Deception Defence 101

Dr. Pedram Hayati

BsidesLjubljana 2017, Ljubljana, Slovenia

March 2017

Who am I?

Pedram Hayati

Partner at elttam, Founder of SecTalks (www.sectalks.org)

PhD (Comp Sci), B. Eng (IT)

$2

¢200

$4

$400

Having cents better than dollars!

1. The square of $1 is equal to $1

   $(\$1)^2 = \$1$

2. $1 equals to 100 cents

   $\$1 = 100 \text{ cents}$

3. The square of 100 cents is equal to 10,000 cents or $100

   $(100 \text{ cents})^2 = 10000 \text{ cents}$

4. So having cents is 100x better than dollars.

Let's find the catch

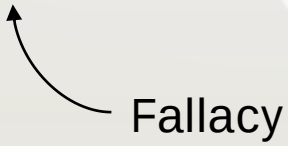
1. Examine usage of 'square' in the geometry.
2. The square of 1 m is 1 m^2

   $(1\ m)^2 = 1x1 = 1\ m^2$
3. 1 m is 100 cm
4. The square of 100 cm is equal to 10000 cm^2 or 1 m^2

   $10000\ cm^2 = 1\ m^2$
5. There is no such thing as dollar square or cents square.

   $(100\ cents)^2 \neq 10000\ cents$

   $(100\ cents)^2 = 10000\ cents^2$



Reasons

Misleading or hidden information in the example

- $\$^2$ or $cents^2$

Error in human's cognitive system

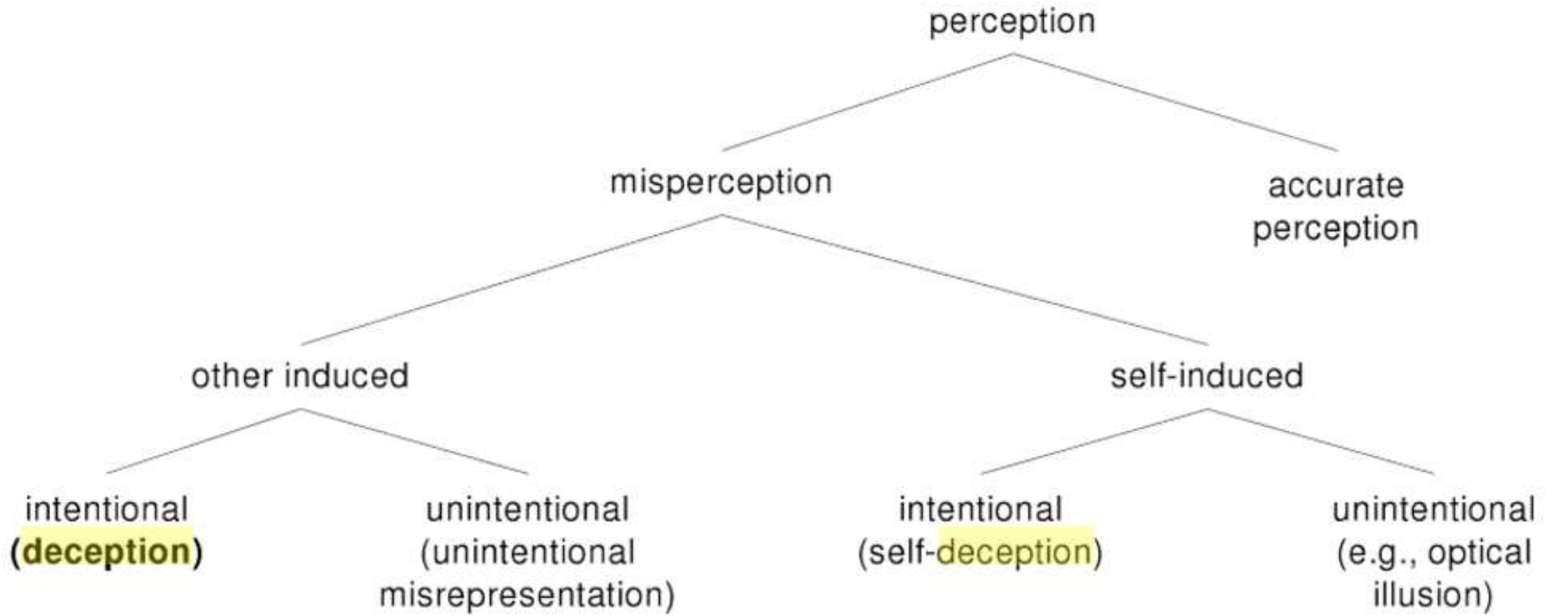
- Generalisation
- Simplification
- Assumption

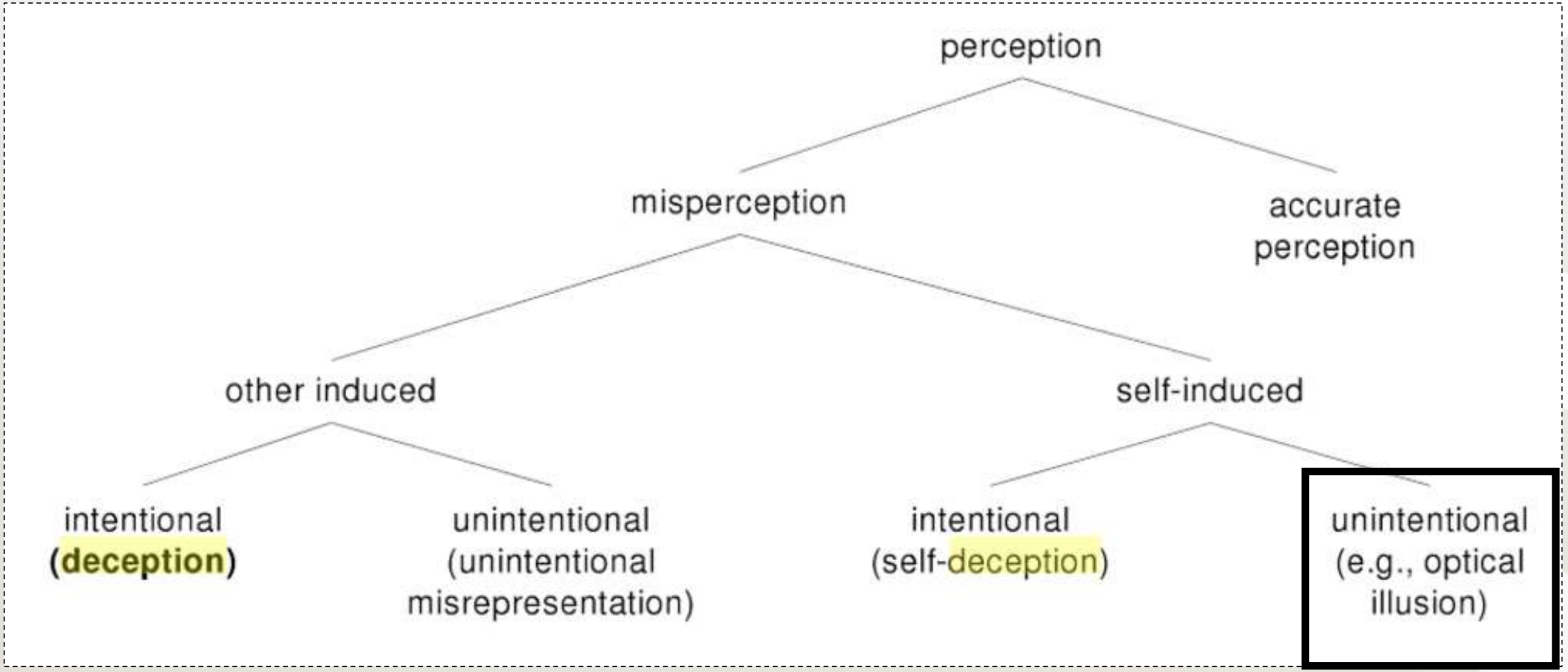
What is Deception?

"The act of hiding the truth, especially to get an advantage. In other words, deception is about exploiting errors in cognitive systems for advantage."

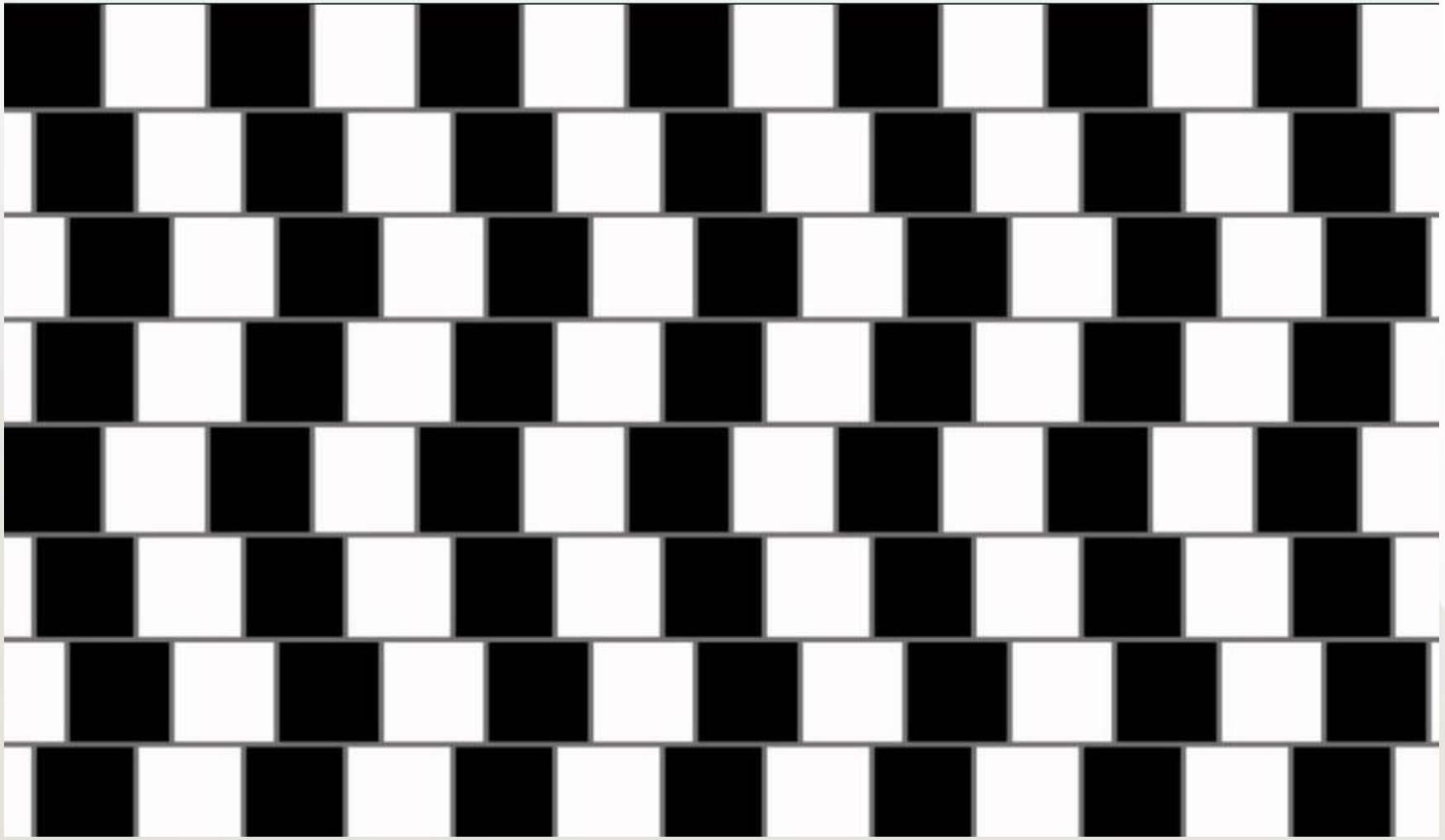
Cambridge English Dictionary

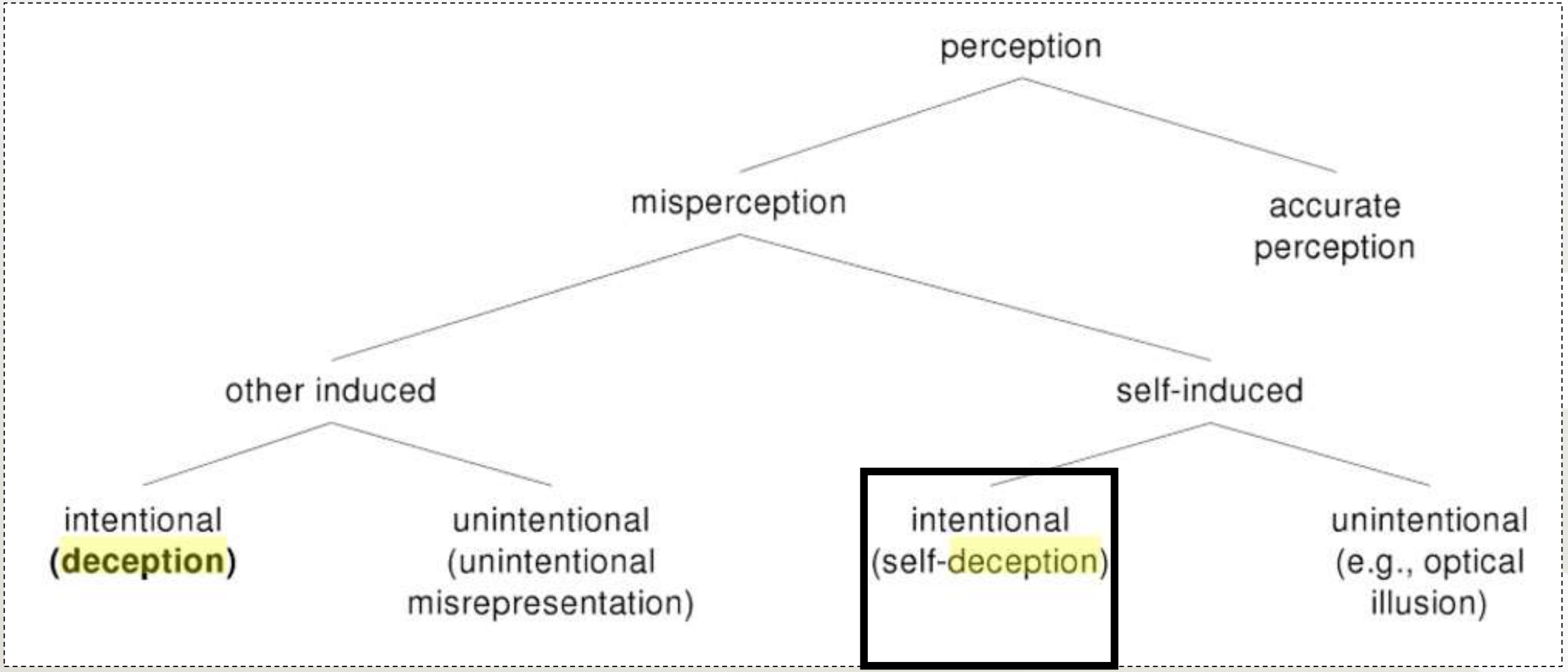
Deception creates misperception



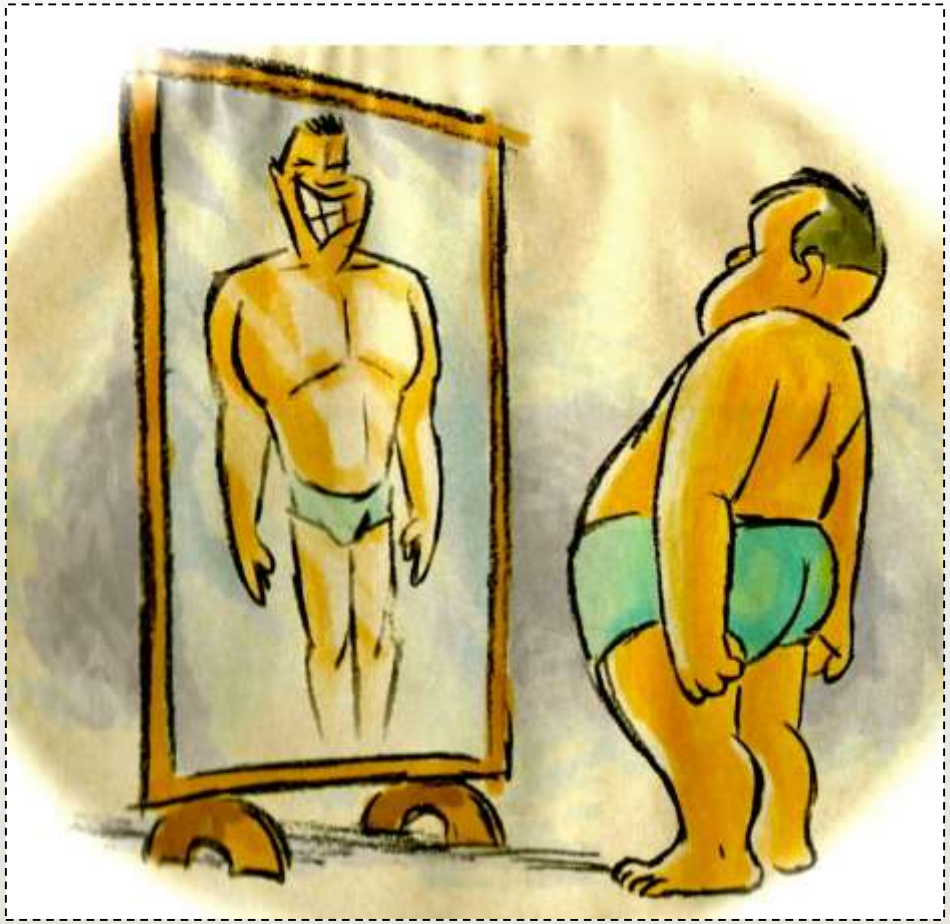

perception
misperception
accurate perception
other induced
self-induced
intentional (deception)
unintentional (unintentional misrepresentation)
intentional (self-deception)
unintentional (e.g., optical illusion)

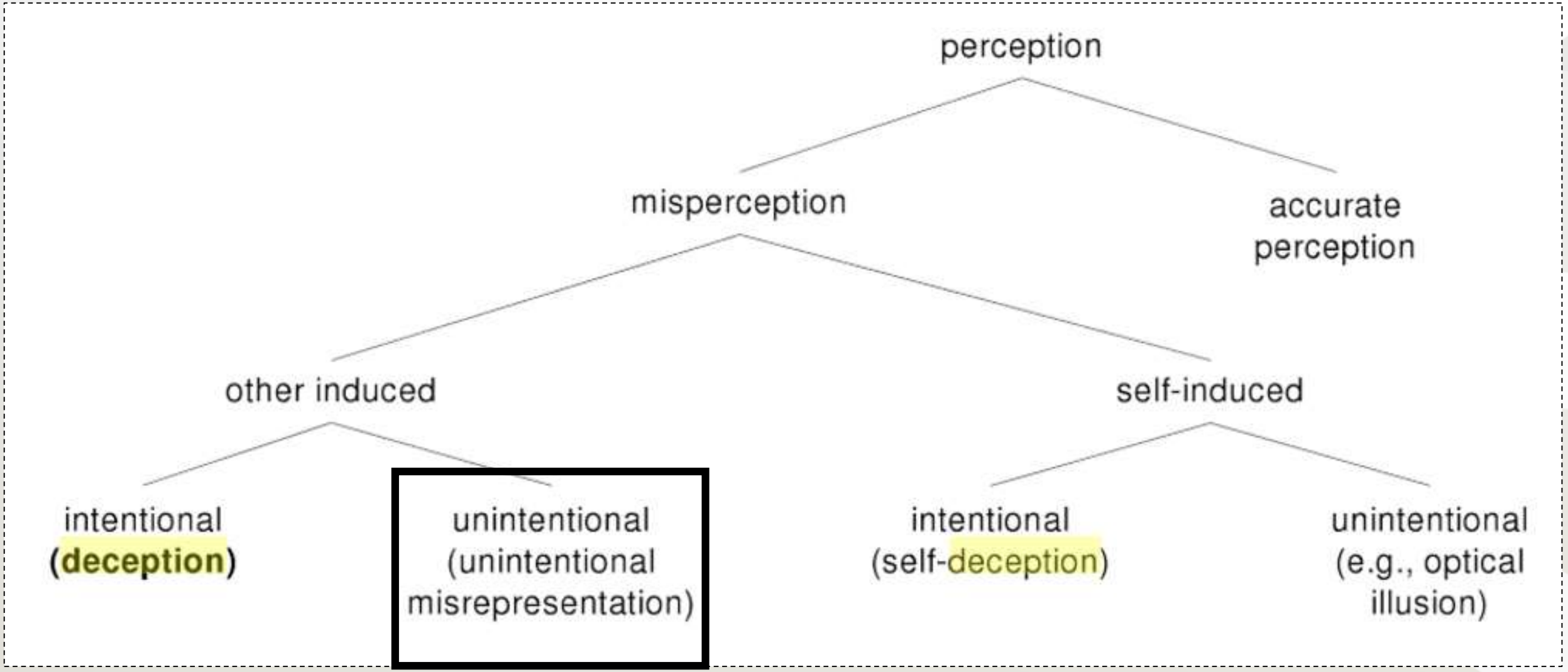
Self-induced and unintentional



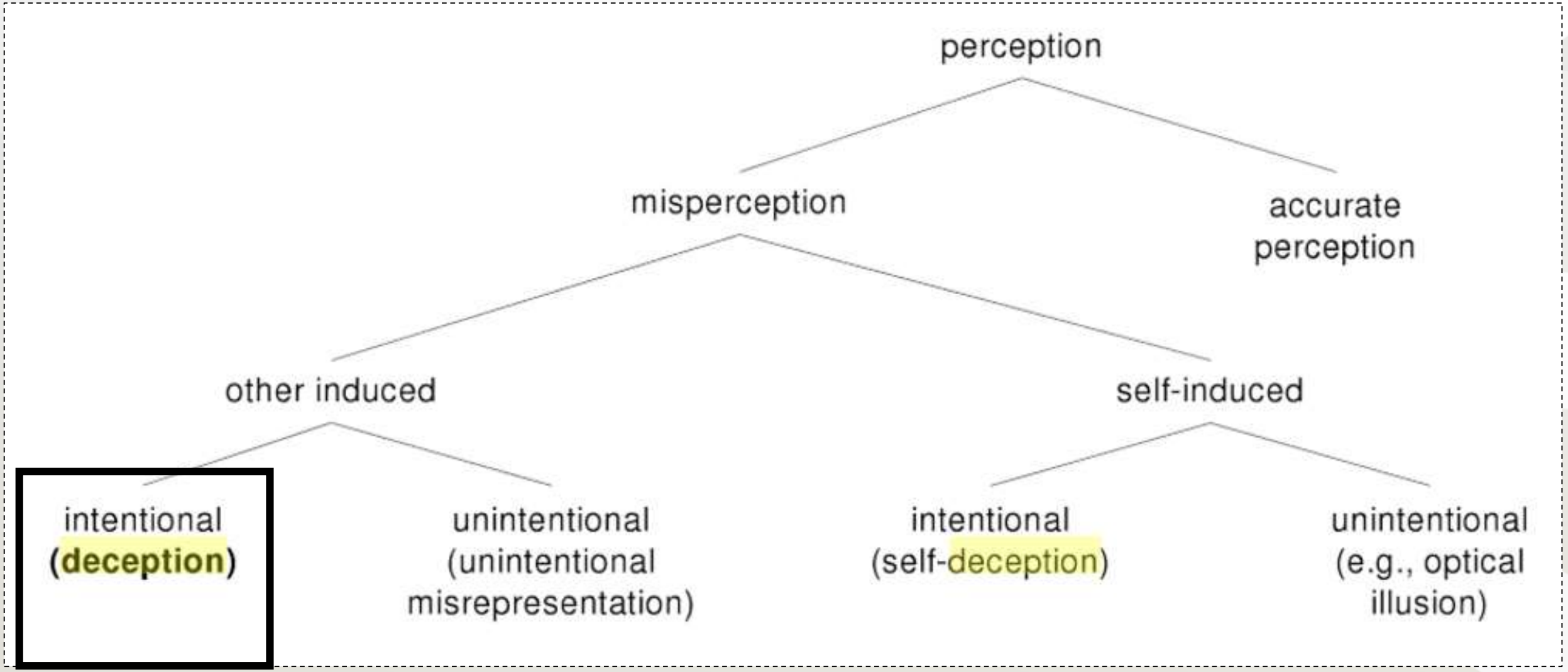

perception
misperception
accurate perception
other induced
self-induced
intentional (deception)
unintentional (unintentional misrepresentation)
intentional (self-deception)
unintentional (e.g., optical illusion)

Self-induced and intentional

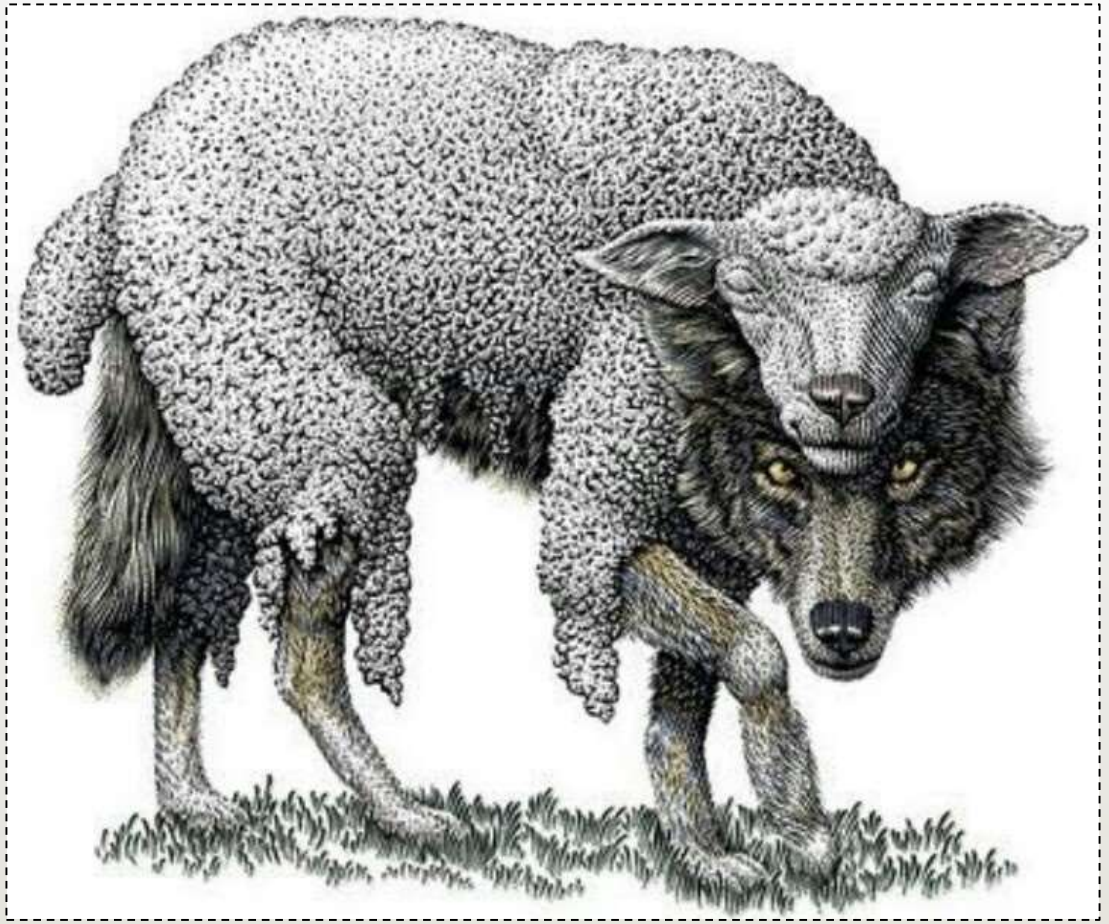



perception
misperception
accurate perception
other induced
self-induced
intentional (deception)
unintentional (unintentional misrepresentation)
intentional (self-deception)
unintentional (e.g., optical illusion)

Other induced and unintentional


perception
misperception
accurate perception
other induced
self-induced
intentional (deception)
unintentional (unintentional misrepresentation)
intentional (self-deception)
unintentional (e.g., optical illusion)

Other induced and intentional



Deception Security

- The act of intentionally misleading attackers in order to protect a computer asset.
- Misleading leads an attacker to take or avoid taking an action.
- Deception Security is also referred as
  - Deceptive Security
  - Deception-base Security
  - Deception Defence
  - Cyberdeception

Objectives

The goal is not to directly stop or detect an attack(er), but to:

1. Increase the attacker's workload,
2. Increate the attacker's uncertainty,
3. Exhaust the attacker's resource (e.g. time, budget, etc.), and
4. Respond early.

Deception Security: fake paths

Example: Fake path

```
C:\Process Injector>pinjector -l
Privilege Switcher for Win32(Private version)
(c) 2006 Andres Tarasco - atarasco@gmail.com

PID    544 smss.exe (  3 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID    852 csrss.exe ( 13 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID    876 winlogon.exe ( 21 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID    928 services.exe ( 16 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID    940 lsass.exe ( 20 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID   1152 vmacthlp.exe (  1 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID   1168 svchost.exe ( 17 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID   1464 svchost.exe ( 67 Threads)  USER: \\AUTORIDADE NT\SYSTEM
   000220: \\AUTORIDADE NT\SYSTEM
   000240: \\AUTORIDADE NT\SYSTEM
PID   1680 vpnagent.exe (  3 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID   1912 explorer.exe ( 15 Threads)  USER: \\814B4254A6DE4CD\bruno
PID    172 spoolsv.exe ( 12 Threads)  USER: \\AUTORIDADE NT\SYSTEM
   000312: \\AUTORIDADE NT\SYSTEM
PID    572 rundll32.exe (  4 Threads)  USER: \\814B4254A6DE4CD\bruno
PID    580 VMwareTray.exe (  1 Threads)  USER: \\814B4254A6DE4CD\bruno
PID    588 vmtoolsd.exe (  6 Threads)  USER: \\814B4254A6DE4CD\bruno
PID    596 XBoxStat.exe (  3 Threads)  USER: \\814B4254A6DE4CD\bruno
PID    600 ctfmon.exe (  1 Threads)  USER: \\814B4254A6DE4CD\bruno
PID    900 WVSScheduler.exe (  7 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID   1104 cvpnd.exe (  3 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID    484 vmtoolsd.exe (  6 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID   1444 TPAutoConnSvc.exe (  5 Threads)  USER: \\AUTORIDADE NT\SYSTEM
PID   1488 wscntfy.exe (  1 Threads)  USER: \\814B4254A6DE4CD\bruno
PID   2776 TPAutoConnect.exe (  1 Threads)  USER: \\814B4254A6DE4CD\bruno
PID   3236 wuauclt.exe (  3 Threads)  USER: \\814B4254A6DE4CD\bruno
PID   2312 xampp-control.exe (  1 Threads)  USER: \\814B4254A6DE4CD\bruno
PID    832 mysqld.exe ( 12 Threads)  USER: \\814B4254A6DE4CD\bruno
```

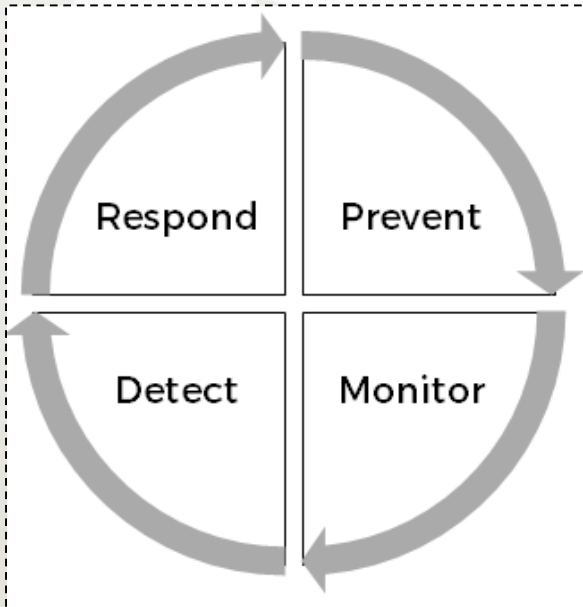
Why do we need Deception Security?

Why Deception Security

1. Introduces different set of strategies and security controls
2. The only or most effective way to defend in specific attack scenarios

   e.g. An attacker that has a remote access to an internal host
3. Targets an attacker at the most vulnerable stage of the attack.
4. An additional layer of protection

   Detection, prevention and respond

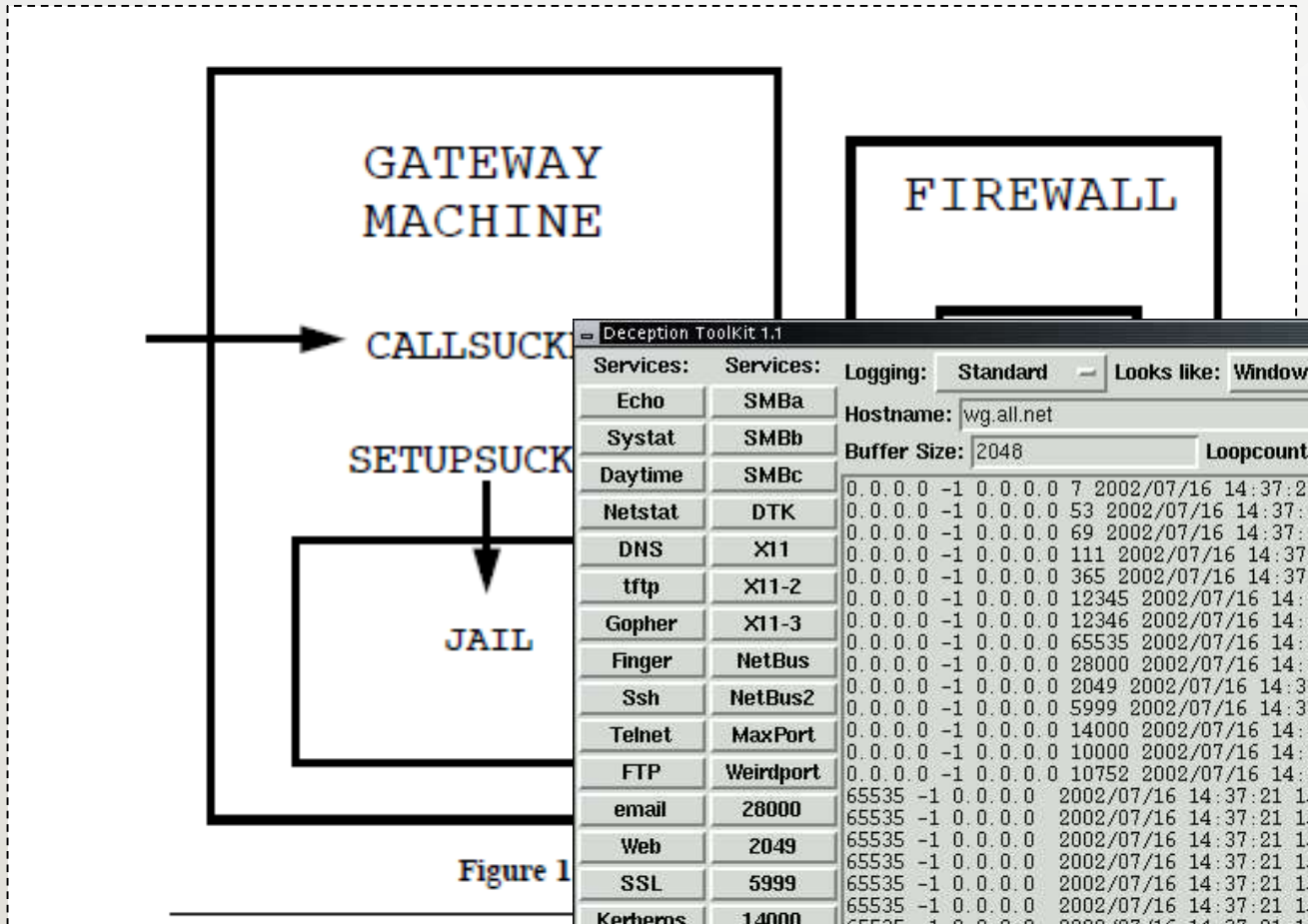


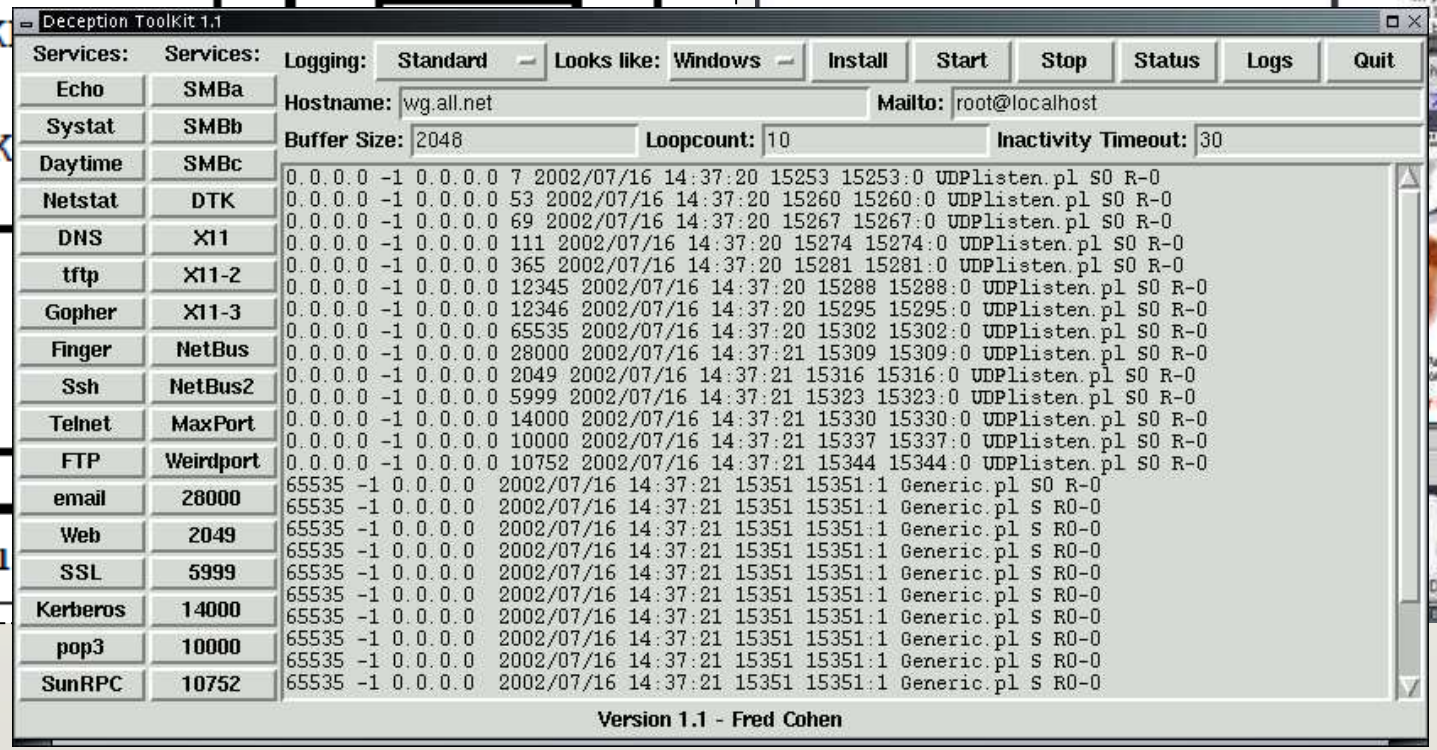
elttam

Is Deception Security a new concept?

The short answer: No.

Jail deception tool





elttam

Honey*

- HoneyPot
- HoneyToken
- HoneyWords
- HoneyEncryption
- HoneyFlow
- HoneyDocuments
- HoneyFS
- Social Honey
- …

We have used Deception Security before

Knowingly or unknowingly we have used it

SMTP service

- Simple Mail Transport Protocol
- Used a Deception Technique to
  - Slow down spam
  - Prevent user enumeration
  - Increase workload on spammers

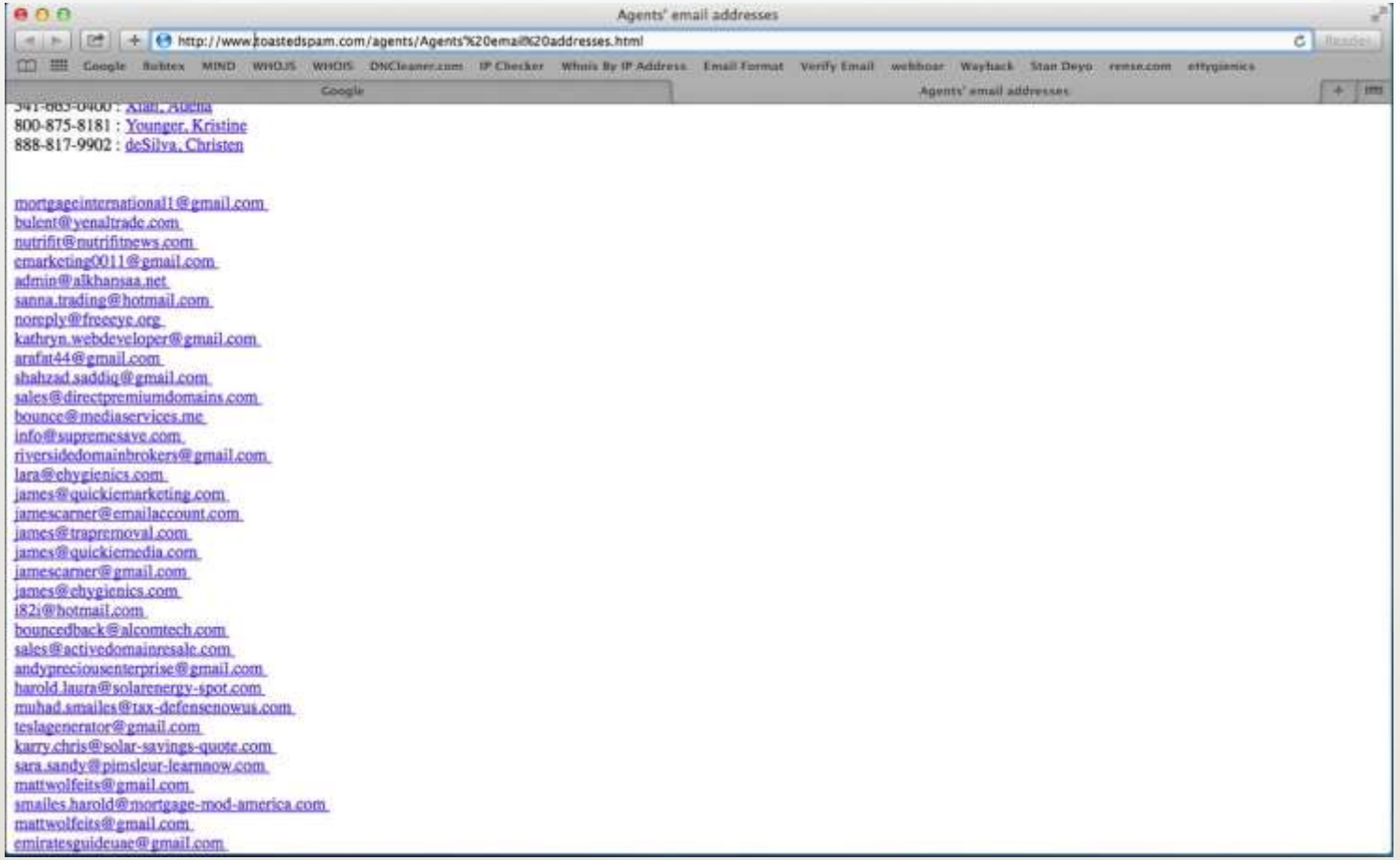
Live Demo: Let's SMTP


```
nc cust25070-2.in.mailcontrol.com 25
```

```
220 cluster-j.mailcontrol.com ESMTP MailControl
HELO example.com
250 cluster-j.mailcontrol.com Hello x.x.x.x [x.x.x.x] (may be forged), pleased to meet you
MAIL FROM: <info@example.com>
250 2.1.0 <info@example.com>... Sender ok
RCPT TO: <NO-SUCH-USER@thecotswoldgroup.co.uk>
250 2.1.5 <NO-SUCH-USER@thecotswoldgroup.co.uk>... Recipient ok
DATA
354 Enter mail, end with "." on a line by itself
FROM: "<info@example.com>"
TO: "<NO-SUCH-USER@thecotswoldgroup.co.uk>"
Subject: test

this is a test email.
.
250 2.0.0 v1NFXukt005661 Message accepted for delivery
```

Example: Fake email lists



Has Deception Security been effective?

Effects of deception technologies

"Applying Deception Mechanisms for Detecting Sophisticated Cyber Attacks" by Omer Zohar et al. October 2016

- A corporate environment filled with
  - fake assets (decoys),
  - fake pointers (mini-traps), and
  - Honeytokens (documents, emails, user accounts, etc.)
- Invited 50 security testers to play a CTF game

Effects of deception technologies

1. All attackers were detected using one or more deception controls.
2. Deception increased attacker's knowledge gap.

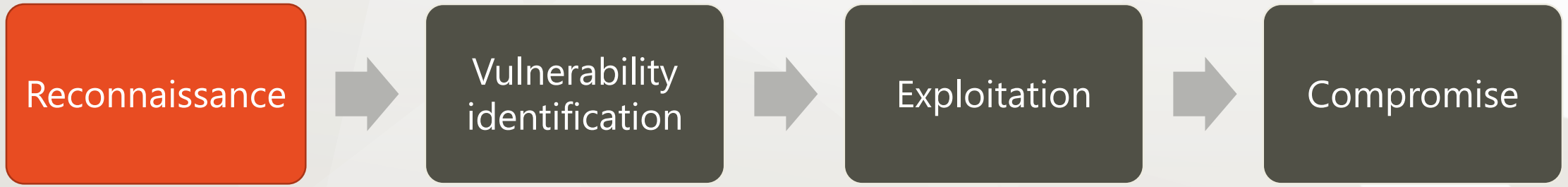
   The more knowledge attacker has the more sophisticated the attack is.
3. Different attackers were drawn into different traps.
4. The more time the attacker spent within the network, the harder to detect them

Very limited usage of Deception Security

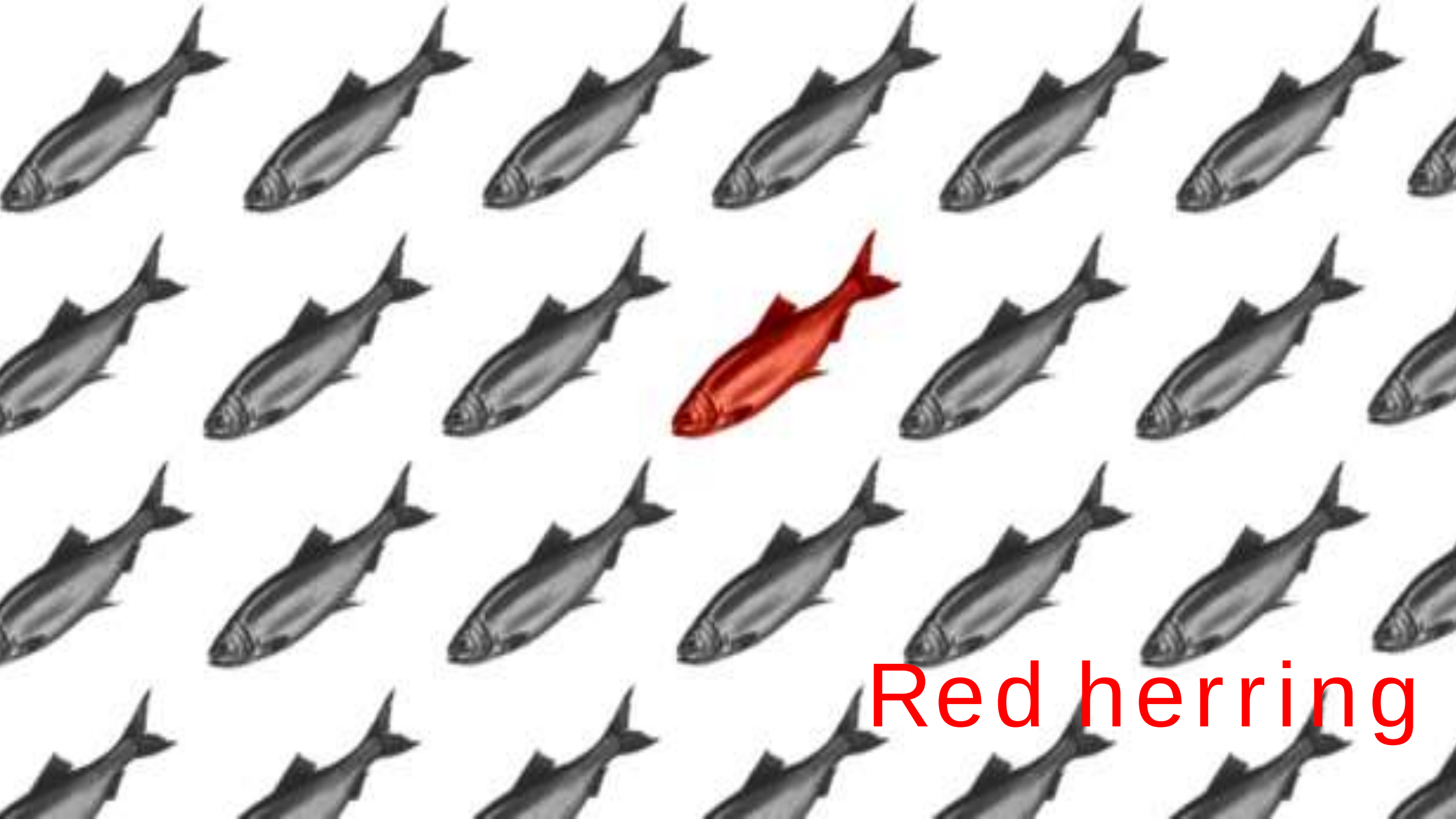
1. Intelligence gathering
2. Observing an attacker's tactics
3. Research
4. Hobby

Deception Security Principles

Attack path



elttam


Red herring

Red herring

No deception situation

- Large number of ‘trial and error’.
- Any change in the response (e.g. size, errors, etc.) will give the attacker an additional clue to gauge her activities to find a right attack path.
- So, with no deception, systems return genuine responses to the attacker's inject.

Red herring

Carefully select and alter the response messages. Introduce fake response, side-channel delay (e.g. time delays) or respond with empty content.

Red herring examples:

1. Generate fake verbose error message
2. No response or no change in response
3. Alter side channel data

Live demo

No additional software or tool.

Minimum amount of configuration change

Use common system tools

Live Demo: red herring w/ nginx

1. Setup an Azure host
2. Reconfigure nginx
3. Setup “upstream”
4. Observe fake responses in the browser

```
#dev.deception.test.conf - nginx

upstream error_deception {
        server localhost:1500;
        server localhost:1501;
        server localhost:1502;
}
..SNIP..

server_name dev.deception.test;

location / {
     proxy_pass http://error_deception;
     proxy_intercept_errors on;
}
```

```
#HTTP 200
while true ; do  echo -e "HTTP/1.1 200 OK\n\n<h1>HTTP 200 Ok</h1>" | nc -l -p 1500  ; done


#HTTP 401
while true ; do  echo -e "HTTP/1.1 401 Access Denied\nWWW-Authenticate: Basic realm="Login"\nContent-Length: 0\n\n" | nc -l -p 1501  ; done


#HTTP 403
while true ; do  echo -e "HTTP/1.1 403 Forbidden\n\n <h1>HTTP 403 Forbidden</h1>" | nc -l -p 1502  ; done
```

http://dev.deception.test


Flood the environment
with fakes

Flood the environment with fakes

No deception situation

Asset is often a rare item that an attacker is after. For example, there is only one table in the database that holds users credentials. Once identified, an attacker knows that this is the only table that store users password, so it worth the time to crack the hashes.

The principle

Generate large number of fakes and distribute them in different parts of the environment.

Examples

1. Fake user tables or rows in a database
2. Fake email addresses
3. Fake open ports

Live demo

No additional software or tool.

Minimum amount of configuration change

Use common system tools

Live Demo: Fake open ports

1. Setup an Azure host
2. Open up first 1024 ports and listen
3. Run portscan and observe the time of completion

```
Nmap scan report for 123.123.123.123
Host is up (0.41s latency).
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 30.97 seconds
```

```
Nmap scan report for 123.123.123.123
Host is up (0.28s latency).
PORT     STATE SERVICE VERSION
80/tcp open  http    Edgecast CDN httpd

Nmap done: 1 IP address (1 host up) scanned in 8.12 seconds
```

```
# redirect 1-1024 ports to port 9999
iptables -t nat -A PREROUTING -i eth0 -p tcp --
dport 1:1024 -j REDIRECT --to-port 9999

# listen on port 9999 and respond with null
echo -e '\0' | nc -l -k -p 9999 &
```

```
Nmap scan report for 123.123.123.123
Host is up (0.27s latency).
Not shown: 846 filtered ports
PORT     STATE SERVICE
1/tcp    open  tcpmux
3/tcp    open  compressnet
4/tcp    open  unknown
6/tcp    open  unknown
7/tcp    open  echo
9/tcp    open  discard
13/tcp   open  daytime

..SNIP..

Nmap done: 1 IP address (1 host up) scanned in 78.94 seconds
```

```
Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-02 14:09 AEDT
Nmap scan report for 123.123.123.123
Host is up (0.26s latency).
PORT   STATE SERVICE VERSION
23/tcp open  telnet?

Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 233.34 seconds
```

2x

Portscan duration

30x

Fingerprinting duration

7 hours

Reconnaissance

Live demo: Outcome

1. Trivial changes to the environment with big impact on the attacker's workload.
2. Little time investment from the defender side (no new tool, no log monitoring, no new hire! etc.)
3. There are many other ways to improve these deception techniques.

And there are more

Deception Defence Principles

Wrap up

1. The concept of Deception Security has been around since early 1990 with a low rate of adaption.
2. Deception Defence aims to increase the attacker's workload, uncertainty, and targets the attacker at the most vulnerable stage.
3. Deception Defence can add additional layer of protection to the defender's life-cycle
4. Two principles:
    1. Flood the environment with fakes, and
    2. Red herring.

Thank you!

pedram@elttam.com.au
Twitter: pi3ch

We are hiring

Sydney, Melbourne, Remote

Security Researchers

Security Consultants

www.elttam.com.au/roles

Come and have chat with me

References

- Fred Cohen. The Use of Deception Techniques: Honeypots and Decoys.
- Whaley, B. “Toward a General Theory of Deception”, The Journal of Strategic Studies, Frank Cass, London, 5(1):178-192, March 1982.
- Omer Zohar et. al. Applying Deception Mechanisms for Detecting Sophisticated Cyber Attacks. October 2016.
- Bill Cheswick. An Evening with Berferd In Which a Cracker is Lured, Endured, and Studied. 1991.
- Greg Hoglund et. al. Rootkits: Subverting the Windows Kernel

References

- Honeyfiles, Deceptive Files for Intrusion Detection
- Honey Encryption Security Beyond the Brute-Force Bound
- Honeywords: Making password-cracking detectable
- Honeytokens: The Other Honeypot
- Kamouflage: loss-resistant password management

elttam

https://www.elttam.com.au

Phone: +61 (02) 8004 5952
Fax: +61 (02) 8005 3867
E-mail: hello@elttam.com.au

Suite 3, Level 27
1 Farrer Place
Sydney NSW 2000
Australia