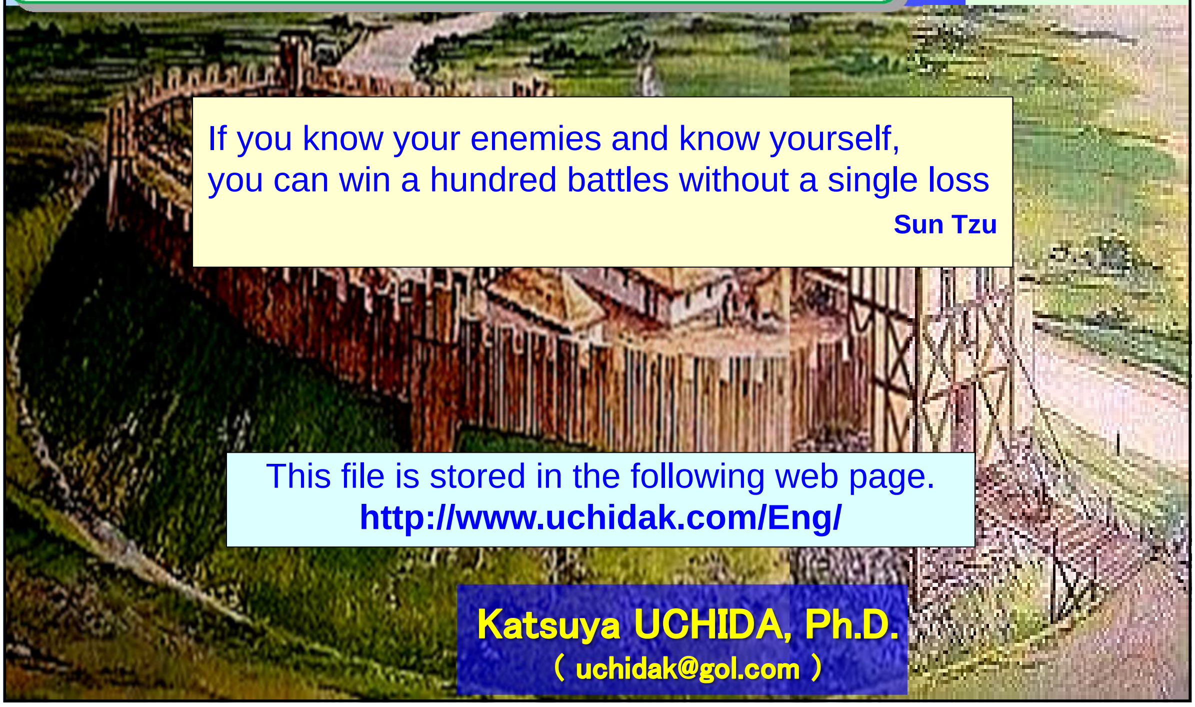
A psychological approach to information security

～ Some ideas for establishing Information security psychology ～

08 Aug., 2015
HCI International 2015



> If you know your enemies and know yourself,
> you can win a hundred battles without a single loss
>
> Sun Tzu

This file is stored in the following web page.
http://www.uchidak.com/Eng/

Katsuya UCHIDA, Ph.D.
（ uchidak@gol.com ）

Definition & Purpose of this paper

- Definition of Social engineering
  - Psychological manipulation of people into performing actions or divulging confidential information (Wikipedia, ”Social engineering”)
  - The act of manipulating a person to take an action that may or may not be in the “target” best interest. This may include obtaining information, gaining access, or getting the target to take certain action. (Hadnagy, R. 2010)

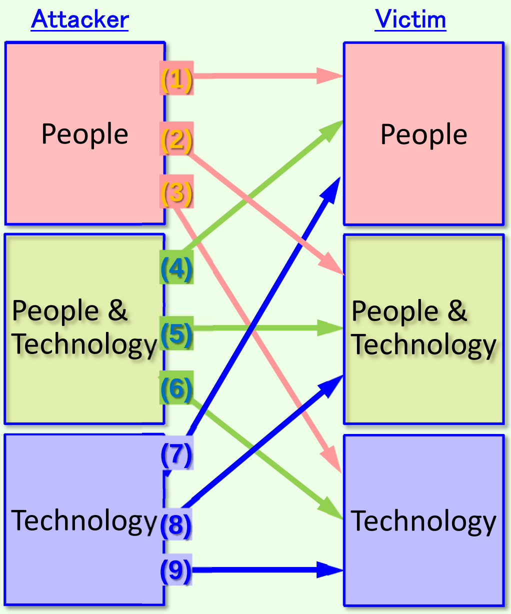
Purpose of this paper (Research areas)

- Social engineering
- In the era of “Internet of Things”(IoT)
  - the attackers and the victims become people, as well as technology and people & technology".
- Defense of victims

  In the following areas, psychology, behavioral science, criminology, etc. are used.
  - To know our enemies and ourselves (Social Engineering)
  - Effective education/training
  - Improve teamwork and communications

I would like to define this as “Information Security Psychology”

Basic Model of Deception



Examples

(1) Fake phone call
(2) Shoulder Hacking / Site Intrusion
(3) Fake biometrics

(4) Vishing
(5) (I have no idea currently. Help me)
(6) Targeted mail

(7) Caller ID Spoofing
(8) Malware
(9) SYN Flood / Mac Spoofing

Some Case of Basic Model of Deception

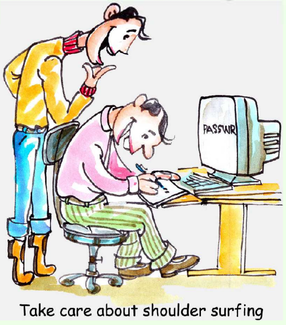
(1) Fake phone call [Attacker: People ⇒ Victim:People]

- 8 Oct, 1981 “Fake phone call” at Japanese Local bank
  The attacker's phone call; "I am a member of COMCEN (the local bank jargon, “computer center”), so please make fund transfer 35 million yen to the account of S branch for computer test." The manager in Savings account department believed the phone call from the data center, and made fund transfer. After the fund transfer, a female accomplice withdrew ¥30million(US$ 300,000) from the account in S branch.
- In October 1978, Stanley Mark Rifkin visited Security Pacific's wire transfer room where the **bank's secret code-of-the-day** was posted on the wall. Rifkin memorized the code and left without arousing suspicion. Soon, bank employees in the transfer room received a phone call from a man who identified himself as Mike Hansen, an employee of the bank's international division. The man ordered a routine transfer of funds into an account at the Irving Trust Company in New York -- and he provided the secret code numbers to authorize the transaction. Nothing about the transfer appeared to be out of the ordinary, and Security Pacific transferred the money to the New York bank. What bank officials did not know was that the man who called himself Mike Hansen was in fact Stanley Rifkin, and he had used the bank's security code to rob the bank of $10.2 million.

Rifkin has never told his own story, so this is based on published reports. (K. Mitnick)
This is TELEX system, not computer system, I think.

Some Case of Basic Model of Deception

(2) Shoulder Hacking / Site Intrusion [Attacker: People ⇒ Victim: People&Technology]



Shoulder hacking is not so easy, almost all people cannot memorize 8 or more long alphanumeric characters.

"Catch me if you can"
Frank **William Abagnale,** ***Jr***

In case of Site intrusion, an intruder often wears the company uniform.

(3) Fake biometrics [Attacker: People ⇒ Victim: People & Technology]

- Fake fingerprint with gelatin (gumi)
  The artificial fingerprint was created with gelatin by Japanese researchers.

http://news.bbc.co.uk/2/hi/science/nature/1991517.stm
Friday, 17 May, 2002

Some Case of Basic Model of Deception

(4) Vishing [Attacker: People & Technology ⇒ Victim: People]

- Vishing (Voice Phishing) is the voice counterpart to phishing. Instead of being directed by e-mail to a Web site, an e-mail message asks the user to make a telephone call. The call triggers a voice response system that asks for user's critical data.

(5) Not yet [Attacker: People & Technology ⇒ Victim: People & Technology]

I have no idea currently. Please help me!

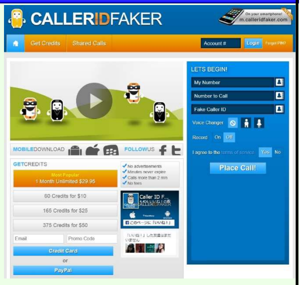
(6) Targeted Mail [Attacker: People & Technology ⇒ Victim: Technology]

Describe later!

Some Case of Basic Model of Deception

(7) Caller ID Faker [Attacker: Technology ⇒ Victim: People]

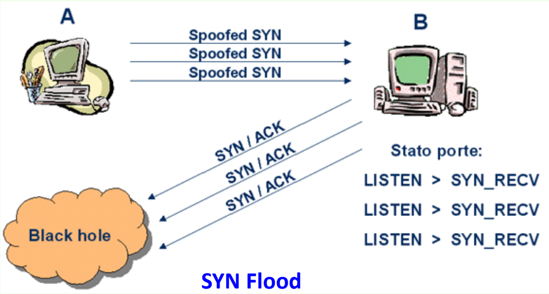
Caller id spoofing: Change the caller id to show any desired number on a recipients caller id display.
Voice change is available, Male to Female and vice versa.



(8) Malware [Attacker: Technology ⇒ Victim: People & Technology]

(9) SYN Flood / Mac Spoofing [Attacker: Technology ⇒ Victim: Technology]

SYN Flood is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.



SYN Flood

Know Your Enemy & Ourselves

Six "weapons of influence"

1. Reciprocation : Reciprocation recognizes that people feel indebted to those who do something for them or give them a gift.
2. Commitment and Consistency : People do not like to back out of deals. We’re more likely to do something after we’ve agreed to it verbally or in writing, Cialdini says. People strive for consistency in their commitments. They also prefer to follow pre-existing attitudes, values and actions.
3. Social Proof : When people are uncertain about a course of action, they tend to look to those around them to guide their decisions and actions. They especially want to know what everyone else is doing – especially their peers.
4. Liking : “People prefer to say ‘yes’ to those they know and like,” Cialdini says. People are also more likely to favor those who are physically attractive, similar to themselves, or who give them compliments. Even something as ‘random’ as having the same name as your prospects can increase your chances of making a sale.
5. Authority : People respect authority. They want to follow the lead of real experts. Business titles, impressive clothing, and even driving an expensive, high-performing automobile are proven factors in lending credibility to any individual.
6. Scarcity : In fundamental economic theory, scarcity relates to supply and demand. Basically, the less there is of something, the more valuable it is. The more rare and uncommon a thing, the more people want it. Familiar examples are frenzies over the latest holiday toy or urban campers waiting overnight to pounce on the latest iPhone.

Robert Cialdini “Influence”

Excellent book for basic tendencies of human nature

Elicitation and Open/Closed Question

Essential knowledge for social engineer

1. The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated.
2. Elicitation attempts can be simple, and sometimes are obvious. If they are obvious, it is easier to detect and deflect. On the other hand, elicitation may be imaginative, persistent, involve extensive planning, and may employ a co-conspirator. Elicitors may use a cover story to account for the conversation topic and why they ask certain questions.
3. Elicitors may collect information about you or your colleagues that could facilitate future targeting attempts.
4. Elicitation can occur anywhere— at social gatherings, at conferences, over the phone, on the street, on the Internet, or in someone’s home.
5. Elicitors use “open question” and “closed question” effectively.
   - Open question: An open question is likely to receive a long answer.
     Open questions have the following characteristics:
     - They ask the respondent to think and reflect.
     - They will give you opinions and feelings.
     - They hand control of the conversation to the respondent.
   - Closed question: A closed question can be answered with either 'yes' or 'no'.
     Closed questions have the following characteristics:
     - They give you facts.
     - They are easy to answer.
     - They are quick to answer.
     - They keep control of the conversation with the questioner.

Pretexting

Also, essential knowledge for social engineer

1. the practice of presenting oneself as someone else in order to obtain private information
   - **Stalking murder in Japan** (Nov. 2012)
     - At the request of a private detective hired by the stalker, the executive of a research company who pretended to be the housewife husband, telephoned some city hall in Japan on the day before the murder occurred and got the information of the housewife. In leakage of personal information from the city hall, the stalker killed a housewife, and also killed himself.
     - The executive used elicitation technique also.

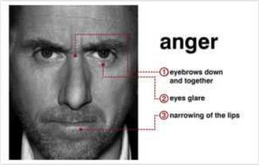
Probably the first case of murder in the information security field

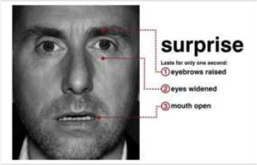
Microexpressions

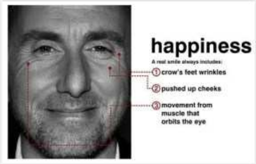
1. A microexpressions are a brief, involuntary facial expression shown on the face of humans. They express the six universal emotions: disgust, anger, fear, sadness, happiness, and surprise. They are very brief in duration, lasting only 1/25 to 1/15 of a second. A social engineer understands the true feelings from microexpression of the victim.

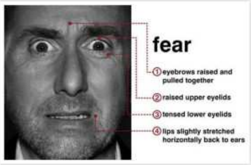
   Example of microexpression, I know only in the movie series, “Lie to me”.

The result of the microexpression is little bit different by ethnic group, I heard.






happiness
A real smile always includes:
①crow's feet wrinkles
②pushed up cheeks
③movement from muscle that orbits the eye

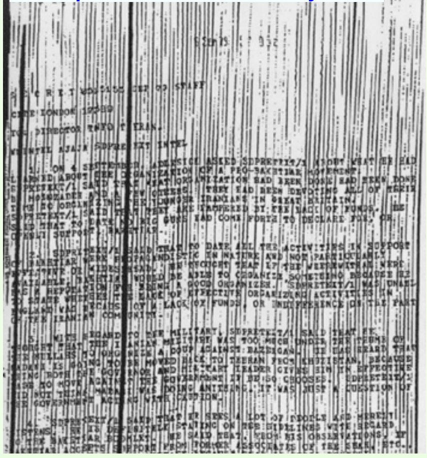

fear
①eyebrows raised and pulled together
②raised upper eyelids
③tensed lower eyelids
④lips slightly stretched horizontally back to ears

Know Your Enemy & Ourselves

Shredder Challenge

1. First generation
   - ◆ At the Iranian revolution
     The movie “ARGO”

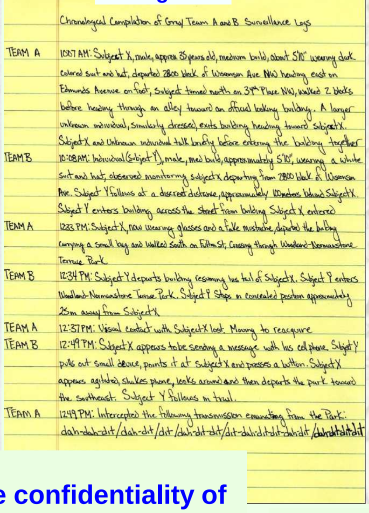
● Strip-cut: reconstructed by hand



Shredder Challenge

2. Second generation
   - ◆ DARPA Shredder Challenge 2011
     Successfully reconstructed and solved all 5 Puzzles

● Original



Chronological Compilation of Gray Team A and B Surveillance Logs

TEAM A 10:07 AM: Subject X, male, approx 35 years old, medium build, about 5'10" wearing dark colored suit and hat, departed 2800 block of Wisconsin Ave NW heading east on Edmunds Avenue on foot, Subject turned north on 34th Place NW, walked 2 blocks before heading through an alley toward an official looking building. A larger unknown individual, similarly dressed, exits building heading toward subject X. Subject X and Unknown individual talk briefly before entering the building together

TEAM B 10:08 AM: Individual (Subject Y), male, med build, approximately 5'10", wearing a white suit and hat, observed monitoring subject X departing from 2800 block of Wisconsin Ave. Subject Y follows at a discreet distance, approximately 100 meters behind Subject X. Subject Y enters building across the street from building Subject X entered

TEAM A 12:33 PM: Subject X, now wearing glasses and a fake mustache, departed the building carrying a small bag and walked south on Fulton St, crossing through Woodland-Normanstone Terrace Park

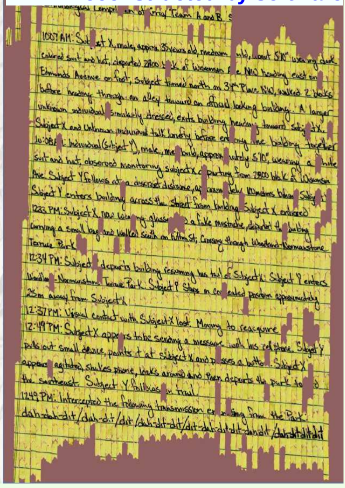
TEAM B 12:34 PM: Subject Y departs building resuming his tail of Subject X. Subject Y enters Woodland-Normanstone Terrace Park. Subject Y stops in concealed position approximately 25m away from Subject X

TEAM A 12:37 PM: Visual contact with Subject X lost. Moving to reacquire

TEAM B 12:49 PM: Subject X appears to be sending a message with his cell phone. Subject Y pulls out small device, points it at subject X and presses a button. Subject X appears agitated, shakes phone, looks around and then departs the park toward the southeast. Subject Y follows in trail.

TEAM A 12:49 PM: Intercepted the following transmission emanating from the Park:
dah-dah-dit/dah-dit/dit/dah-dit-dit/dit-dah-dit-dit-dah-dit/dah-dit-dit-dit

● Cross-cut:
Reconstructed by software



Never forget physical security!
Type of the shredder depends on the confidentiality of the materials you are shredding.

DARPA: http://archive.darpa.mil/shredderchallenge/

Education, Training & Awareness

Training of Targeted Attacks

Following are the results of targeted attacks in Japan.

1. Targeted attacks training without prior information
   - ◆ About 40% people clicked an attached file
2. Targeted attacks training given enough information
   - ◆ About 10% people clicked an attached file
3. Targeted attacks training without prior information two years later
   - ◆ About 12.5% people clicked an attached file
4. Targeted attacks training given enough information two years later
   - ◆ About 6.3% people clicked an attached file

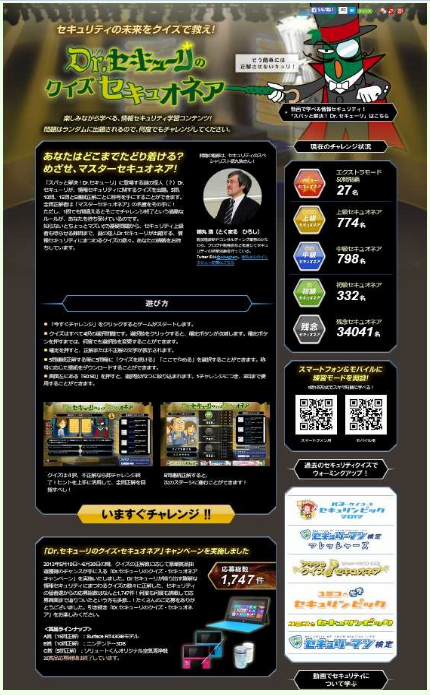
Source
1. Three Japanese local government
2. Japanese government
3. One Japanese local government
4. One Japanese local government

- ● In USA (Lance Spitzner, SANS @RSA Conf. 2014)
  - ◆ The more often the assessments, the more effective the impact.
    - ➢ Quarterly: 19%
    - ➢ Every other month: 12%
    - ➢ Monthly: 4%
  - ◆ Over time you will most likely have to increase difficulty of phishing tests, as they become too simple.

Education, Training & Awareness

Gamification

1. **Gamification is the use of game elements and game design techniques in non-game contexts.** (Werbach, K. et al., 2012)
2. Gamification is about learning, learning from game design but also learning from fields like psychology and management and marketing and economics.
3. It's a way in to understand things about motivation.
4. The most important things of gamification are;
   - To Whom (People)
   - How (Method)
   - What (Concept)
   - Where (Business Practices)
   - When (Situation)



セキュリティの未来をクイズで救え！

Dr.セキューリのクイズセキュオネア

せう簡単には正解させないキュリ！

楽しみながら学べる、情報セキュリティ学習コンテンツ！
問題はランダムに出題されるので、何度でもチャレンジしてください。

動画で学べる情報セキュリティ！「スパッと解決！Dr. セキューリ」はこちら

あなたはどこまでたどり着ける？
めざせ、マスターセキュオネア！

「スパッと解決！Dr.セキューリ」に登場する謎の怪人（？）Dr.セキューリが、情報セキュリティに関するクイズを出題。5問、10問、15問と5連続正解ごとに称号を手にすることができます。全問正解者は「マスターセキュオネア」の名誉をその手に！ただし、1問でも間違えるとそこでチャレンジ終了という過酷なルールが、あなたを待ち受けているのです。知らないとちょっとマズい!?基礎問題から、セキュリティ上級者も唸らせる難問まで、謎の怪人Dr.セキューリが出題する、情報セキュリティにまつわるクイズの数々。あなたの挑戦をお待ちしています。

問題の監修は、セキュリティのスペシャリスト徳丸浩さん！

徳丸 浩（とくまる ひろし）

現在のチャレンジ状況

エクストラモード 50問制覇 27名

上級セキュオネア 774名

中級セキュオネア 798名

初級セキュオネア 332名

残念セキュオネア 34041名

遊び方

- 「今すぐチャレンジ」をクリックするとゲームがスタートします。
- クイズはすべて4択の選択問題です。選択肢をクリックすると、確定ボタンが点滅します。確定ボタンを押すまでは、何度でも選択肢を変更することができます。
- 確定を押すと、正解または不正解の文字が表示されます。
- 5問連続正解する毎に5問毎に「クイズを続ける」「ここでやめる」を選択することができます。称号に応じた壁紙をダウンロードすることができます。
- 画面左にある「50:50」を押すと、選択肢が2つに絞り込まれます。1チャレンジにつき、3回まで使用することができます。

クイズは4択、不正解なら即チャレンジ終了！ヒントを上手に活用して、全問正解を目指すべし！

5問連続正解すると、次のステージに進むことができます！

いますぐチャレンジ !!

スマートフォン&モバイルに練習モードを開設！

スマートフォン用　モバイル用

過去のセキュリティクイズでウォーミングアップ！

「Dr.セキューリのクイズ・セキュオネア」キャンペーンを実施しました

2013年5月10日～6月30日の間、クイズの正解数に応じて豪華賞品抽選獲得のチャンスが手に入る「Dr.セキューリのクイズ・セキュオネアキャンペーン」を実施いたしました。Dr.セキューリが繰り出す難解な情報セキュリティにまつわるクイズの数々に正解した、セキュリティの猛者達からの応募総数はなんと1,747件！何度も何度も挑戦して応募資格まで辿りついたという方も多数…！たくさんのご応募ありがとうございました。引き続き「Dr.セキューリのクイズ・セキュオネア」をお楽しみください。

応募総数 1,747件

<賞品ラインナップ>
A賞（15問正解）：Surface RT43GBモデル
B賞（10問正解）：ニンテンドー3DS
C賞（5問正解）：ソリュートくんオリジナル空気清浄機
※賞品応募期間は終了しています。

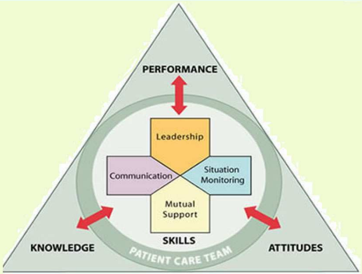
動画でセキュリティについて学ぶ

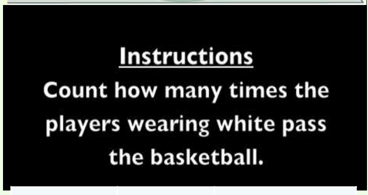
http://securityblog.jp/securie_challenge/campaign.html

Education, Training & Awareness

Teamwork & Anti-Teamwork

1. Training in the medical field, also effective for training of information security, "Team STEPPS" is one of them.
2. Knowledge of Human Error
3. The so-called "invisible gorilla" test had volunteers watching a video where two groups of people — some dressed in white, some in black — are passing basketballs around. The volunteers were asked to count the passes among players dressed in white while ignoring the passes of those in black.
   How people can focus so hard on something that they become blind to the unexpected, even when staring right at it. When one develops "inattentional blindness," as this effect is called, it becomes easy to miss details when one is not looking out for them.
   (http://www.theinvisiblegorilla.com/videos.html)
4. Ringelmann Effect (Anti-Teamwork)
   As shown right table, the additional effort of each rope pulling person declines as more rope pullers are added to the team.
   (The Free-Riding Problem in Research & Development Projects: http://pure.au.dk/portal-asb-student/files/39956847/master_thesis_daniel_levitan.pdf)



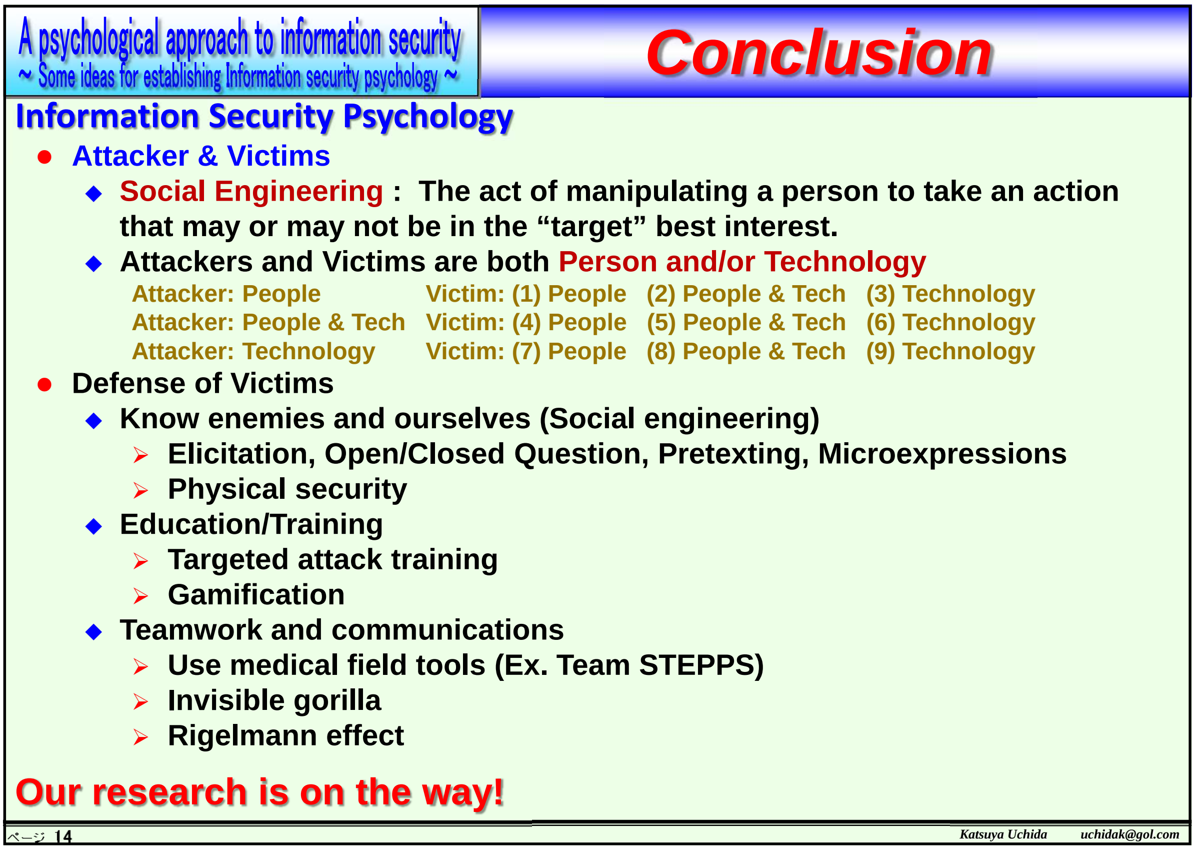


Instructions

Count how many times the players wearing white pass the basketball.

No. of rope pullers	Total weight	Av. Weight per rope puller
1	1.00	1.00
2	1.86	0.93
3	2.55	0.85
4	3.08	0.77
5	3.50	0.70
6	3.78	0.63
7	3.92	0.56
8	3.92	0.49

Ringelmann's rope-pulling experiment (1913)



Conclusion

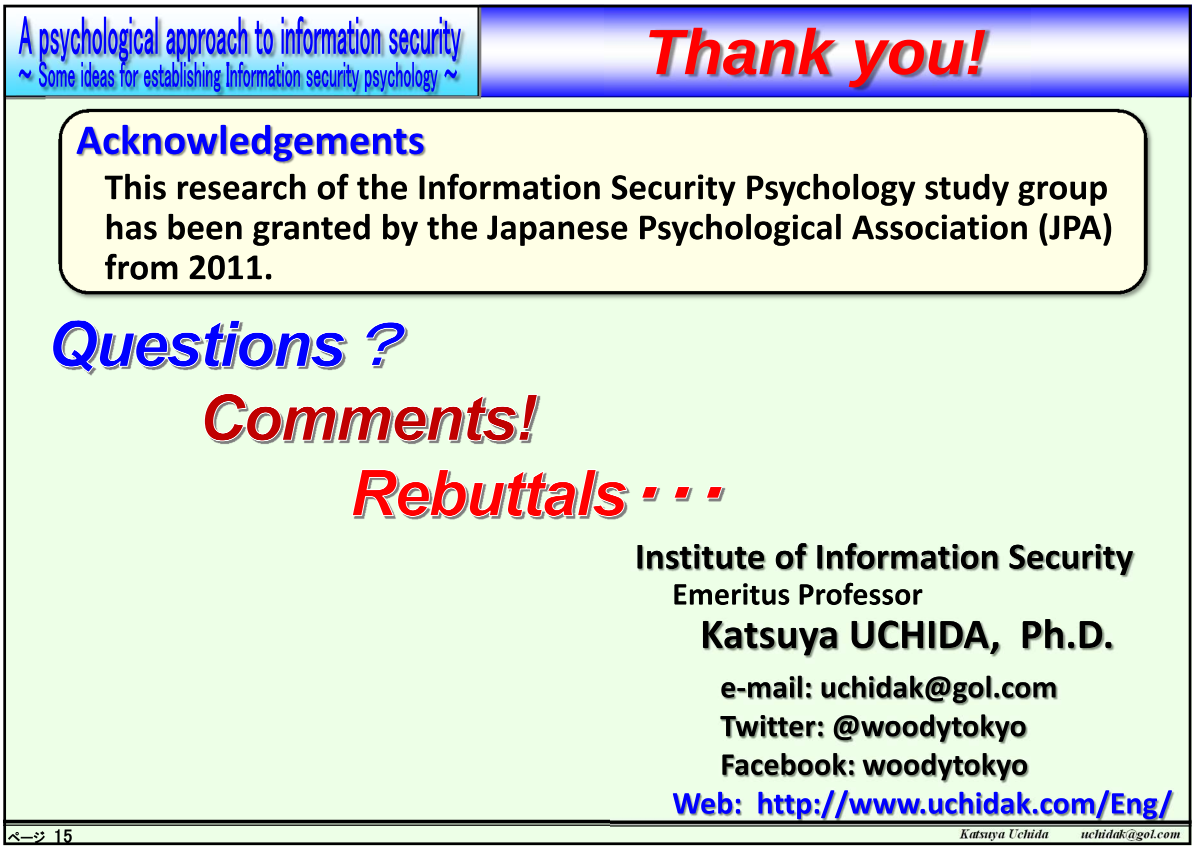
Information Security Psychology

- Attacker & Victims
  - Social Engineering : The act of manipulating a person to take an action that may or may not be in the "target" best interest.
  - Attackers and Victims are both Person and/or Technology

Attacker: People	Victim: (1) People	(2) People & Tech	(3) Technology
Attacker: People & Tech	Victim: (4) People	(5) People & Tech	(6) Technology
Attacker: Technology	Victim: (7) People	(8) People & Tech	(9) Technology

- Defense of Victims
  - Know enemies and ourselves (Social engineering)
    - Elicitation, Open/Closed Question, Pretexting, Microexpressions
    - Physical security
  - Education/Training
    - Targeted attack training
    - Gamification
  - Teamwork and communications
    - Use medical field tools (Ex. Team STEPPS)
    - Invisible gorilla
    - Rigelmann effect

Our research is on the way!



Thank you!

Acknowledgements

This research of the Information Security Psychology study group has been granted by the Japanese Psychological Association (JPA) from 2011.

Questions ?

Comments!

Rebuttals・・・

Institute of Information Security
Emeritus Professor
Katsuya UCHIDA, Ph.D.
e-mail: uchidak@gol.com
Twitter: @woodytokyo
Facebook: woodytokyo
Web: http://www.uchidak.com/Eng/