Psychological Fundamentals of Social Engineering

Stefan Schumacher

www.kaishakunin.com

DeepSec Security Conference
Vienna, Austria
November 11 – 14 2008

解釈人

About Me

- NetBSD-Developer (Stefan@NetBSD.org)
  President of the German NetBSD Foundation (e.V.)
- Interested in Cryptography, Security and Social Engineering
- Student of Educational Science and Psychology at University of Magdeburg
- Freelance Security Consultant (www.Kaishakunin.com)

解釈人

Table of Contents

1 Fundamentals

2 Reciprocation

3 Commitment and Consistency

4 Social Proof

5 Obedience to Authority

6 Liking

7 Scarcity

解釈人

Social Engineering

What is Social Engineering?

- A Theory from Social Science / Mass Psychology
- influencing masses to a predictable, predetermined behavior
- sth. totalitarian regimes want
- Think of *We* (Jewgenij Samjatin), *1984*, *Brave New World*

解釈人

Social Engineering

What is Social Engineering?

- in IT Security/Hacking:
- a technique to circumvent security mechanisms by misusing human behavior
- Â»Hacking PeopleÂ«
- misuse of fundamental human psychology
- Why should I crack `/etc/master.passwd`, if I can talk a user into revealing his password?

解釈人

Social Engineering

What is Social Engineering?

- in IT Security/Hacking:
- a technique to circumvent security mechanisms by misusing human behavior
- Â»Hacking PeopleÂ«
- misuse of fundamental human psychology
- Why should I crack `/etc/master.passwd`, if I can talk a user into revealing his password?

解釈人

Table of Contents

1 Fundamentals

2 Reciprocation

3 Commitment and Consistency

4 Social Proof

5 Obedience to Authority

6 Liking

解釈人

Fundamentals

Fixed Action Patterns

- Animal behaviorists discovered *fixed action patterns*
- Konrad Lorenz Grey-Goose experiments
- M. W. Fox (1974):
  - stuffed Polecat filled with a audio player
  - Turkey attacked Polecat
  - audio player played turkey cheep-cheep
  - Turkey accepted Polecat as baby turkey
  - in reality, a Polecat does not cheep-cheep
- think of cuckoos

解釈人

Fundamentals

Stereotyped Behaviour

humans are also just animals ...

- fight-or-flight-reactions
- expensive is good (Mercedes, Chivas Regal) cheap, billig
- experts know what they are talking about ...
- good looking woman passing by ...
- women and shoe shops ...

解釈人

Fundamentals

Stereotyped Behaviour

humans are also just animals ...

- fight-or-flight-reactions
- expensive is good (Mercedes, Chivas Regal) cheap, billig
- experts know what they are talking about ...
- good looking woman passing by ...
- women and shoe shops ...
- the first impression is very important

解釈人

Fundamentals

Stereotyped Behaviour

humans are also just animals ...

- fight-or-flight-reactions
- expensive is good (Mercedes, Chivas Regal) cheap, billig
- experts know what they are talking about ...
- good looking woman passing by ...
- women and shoe shops ...
- the first impression is very important
- that's why I switched from Geek Shirts and Army Boots to Business Look ;-)

解釈人

Fundamentals

Stereotyped Behaviour

humans are also just animals ...

- fight-or-flight-reactions
- expensive is good (Mercedes, Chivas Regal)
  cheap, billig
- experts know what they are talking about ...
- good looking woman passing by ...
- women and shoe shops ...
- the first impression is very important
- that's why I switched from Geek Shirts and Army Boots to Business Look ;-)

解釈人

Fundamentals

Stereotyped Behaviour

- automatic, stereotyped behavior is the most efficient form of behaving
- This world is to fast and to complex to be analyzed at every decision to be made
- *Termed judgmental heuristics* as shortcuts triggered by so called trigger features
- trigger features are inherent to a culture (obey the old, expensive is good, women are worthless)
- *controlled responding* of thorough analysis only, when decision is considered to be important
- we expect our advisors (lawyer, physician, accountants) to do controlled responding

解釈人



"Perhaps Monsieur would care for something more expensive?"

解釈人

Stereotyped Behaviour

perceptual contrast

- things are judged by their differences
- Lab: 3 bins of water: ice-cold, hot, normal warmth
- put the left hand in the ice-cold water, the right in the hot
- then put both hands into the normal water – what will you feel?

解釈人

Table of Contents

1 Fundamentals

2 Reciprocation

3 Commitment and Consistency

4 Social Proof

5 Obedience to Authority

6 Liking

解釈人

Reciprocication

Fundamentals

- try to repay, what another person has provided us
- Sociologists reported that Reciprocication exists in *all* cultures
- Leaky & Lewin (1978) claim that we are human, because we share foods and skills Â»in an honored network of obligationÂ«
- Society benefits from a System of Reciprocation
- ethologist claim, that reciprocication helped us in breaking the Â»grey barreerÂ«

解釈人

Reciprocication

Example

- 1985, Mexico suffered from an earthquake, Ethiopa suffered from starvation
- The Ethiopian Red Cross donated $5,000,– to Mexico

解釈人

Reciprocication

Example

- 1985, Mexico suffered from an earthquake, Ethiopa suffered from starvation
- The Ethiopian Red Cross donated $5,000,– to Mexico
- 1935 Ethiopia was invaded by fascist Italy and Mexico donated to Ethiopia
- The Ethiopian Red Cross felt the need to donate to Mexico

解釈人

Reciprocication

Example

- 1985, Mexico suffered from an earthquake, Ethiopa suffered from starvation
- The Ethiopian Red Cross donated $5,000,– to Mexico
- 1935 Ethiopia was invaded by fascist Italy and Mexico donated to Ethiopia
- The Ethiopian Red Cross felt the need to donate to Mexico

解釈人

Reciprocication

Example

- Hare Krishna sect was giving away free roses
- usually, answered mailing surveys where payed with 50$
- in a test, a 5$ cheque was attached to the survey – the response rate doubled
- free give-aways at supermarkets ...

解釈人

Reciprocication

Power

- reciprocication can override disliking
- bringing a gift will enhance the first impression you make
- the rule can trigger unequal exchange (Joe's Coca Cola)
- every culture enforces reciprocication by social pressure
- with one exception: if people are not able to repay (eg. children)

解釈人

Reciprocication

a subtle way

- there is a more subtle way:
- offer a concession, this concession os considered as gift $\rightsquigarrow$ reciprocication
- example: Can you borrow me 100 Euro? No? Maybe 10 Euro?
- You are required to have a 25 character long password and change it every two weeks!
  OK, but what about 10 characters and a change every 4 weeks?
- this also plays with the contrast

解釈人

Reciprocication

Countermeasures

- reject the present is a hard decision
- there will always be generous people (We are not Homo Oeconomicus!)
- accept a favor **but** if it turns out to be a trick device, treat it as a trick device $\rightsquigarrow$ don't feel the need to repay it

解釈人

Reciprocication

Questions

- What are the advantages of Reciprocication?
- What are the disadvantages?
- Who enforces us to obey the principle?
- I want to buy a 3-piece suit, a sweater and gloves. What do you offer me?

解釈人

Table of Contents

1 Fundamentals

2 Reciprocation

3 Commitment and Consistency

4 Social Proof

5 Obedience to Authority

6 Liking

解釈人

Commitment and Consistency

Commitment Theory

- the desire for consistency is viewed as a central motivator of behavior
- consistency is valued and adaptive (remember Luhmann's trust)
- inconsistency is commonly thought to be an undesirable personality trait
- inconsistency can be viewed as mental illness

解釈人

Commitment and Consistency

Example

- an assistant went to a beach, took a sunbath and listened to a portable radio
- after ca. 10 minutes he went away to buy sth. to drink
- another assistent Â»stoleÂ« the radio
- only 4 out of 20 people stopped the thief
- but when the 1st assistant asked his neighbour to have a look after the radio, 19 out of 20 persons stopped the thief
- some used violence to stop him

解釈人

Commitment and Consistency

Example

- an assistant went to a beach, took a sunbath and listened to a portable radio
- after ca. 10 minutes he went away to buy sth. to drink
- another assistent Â»stoleÂ« the radio
- only 4 out of 20 people stopped the thief
- but when the 1st assistant asked his neighbour to have a look after the radio, 19 out of 20 persons stopped the thief
- some used violence to stop him

解釈人

Commitment and Consistency

Furby



解釈人

Commitment and Consistency

What makes consistency work?

- How can one misuse the consistency principle? What is the trigger feature?
- a commitment made by someone triggers consistent behavior (it's a promise)
- the commitment has to be made voluntarily, without pressure or a reward
- an active opt-in is the best commitment
- a commitment can change the self image of a person
- so you have to Â»win the hearts and mindsÂ« of your workforce

解釈人

Commitment and Consistency

What makes consistency work?

- How can one misuse the consistency principle? What is the trigger feature?
- a commitment made by someone triggers consistent behavior (it's a promise)
- the commitment has to be made voluntarily, without pressure or a reward
- an active opt-in is the best commitment
- a commitment can change the self image of a person
- so you have to Â»win the hearts and mindsÂ« of your workforce

解釈人

Commitment and Consistency

Examples

- initiation rituals (fraternities, army, team building)
- people who have to pass such an initiation support the group better

解釈人

Commitment and Consistency

Countermeasures

- once again, we cannot simply drop commitment and consistency
- listen to your stomach signs! we still have our instincts ...
- listen to your heart! (the stomach is not that sensitive)
- ask yourself: who I do the same again?

解釈人

Commitment and Consistency

Summary

- good personal consistency is highly valued by society
- consistent conduct provides a beneficial approach to daily life
- a consistent orientation affords a valuable shortcut through the complexity of modern existence
- After making a commitment people are more willing to agree to requests that are in keeping with the prior commitment
- even erroneous commitments have a tendency to be self-perpetuating

解釈人

Commitment and Consistency

Summary

- Why do we want to look and be consistent in most situations?
- Why do we find even rigid, stubborn consistency desirable in many situations?
- Is a written commitment better than a oral one? If so, why?
- Why are wedding ceremonies held in public?

解釈人

Table of Contents

1 Fundamentals

2 Reciprocation

3 Commitment and Consistency

4 Social Proof

5 Obedience to Authority

6 Liking

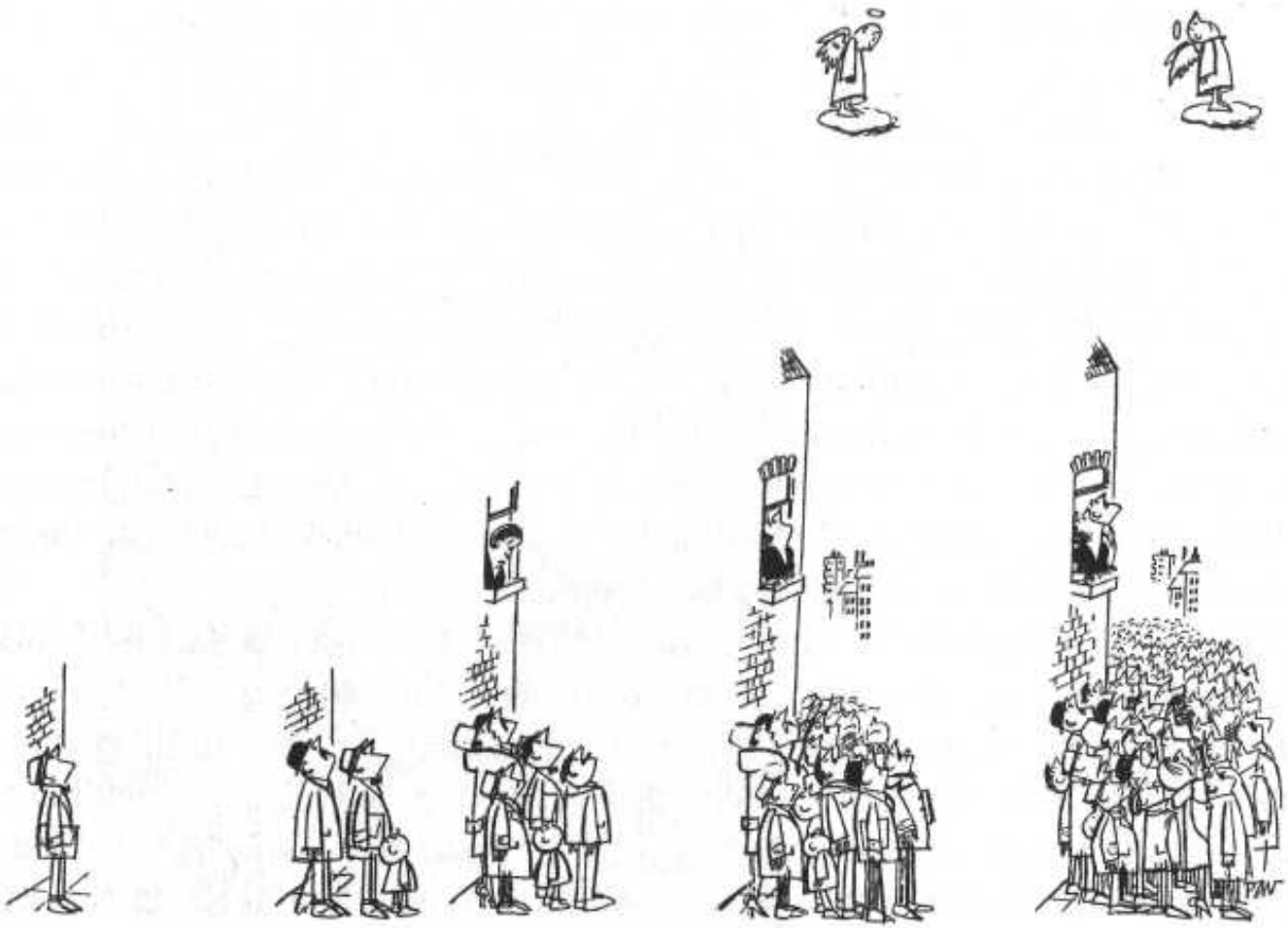
解釈人

Social Proof

Principle

- we determine what is correct by finding out what other people think is correct
- we see an action as appropriate when others are doing it
- when a lot of people are doing something, it is the right thing to do
- works well when people are uncertain (Luxembourg)
- works well with similar people (rebelling Teenagers)

解釈人



Looking for Higher (and Higher) Meaning
The draw of the crowd is devilishly strong.
© Punch/Rothco

解釈人

Social Proof

Examples

- canned laughter at TV shows
- someone staring at the church tower
- everybody is doing/buying/using X
- Crashing a Bank
- stampedes
- children dog training worked even with videos
- experiments with drunk/hurt people (passive bystander effect)

解釈人

Social Proof

Usage

- if everybody is ignoring your security guidelines, you have lost
- if the majority is obeying your security guidelines, you have won
- reach the critical mass

解釈人

Table of Contents

1 Fundamentals

2 Reciprocation

3 Commitment and Consistency

4 Social Proof

5 Obedience to Authority

6 Liking

解釈人

Obedience to Authority

- Stanley Milgram
- Stanford Prison
- we do believe in authorities, it helps us (Luhmann is older)
- Connotation
- Example: Hape Kerkeling (hape5), titles, uniforms, 08/15
- surprise helps

解釈人

Obedience to Authority

- When reacting to authority in an automatic fashion, there is a tendency to do so in response to the mere symbols of authority rather than to its substance.
  Research: Titles, Clothing, Automobiles
- Is this authority truly an expert?

解釈人

Table of Contents

1 Fundamentals

2 Reciprocation

3 Commitment and Consistency

4 Social Proof

5 Obedience to Authority

6 Liking

解釈人

Liking

Principle

- people are more influenced by people they like
- a hint from a friend ...
- this is used by marketing (AT&T)
- Susanne Klatten

解釈人

Liking

Why do we like people?

- Physical Attractiveness (Halos)
- Similarity (telephone money, mirror/photos, names)
- Compliments
- Conditioning and Association (Does *Pawlow* ring a bell? Wheatherman)
- working together an be succesfull together (attribution)

解釈人

Liking

Countermeasures

- listen to your feelings
- is someone interested in being liked by me?
- does someone stress our similarity?

解釈人

Liking

Questions

- What is a *Halo*?
- How can you reduce hostilities between two rival groups?
- How can you make me like you?

解釈人

Table of Contents

1 Fundamentals

2 Reciprocation

3 Commitment and Consistency

4 Social Proof

5 Obedience to Authority

6 Liking

解釈人

Scarcity

- Less is best and loss is worst
- Limited Numbers (special limited edition)
- Time Limits
- Censorship (Wolfenstein, Doom)
- Ebay
- Terrible Two

解釈人

Scarcity

- people assign more value to opportunities when they are less available
- things that are difficult to attain are typically more valuable
- as things become less accessible, we lose freedoms
- the act of limiting access to a message causes individuals to want to receive it more and to become more favorable to it
- don't rely on a single Source of information

解釈人

Scarcity

- people assign more value to opportunities when they are less available
- things that are difficult to attain are typically more valuable
- as things become less accessible, we lose freedoms
- the act of limiting access to a message causes individuals to want to receive it more and to become more favorable to it
- don't rely on a single Source of information

解釈人

Conclusions

- Social Engineering (mis)uses fundamentals of Human Behaviour
- cognitive processes are suppressed by our emotional reaction
- Security Awareness Campaigns can be used to raise Security Awareness
- but: Human Beeings are not Deterministic Automatons
- controlling humane behavior is complex

解釈人

Conclusions

- Social Engineering (mis)uses fundamentals of Human Behaviour
- cognitive processes are suppressed by our emotional reaction
- Security Awareness Campaigns can be used to raise Security Awareness
- but: Human Beeings are not Deterministic Automatons
- controlling humane behavior is complex

解釈人

Conclusions

- There is no 100% protection against Social Engineering
- There will never be 100% Security
- Design resilient Systems with Social Engineering in Mind
- Use a Defense in Depth Strategy (Clausewitz: Vom Kriege)
- Overlapping Security Mechanisms

解釈人

Conclusions

- Social Engineering (mis)uses fundamentals of Human Behaviour
- Security Awareness Campaigns can be used to raise Security Awareness
- but: Human Beeings are not Deterministic Automatons

解釈人

Conclusions

- Social Engineering (mis)uses fundamentals of Human Behaviour
- Security Awareness Campaigns can be used to raise Security Awareness
- but: Human Beeings are not Deterministic Automatons

解釈人

Conclusions

- There is no 100% protection against Social Engineering
- There will never be 100% Security
- Security reacts with Trust, Responsability in *Social* Relations
- Security has no Technological Dimension
- Design resilient Systems with Social Engineering in Mind
- Use a Defense in Depth Strategy (Clausewitz: Vom Kriege)
- Overlapping Security Mechanisms

解釈人

Conclusions

- There is no 100% protection against Social Engineering
- There will never be 100% Security
- Security reacts with Trust, Responsability in *Social* Relations
- Security has no Technological Dimension
- Design resilient Systems with Social Engineering in Mind
- Use a Defense in Depth Strategy (Clausewitz: Vom Kriege)
- Overlapping Security Mechanisms

解釈人

Conclusions

-
-
-

解釈人



CIALDINI, Robert B.:
Influence – Science and Practice.
Boston : Allyn and Bacon, 2001. –
ISBN 0-321-01147-3

解釈人

Questions?
Stefan.Schumacher@Kaishakunin.com

解釈人