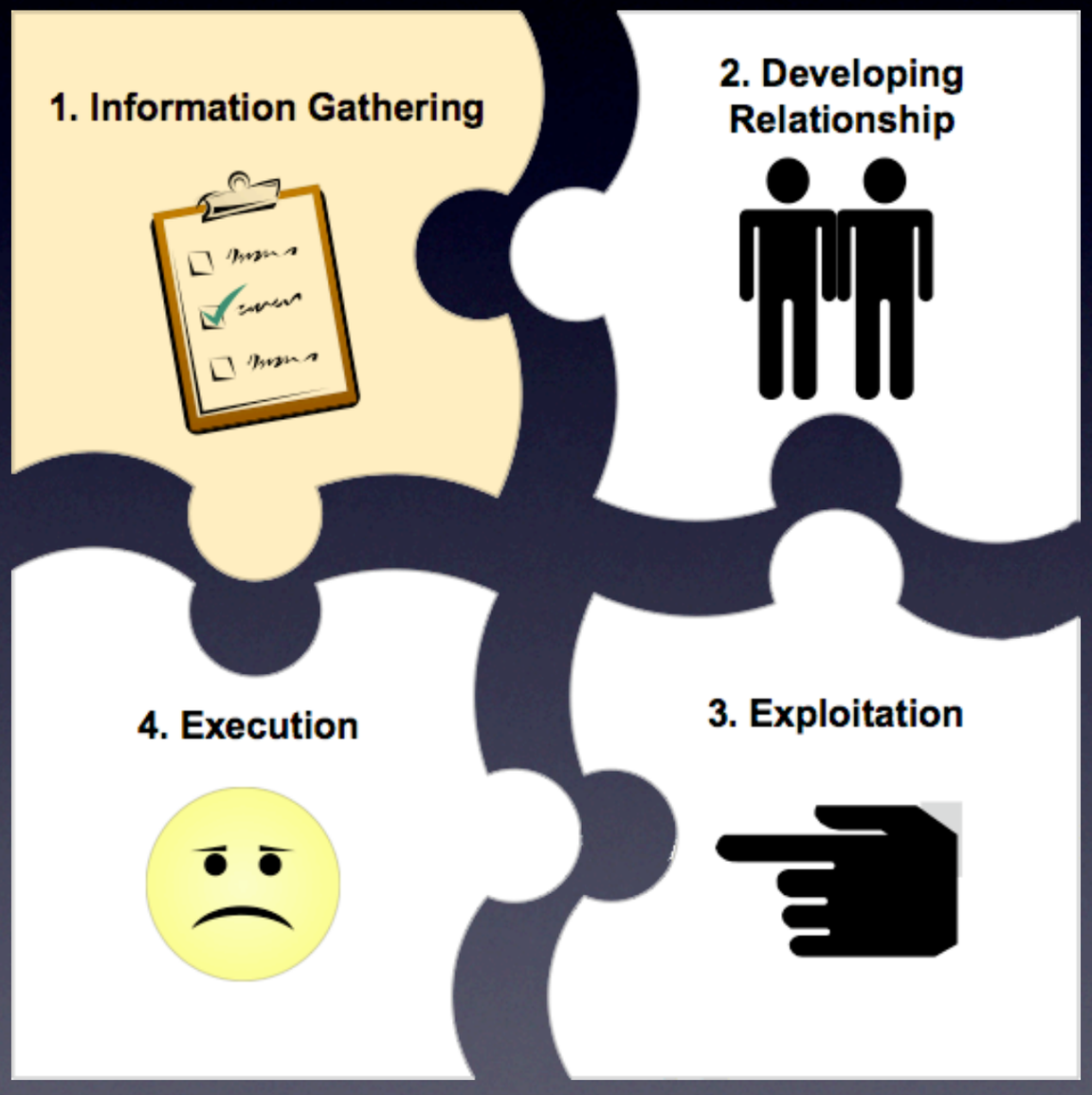
Attack Pattern

Attack - Pattern



- Each attack is unique
- Possibly multiple cycles

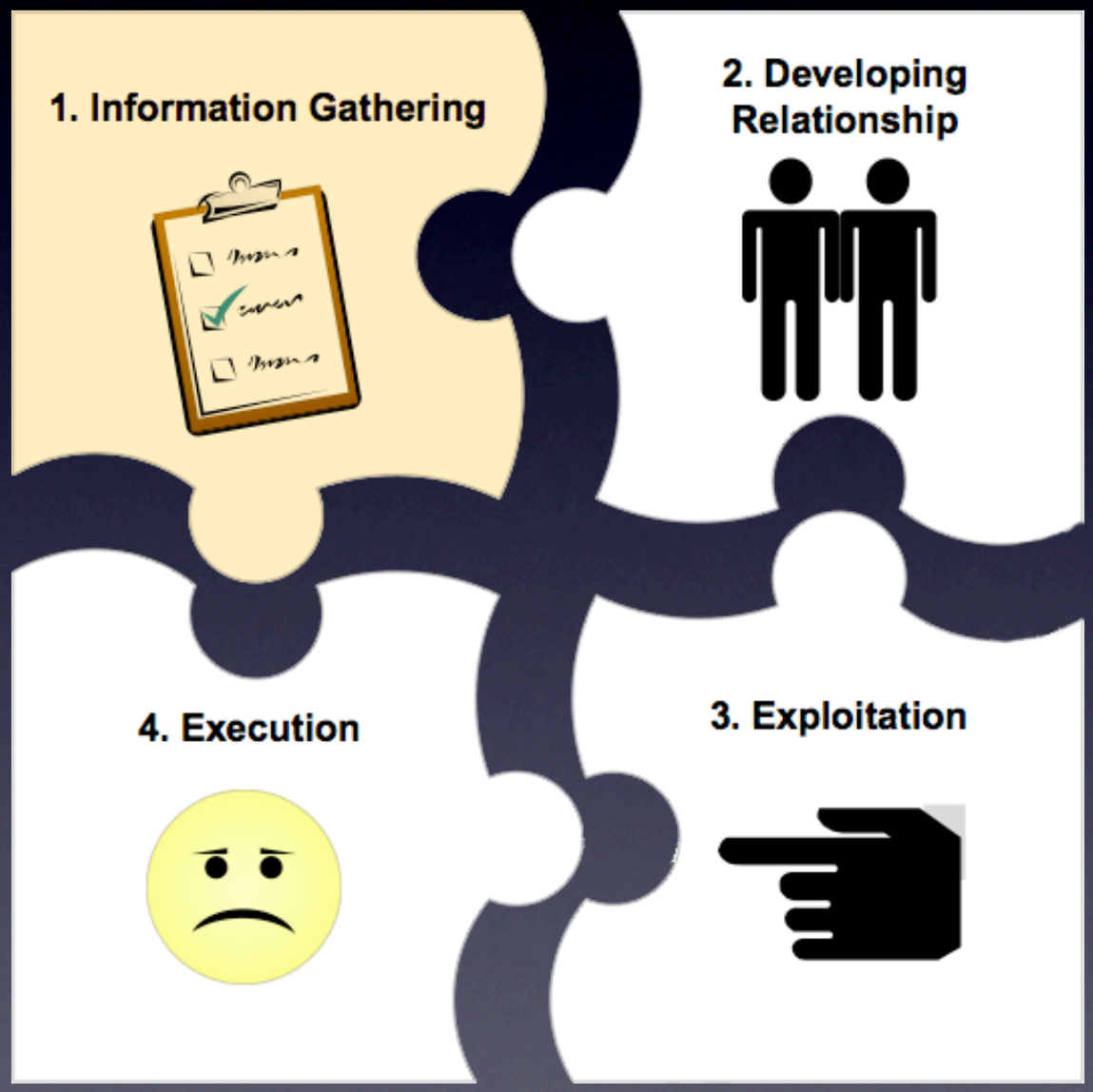
Attack - Pattern



1. Information Gathering

- Open source information e.g. phone lists, date of birth, flyers.

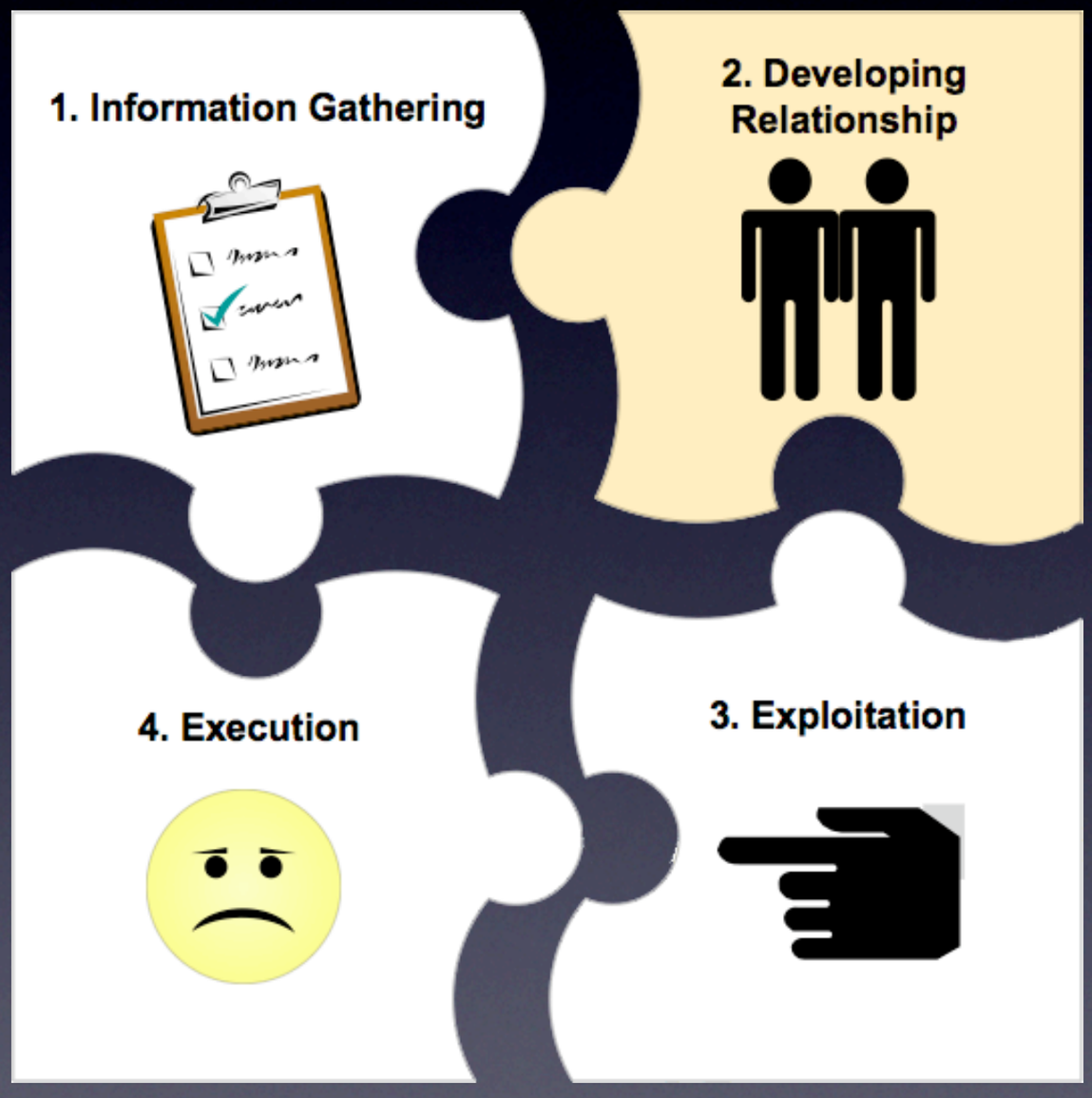
Attack - Pattern



1. Information Gathering

- Dumpster diving (100% legal)

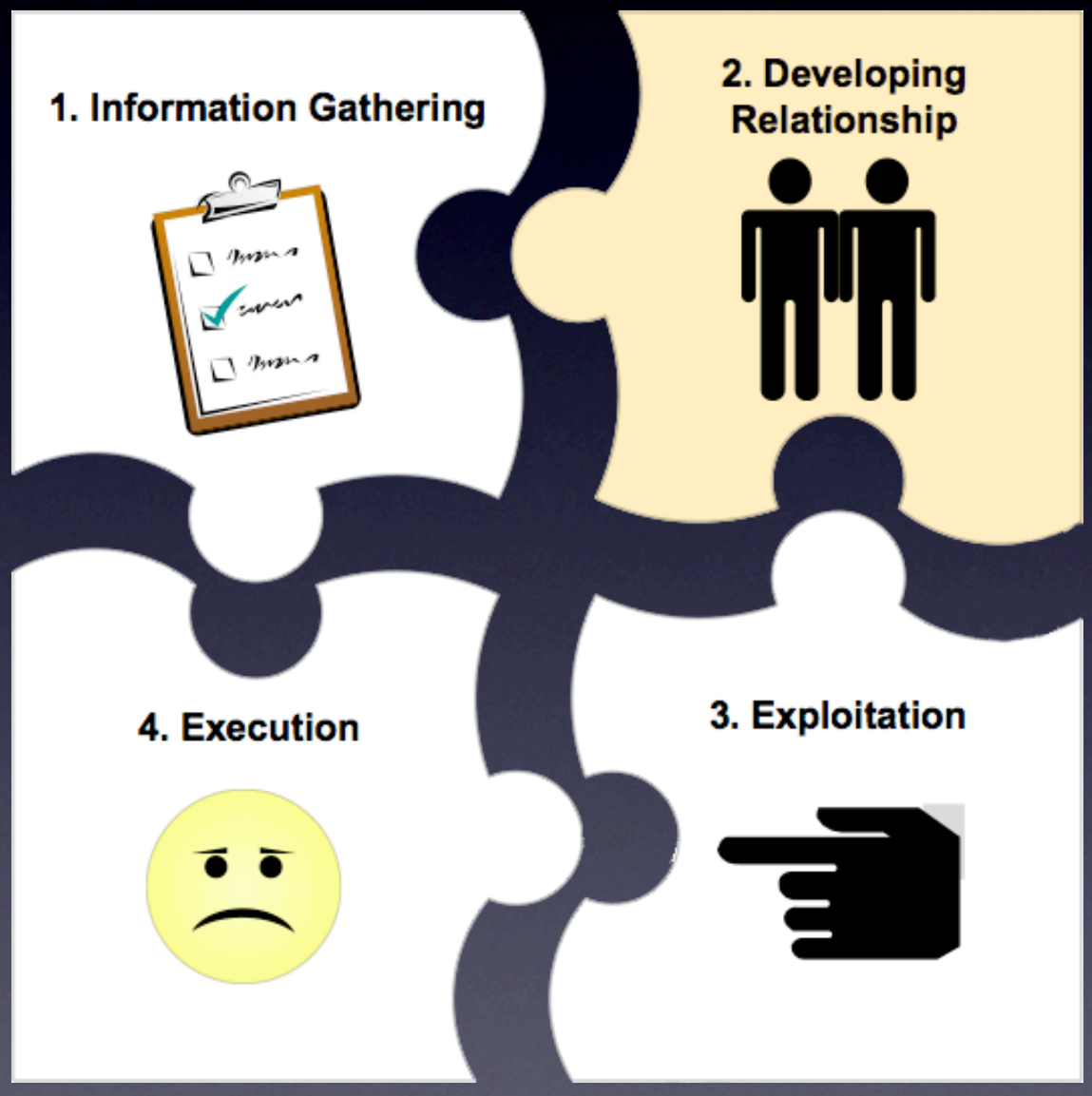
Attack - Pattern



2. Developing Relationship

- Insider information
- Company Language
- Misrepresenting identity

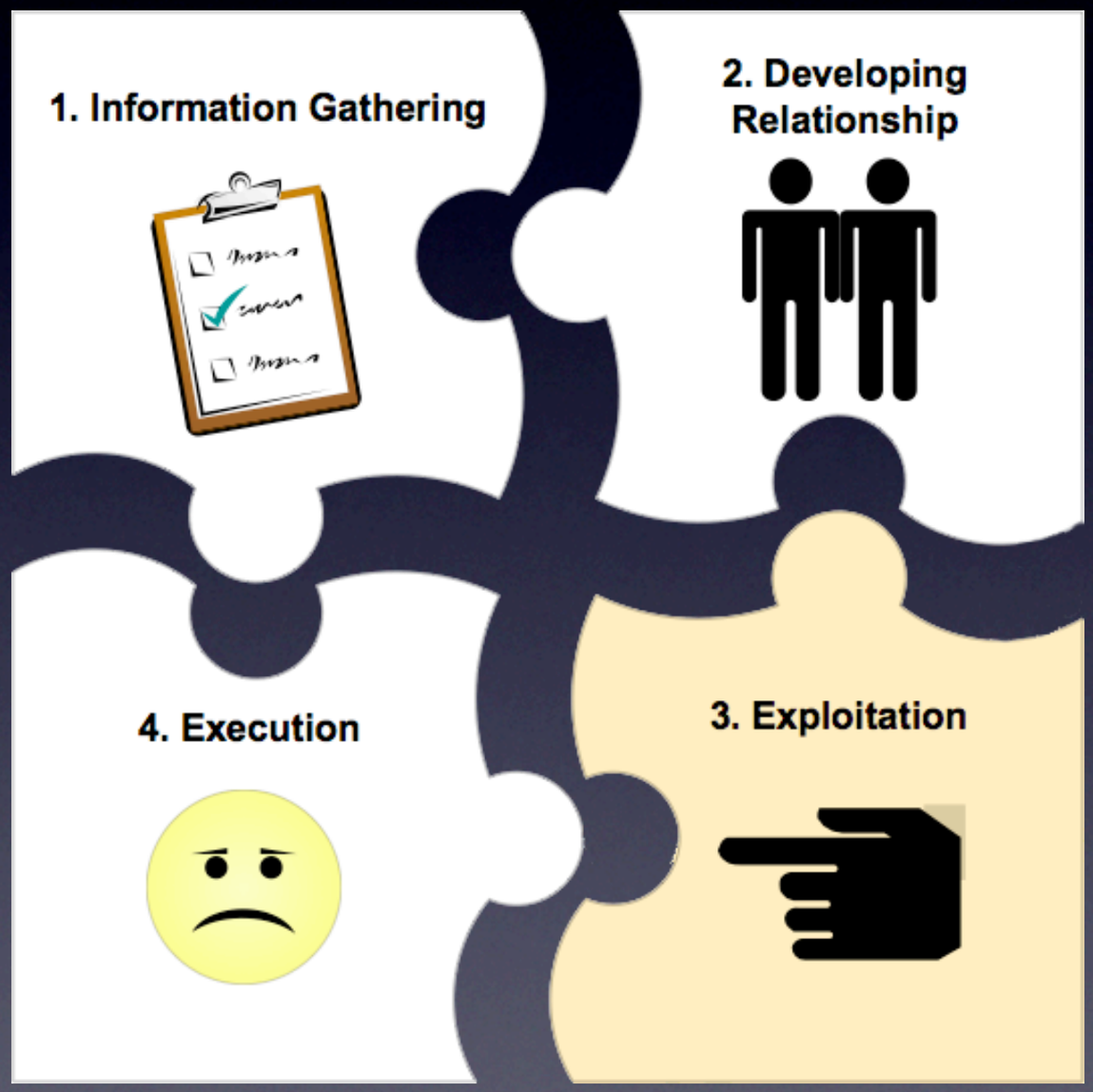
Attack - Pattern



2. Developing Relationship

- Cite people known to victim
- Need for help
- Authority (name dropping)

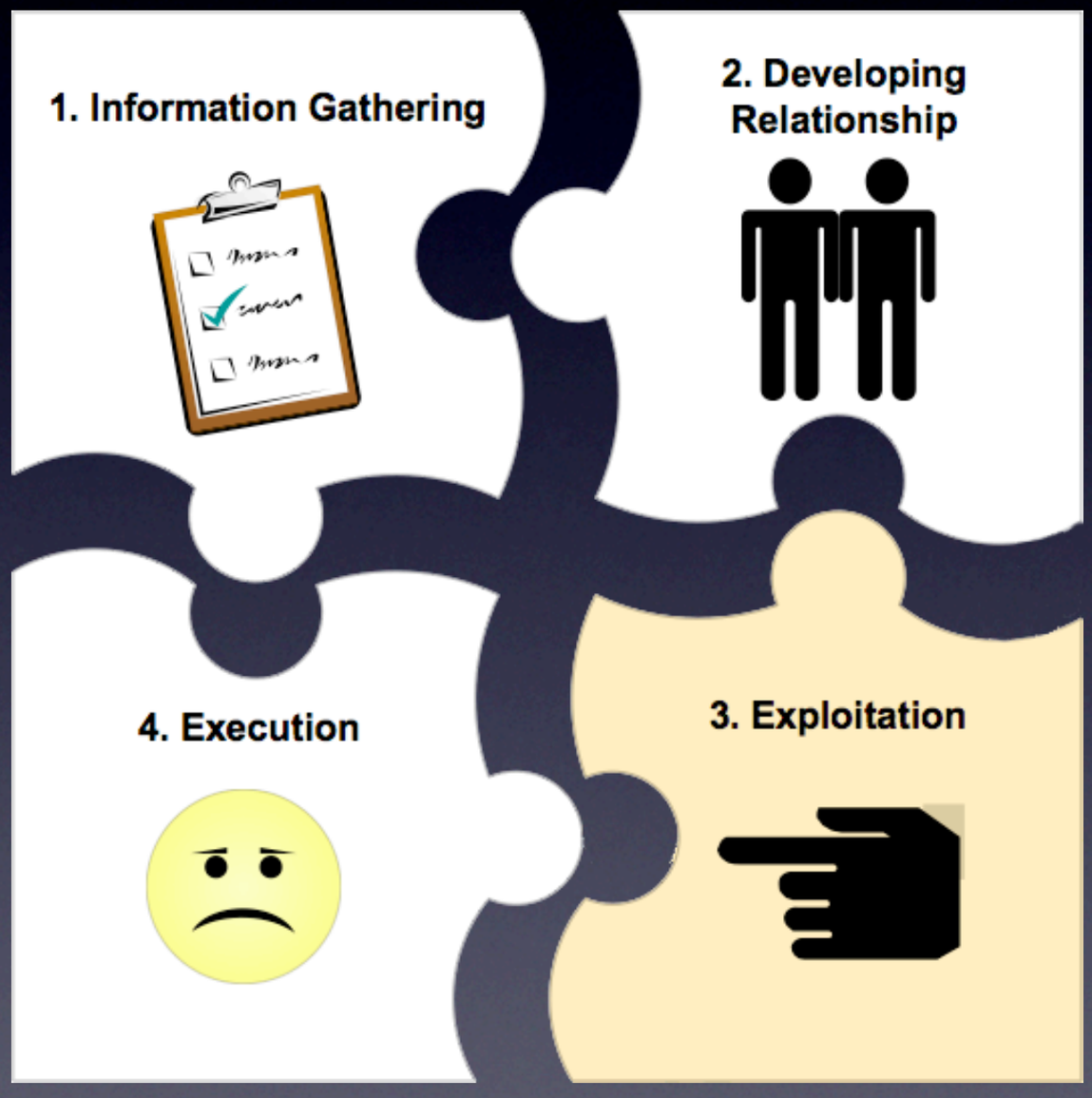
Attack - Pattern



3. Exploitation

- Ask for information/ action on the part of the victim

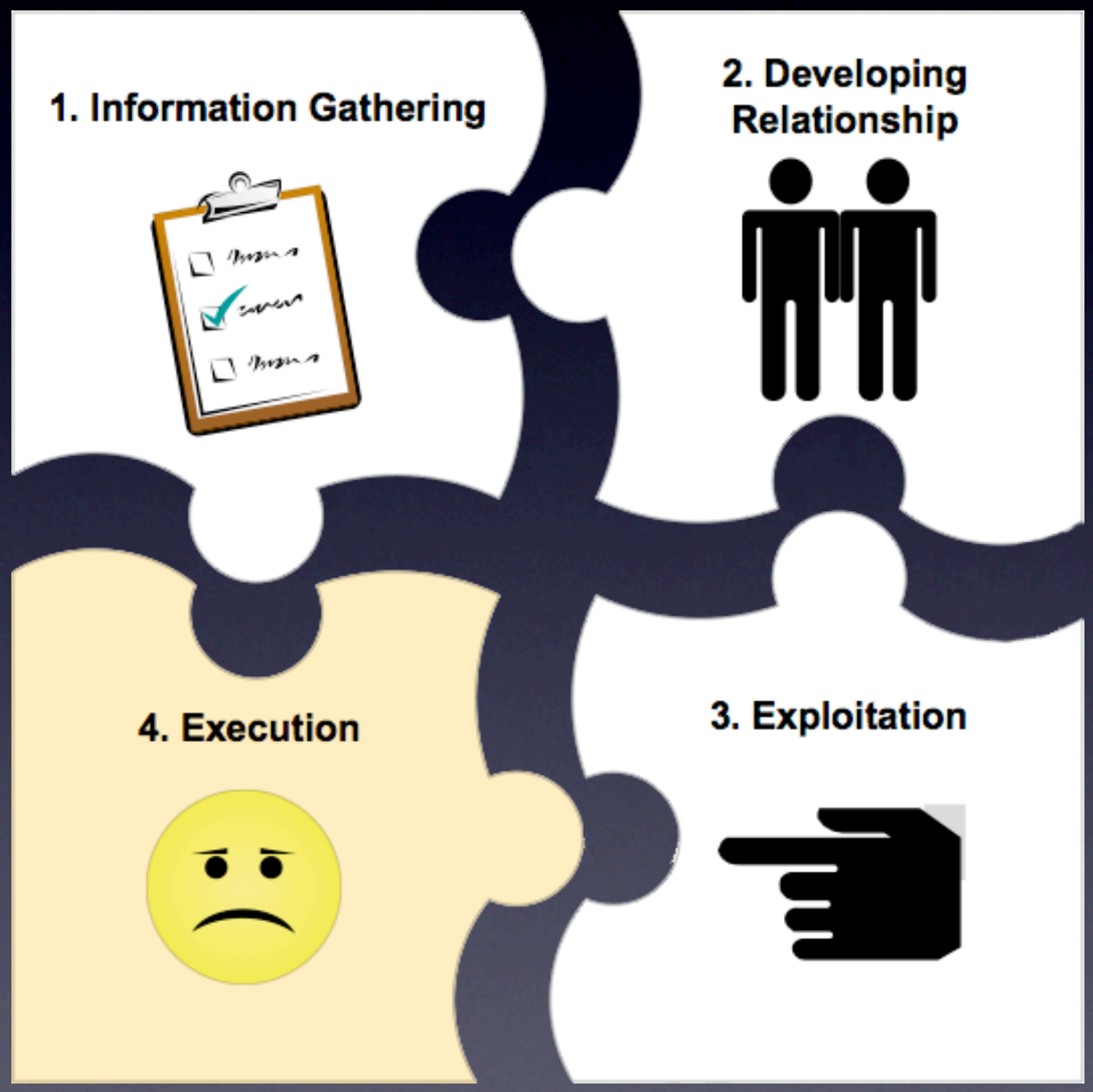
Attack - Pattern



3. Exploitation

- Reverse social engineering: manipulate victim to ask attacker for help

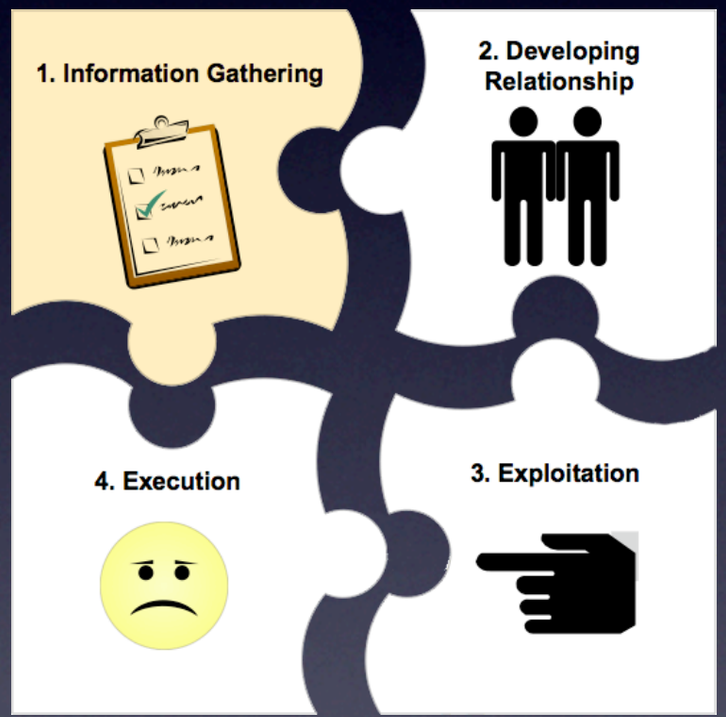
Attack - Pattern



4. Execution

- Have fun! (But be nice!)

Example: Reverse Social Engineering Scenario

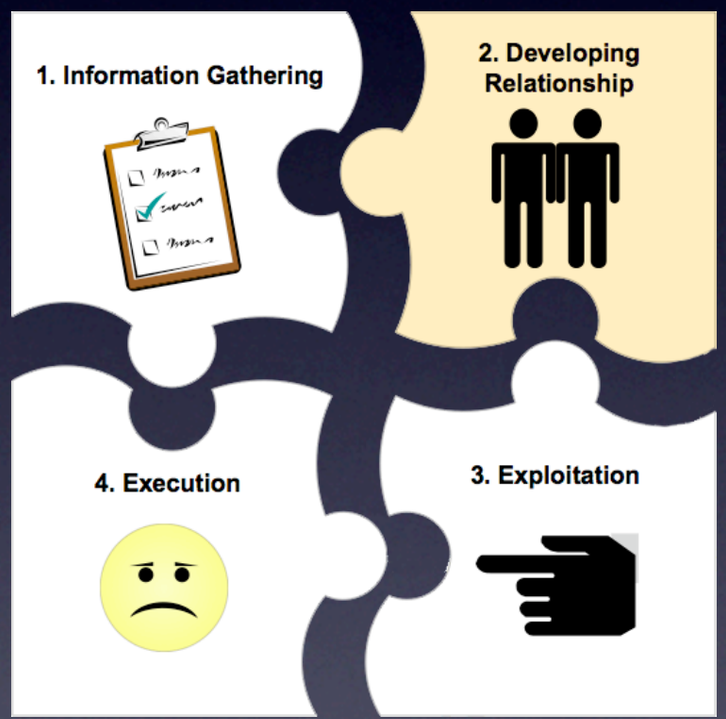


1. Information Gathering

Story from the book "The Art of Deception" by Kevin Mitnick.

- The attacker gets information about the IT infrastructure as well as telephone numbers of IT security and management people.

Example: Reverse Social Engineering Scenario



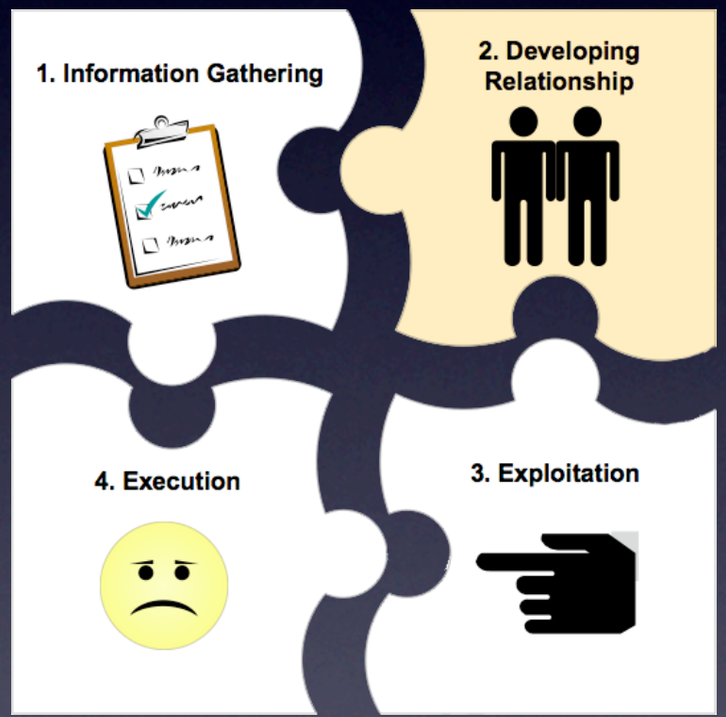
2. Developing Relationship

- Attacker calls person in management, pretends to be from help-desk:

Attacker: "We have network problems here, does your PC work now?"

Target: "Everything works fine."

Example: Reverse Social Engineering Scenario

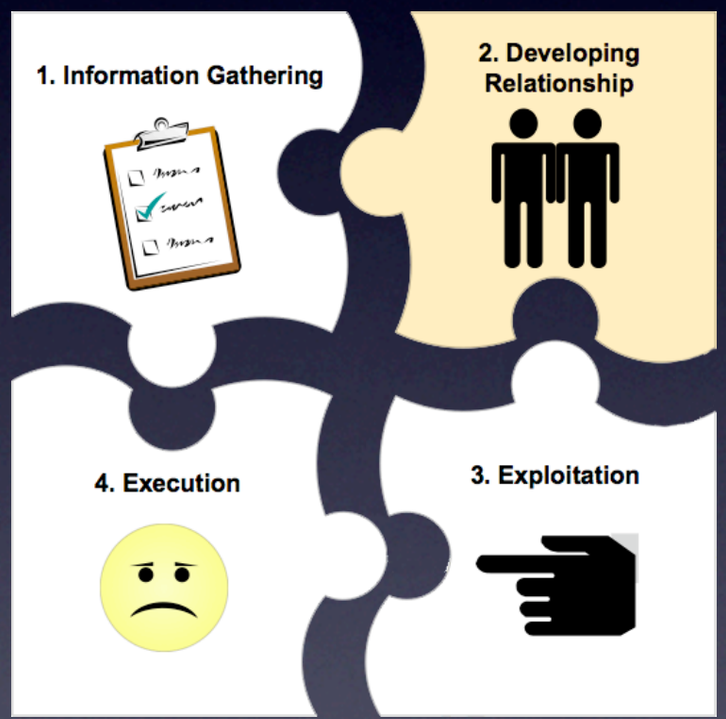


2. Developing Relationship

Attacker: "Ok, just in case something goes wrong, call me at 22232..."

Target: "Alright, I write your number down."

Example: Reverse Social Engineering Scenario



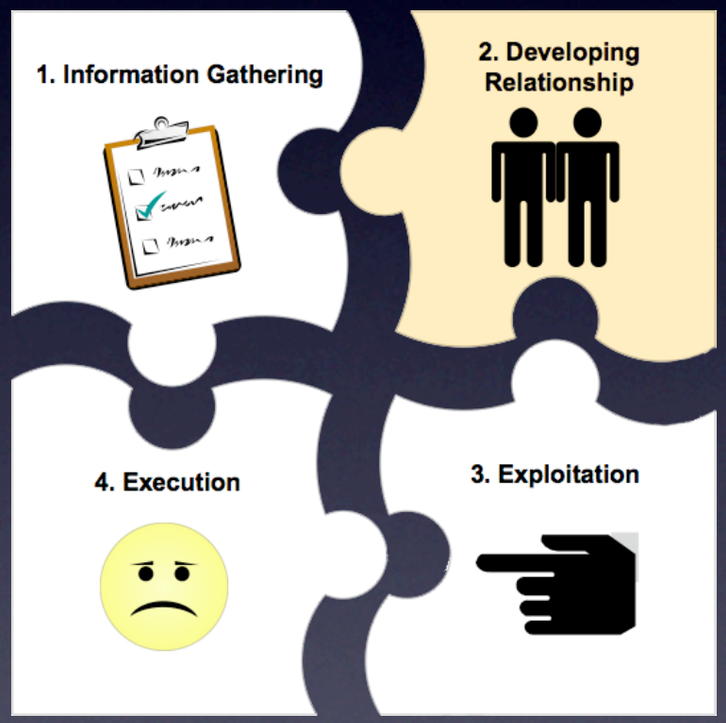
2. Developing Relationship

- Attacker calls IT support.

Attacker: "This is Eddie, we have a problem with the network. Can you disable port 34-2?"

IT guy: "Ok, in a few minutes." (shortened conversation!)

Example: Reverse Social Engineering Scenario



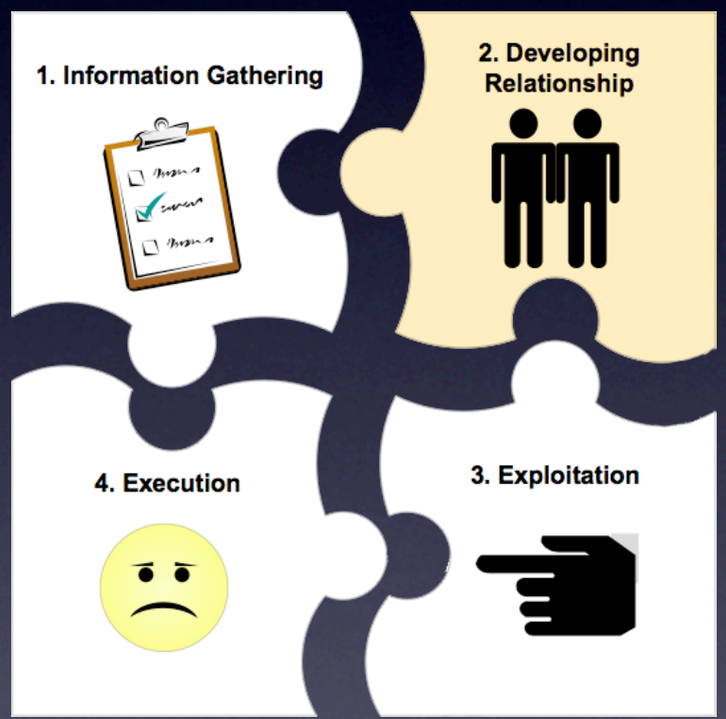
2. Developing Relationship

- Attacker is being called by target as the network is down.

Target: "This is Maggie, the network doesn't work."

Attacker: "Ok I will look at the network. We need about 30 minutes for repairing your connection."

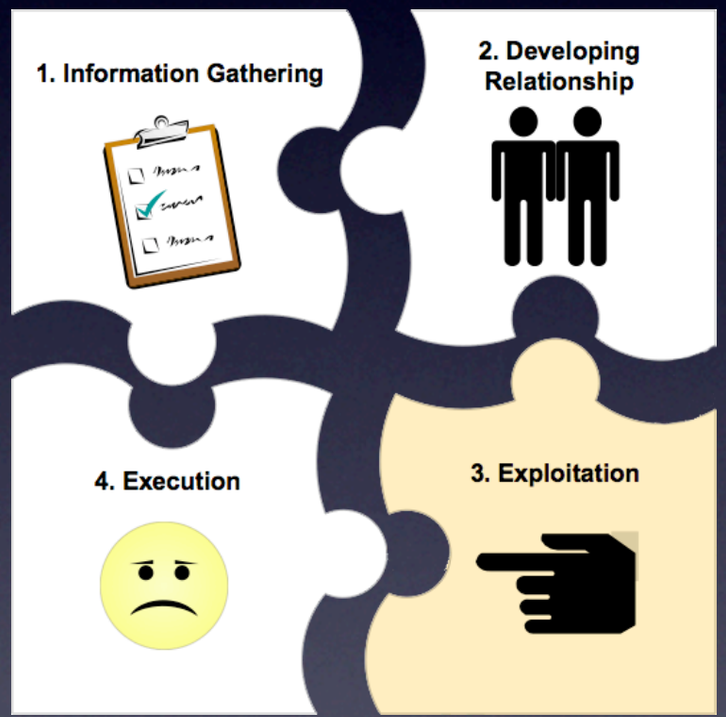
Example: Reverse Social Engineering Scenario



2. Developing Relationship

- Attacker calls IT support for enabling port 34-2.

Example: Reverse Social Engineering Scenario



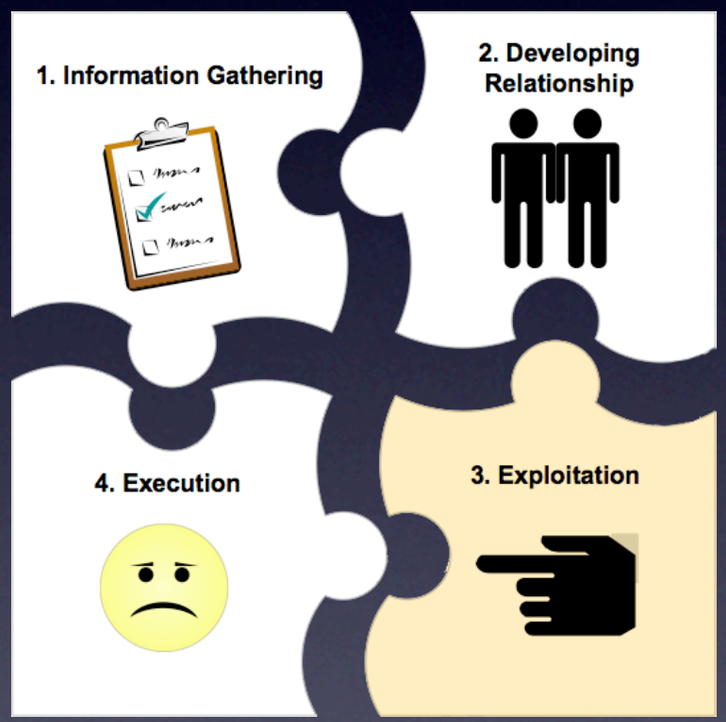
3. Exploitation

- Attacker calls target.

  Attacker: "Does the connection work now?"

  Target: "Yes, thanks a lot!"

Example: Reverse Social Engineering Scenario

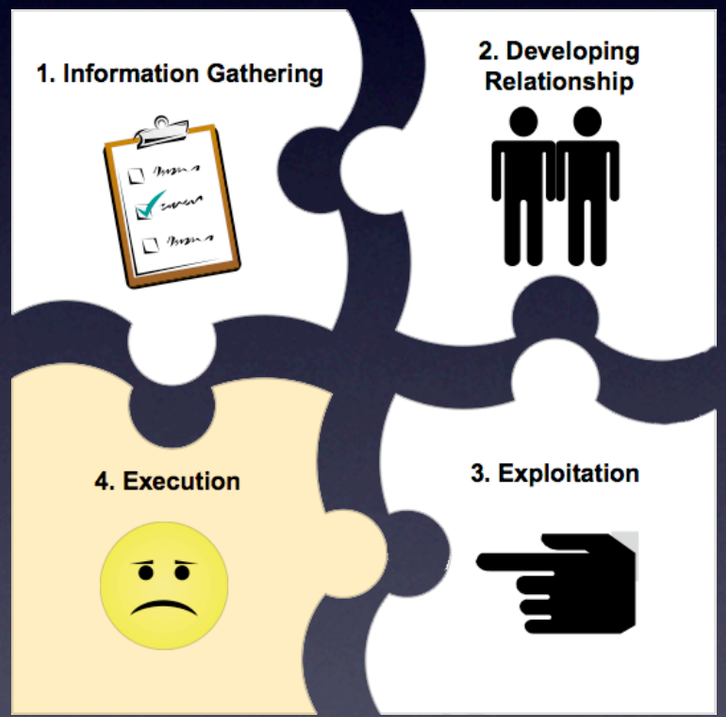


3. Exploitation

Attacker: "Listen if you want to make sure that your connection doesn't go down again, you need to install a program."

- Attacker prompts the target to install a hidden vnc server.

Example: Reverse Social Engineering Scenario



4. Execution

- Attacker is able to get secret files from the target computer.

Psychological Triggers

Psychological Triggers

- Strong Affect

  Triggers strong emotions such as

  - fear
  - excitement
  - panic

  ⇒ Bad evaluation /not logical thinking

Psychological Triggers

- Overloading

  Having to deal with a lot of information.

  - sensory overload
  - people absorb information rather than evaluate

Psychological Triggers

- Reciprocation

  If someone gives/promises us something we should return favor.

- Someone who helps does not do any harm.
- Reverse social engineering uses this trigger.

Psychological Triggers

- Deceptive Relationships

  Building relationships for exploiting other persons.

  - sharing information
  - discussing a common enemy

Psychological Triggers

- Diffusion of Responsibility and Moral Duty

Target is made to feel that he/she is not solely responsible for his/her actions.

Psychological Triggers

- Authority

  People are conditioned to respond to authority.

  - Fake director
  - Fake vice-president

Psychological Triggers

- Integrity and Consistency

"do what you say you are going to do"

People have a tendency to believe that others are expressing their true attitudes when they make a statement. (luckily!)

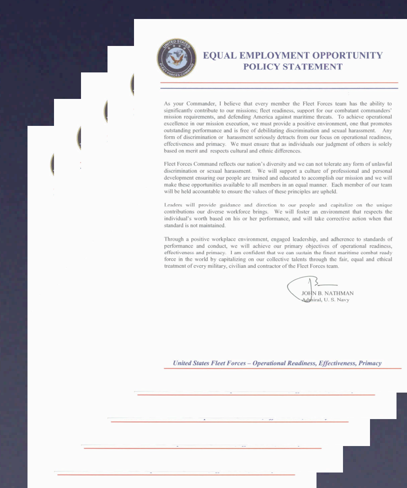
Multilayered Defense

Multi-layered Defense

- Foundational Level (Level 0)

  Security Policy addressing social engineering:

  - access control
  - changing regular passwords
  - shredding paper etc.


EQUAL EMPLOYMENT OPPORTUNITY
POLICY STATEMENT

As your Commander, I believe that every member the Fleet Forces team has the ability to significantly contribute to our missions; fleet readiness, support for our combatant commanders' mission requirements, and defending America against maritime threats. To achieve operational excellence in our mission execution, we must provide a positive environment, one that promotes outstanding performance and is free of debilitating discrimination and sexual harassment. Any form of discrimination or harassment seriously detracts from our focus on operational readiness, effectiveness and primacy. We must ensure that as individuals our judgment of others is solely based on merit and respects cultural and ethnic differences.

Fleet Forces Command reflects our nation's diversity and we can not tolerate any form of unlawful discrimination or sexual harassment. We will support a culture of professional and personal development ensuring our people are trained and educated to accomplish our mission and we will make these opportunities available to all members in an equal manner. Each member of our team will be held accountable to ensure the values of these principles are upheld.

Leaders will provide guidance and direction to our people and capitalize on the unique contributions our diverse workforce brings. We will foster an environment that respects the individual's worth based on his or her performance, and will take corrective action when that standard is not maintained.

Through a positive workplace environment, engaged leadership, and adherence to standards of performance and conduct, we will achieve our primary objectives of operational readiness, effectiveness and primacy. I am confident that we can sustain the finest maritime combat ready force in the world by capitalizing on our collective talents through the fair, equal and ethical treatment of every military, civilian and contractor of the Fleet Forces team.

JOHN B. NATHMAN
Admiral, U. S. Navy

United States Fleet Forces – Operational Readiness, Effectiveness, Primacy

Multi-layered Defense

- Parameter Level (Level I)

  Security awareness training for all users:

  - Know what has value
  - Friends are not always friends
  - Passwords are personal etc.

Multi-layered Defense

- Fortress Level (Level II)

  Resistance training for key personnel:

  - Help Desk personnel
  - Costumer Service
  - Receptionist etc.

Multi-layered Defense

- Persistence Level (Level III)

Ongoing regular and creative reminders:

- Screen-savers
- Popups etc.

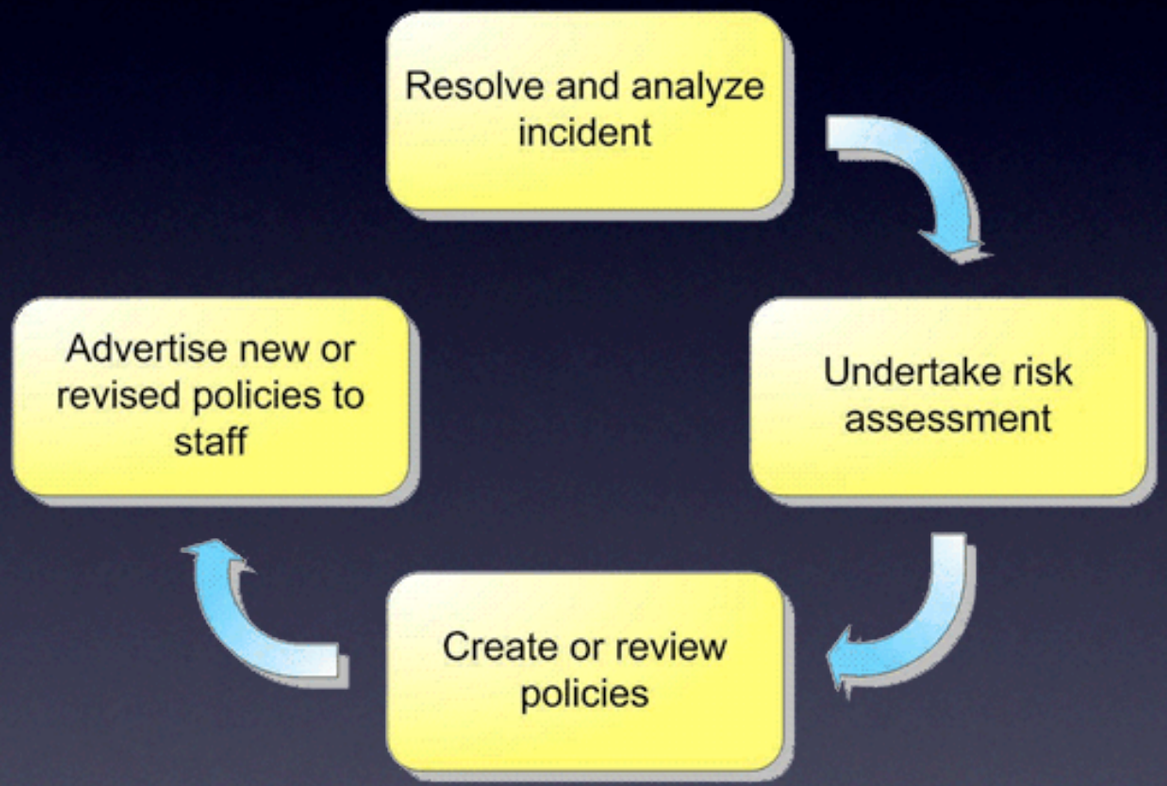
Multi-layered Defense

- Gotcha Level: Social Engineering Land Mines (SELMs) (Level IV)

  Traps that are set up to expose and stop attack.

  - Centralized Security Logs
  - Call Backs by Policy
  - Key Questions (e.g. Bogus question) etc.

Multi-layered Defense



- Offensive Level: Incident Response (Level V)

Undertake risk assessment:

- Create logs in database.
- Inform other potential victims.

Conclusion

- Computer Security ⊂ Information Security
  - Develop good policies
  - Train people
  - Do not forget help personal e.g cleaning people etc.

  Security is not a product, it is a process!

References

Mitnick, K., and Simon, W., The Art of Deception. Indianapolis, IN: Wiley, 2002.

Mitnick, K., and Simon, W., The Art of Intrusion. Indianapolis, IN: Wiley, 2005.

White, S.M., Social engineering. Engineering of Computer-Based Systems, 2003. Proceedings. 10th IEEE International Conference and Workshop on the 7-10 April 2003, Page(s):261 - 267, Digital Object Identifier 10.1109/ECBS.2003.1194807

Wendy Arthurs, A Proactive Defence to Social Engineering. October 31, 2003.

Malcolm Allen, Social Engineering: A Means To Violate A Computer System. June 22, 2006.

Laribee, L., Barnes, D.S., Rowe, N.C., Martell, C.H., Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems. 2006 IEEE Information Assurance Workshop, June 2006, 21-23 Page(s):388 - 389.

Ira S. Winkler, Case study of industrial espionage through social engineering. National Computer Security Association, 1996.

David Gragg, A Multi-Level Defense Against Social Engineering, October 31, 2003.

Sarah Granger, Social engineering reloaded. Retrieved December 10, 2006 from http://www.securityfocus.com/infocus/1860