Project 2: 37 days left

Deception-Based Cyber Security: Art of Cyber Deception

CS 459/559: Science of Cyber Security
18th Lecture

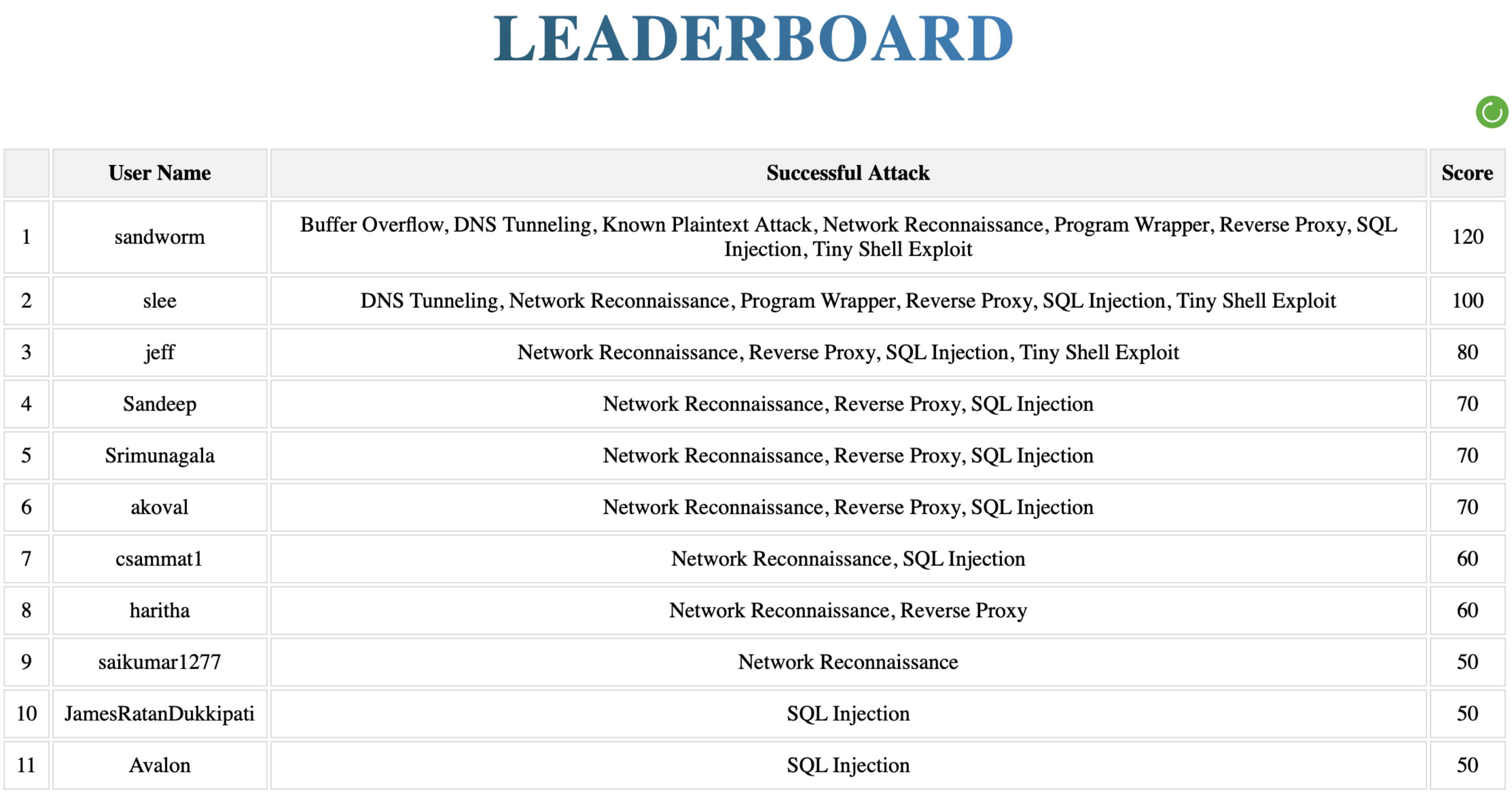
Instructor:

Guanhua Yan

Agenda

- ~~Quiz 1: September 29 (closed book)~~
- ~~Project 1 (offense): October 10~~
- Quiz 2: November 12
- Presentations: 11/17, 11/19, 11/24, 12/1, 12/3
- CTF competition: November 26
- Project 2 (defense): December 5
- Final report: December 15

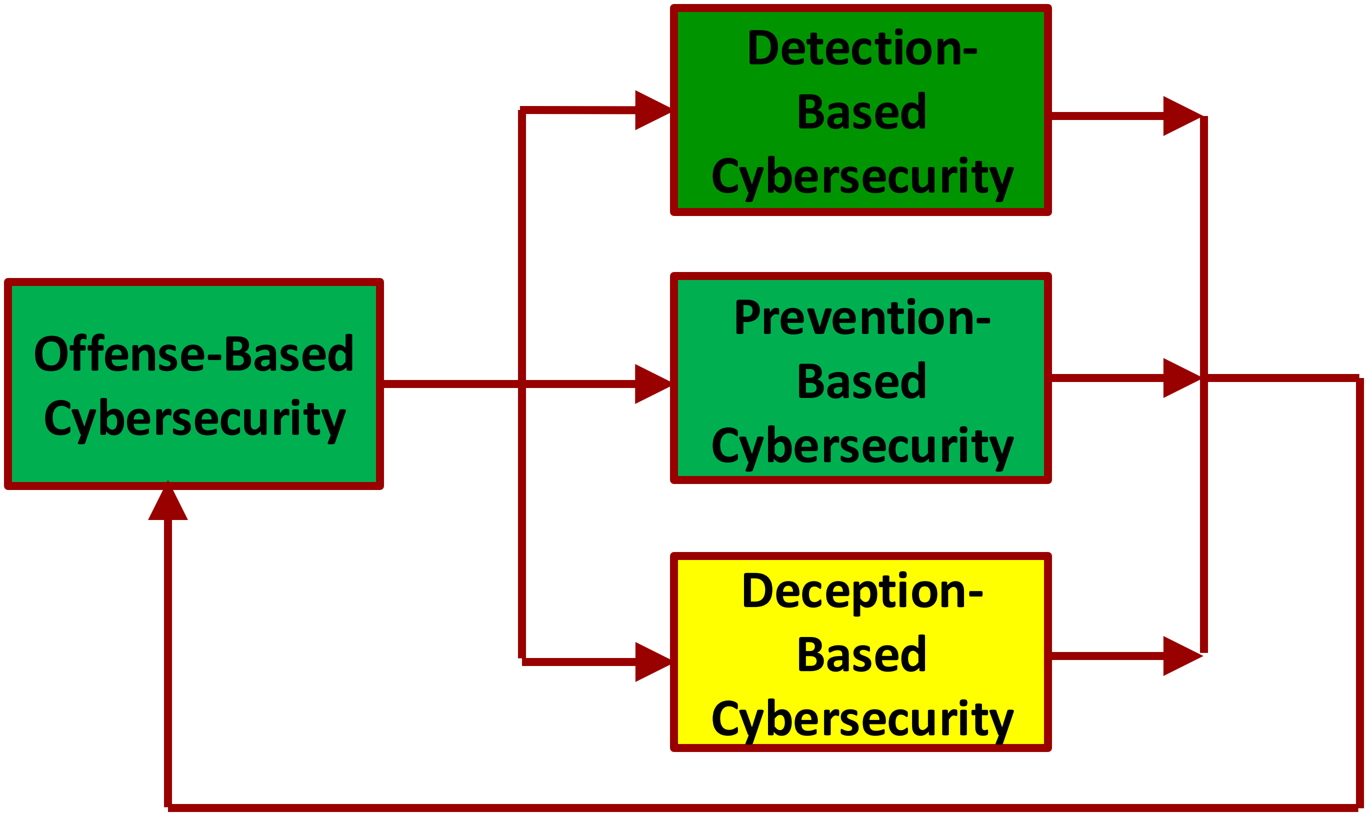
CTF leaderboard



LEADERBOARD

	User Name	Successful Attack	Score
1	sandworm	Buffer Overflow, DNS Tunneling, Known Plaintext Attack, Network Reconnaissance, Program Wrapper, Reverse Proxy, SQL Injection, Tiny Shell Exploit	120
2	slee	DNS Tunneling, Network Reconnaissance, Program Wrapper, Reverse Proxy, SQL Injection, Tiny Shell Exploit	100
3	jeff	Network Reconnaissance, Reverse Proxy, SQL Injection, Tiny Shell Exploit	80
4	Sandeep	Network Reconnaissance, Reverse Proxy, SQL Injection	70
5	Srimunagala	Network Reconnaissance, Reverse Proxy, SQL Injection	70
6	akoval	Network Reconnaissance, Reverse Proxy, SQL Injection	70
7	csammat1	Network Reconnaissance, SQL Injection	60
8	haritha	Network Reconnaissance, Reverse Proxy	60
9	saikumar1277	Network Reconnaissance	50
10	JamesRatanDukkipati	SQL Injection	50
11	Avalon	SQL Injection	50

Course structure



Offense-Based Cybersecurity

Detection-Based Cybersecurity

Prevention-Based Cybersecurity

Deception-Based Cybersecurity

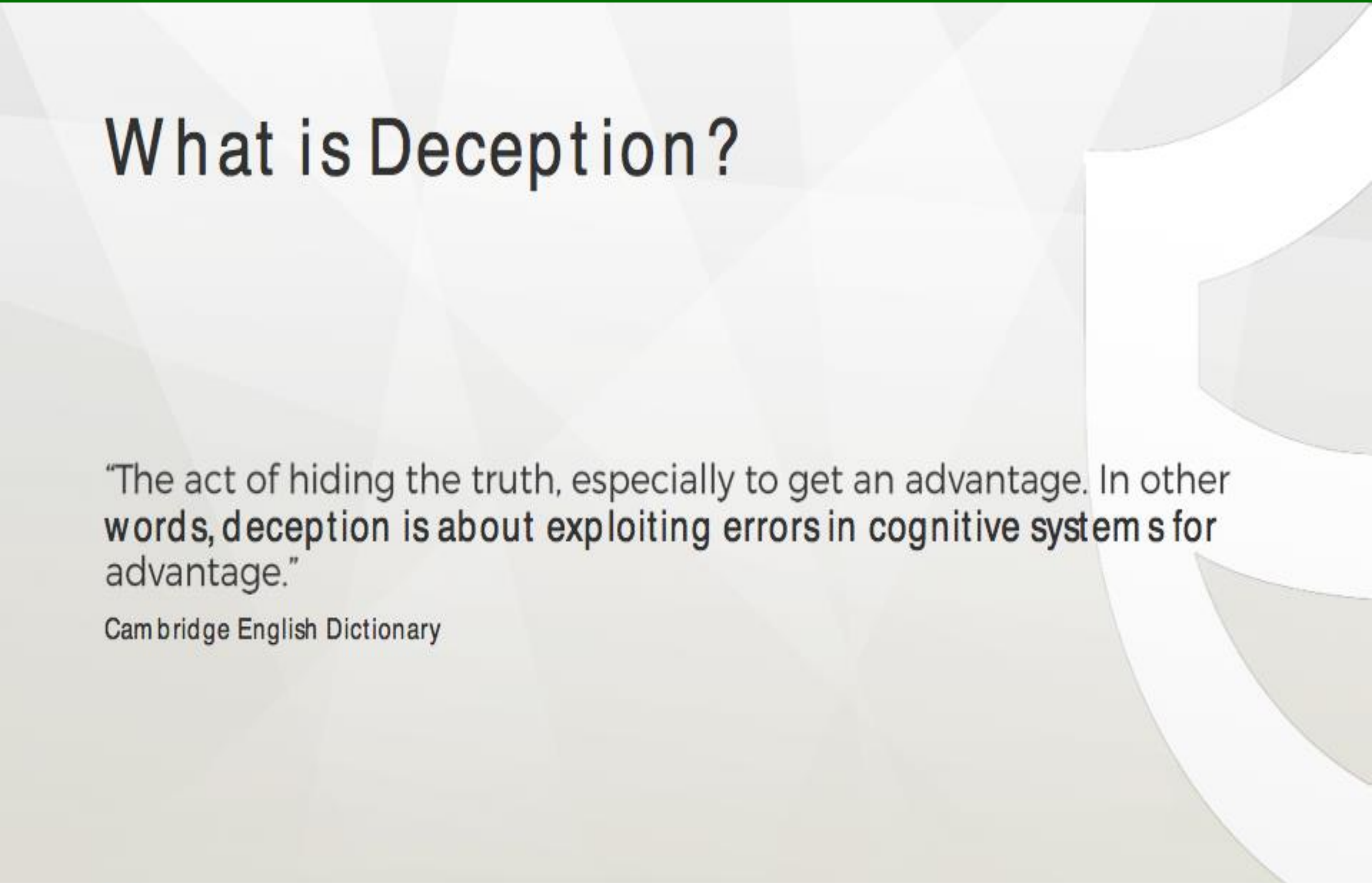
Outline

- Deception

- Cyber deception

- Deception consistency

Introduction to deception

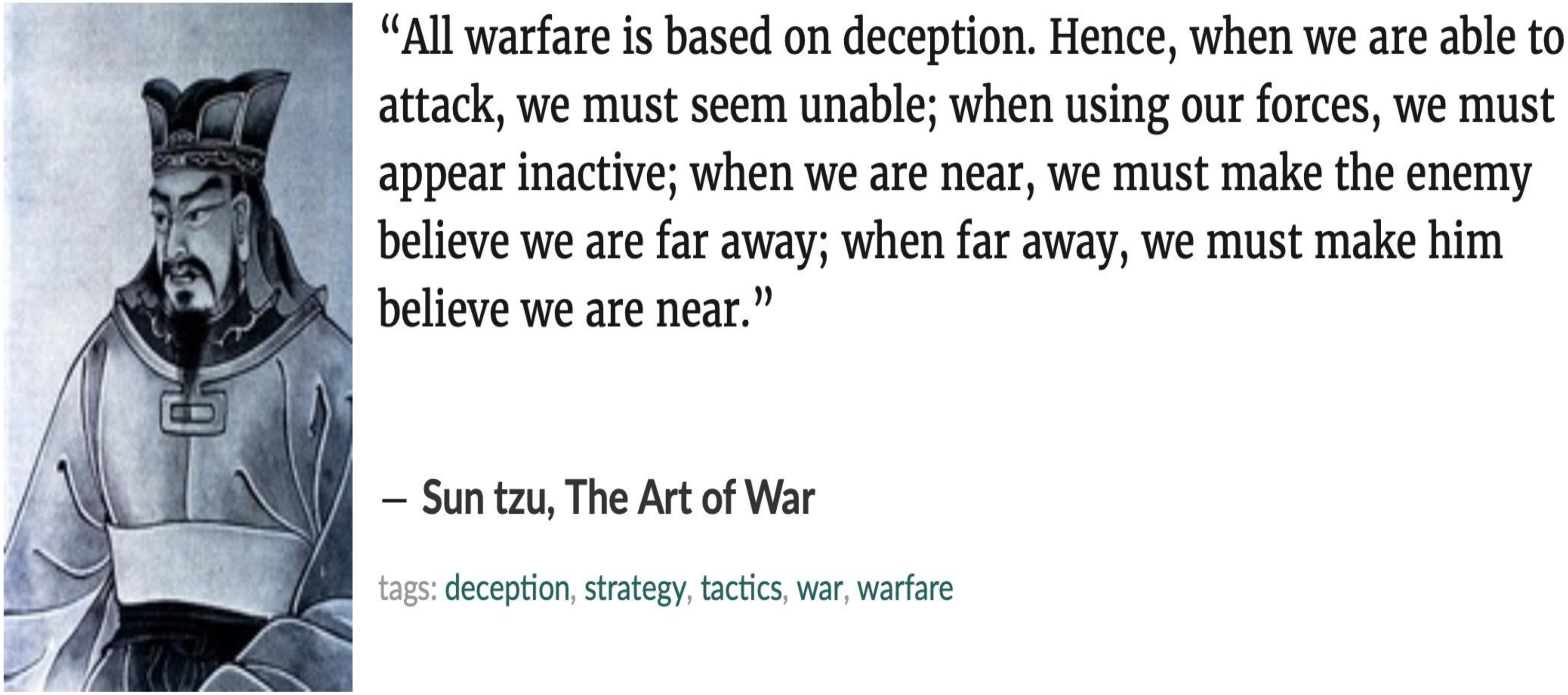


What is Deception?

"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

Quote

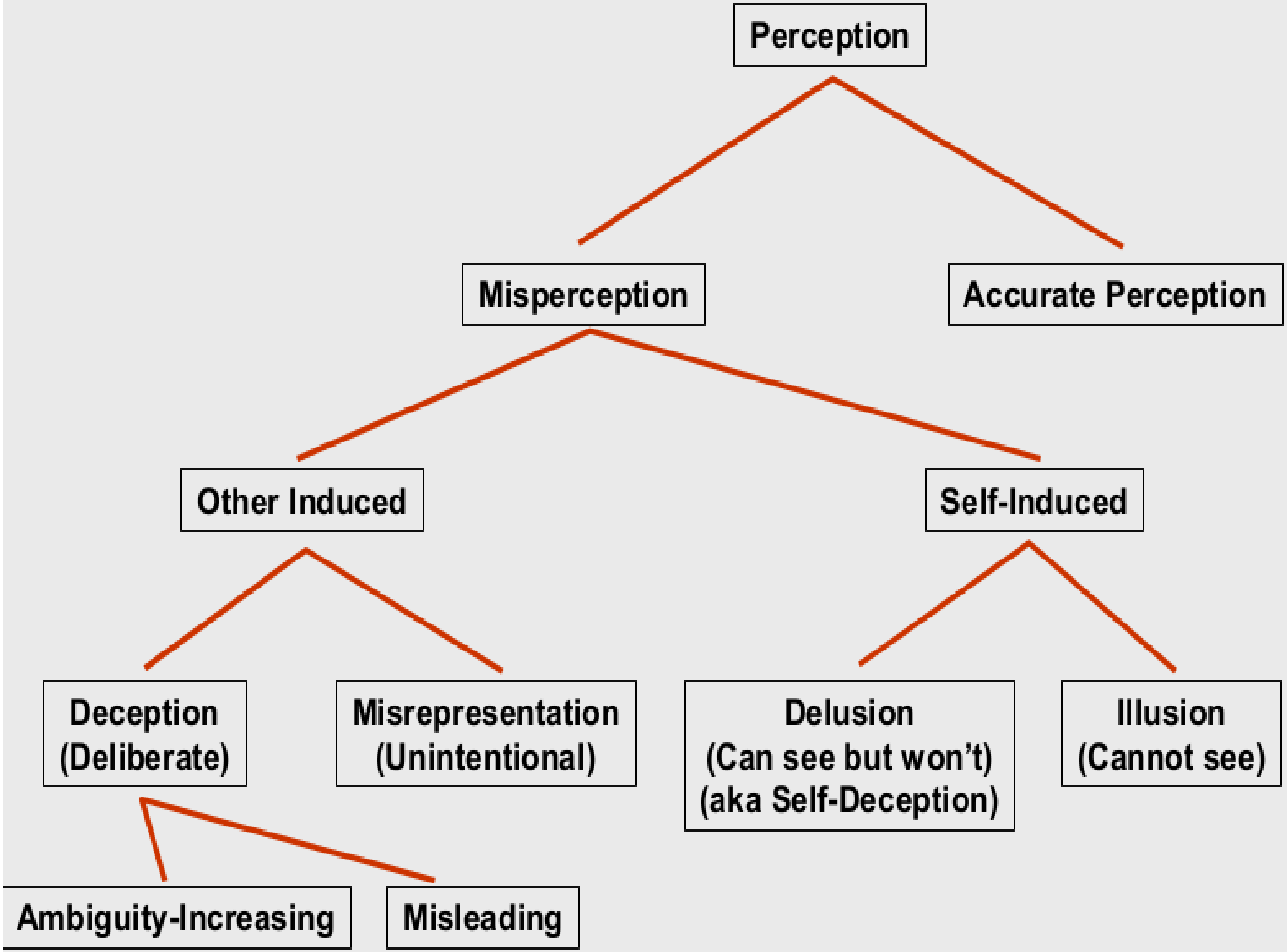


“All warfare is based on deception. Hence, when we are able to attack, we must seem unable; when using our forces, we must appear inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near.”

― **Sun tzu, The Art of War**

tags: deception, strategy, tactics, war, warfare

A TYPOLOGY OF PERCEPTION



Perception

Misperception

Accurate Perception

Other Induced

Self-Induced

Deception
(Deliberate)

Misrepresentation
(Unintentional)

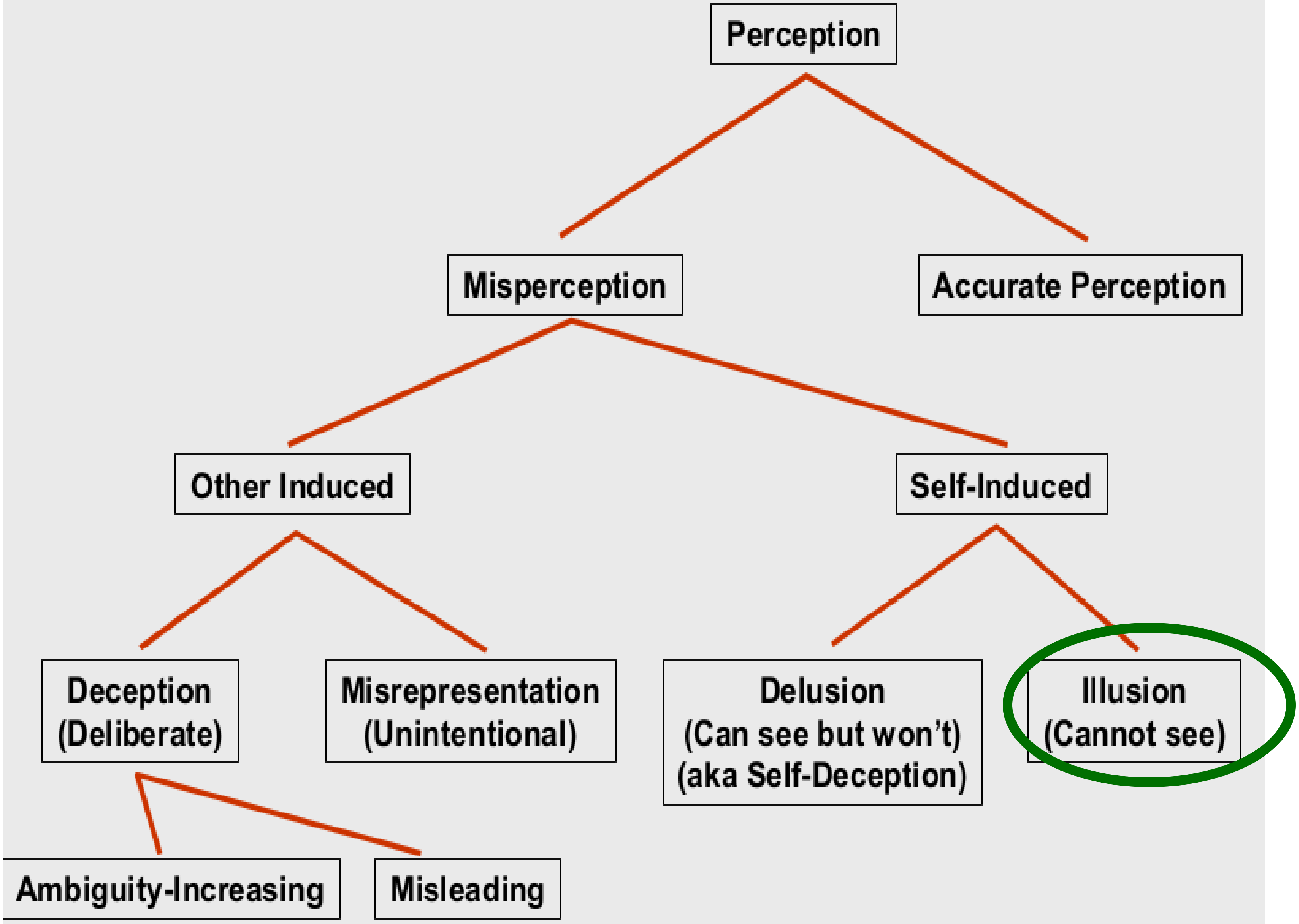
Delusion
(Can see but won’t)
(aka Self-Deception)

Illusion
(Cannot see)

Ambiguity-Increasing

Misleading

A TYPOLOGY OF PERCEPTION



Perception

Misperception

Accurate Perception

Other Induced

Self-Induced

Deception
(Deliberate)

Misrepresentation
(Unintentional)

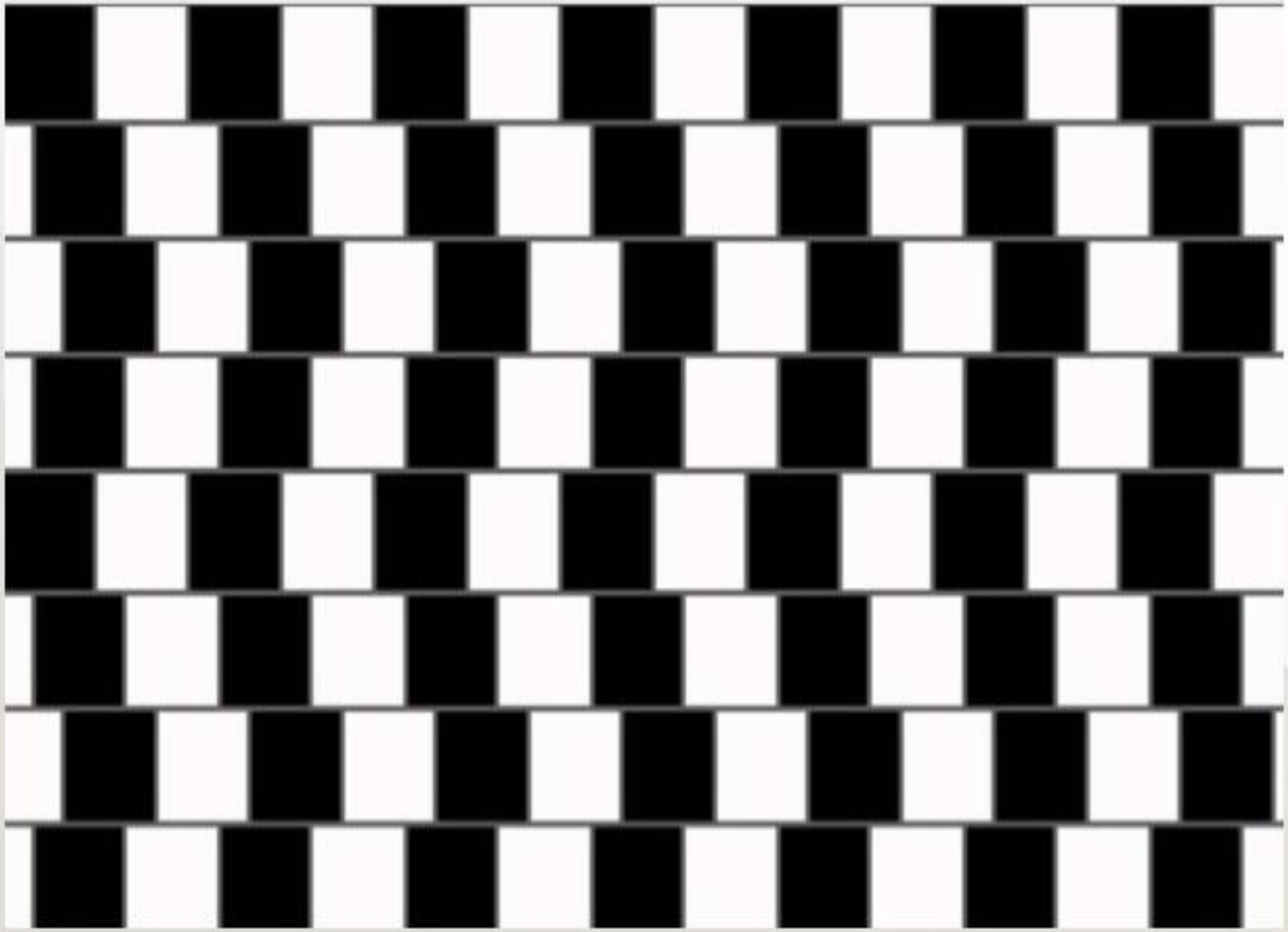
Delusion
(Can see but won't)
(aka Self-Deception)

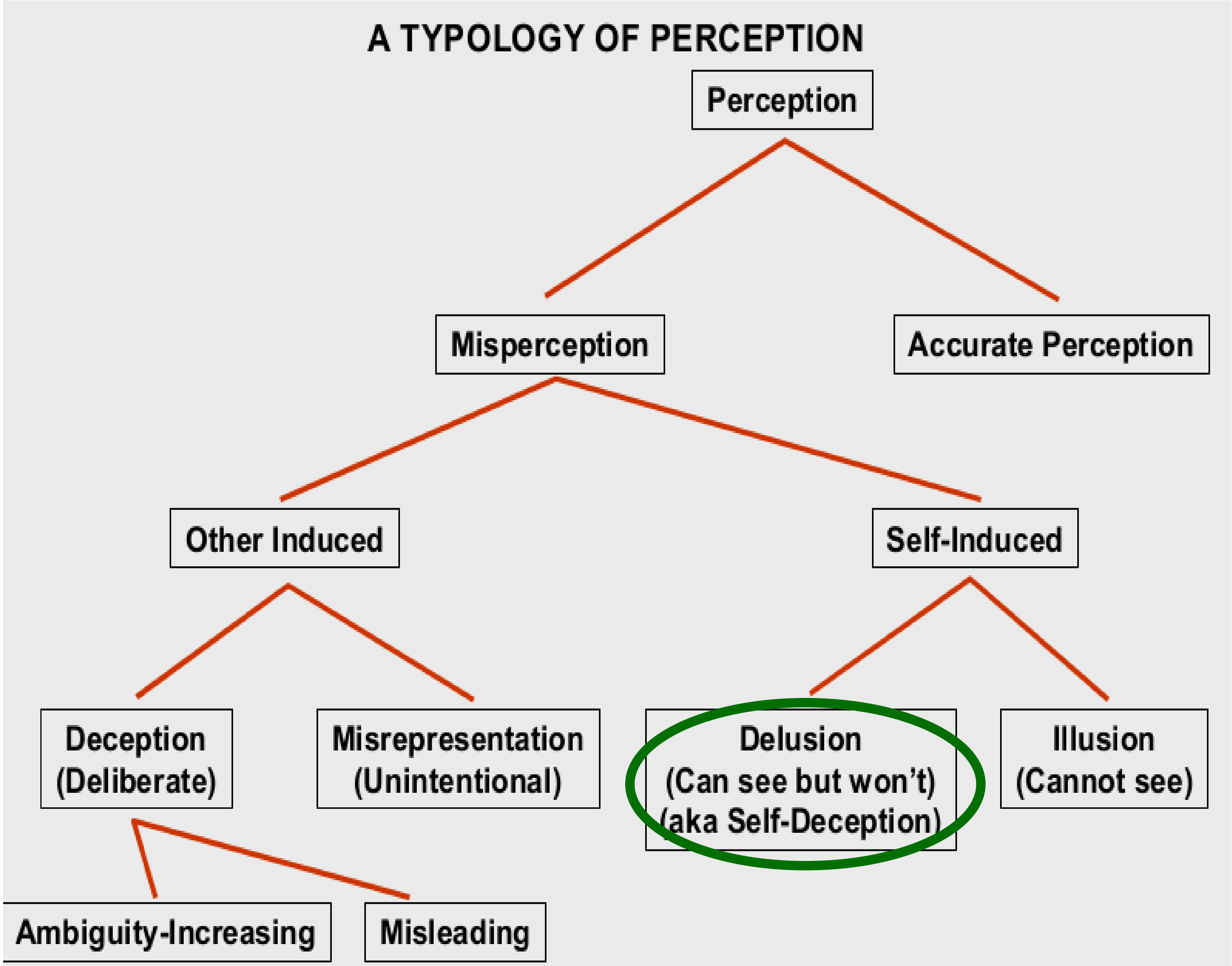
Illusion
(Cannot see)

Ambiguity-Increasing

Misleading

Self-induced and unintentional





A TYPOLOGY OF PERCEPTION

Perception

Misperception

Accurate Perception

Other Induced

Self-Induced

Deception
(Deliberate)

Misrepresentation
(Unintentional)

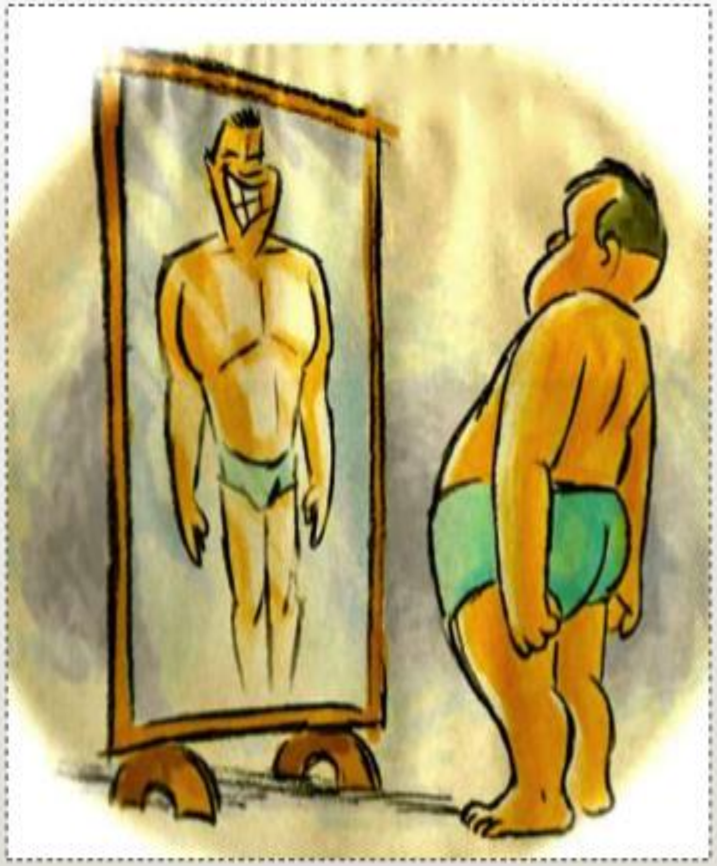
Delusion
(Can see but won't)
(aka Self-Deception)

Illusion
(Cannot see)

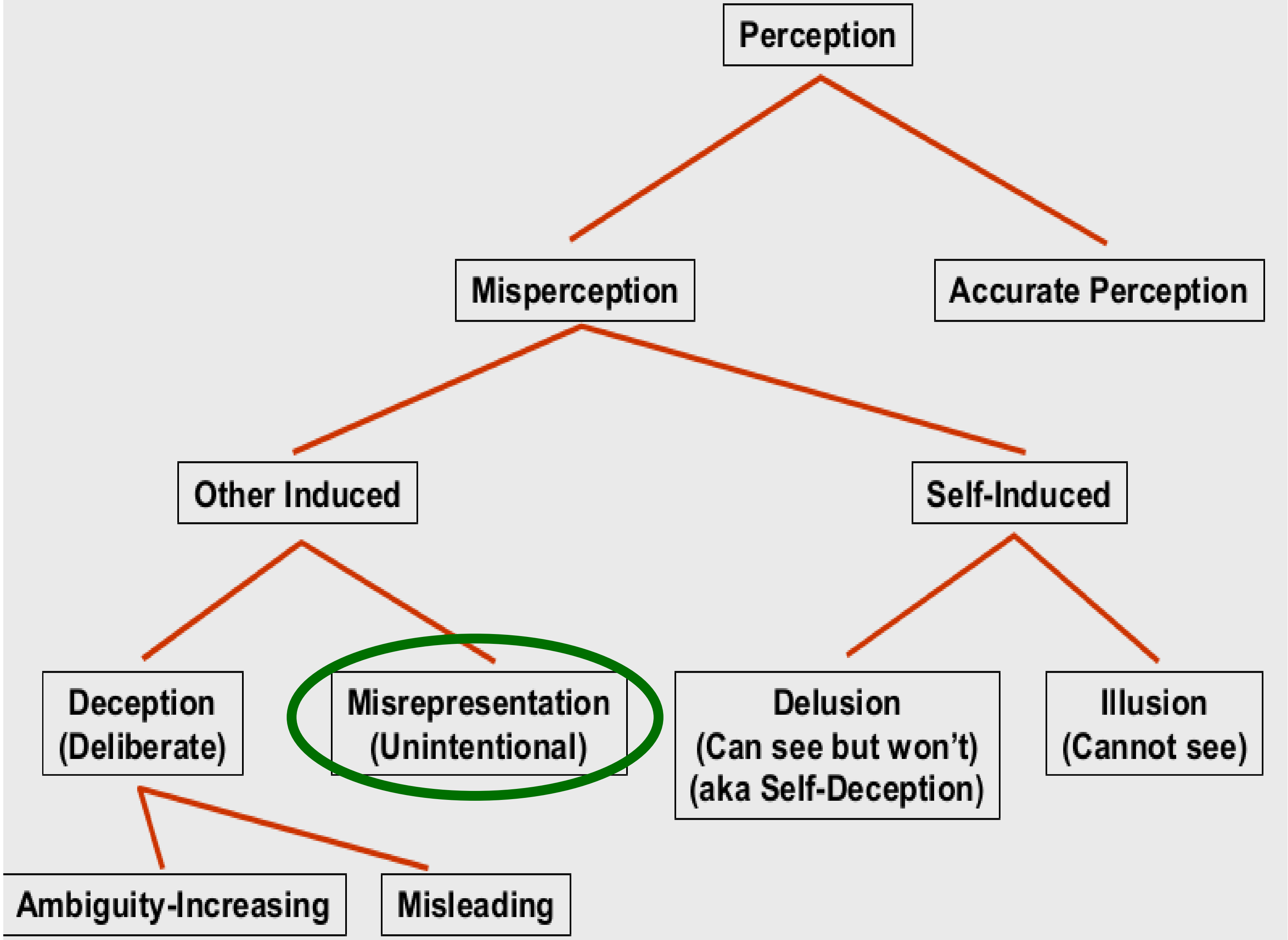
Ambiguity-Increasing

Misleading

Self-induced and intentional



A TYPOLOGY OF PERCEPTION



Perception

Misperception

Accurate Perception

Other Induced

Self-Induced

Deception (Deliberate)

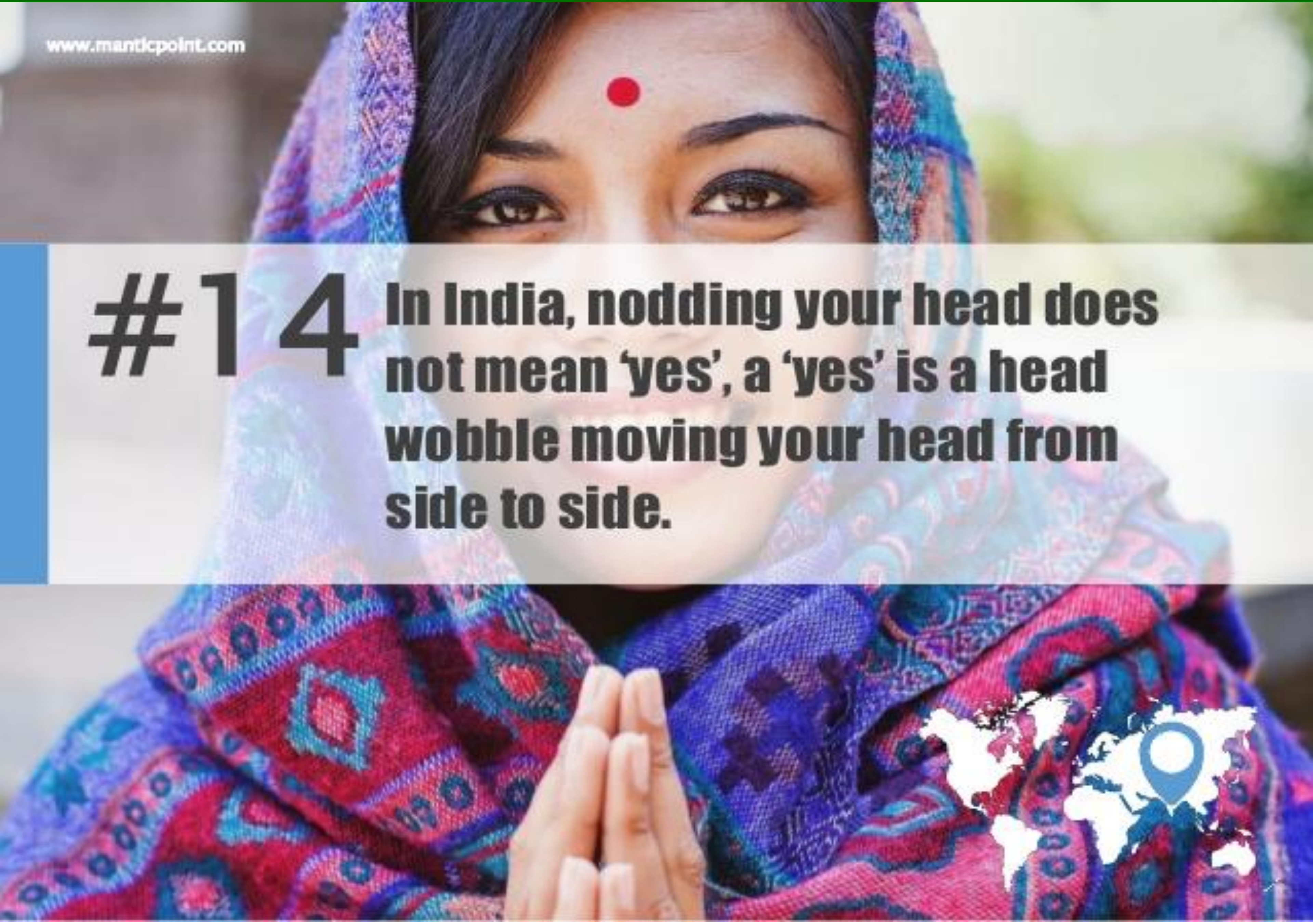
Misrepresentation (Unintentional)

Delusion (Can see but won't) (aka Self-Deception)

Illusion (Cannot see)

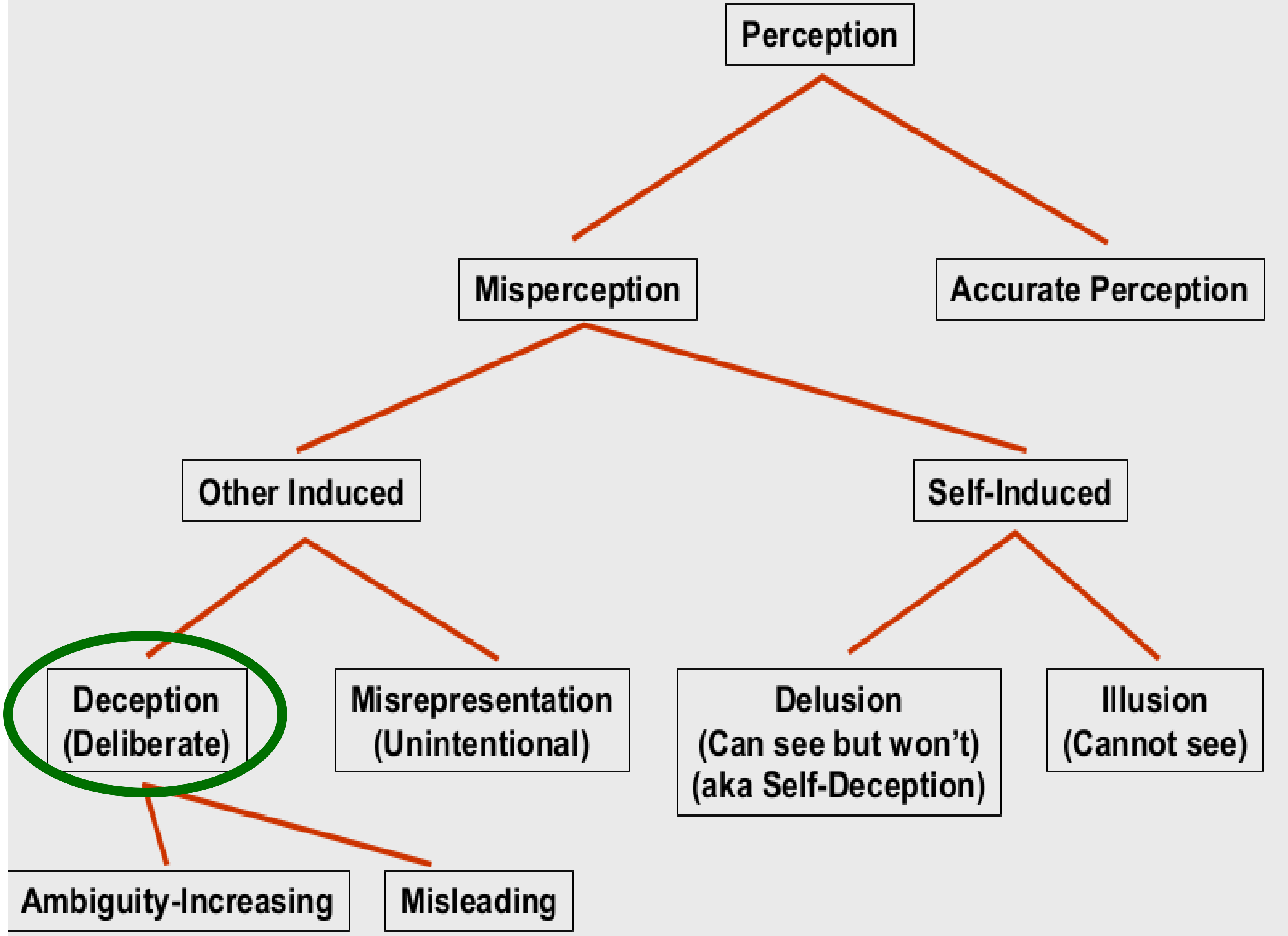
Ambiguity-Increasing

Misleading



#14 In India, nodding your head does not mean 'yes', a 'yes' is a head wobble moving your head from side to side.

A TYPOLOGY OF PERCEPTION



Perception

Misperception

Accurate Perception

Other Induced

Self-Induced

Deception
(Deliberate)

Misrepresentation
(Unintentional)

Delusion
(Can see but won't)
(aka Self-Deception)

Illusion
(Cannot see)

Ambiguity-Increasing

Misleading

Other induced and intentional

Cyber deception

What is cyber deception?

- Cyber deception is an advanced computer security strategy that uses various mechanisms to manipulate the cognitive beliefs of a specific target.

- Example: A financial institution might implement cyber deception by deploying a realistic but isolated decoy database containing fake customer data.

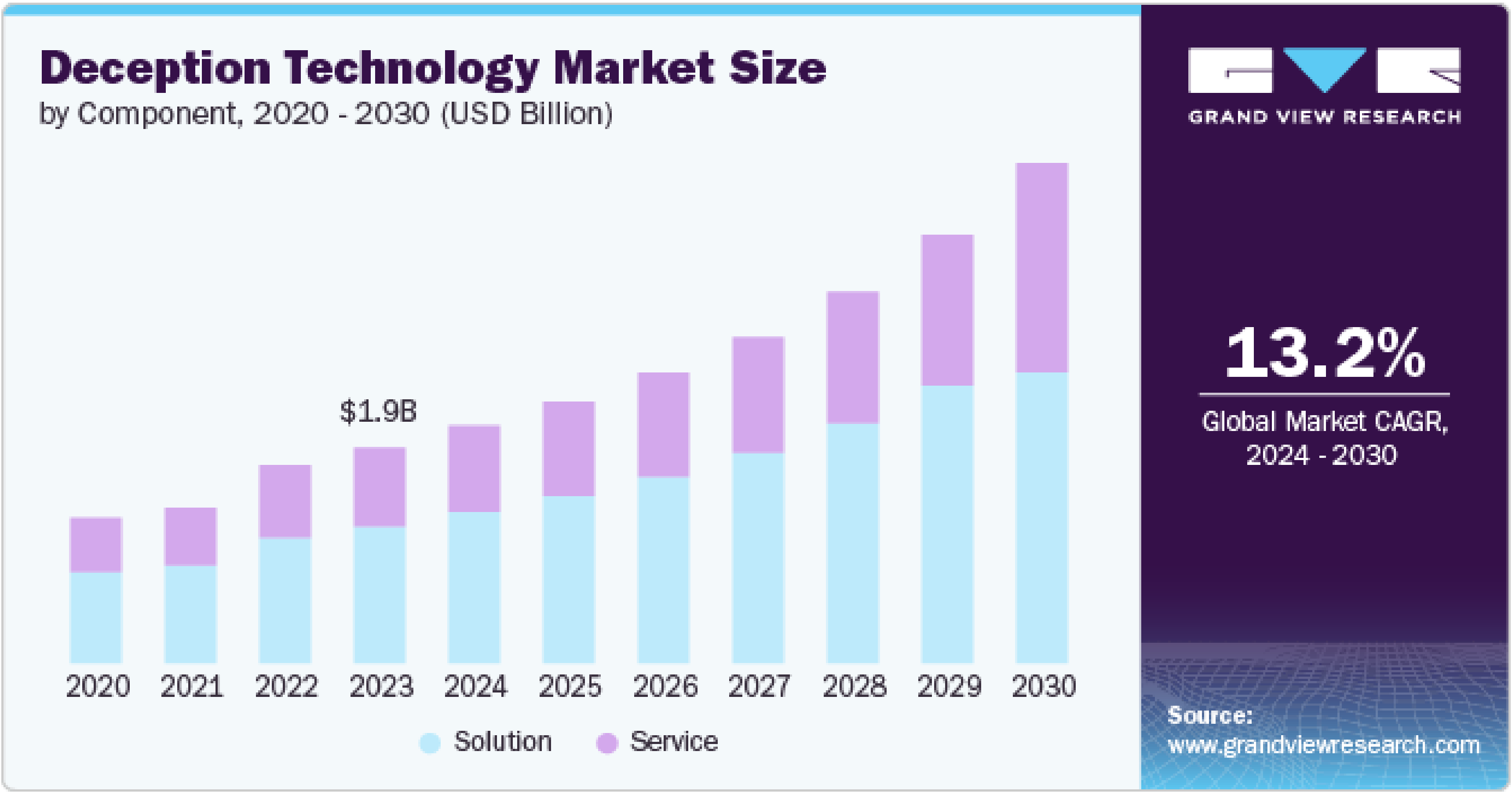
Attack vs. defense

- Cyber deception can be used for both attack and defense.

- In the case of defense, defenders can carry out actions that deceive the attacker to mitigate and even learn from his/her actions.

- In the case of an attack, attackers can use deception to improve stealth when entering a system or make the defender focus on some hidden point in the system (distract).

Deception market prediction



Question 1

- **Advantages: why cyber deception?**

Advantage: make attacks more difficult

- Cyber deception introduces uncertainty and confusion into the cyber environment, making the attackers’ task more difficult.
- Flooding the digital space with lures and traps increases complexity for adversaries.
- For instance, an e-commerce company might deploy decoy user accounts with fake transaction histories.

Advantage: improve early detection

- By placing digital decoys at strategic locations in the network, cyber deception facilitates early detection of malicious activity.

- These false signals act as early warning signs, allowing security teams to quickly identify and respond to intrusion attempts before they can cause significant damage

Advantage: reduce attack surface

- Creates a misleading landscape with decoys
- Obscures real assets

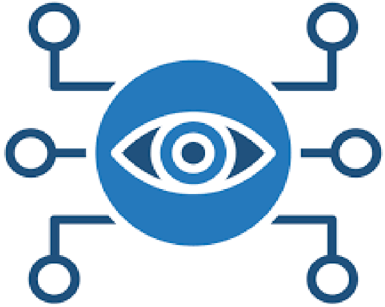
Advantage: discourage adversaries

- The presence of cyber deception elements can deter cyber adversaries by leading them to believe that the environment is well protected and that their activities can be easily detected and thwarted.

- This heightened risk perception can lead attackers to seek easier and less protected targets rather than confront robust defenses.

Advantage: gather threat intelligence

- **Cyber deception protects against cyberattacks and provides a unique opportunity to gather intelligence on adversaries' TTP.**
  - Tactics: high-level, strategic goals, such as gaining initial access.
  - Techniques: specific methods used to achieve those goals, like phishing or port scanning.
  - Procedures: specific, step-by-step actions an adversary takes to carry out a technique (e.g., a particular email template used in a phishing campaign)
- **By observing how attackers interact with lures and traps, security teams can gain valuable information to improve their defense strategies further and anticipate future attacks.**



Question 2

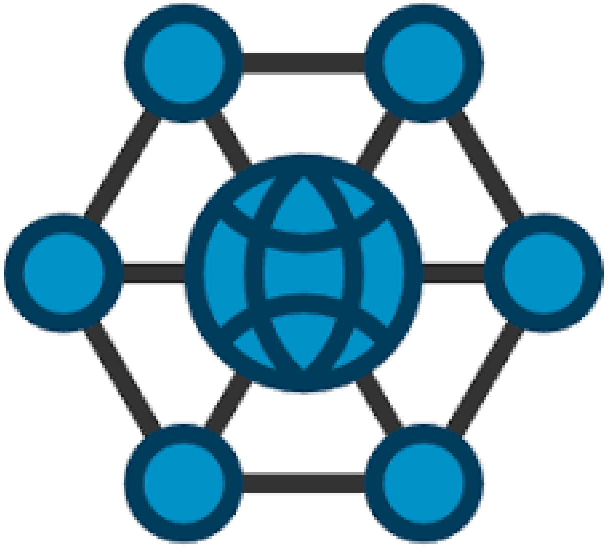
- **Dimensions: where to apply cyber deception?**

Dimension: data

- Data manipulation aims to erode adversaries' trust in information, weakening their strategies.
- It involves altering authentication, system activity, or information flow, either by falsifying records or subtly modifying data.

Dimension: network

- **Network deception manipulates transmitted data and components through redirections, decoys, or modifications.**



Dimension: system

- This dimension alters essential system components, including OS, hardware, and storage, to deceive adversaries.

Dimension: software

- **Software deception manipulates applications and scripts.**

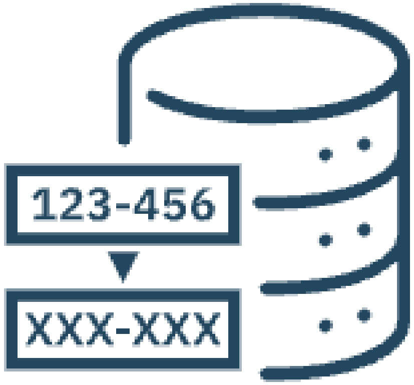
Question 3

- **Strategies: what are the goals of cyber deception?**

Strategy: masking

- Masking **hides sensitive information** to prevent detection by adversaries.

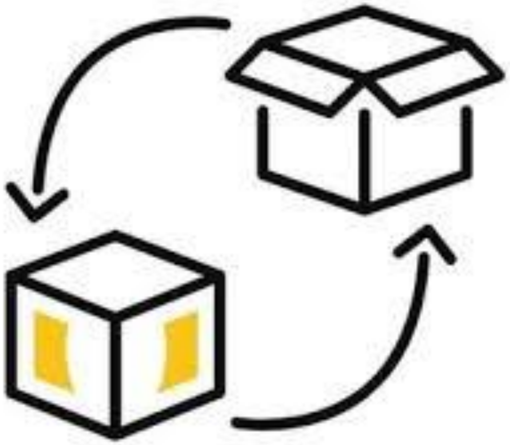
- For example, encrypting database query logs can prevent attackers from identifying access patterns, while services can be hidden by operating on non-standard ports.



Strategy: repackaging

- Repackaging alters the appearance of digital objects to evade detection or exploit user trust.

- An example is disguising critical files as innocuous images or text documents to deter attackers.



Strategy: dazzling

- Dazzling overwhelms adversaries with excessive information, making analysis difficult.

- For instance, defenders can flood an attacker's monitoring system with fake alerts or dummy network traffic, delaying their ability to identify real targets.

Strategy: mimicking

- Mimicking replicates legitimate entities or behaviors to deceive attackers.
- A common use case is deploying fake login pages in honeypots to capture credentials.

Strategy: inventing

- Inventing creates fictitious scenarios to mislead adversaries.
- An example is deploying fake administrative accounts to lure attackers into attempting privilege escalation.

Strategy: decoying

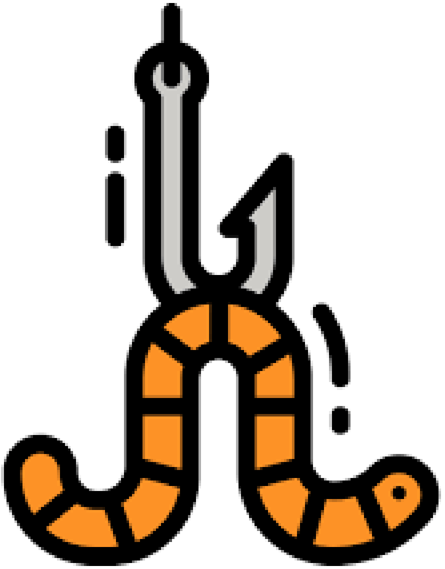
- Decoying redirects adversaries to false targets to protect critical assets.

- For example, fake servers mimicking financial databases can divert attackers from real systems.

Strategy: bait

- Bait uses enticing but false information to lure adversaries.

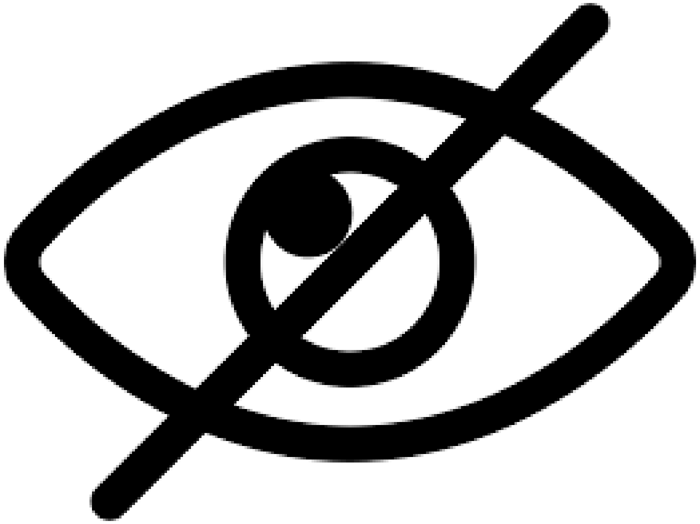
- An example is deploying files labeled *Confidential Passwords* that trigger security alerts when accessed.



Strategy: concealment

- Concealment actively hides critical resources or information.

- For example, encrypting sensitive data and storing it in obscure file locations makes it difficult for attackers to find.



Strategy: camouflage

- Camouflage disguises digital elements to blend into their environment.

- A use case includes embedding critical network traffic within normal traffic patterns to prevent identification.

Strategy: tarpit

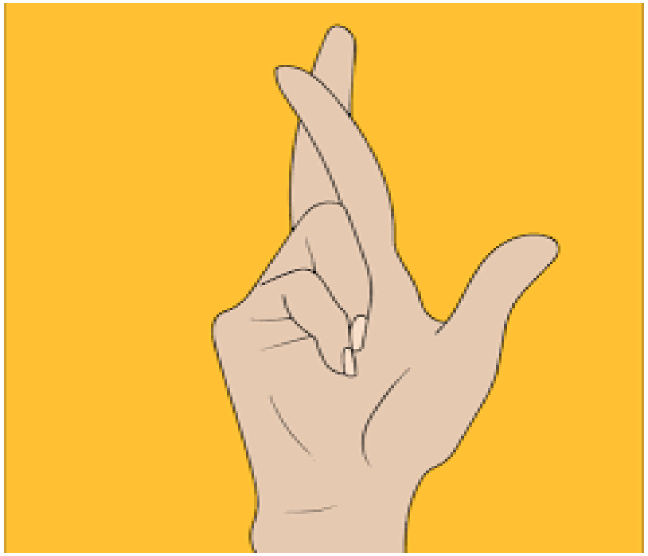
- Tarpit is a type of false information that delays the adversary's attack actions.

- For instance, defenders can inject false configuration files with fake IP addresses to waste an attacker's time.

Strategy: lies

- Lies provide false responses to mislead attackers.

- An example is reporting incorrect software versions to deceive attackers into exploiting nonexistent vulnerabilities.



Strategy: display

- Display manipulates the presentation of information to mislead adversaries.

- For example, a system might display misleading login error messages to trick brute-force attackers while logging their activity.

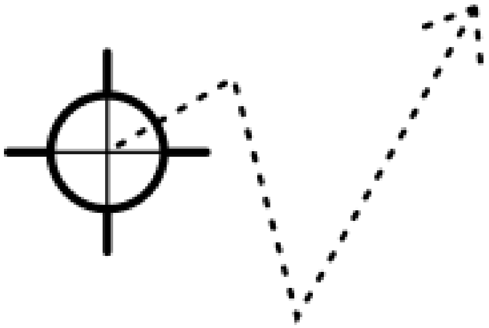
Question 4

- **Mechanisms: how to achieve cyber deception?**

Mechanism: MTD

- Moving target defense (MTD) dynamically reconfigures network assets to disrupt attacks.

- For example, periodic IP and port changes prevent adversaries from maintaining persistent access.

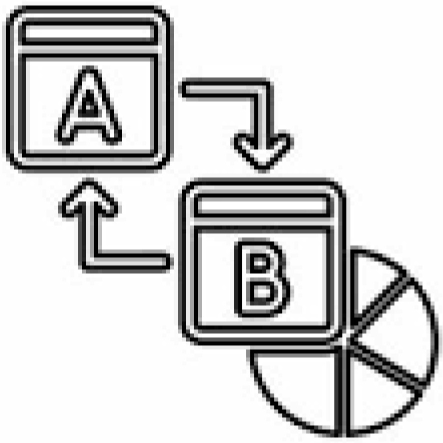


Mechanism: Honey-X (decoy)

- Honey-X uses decoys and traps to detect and analyze attacks.
- A common example is a fake admin portal that logs unauthorized access attempts.

Mechanism: obfuscation

- Obfuscation confuses adversaries by altering system visibility.
- Defenders can obfuscate filenames and directory structures to hinder attackers’ access to sensitive data.

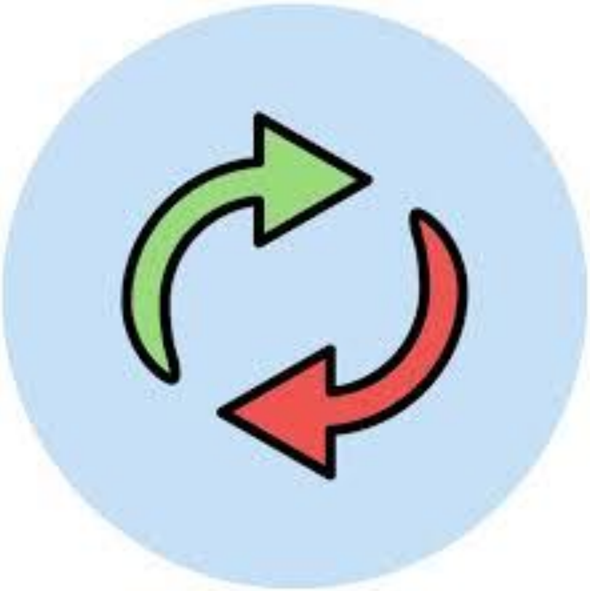


Mechanism: redirection

- Redirection means redirecting adversaries to fake targets to protect real assets.
- Suspicious traffic can be rerouted to honeypots for monitoring.

Mechanism: perturbation

- Perturbation adds noise or distractions to obscure real data.
- For instance, generating synthetic system logs can make it harder for attackers to extract meaningful insights.

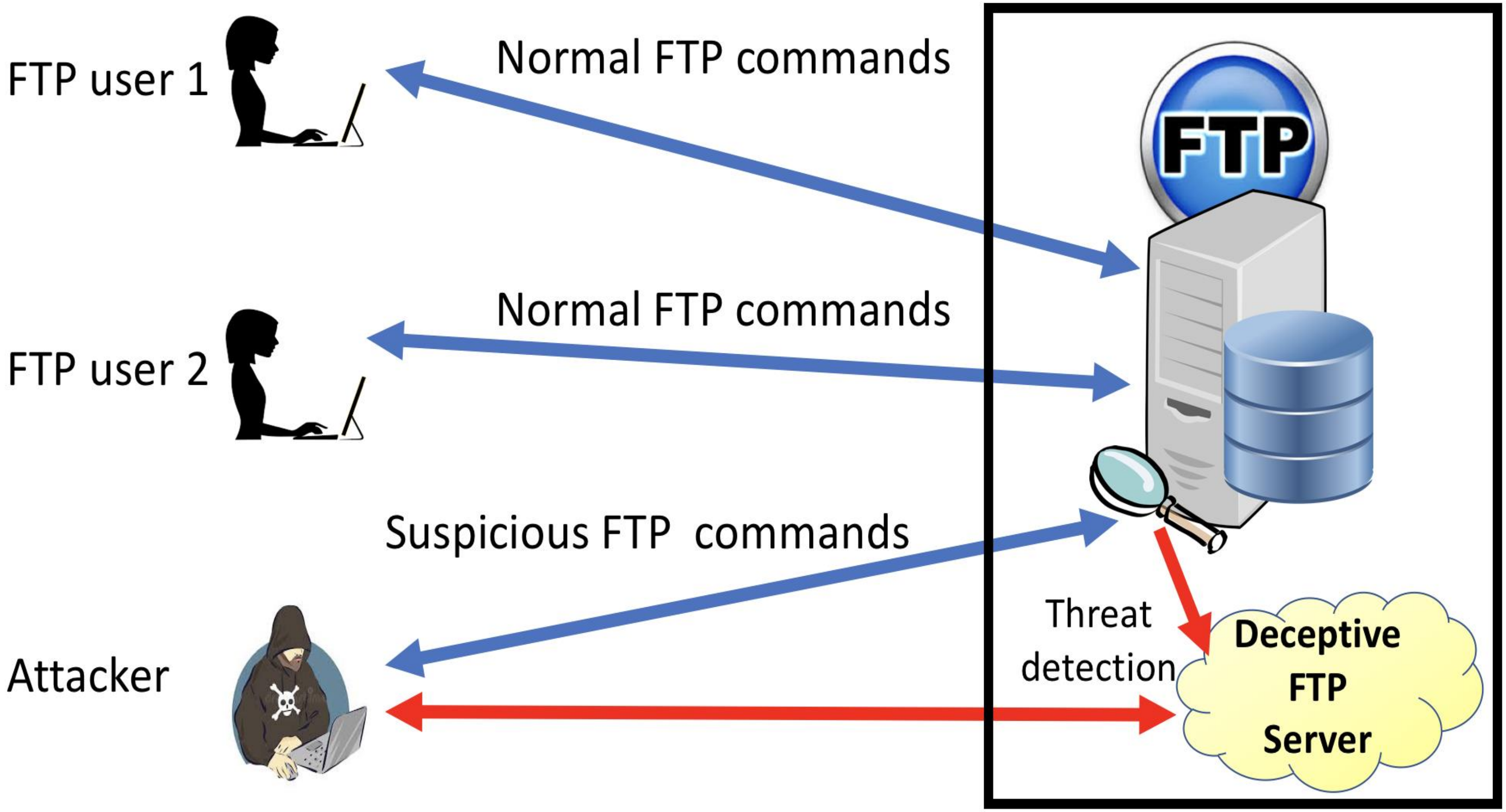


Deception consistency

Deception consistency

- **Motivation: In our common sense, we know that it’s easy to lie, but hard to make consistent lies**
- **We focus on exploring how to achieve deception consistency in building deception-based defense systems**
  - Role of consistency in deception is gaining attention in other fields.
  - E.g., J. Pete Blair, Torsten O. Reimer & Timothy R. Levine (2018) The Role of Consistency in Detecting Deception: The Superiority of Correspondence over Coherence, Communication Studies, 69:5, 483-498.
- **We start from working on FTP network services and are interested in using deception to harden a variety of networked services against APTs**

In the case of attacks against FTP service



Suspicious FTP connections

- **We add decoy software vulnerabilities in FTP services to monitor if the attacker tries to exploit them**
  - E.g., buffer overflow attacks for incoming FTP commands
- **We can also add decoy sensitive files in the FTP file system to monitor suspicious access patterns**
- **Any other detection techniques, as long as they can be used to separate attackers from legitimate users**
  - Orthogonal to our current research

Implementation goals

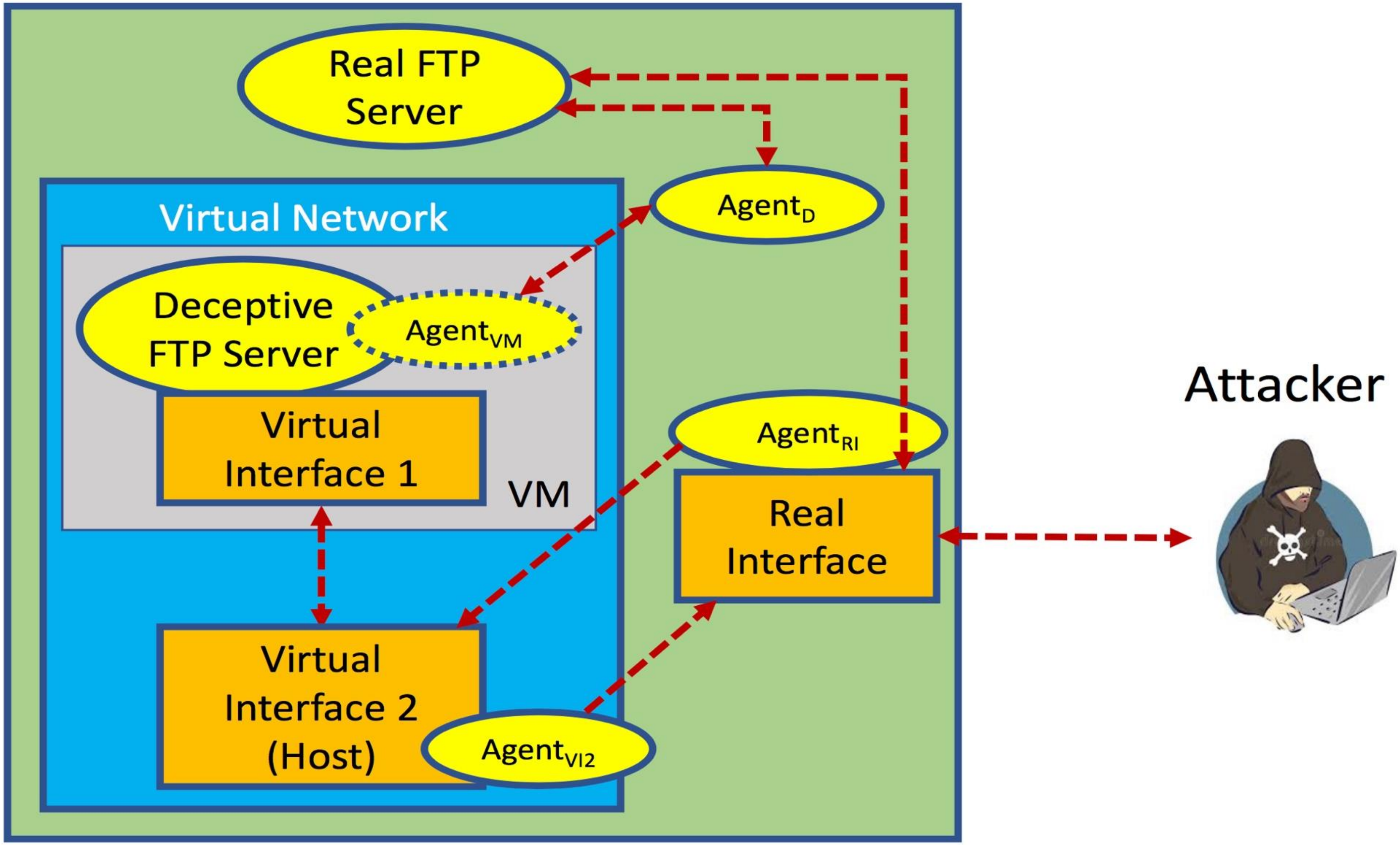
- **Service transparency: the FTP service provided by the deceptive FTP service should continue without noticeable changes of the underlying network status to the attacker.**
  - IP addresses, etc.
  - Similar round trip delays

- **Migration transparency: the process of migrating the attacker’s FTP connections to the deceptive FTP server should be done with low latency so that the attacker can’t tell whether process migration has occurred.**

Implementation issues

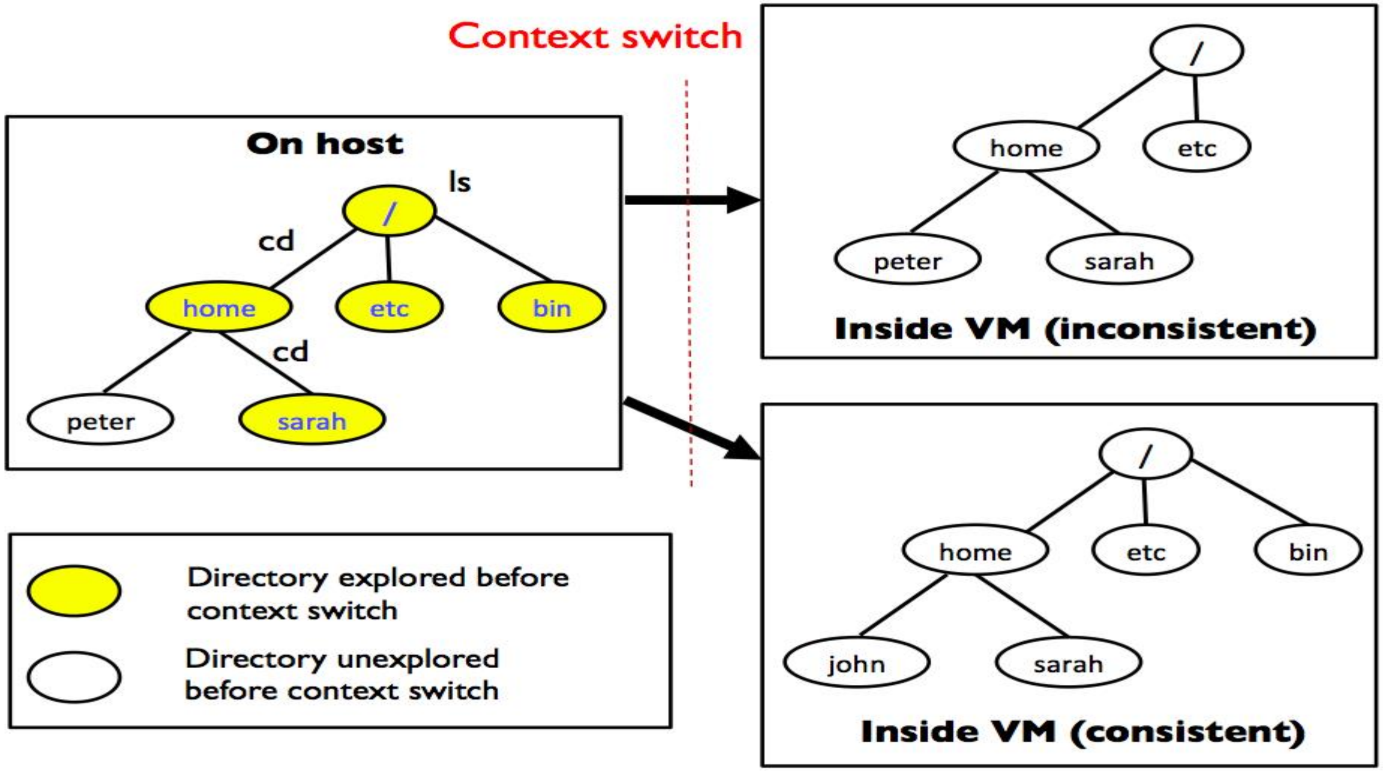
- **Deceptive FTP service runs inside a VM on the same host**
  - We can’t just migrate the attacker’s FTP connection (a process); the deceptive FTP service must also run because for some FTP commands, a separate FTP connection is created to deal with file transfers
- **Suspicious FTP connections are migrated into the VM using CRIU (Checkpoint/Restore In Userspace)**
  - We have made this work for both proFTPd and Bftpd
- **IP address translation is done on the host machine to ensure that the deceptive FTP service should use exactly the same IP address as before**

Deceptive FTP service within a VM on same host

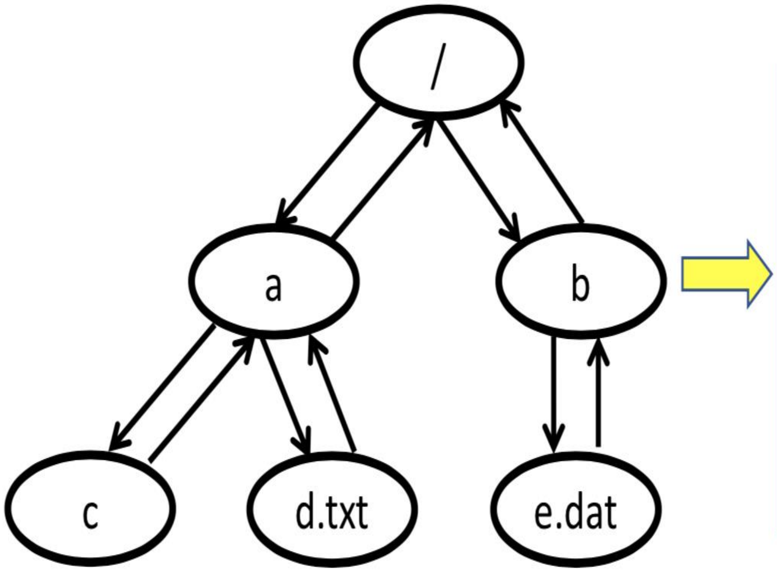


File system for the deceptive FTP service

- **Option 1: the same as the one on the host machine**
  - Bad, because it may have sensitive data
- **Option 2: a fake file system that is different from the real one**
  - The attacker may recognize the deceptive file system



Model attacker's best knowledge with constraint tree



- state: {FILE, DIR, EXIST, NOTEXIST, UNCERTAIN}
- terminal: {YES, NO, UNCERTAIN}
- listed: {YES, NO}
- subpath_constrained: {YES, NO}
- contents_seen: {YES, NO}
- metadata: { (size, user, group, permission, modtime) }

Raw FTP Commands

- LIST(path)
- CWD(path)
- USER(path), GROUP(path)
- MKD(path)
- RMD(path)
- STOR(path), APPE(path)
- RETR(path)
- DELE(path)
- RNFR(oldp, newp)
- MDTM(path, new_time)
- SIZE(path, new_size)
- CHMOD(path, new_perm)

Instantiation of deceptive file systems

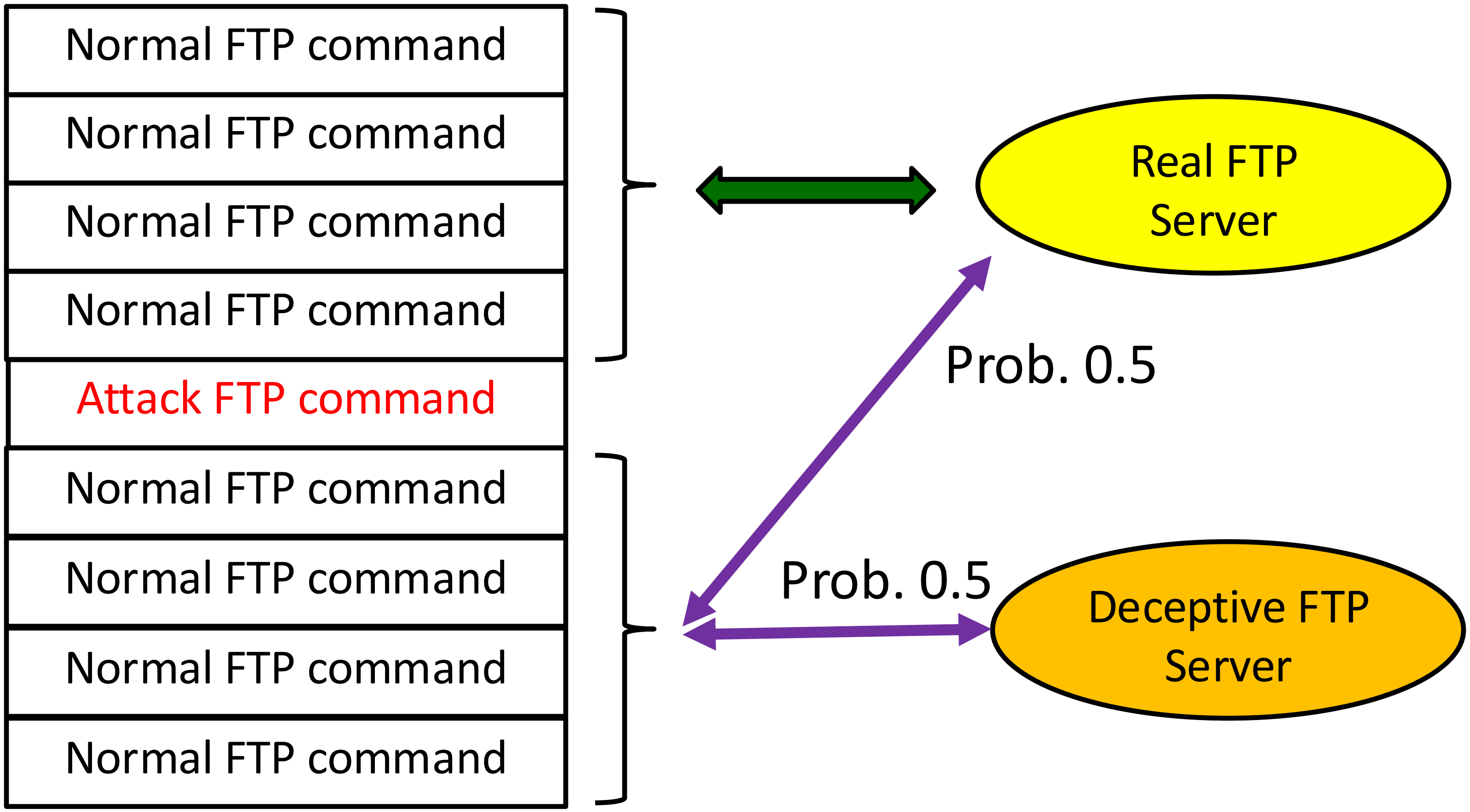
- **LIFT**
  - Use the attacker's positive knowledge in the constraint tree to create a minimal file system without leading to any observation inconsistency
  - Non-determinism is used to deal with uncertain knowledge

- **EXPAND**
  - Expand the file system with new files or directories, while ensuring that they don't conflict with the attacker's negative knowledge

Experiments with 32 student participants

- Two laptops, one FTP client and the other server in my office
- Sample FTP commands were offered in case that students are not familiar with FTP, including one long attack string intended for buffer overflow
- Students were allowed to use cell phones to take pictures of command outputs
- Students spent 10 minutes up to an hour in an experiment
- After the attack, with probability 50%, the environment was switched to a deceptive FTP service contained within a VM

Deception tests



Normal FTP command

Normal FTP command

Normal FTP command

Normal FTP command

Attack FTP command

Normal FTP command

Normal FTP command

Normal FTP command

Normal FTP command

Real FTP Server

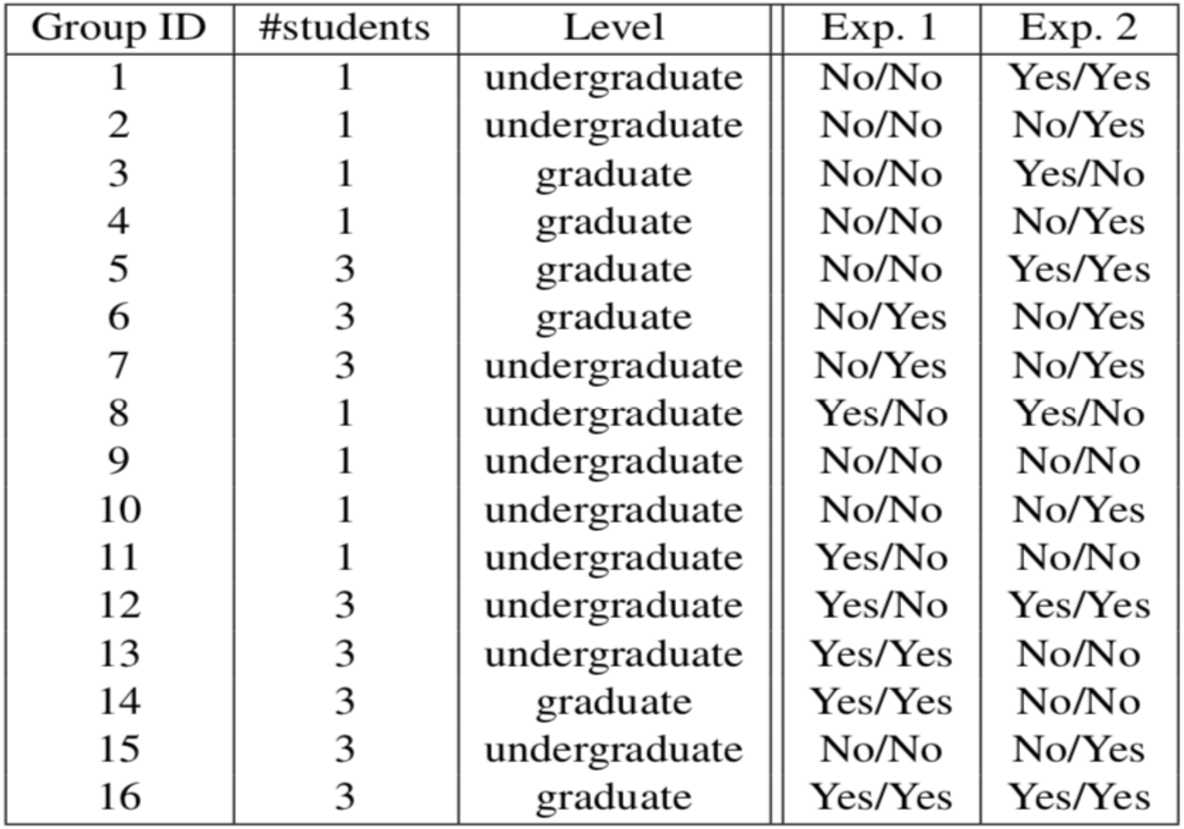
Prob. 0.5

Prob. 0.5

Deceptive FTP Server

After each experiment, the participants were asked if they had encountered a deceptive environment

Experimental results



Group ID	#students	Level	Exp. 1	Exp. 2
1	1	undergraduate	No/No	Yes/Yes
2	1	undergraduate	No/No	No/Yes
3	1	graduate	No/No	Yes/No
4	1	graduate	No/No	No/Yes
5	3	graduate	No/No	Yes/Yes
6	3	graduate	No/Yes	No/Yes
7	3	undergraduate	No/Yes	No/Yes
8	1	undergraduate	Yes/No	Yes/No
9	1	undergraduate	No/No	No/No
10	1	undergraduate	No/No	No/Yes
11	1	undergraduate	Yes/No	No/No
12	3	undergraduate	Yes/No	Yes/Yes
13	3	undergraduate	Yes/Yes	No/No
14	3	graduate	Yes/Yes	No/No
15	3	undergraduate	No/No	No/Yes
16	3	graduate	Yes/Yes	Yes/Yes

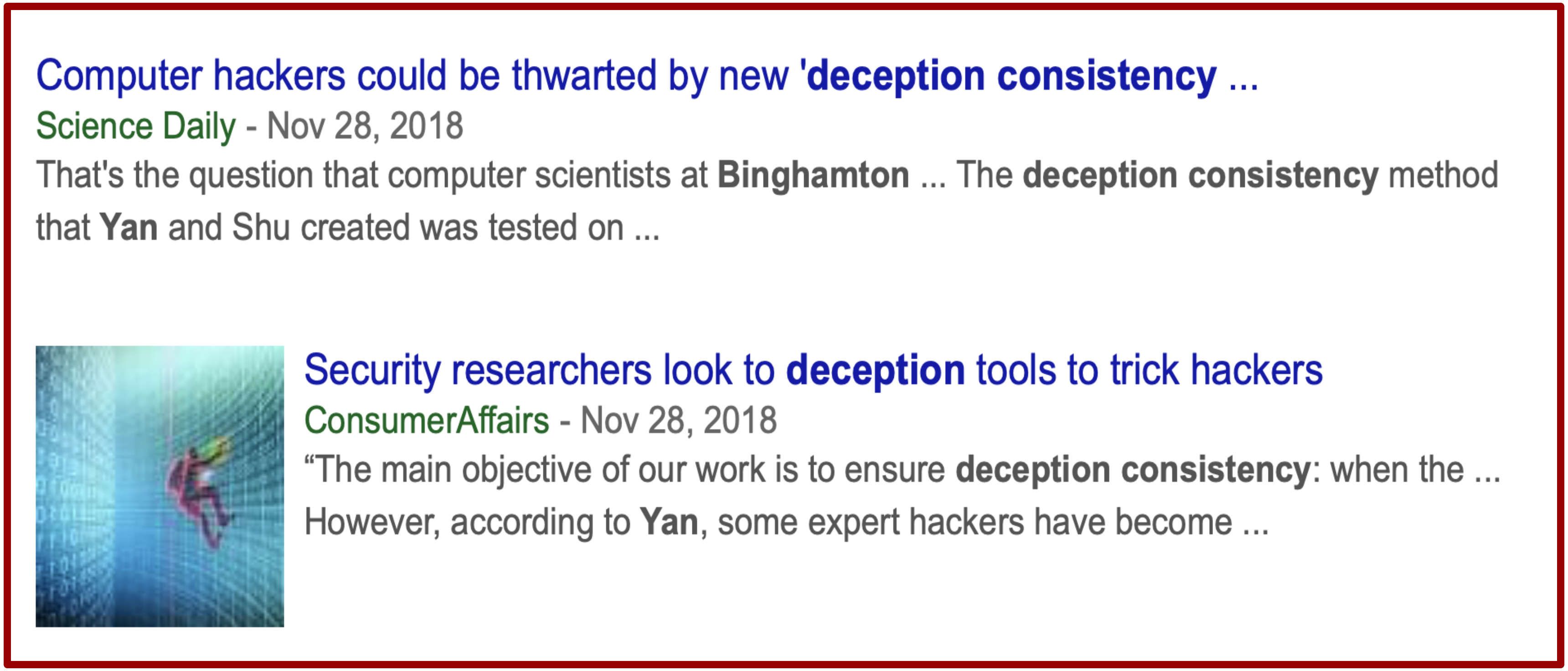
Exp. 1: a project file system; **Exp. 2**: random file system

Results in table: Ground Truth / Answer

Accuracy: 68.8% for first experiment and 50% for second one

More details…

- **Zhan Shu and Guanhua Yan. "Ensuring Deception Consistency for FTP Services Hardened against Advanced Persistent Threats."** ***Proceedings of the 5th ACM Workshop on Moving Target Defense*****. ACM, 2018**



Computer hackers could be thwarted by new '**deception consistency** ...

Science Daily - Nov 28, 2018

That's the question that computer scientists at **Binghamton** ... The **deception consistency** method that **Yan** and Shu created was tested on ...

Security researchers look to **deception** tools to trick hackers

ConsumerAffairs - Nov 28, 2018

“The main objective of our work is to ensure **deception consistency**: when the ... However, according to **Yan**, some expert hackers have become ...

End of Lecture 18