國立交通大學

資訊科學系

碩士論文

基於遊戲式學習之釣魚網站防範訓練模式

Game-Based Anti-Phishing Training

研究生：陳楷元

指導教授：曾憲雄　博士

　　　　　譚建民　博士

中華民國一百年十月

基於遊戲式學習之釣魚網站防範訓練模式
Game-Based Anti-Phishing Training

研究生：陳楷元　　Student：Kai-Yuan Chen

指導教授：曾憲雄　　Advisor：Dr. Shian-Shyong Tseng

譚建民　　Dr. Jimmy J.M. Tan

國立交通大學
資訊科學系
碩士論文

A Thesis
Submitted to Department of Computer and Information Science
College of Electrical Engineering and Computer Science
National Chiao Tung University
in partial Fulfillment of the Requirements
for the Degree of
Master
in

Computer and Information Science

June 2011

Hsinchu, Taiwan, Republic of China

中華民國一百年十月

基於遊戲式學習之釣魚網站防範訓練模式

學生：陳楷元　　　　　　　　　　　　　　指導教授：曾憲雄博士

譚建民博士

國立交通大學資訊科學與工程學系研究所碩士班

摘　要

根據 APWG 統計，釣魚網站的數量不斷在迅速增加，而釣魚網站的手法也不斷在更新，造成大眾財產的損失，即便有工具可以偵測釣魚網站，但是他們仍然會有誤判的機會。所以教會使用者如何防範釣魚網站是一件很重要的事。然而一般使用者對於傳統以文件主的教學沒有興趣也未必看得懂，所以可以利用遊戲的方式來教使用者防範釣魚，但是要將這些日新月異的釣魚手法加入遊戲式的教材非常曠日費時。在這篇研究中，我們利用專家系統的技術來跟釣魚網頁的專家擷取這些釣魚的知識，以及 WIKI 的方式讓大眾可以提供網頁的情境，最後利用推論引擎根據使用者的學習狀態以及擷取來的知識以及情境來產出適合使用者學習的教材。實驗結果顯示，我們所提出的方法跟傳統文件的教學可以提昇使用者的學習效率。

關鍵字：釣魚網頁、知識擷取、專家系統、遊戲式學習、自動產生題目、適性化學習

Game-Based Anti-Phishing Training

student：Kai-Yuan Chen　　**Advisors：Dr. Shian-Shyong Tseng**
Dr. Jimmy J.M. Tan

Institute of Computer Science and Endineering
National Chiao Tung University

ABSTRACT

APWG Statistics shows that phishing attack is increasing and causing enormous economic loss. However, existing phishing detection tools still suffer from false alarms and false negative. Educating user to defense phishing attack is important. Users do not have motivation for reading traditional document-based education materials. Therefore, several anti-phishing games have been proposed. These games are not sufficient for user to learn the phishing knowledge with limited learning case. We need to generate a large item bank of phishing cases. However, it is costly and time consuming to create phishing pages with the carious and reasonable scenario. We apply expert system approach to solve the issue. First, we implement a knowledge acquisition tool to gather phishing knowledge form multiple experts. Next, we provide adaptive education materials which are auto-generated for user. The experimental results show that students can make significant progress in identifying phishing page by using our approach.

Keywords: anti-phishing, knowledge acquisition, expert system, game-based learning, Game content generation, adaptive learning.

誌　謝

學過程中是在一生中難忘的回憶。本篇論文的完成，首先最要感謝我的指導教授，曾憲雄老師，老師總是犧牲自己的休息時間來指導我們並且不厭其煩的領導一步一步思考與探究；並從中學到研究的方法以及正確的思考邏輯並釐清我們的迷思概念。這是在碩士兩年的求學過程中，最寶貴的知識。此外，也要特別感謝我的共同指導教授，譚建民老師，在口試時給我很多寶貴的意見，同時也要感謝我的口試委員，黃國禎教授，袁賢銘教授，感謝你們許多寶貴的意見，讓這篇論文更有深度。

再來要感謝在此研究過程中，給予我許多鼓勵及建議的學長們，宗儒學長、瑞鋒學長以及衍旭學長，感謝你們的付出極大的耐心教導我讓我得以順利完成此篇論文。還要要感謝在 605 的學長姊：喚宇學長、怡利學姐、佳榕學姐，感謝你們的鼓勵以及教導讓我度過了研究的瓶頸。另外也要感謝實驗室的其他學長姊、哲青學長、莉玲學姐，謝謝你們曾經給過得意見和幫助。再來是我最親愛的同學們，佳玟、嘉凱，這兩年來我們一起互相扶持，這些回憶我會一輩子珍藏。

最後我要感謝我的家人及朋友們，感謝爸媽從小栽培與關心，因為有你們的付出才能有現在的我，也要感謝我的朋友們，在我低潮的時候陪伴在我身邊。

感謝所有經歷過的一切，無論是好是壞，都賦予我成長的力量，在此我獻上最誠摯的感謝

謝謝你們。

Table of Content

List of Figures

List of Tables

Chapter1 Introduction

Phishing attack has become the fastest growing scam on the Internet [1]. Phishers usually lure customers into giving their personal sensitive information by utilizing different mediums, such as email, spoofed websites and advertisements. Afterward, the sensitive information would be used for criminal purposes, and cause enormous economic loss [1]. Nowadays, phishing attacks become more and more complex and usually become compound strategies, in which users barely distinguish legitimate information from fake one [2].

Traditional strategies to protect users from phishing can be categorized into *silently eliminating the threat*, *warning users about the threat* and *training users not to fall for attacks* [3][4][5][6][7][8]. However, existing phishing detection tool still suffers from false alarms and false negatives. Educating users to identify suspicious emails and websites is quite important in defense of phishing [3].

Most anti-phishing education materials are presented as documental. Users do not have motivation for reading these documents, especially when surf website, network security is not their primary concern. Most users are unlikely to spend much time reading them [3]. The use of game-base learning increases both the motivation and the quality of the learning experience [9]. Therefore, several anti-phishing education games have been proposed [10][3]. However, existing anti-phishing education games train users the skills of detecting phishing with limited phishing cases. It is not sufficient for users to learn the phishing knowledge with limited learning cases.

To solve the issue, we need to generate a large item bank of phishing cases. However, it is costly and time consuming to create phishing pages with the various and reasonable scenarios. Therefore, how to automatically construct phishing pages is an important issue.

With our observation, the phishing pages are composed of the phishing attack techniques called Phishing Attack Knowledge and the Web page content information called Page Scenario.

For example, in Fig. 1, the phishing page “***http://www.yahO0.bid/…***” is composed of the Phishing Attack Knowledge “***(Replace ”o” by “0“)***” and the Page Scenario about legitimate page “***https://www.yahoo.bid/...***”. Different phishing knowledge or page scenario will lead the original case into new one. Therefore, the Adaptive Simulation Anti-phishing education game (ASAPEG) which systematically sort out the anti-phishing knowledge to generate large item bank for anti-phishing education game is proposed. In this game, we provide users a real-simulation environment for learning by doing, and provide adaptive learning for use learning anti-phishing in a short time.

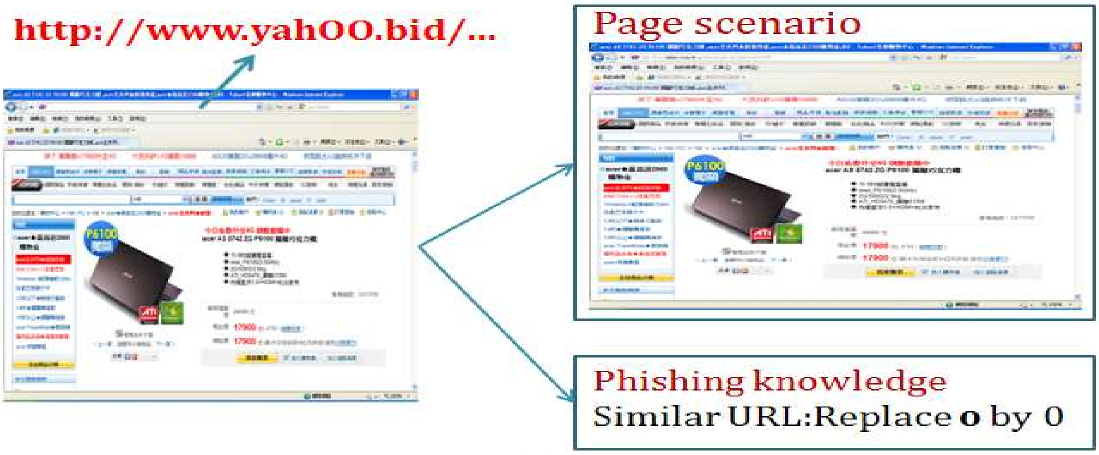


Figure 1. The Decomposition of Phishing Page

To acquire the phishing knowledge from domain experts, the improved multi-value repertory grids (MVRG) is proposed to integrate attributes of phishing cases from multi-experts. To extend phishing knowledge of multiple experts’ to obtain new phishing knowledge combinations, the Attribute Ordering Table (AOT) is applied to sort out the slots of page repository to provide more phishing cases.

From the defined model, the proposed Game Mission Generation Algorithm (GMGA) will generate great amount phishing pages by combining existing phishing knowledge and page scenarios. With large item bank of phishing cases, we can provide adaptive learning in ASAPEG.

In the experiment, the TMD-based satisfaction questionnaire is used to evaluate the degree of usage satisfaction of the proposed mission management system. In addition, pretests and posttests are used to evaluate students' performances after using ASAPEG. Several security experts and students are involved in the experiment. The evaluation results show that most of experts are satisfied with our proposed system, and student makes progress in identifying phishing page.

The remainder of this thesis is organized as follows. Chapter 2 discusses related works. In Chapter 3, the phishing knowledge acquisition is proposed using multi-value repertory grids integrating and knowledge combination approaches. In Chapter 4, the model of phishing knowledge and page scenario and game content generation approaches are presented. In Chapter 5, adaptive learning using ASAPEG system is proposed. In Chapter 6, the implementation and experiment of ASAPEG are discussed. In Chapter 7 the conclusion and future works are presented.

Chapter2 Related Work

In the chapter, we will introduce several different anti-phishing training material, and automatic game content generation.

2.1 Anti-Phishing Education

Education is a way to prevent phishing [11]. Existing anti-phishing educations can be classified into educational documents and education games. In the following sections, we will discuss existing anti-phishing education and the corresponding weaknesses.

2.1.1 Educational Documents

Documental education materials are the most popular form of anti-phishing education. Many e-commerce companies usually provide educational documents for educating their customers to avoid phishing attacks [12][13][14][15][16][17]. Phishing IQ Test (Mail Frontier) is a Web-based examination to evaluate whether users can identify legitimate email or not. Robila et al. [18] used Phishing IQ Test and class discussions to educate students.

However, some studies indicated that security educational materials are useless [19]. Another studies [20], is argued that Phishing IQ Test cannot measure susceptibility to phishing attacks directly. The primary reason is that user seldom actively and patiently learned these materials, which results in ineffective. In summary, users usually have low motivation of studying documental anti-phishing materials.

2.1.2 Educational Games

Games have the power of engaging people. They provide interaction, interactivity, problem solving, story and other elements that give the user involvement, structure, motivation and creativity, among other benefits [21] [22] [23][24]. A key factor is that games also provide outcomes and feedback in real-time [25]. Therefore, game-based learning supports the learning process by allowing players to acquire learning experiences in games

[26]. Several anti-phishing education games have been proposed for improving the learning motivation of users [27] [28] [29] [30]. However, without realistic simulation, non-simulation games may require students to be capable of applying anti-phishing knowledge in real environment. Moreover, these non-simulation games contain only general principles or limited phishing attacks knowledge (basic URL obfuscations). Compared to numerous advanced attack techniques, users may not observe these phishing features easily. For example, there is no visual difference between legitimate and phishing URLs when applying graph substitution attack utilizing a graph of legitimate URL to redirect users into phishing site.

Simulation games additionally provide good opportunities for procedural knowledge learning since learners can learn by doing in the simulation environment [31]. On the other hand, students make decisions, and see the results of those decisions [32]. However, it is costly and time consuming to update new phishing case in education material. Considering the changes of network security is extremely fast. Anti-phishing educational materials should be updated as quickly as possible to able to teach users new knowledge and to prevent themself suffering new threats. That issue of game-base anti-phishing is how to automatically generate phishing cases.

2.2 Automatic Game Content Generation

Deane, P., et. al. proposed a natural language generation approach for automatic general verbal items , which can automatic generate verbal content according to concept [33]. They defined an arithmetic word problem consisting of generic concepts, for example, the “distance-rate-time” word problem consists of generic concepts like VEHICLE, MOVE, DISTANCE, RATE, or TIME. The natural language generation system can generate arithmetic word problem described by different generic concepts.

Zualkernan, et. al. proposed an automatic generation of online assessments which is used to judge a software engineer’s comprehension artifacts representing software designs [34].

Activity diagrams are a type of model commonly used in software design, which captures control flow in a situation. Bloom's taxonomy-based question generating assessments for each level consists of a number of questions from each level of understanding. The questions about the misunderstood are commonly occurring differences between the activity diagrams. This research uses the Hazard Operators (HAZOP) [35] to generate multiple choice questions which classed misunderstandings to assess their understanding of activity model.

Branko [36] used Web Ontology Language (OWL) to build a dynamic test generation system which use templates and algorithms for dynamical generation of questions. In OWL, every concept consists of specific elements. The reasoning algorithm will determine which templates match the specific elements, and choose these templates to generate multiple choice questions. This ontology-based test generating approach can be applied to different domain. However it is time-consuming to construct an OWL.

In previous researches, the fixed question templates are not appropriate for generating phishing pages with different page scenarios and phishing attack knowledge. Moreover, it is necessary to embed the scenarios in web page to test whether users can apply phishing attack knowledge to real environment. But the previous researches did not take question scenarios into consideration. Thus, the issue to automatically generate game content is how to extend items to generate new phishing pages.

2.3 Adaptive Education

The term adaptive is defined as a capability to change when necessary in order to deal with different situations [37]. Adaptive learning (AL) is considered to be an alternative to the traditional ''one size fits all'' approach and has encouraged the development of teaching and learning towards a dynamic learning process for learning [37].

Most of researchers have suggested that four main approaches can be identified to present all adaptive e-learning systems: macro-adaptive, aptitude-treatment, micro-adaptive and constructivist-collaborative approaches [37]. Macro-adaptive approach selects courses according to characteristics of learners such as learning preferences, prior knowledge and experience. Aptitude-treatment interaction approach suggests different types of instructions and/or different types of media for different students [37]. In Micro-adaptive approach, it requires monitoring the learning behavior of the student while running tasks and adapting the instructional design afterwards, based on quantitative information [37]. Constructivist-collaborative approach focuses on how the student actually learns while sharing her/his knowledge and activities with others.

Computer adaptive testing requires a large item pool for each area of content domain to be developed, with sufficient numbers, variety and spread of difficulty [38]. It is important to establish large item bank of test item efficiently.

Chapter 3 Phishing Page Model

Science phishing attacks change with each passing day, it is important to build new generated phishing case in simulation game in a short time and teach user efficiently and effectively. Thus, we want to automatic generate simulation game content for an adaptive anti-phishing game. However, without good model of phishing case, it's difficult to reach the goal.

As mentioned above, we want to educate user anti-phishing knowledge. We need to systemically describe classification of phishing attack. Thus, we need to acquire phishing knowledge from experts. In our observation from phishing attack, phishing attack can be described by attributes. How to acquire attributes of phishing knowledge from experts is necessary. Thus, we use repertory grid to acquire phishing attack attributes from users [39].

3.1 Phishing Knowledge Acquisitions

Researchers have indicated the need to develop learning guidance mechanisms or tools for assisting students to learn in such a complex learning scenario[40], and many knowledge acquisition methodologies have been proposed to help knowledge engineers acquire the useful knowledge and then to transfer this knowledge into a knowledge base or other computerized representation forms [41] [42][43][44].

The goal of anti-phishing education is to teach user classify phishing attack. We use repertory grid to classify knowledge which will be used to teach user anti-phishing.

At First, we use repertory grid with multi-representation to acquire attributes from experts. We apply knowledge acquisition from multiple expert approaches to acquire knowledge from experts shown in Figure 2. First we need to acquire knowledge from experts, we asks expert to fill the phishing knowledge repertory grid. Next we apply knowledge acquisition from multiple expert approaches to shrink synonyms attribute row by row and integrate multiple repertory grids. According to the structure of the integrated grid, the AOT which describes importance of each attribute to object is constructed. Expert will fill their own AOT. With the AOT table, we propose a Phishing Knowledge Combination Method (PKCM) to derive more phishing knowledge and construct phishing knowledge hierarchy.

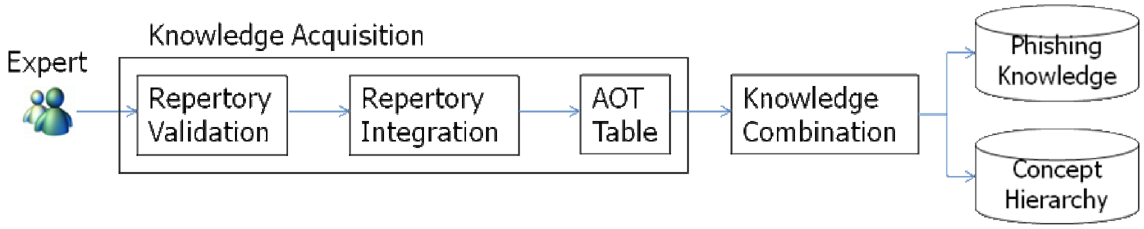
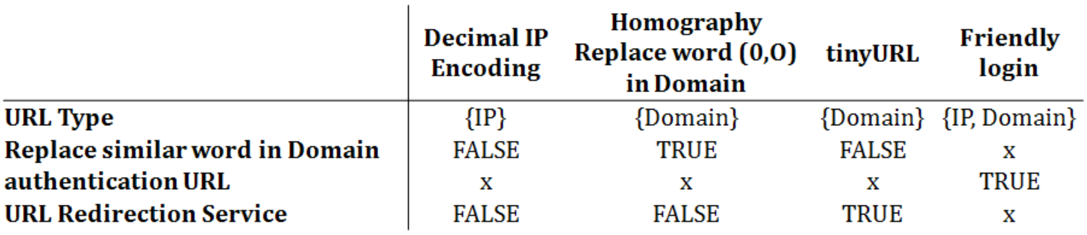


Figure 2. Knowledge Acquisition

To support the phishing knowledge acquisition, the multi-datatype repertory grid is applied [45].

As shown in Figure 3, a grid with such a representation is called an acquisition table, there are four phishing attack knowledge. The attack “Decimal IP Encoding” is a phishing attack which use phishing IP to spoof user, for example, this attack uses “81.174.70.14” to spoof user. The attack “Homography Replace word (0,o) in Domain” replaces substring “o” in URL domain name with its similar word “0” to spoof user, for example, attacker registers domain name “http://www.yah00.com” which is similar to “http://www.yah00.com”. ”TinyURL” is the phishing attack that use redirection service to hide phishing URL, for example, the address “http://tinyurl.com/5w4llmw” which will be redirected to phishing web site “http://www.phishingsite.com”. ”Friendly Login” use URL’s that can include authentication information such as “http://www.yahoo:com@phishingsite.com”, however, the destination website is “http: //www.phishingsite.com”. Assume that experts give the following attributes to distinguish the phishing knowledge. “URL Type” means the type phishing URL, for example, the URL type of “http://140.113.167.118” is IP. “Replace similar word in Domain” means phishing attack will replace “o” with “0”. “Authentication URL” means the URL includes authentication information such as a login name and password. In general the format is “URI://**username:password@hostname**/path” [**46**]. “URL Redirection Service” means phishing attack uses redirection service to spoof user.



	Decimal IP Encoding	Homography Replace word (0,O) in Domain	tinyURL	Friendly login
URL Type	{IP}	{Domain}	{Domain}	{IP, Domain}
Replace similar word in Domain	FALSE	TRUE	FALSE	x
authentication URL	x	x	x	TRUE
URL Redirection Service	FALSE	FALSE	TRUE	x

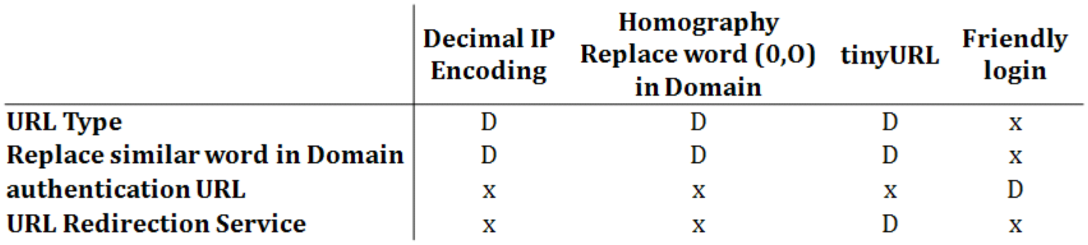
Figure 3. An example of SKCRG

The data types used for describing the attributes of phishing knowledge patterns are shown in Table 1.

Table 1. Date Type of Multi-Data Type Repertory Grid

- **Bool** : True or false
- **Set of Value** : A set of intersection symbols
- **Single of Value** : A symbols, an integer or a real number
- **Range of Value** : An integer or a real with rating

The Attribute Ordering Table (AOT) is provided to record the importance of each attribute to object [45]. The value of each entry is labeled ‘X’, ’D’ or an integer number. ‘X’ means the attribute has no relationship with the object. ‘D’ means that the attribute dominates the object. An integer means the degree of importance for the attribute to the object. An example of AOT of Figure 4 is shown in Figure 5. Experts are asked to fill an AOT table according to repertory grid in Figure 4.



	Decimal IP Encoding	Homography Replace word (0,0) in Domain	tinyURL	Friendly login
URL Type	D	D	D	x
Replace similar word in Domain	D	D	D	x
authentication URL	x	x	x	D
URL Redirection Service	x	x	D	x

Figure 4. An example of AOT

3.2 Integrating Knowledge from Multiple Experts

3.2.1 Introduction of Integrating Knowledge from Multiple Experts

The construction of a reliable knowledge-based system usually requires the cooperation of several domain experts. The knowledge base integrated from several experts is usually more abundant and objective than that derived from single expert [45]. There are possible situations of integrating knowledge from experts such as consensus, conflict, correspond and contrast [45]. Huang purposed methods to integrate knowledge, called KAME (Knowledge acquisition from multiple expert), and to integrate Attribute Ordering Table (AOT), called AOTI(AOT Integration), form multiple experts [45]. The corresponding KAME procedure and AOTI procedure are listed below. The flowchart of integrating knowledge from multiple is shown in Figure 5

Knowledge Acquisition from Multiple Experts Procedure (KAME)

Input : Repertory Grid G_1,G_2,…,G_n

Output : Integrated Repertory Grid G

Step1 Acquire phishing knowledge form experts: Apply multi-type repertory grid-method to derive the initial knowledge from a group of experts individual [45]

Step2 Invoke **Grid Row Validation Procedure**

Step3 Invoke **Knowledge Integration Procedure**

Step4 Invoke **Grid Row Validation Procedure**

Attribute Ordering Table Integration Procedure (AOTI)

Input : Attribute Ordering Table T_1,T_2,…,T_n

Output : Integrated Attribute Ordering Table T

Step1 Elicit AOTs: According to the structure of final multi-type repertory grid in KAME, the AOT is constructed. Experts are asked to fill their own AOT [45]

Step2 Integrate AOTs

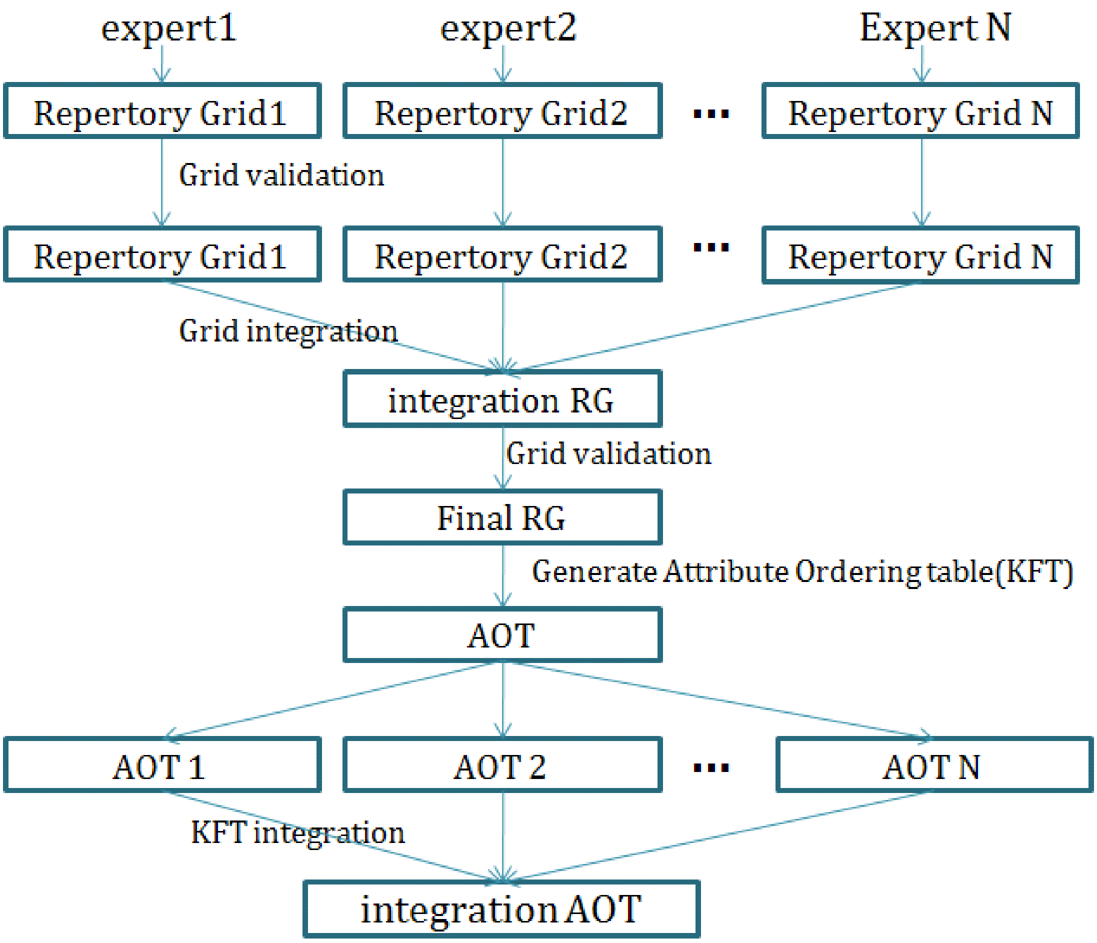


Figure 5. Integration of repertory grid and AOT

However, in KAME, they do not consider multi-type repertory grid. Thus, we further extend KAME to integrate multi-type repertory grid by extending Repertory Grid Validation Procedure. The details of this extension are provided in the following section.

3.2.2 Multi-type Repertory Grid Validation

Multi-type Repertory Grid Validation validates the initial grid by shrinking synonymous. Synonyms of attribute may exist in the grid originally elicited from experts or the integrated grid, and can be discovered by using a similarity analysis.

Before discussing the rest steps of Synthesis Knowledge Capturing Repertory Grid Validation, the details of similarity analysis and the algorithm of grid validation are introduced.

For any given attribute, the associated values of the grid may be regarded as a vector of values. The vector a=[a_1,a_2,…,a_n] and b=[b_1,b_2,…,b_n] representing two attributes. There are different similarity formulas to calculate the different data type of value between them, and the formulas are defined as follows. In Formula 1 we want to determine whether two vectors have different unit. In Formula 2 we want to measure distance of two integer vectors. In Formula 3 we want to determine whether two enumerations represent the same unit with different symbols. In Formula 4, we want to determine whether two sets represent the same unit with different symbols. In Formula 5, we want to measure similarity of two bool vectors. In Formula 6, we want to measure distance of two real vectors. In Formulas 7 and 8, we want to measure slope of two vectors.

Formula 1: Correlation coefficient Feature similarity (CCSIM)

CCSIM(x ,y)=Correlation coefficient r of x and y

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{(n-1)s_x s_y} = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2 \sum_{i=1}^{n}(y_i-\bar{y})^2}},$$

Where $\bar{x}$ and $\bar{y}$ are the sample means of *X* and *Y*, and s_x and s_y are the sample standard deviations of *X* and *Y*.

Formula2: Integer similarity (INTSIM)

INTSIM (a ,b)=$|a_1-b_1|$ +$|a_2-b_2|$+$|a_3-b_3|$+...+$|a_n-b_n|$

Formula3: Enumeration similarity (ESIM)

$$\mathrm{ESIM}(a,\ b) = \min_{p} \sum I(ai\ ,bi\ ) \begin{cases} 0 \text{ if } ai=bi \\ 1 \text{ if } ai\neq bi \end{cases}$$

Formula4: Set similarity (SSIM)

$$\mathrm{SSIM}(a\,,b)=\sum\frac{|ai\cup bi|-|ai\cap bi|}{|ai\cup bi|}$$

Formula5: bool similarity(BSIM)

If ai=bi for each i THEN BSIM (a ,b)=1

ELSE If there exists i such that ai≠bi THEN BSIM (a, b) =0

Formula6: Real similarity(RSIM)RSIM (a ,b)=$|a_1-b_1|$ +$|a_2-b_2|$+$|a_3-b_3|$+…..+$|a_n-b_n|$

Formula7: cos similarity(COSSIM)

$$\mathrm{COSSIM}(a,b)=\frac{a\bullet b}{|a||b|}$$

Formula8: Attribute relation(AR)

IF the vector a=[a_1,a_2,…,a_n]

Vector AR(a)=[a_1-a_2, a_2-a_3 ,…, a_{n-1} -a_n]

Based on the above similarity functions, we propose an enhanced grid row validation procedure to validate multi-type repertory grid. The proposed enhanced grid row validation procedure is listed below:

Enhanced Grid Row Validation Procedure

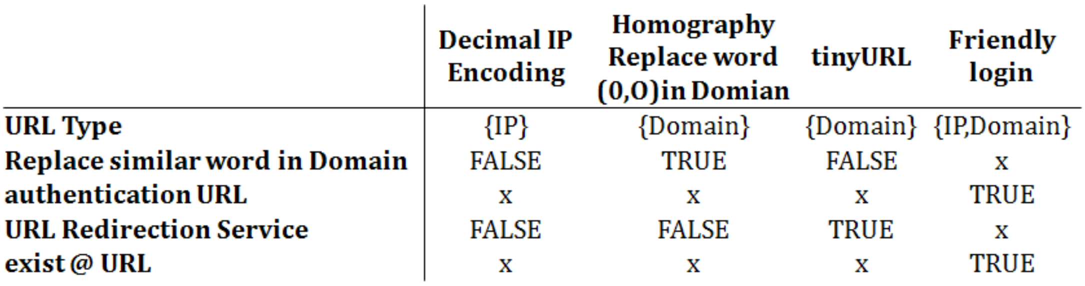
Input : A initial multi type repertory grid G

Output : A validated version of grid G

```
Step1: For each two vectors a,b with the same data type
        1.1 IF data type is Boolean
              IF BSIM(a,b)=1 THEN SHRINK ROWS
        1.2 IF data type is rating value
              IF COSSIM(a,b)>Threshold AND COSSIM(AR(a),AR(b)) THEN SHRINK ROWS
              ELSE IF CCSIM(x ,y)> Threshold    THEN SHRINK ROWS
        1.3 IF data type is non rating value
              IF ESIM(a,b)<threshold THEN SHRINK ROWS
        1.4 IF data type is enumeration
              IF ESIM(a,b)<threshold THEN SHRINK ROWS
        1.5 IF data type is Set
              IF SSIM(a,b) < threshold THEN SHRINK ROWS
Step2: Return A validated version of grid G
```

Example 1: A multi-type repertory grid validation example

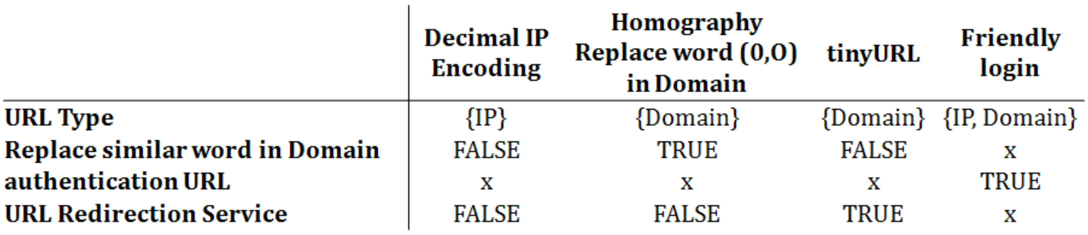
As shown in Figure 6, there are six attributes and four phishing attacks in the repertory grid.



	Decimal IP Encoding	Homography Replace word (0,O)in Domian	tinyURL	Friendly login
URL Type	{IP}	{Domain}	{Domain}	{IP,Domain}
Replace similar word in Domain	FALSE	TRUE	FALSE	x
authentication URL	x	x	x	TRUE
URL Redirection Service	FALSE	FALSE	TRUE	x
exist @ URL	x	x	x	TRUE

Figure 6. SKCRG before validation

At first, the corresponding vectors a and b of two Boolean attribute*s* ***"authentication URL " and "URL exist @"*** can be represented by ***a=(x,x,x,TRUE)*** and ***b=(x,x,x,TRUE)***, respectively. Since BSIM(a,b)=1, we can treat these two attributes as synonymous attributes and then shrink these two attributes. The resulting repertory grid is shown in Figure 7.



	Decimal IP Encoding	Homography Replace word (0,O) in Domain	tinyURL	Friendly login
URL Type	{IP}	{Domain}	{Domain}	{IP, Domain}
Replace similar word in Domain	FALSE	TRUE	FALSE	x
authentication URL	x	x	x	TRUE
URL Redirection Service	FALSE	FALSE	TRUE	x

Figure 7. SKCRG after validation

3.2.3 Integrating multiple multi-type repertory Grid from Multiple Experts

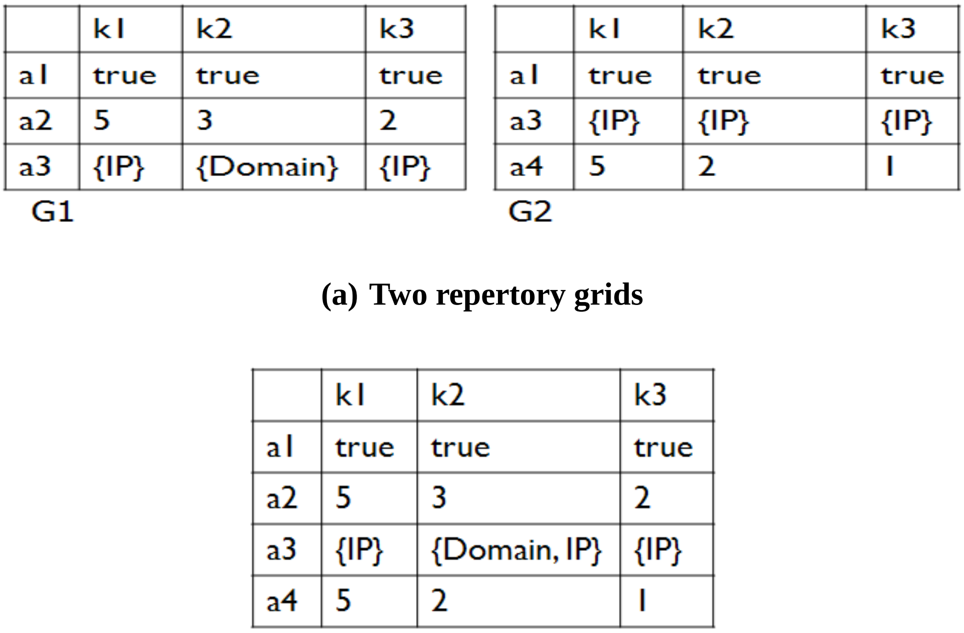
In this section, we extend Huang's Knowledge Integration Procedure [45] to support multi-type repertory grid. To integrate knowledge from expert, we assume that all experts are of equal importance. The proposed enhanced knowledge integration procedure is listed below.

```
Enhanced Knowledge Integration Procedure

Input : Repertory grids, $G_1$,$G_2$,…,$G_N$
Output : An integrated repertory grid G

Step1: For each attribute with the same data type in more than two grids
        1.1  If each attribute has the same value THEN shrink
        1.2  If each attribute has different value THEN Invoke Conflict Handler
Step2: For the attribute appear in only one grid
        2.1 Copy the attribute together with its value to integrated grid.
```

Figure 8.(a) shows two repertory grids G1 and G2. First, Enhanced Knowledge Integration Procedure check that the (a1,k1) entries of both girds have the same type, and the new value of (a1,k1) entry is set as true. Since the (a3,k2) entries are conflict, the new value of the (a3,k2) entry is set as {IP, Domain} by Conflict Handler. Figure 8.(b) shows the resulting repertory grid after Enhanced Knowledge Integration Procedure.



	k1	k2	k3
a1	true	true	true
a2	5	3	2
a3	{IP}	{Domain}	{IP}

G1

	k1	k2	k3
a1	true	true	true
a3	{IP}	{IP}	{IP}
a4	5	2	1

G2

(a) Two repertory grids

	k1	k2	k3
a1	true	true	true
a2	5	3	2
a3	{IP}	{Domain, IP}	{IP}
a4	5	2	1

(b) Integrated repertory grid

Figure 8. Illustration for Enhanced Knowledge Integration Procedure

After we integrate repertory grid from multiple user, we apply further IAOT [45] to acquire integrated AOT from multiple expert. Modern phishing attacks usually are compounded with different phishing attack techniques. Based on this observation, we further propose a Phishing Knowledge Combination Method in the next Section.

3.3Phishing Knowledge Combinations

To provide adaptive learning, it is necessary to build a large item bank of phishing case. To achieve this goal, we observe phishing knowledge can combine each other. And we need to represent the relations between phishing knowledge. Thus, we propose **Phishing Knowledge Combination Method (PKCM) by extending KAME**. The proposed Phishing Knowledge Acquisition Algorithm involving Knowledge Acquisition from Multiple Experts (KAME), Attribute Ordering Table Integration (AOTI) and PKCM is listed below.

```
Phishing Knowledge Acquisition Algorithm
Input : Phishing Attack $K=\{ K_1,K_2,\ldots,K_n\}$
Output : Game Content
Step 1: Knowledge Acquisition from Multiple Experts Procedure (KAME)
    Step1.1 Acquire phishing knowledge form experts by using multi-datatype repertory grid
    Step1.2 Invoke Grid Row Validation Procedure to Validation multi-datatype repertory grid
    Step1.3 Invoke Knowledge Integration Procedure to Integration multi-datatype repertory grid
    Step1.4 Invoke Grid Row Validation Procedure to Integrated repertory grid
Step 2: Attribute Ordering Table Integration Procedure (AOTI)
    Step1.1 Elicit of AOT
    Step1.2 Integrate of AOT
Step 3:Invoke Knowledge Combination Procedure to Combine Phishing Knowledge
Step 4:Invoke Column Analysis Procedure to construct concept hierarchy
```

The combined phishing knowledge can become more complicated than original phishing because the combined phishing knowledge emerges features from original phishing knowledge. For example in Figure 9, phishing attacks “third party” and “friendly login” can be combined into new phishing knowledge which emerges the feature of “third party” and “friendly login”.

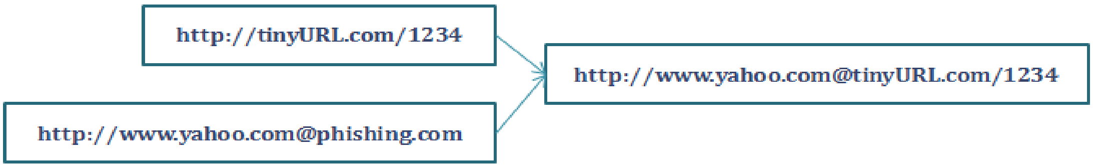
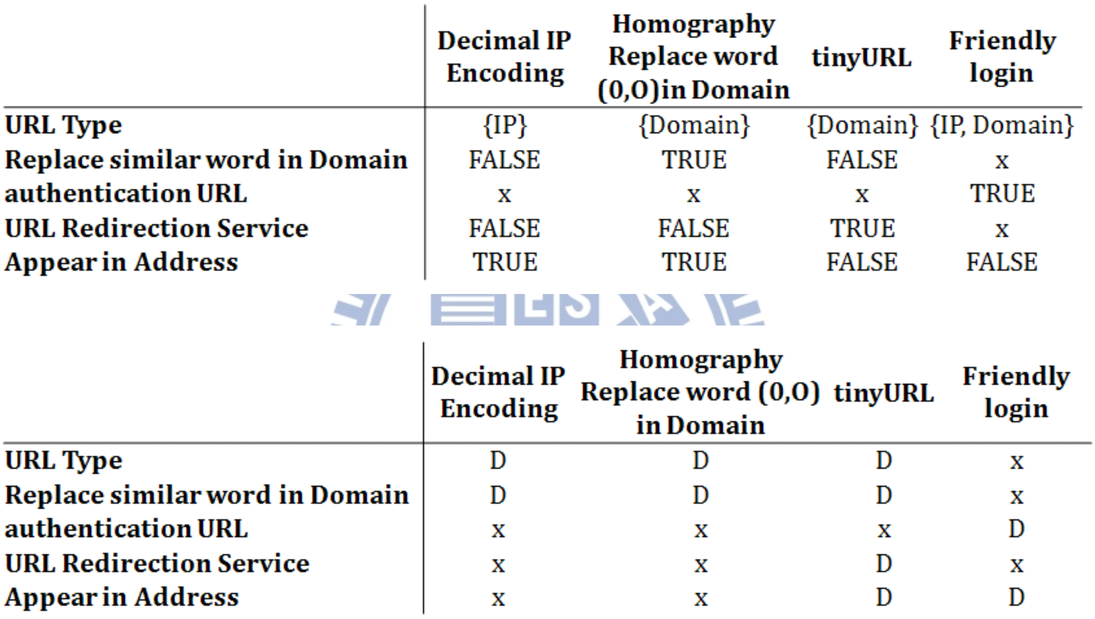

http://tinyURL.com/1234
http://www.yahoo.com@phishing.com
http://www.yahoo.com@tinyURL.com/1234

Figure 9. Combining two phishing attacks

To achieve our goal, we employ AOT which records the attribute which is dominating phishing knowledge. An example of integrated AOT and integrated repertory grid of phishing attacks is shown in Figure 10.



	Decimal IP Encoding	Homography Replace word (0,O)in Domain	tinyURL	Friendly login
URL Type	{IP}	{Domain}	{Domain}	{IP, Domain}
Replace similar word in Domain	FALSE	TRUE	FALSE	x
authentication URL	x	x	x	TRUE
URL Redirection Service	FALSE	FALSE	TRUE	x
Appear in Address	TRUE	TRUE	FALSE	FALSE

	Decimal IP Encoding	Homography Replace word (0,O) in Domain	tinyURL	Friendly login
URL Type	D	D	D	x
Replace similar word in Domain	D	D	D	x
authentication URL	x	x	x	D
URL Redirection Service	x	x	D	x
Appear in Address	x	x	D	D

Figure 10. An example of integrated AOT and integrated repertory grid

To combine the phishing knowledge, we propose knowledge combination algorithm (KCA) according to phishing knowledge repertory grid and knowledge combination table. According to AOT, knowledge combination algorithm will determine whether the knowledge is conflict or not.

Knowledge Combination Procedure

Input : Column AOT K={K1,K2,…,Kn}

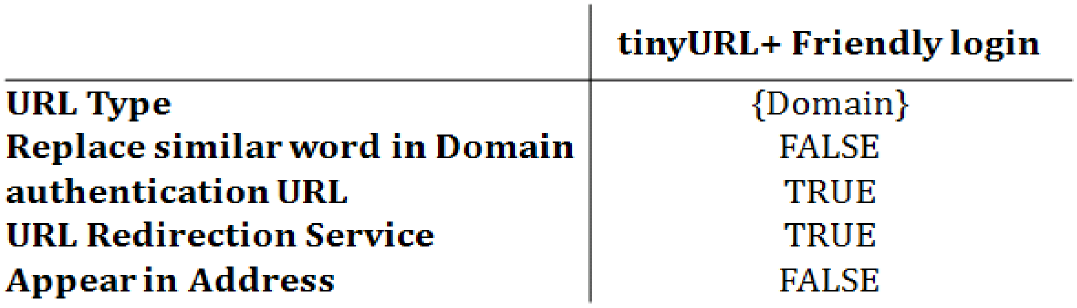
Corresponding column in repertory grid R={c1,c2,…,cn}

C(R) is number of attribute in R

Output : New repertory grid column r’

```
Step1:For each m column Ki1,Ki2,….,Kim in AOT K
    Step 1.1 check Kii,j,Ki2,j,…Kim,j
        If |{Kit,j=D|t=1,….m}|≧2 AND (Cfj=Cf’j if Kfj=Kfj=D)
            Combine(Cii,j,Ci2,j,…Cim,j)
        ELSE Repeat Step 1
    Step 1.2 check Kii,j,Ki2,j,…Kim,j If |{Kit,j=D|t=1,….m}|=1
        Combine(Cii,j,Ci2,j,…Cim,j)
    Step 1.3 check Kii,j,Ki2,j,…Kim,j If |{Kit,j=D|t=1,….m}|=0
        Combine(Cii,j,Ci2,j,…Cim,j)
    Step 1.4 j=j+1 Repeat Step 1.1, UNTIL J>C(R)
Step 2: Repeat step1
```

For example, we use **Knowledge Combination Procedure** to synthesize phishing knowledge “tiny URL” and “Friendly login” in Figure 9 by AOT shown in Figure 11. According to AOT, the attribute “Appear in Address” is necessary for both “tiny URL” and “Friendly login”, then check their corresponding value in SKCRG whether the values in entries [tiny URL, Appear in Address] and [Friendly login, Appear in Address] are the same. Thus, there is no conflict in this necessary attribute. We check the necessary attribute each other. If there is no conflict, we can combine knowledge “tiny URL” and “Friendly login” into a new knowledge shown in Figure 11.



	tinyURL+ Friendly login
URL Type	{Domain}
Replace similar word in Domain	FALSE
authentication URL	TRUE
URL Redirection Service	TRUE
Appear in Address	FALSE

Figure 11. A new knowledge obtained by combining “tinyURL” and “Friendly login”

On the contrary, according to AOT, the attribute “URL Type” is necessary for both “Decimal IP Encoding” and “Homography”, then check their corresponding value in SKCRG whether the value in entry [Decimal IP Encoding, URL Type] and [Homography, URL Type] are different. Thus, “Decimal IP Encoding” and “Homography” cannot be combined because of incompatibility.

3.4 Concept Hierarchy Creation

The concept hierarchy describes relation between the concept and its sub-concept. With the concept hierarchy, we can adjust the training level according to user learning situation. For example, if user is positive in learning anti-phishing, we can choose more detailed phishing knowledge for user to learn. Otherwise, we just choose high level for user to learning. Using adaptive learning to shorten learning period, we do not teach each case of anti-phishing. Comparatively, we adaptively teach user anti-phishing by a diagram showing the relationships among concepts. To build concept map, we use hierarchy clustering to analyze knowledge of repertory grid by calculating the similarity between knowledge in **Column Analysis Procedure**.

```
Column Analysis Procedure

Input : Phishing Repertory Grid column Vector Set
        C={Vi | Vi is<a1,a2,…,ai> where ai is attribute }
Output : Relation vector

Step1: Find the two cloumes $c_i$,$c_j$   with the largest number of same element
    Step1.1 Merge $c_i$ and cj   into a new attack called {$c_{i,}c_j$}
    Step1.2 Remove $c_i$ ,$c_j$ from C
    Step1.3 Add {$c_i$,$c_j$} into C
    Step1.4 If all objects are in one cluster, return the cluster. Else, go to step 1
```

For the Example given a repertory grid in Figure 12, Column Analysis Algorithm is performed as follows:

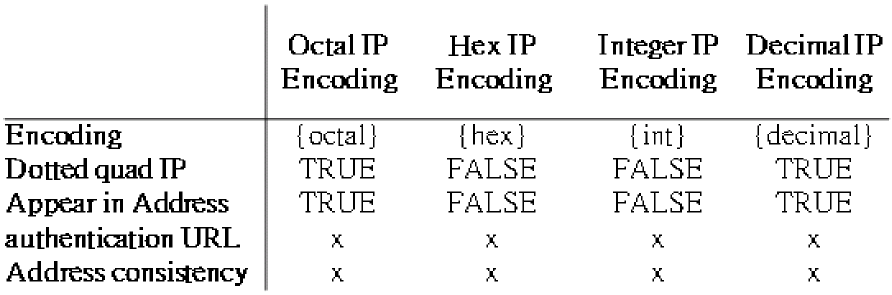
1. Initial C= {Decimal IP Encode, Octal IP Encode, Hex IP Encode , Int IP Encode} Where

    Decimal IP Encode= ({decimal}, TRUE, TRUE, x, x)

    Octal IP Encode= ({octal}, TRUE, TRUE, x, x)

    Hex IP Encode= ({hex}, FALSE, FALSE, x, x)

    Integer IP Encode= ({int}, FALSE, F, x, x)



	Octal IP Encoding	Hex IP Encoding	Integer IP Encoding	Decimal IP Encoding
Encoding	{octal}	{hex}	{int}	{decimal}
Dotted quad IP	TRUE	FALSE	FALSE	TRUE
Appear in Address	TRUE	FALSE	FALSE	TRUE
authentication URL	x	x	x	x
Address consistency	x	x	x	x

Figure 12. An example of phishing repertory grid

2. Octal IP Encode and Decimal IP Encode has largest number of same value
3. Add {Decimal IP Encode, Octal IP Encode} in C
4. Delete Decimal IP Encode, Octal IP Encode in C

5. C= {{Decimal IP Encode ,Octal IP Encode}, Hex IP Encode , Int IP Encode }

The resulting hierarchy in this round is shown in Figure 13.

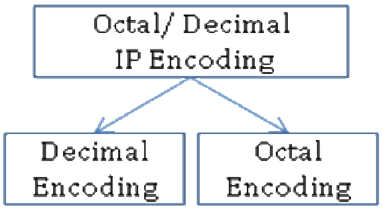


Figure 13. An example of hierarchy

Chapter 4 Automatic Game Content Generation

In this chapter, we introduce automatic game content generation by the instantiation properties of knowledge frame model and page repository.

4.1 Phishing Page Representations

We observe that Phishing page is with two components, phishing knowledge and page scenario. Phishing knowledge stands for the attack techniques which phishers use in spoofing user. Page scenario connects attack techniques and real situations. From the above observation, our idea is to decompose the phishing page into page scenario and phishing knowledge. With different phishing knowledge and page scenario will lead the original case into new one. Figure 14 shows a simple example. A spoofed yahoo page with the phishing URL "http:// www.yahO0.com.tw", we can decompose this phishing page into phishing knowledge and page scenario. The page scenario is yahoo, and this phishing attack technique is using the strategy to replace "o" in original URL with its similar word "0". Finally, we can compose this phishing attack technique and another page scenario such as pchome into a new phishing page.

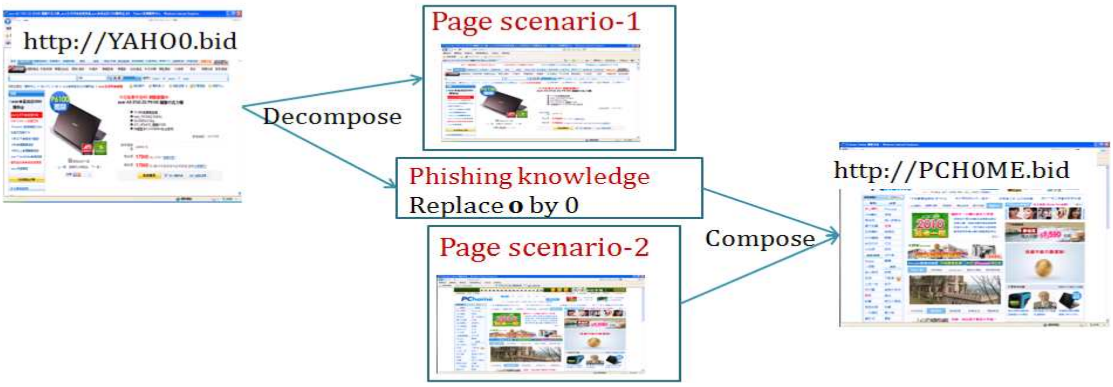
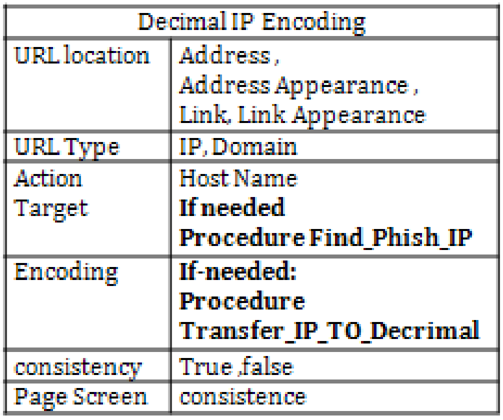


Figure 14. The Decomposition and Generation of a Phishing Page

Phishing page representations including phishing knowledge representation and page repertory are essential of generating phishing page automatically. A well-defined page repertory can support wiki-based platform of collecting page scenarios. In the next two sections, we first introduce our phishing knowledge representation and then page repertory.

4.1.1 Phishing Knowledge Frame

As mentioned before, we want to generate phishing pages by composing phishing knowledge and page scenario. The phishing attributes acquired from experts via repertory grid are stereotyped. Therefore, frame model can be applied to knowledge structure of phishing attack knowledge. Figure 15 shows the slot attributes of phishing attack knowledge frame (PAKF) which is a “Decimal IP Encoding” frame. This attack converts the hostname of URL into Decimal IP representation to cheat users.



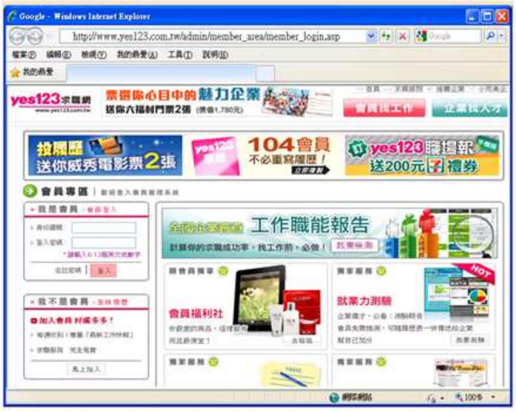
Decimal IP Encoding	
URL location	Address , Address Appearance , Link, Link Appearance
URL Type	IP, Domain
Action Target	Host Name **If needed** **Procedure Find_Phish_IP**
Encoding	**If-needed:** **Procedure** **Transfer_IP_TO_Decrimal**
consistency	True ,false
Page Screen	consistence

Figure 15. An example of PAKF

Besides, the inheritance and instantiation properties of our proposed frame-based knowledge representation can further extend the original phishing pages to new one. Inheritance properties including single inheritance and multiple inheritance properties can be used to generate new phishing attack knowledge. Instantiation property can be used to apply phishing attack knowledge to different scenario; thus a large amount of phishing pages can be generated.

4.1.2 Page repository

The goal of anti-phishing education game is to develop the users’ skill of distinguishing phishing pages in real world. Hence, phishing page model should be represented by features which user can easily observe. Page Scenario Repository (PSR) is proposed for representing phishing features according to the phishing features from expert by SKCRG. Figure 16 shows an example PSR of the homepage of yes123. The screen shot of this page is stored in the "Page content" slot by yes123.jpg. "Address" and "Address appearance" record the actual address of this page and the corresponding visual information. The embedded hyperlinks information is also stored in "Link type", "Link Target", "Link Appearance", "Link Location" and "Link Flag".


Google - Windows Internet Explorer
http://www.yes123.com.tw/admin/member_area/member_login.asp
yes123求職網
票選你心目中的魅力企業
送你六福村門票2張
104會員 不必重寫履歷！
yes123職場報 送200元 7 禮券
會員專區
工作職能報告
會員福利社
就業力測驗
HOT

Slot name	Slot value
Game	"yes123"
Media	"IE8"
Page content	"yes123.jpg"
Address	"https://www.yes123.com"
Address Appearance	"https://www.yes123.com"
Address Flag	2.2
Link Type	"string"
Link Target	"https://www.yes123.com/ login.php"
Link location	(100,100,200,200)
Link Appearance	"會員專區"
Link Flag	2.2

Figure 16. An example PSR of yes123

PSG can describe a network topology which is a serial behavior of user. It is important to simulate users' daily experiences. For example, if a user wants to search available job positions in "yes123", then he/she can either search yes123 by Google or check mail send from "yes123" in Gmail to achieve the URL of "yes123". Figure 17 shows this simple scenario. There are three pages in this scenario, "Google", "Gmail", and "yes123homepage" and two hyperlinks including one from "Google" to "yes123" and the other from "Gmail" to "yes123".

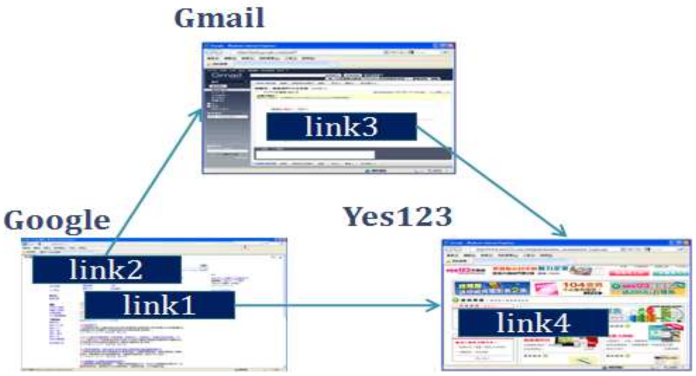


Figure 17. An example scenario of “Find Job”

For a real-simulation game, a reasonable scenario (game mission) is essential. Compared to game content generation, it requires generating a set of game contents with certain dependences among them. In the next section, we will introduce our game mission generation algorithm.

4.2 Game Mission Generation

With the PAKF and PSR, we propose game mission generation algorithm to support adaptive real-simulation anti-phishing education game. For simulating users' daily experiences, there are several constraints in generating game mission.

Constraint 1:

According to real environment situation, the target of link address is equal to the target web page. Thus, if a link is changed to a phishing link then the target page of link must be changed to phishing page.

Constraint 2:

There must be a phishing feature in the phishing page. Thus, if a page is changed to phishing page then one of features in this page must be changed to phishing one.

In ASAPEG, we simulate user behavior when browsing a serial web page; for example, if users want to go to ”104” to find job. First, user may visit “104 after using Google to search “104”. Users need to login to find available job position in “104”. In above scenario, user will browse three pages, “GOOGLE”,”104 home page”, and”104 login page”. Thus, we simulate the scenario by giving a mission “Go to 104 Find Job”. In this scenario, phishers may lure users into providing their 104 account information by various attack techniques. Our goal is to generate possible phishing scenarios by applying phishing attack knowledge to legitimate scenarios. By considering game constraints, the proposed Game Mission Generation Algorithm is listed below.

Algorithm 2 : Game Mission Generation Algorithm

Input : Mission List M
Knowledge List K
Output : Phishing Knowledge List PM

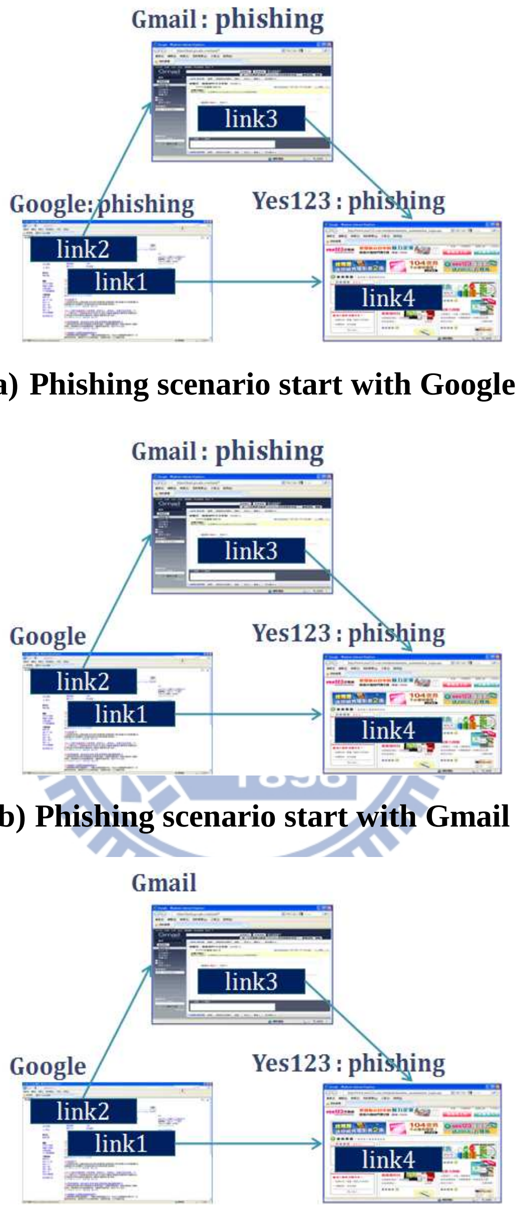
```
For each mission m from M
    For each knowledge k From K
        Select page p from P
            Invoke Modify Page Procedure(k,p)
```

Subroutine of Algorithm 2 : Modifying Page Procedure

Input : Page p
Knowledge k
Output : phishing page

```
Step1:For each repository r of  p
        1.1 Check precondition of knowledge k
        1.2 IF conform precondition of k
            Then Change slot value in p according to action of k
        1.3 IF link is modified Then Invoke Modify Page Procedure(k ,next page)
```

Figure 17 illustrates that our proposed game mission generation algorithm generates possible phishing “Go to yes123 Find Job”, shown in Figure 16, scenarios with “Decimal IP Encoding” technique, shown in Figure 14. First, we check whether the “Decimal IP Encoding” can be applied to the page “Google” or not. Next, according to the game constraints, we apply “Decimal IP Encoding” technique to the next selected pages, “Gmail” and “Yes123”. Repeat this procedure, we can generate all possible phishing “Go to yes123 Find Job” with “Decimal IP Encoding” technique. The generated phishing scenarios are shown in Figure 18.



(a) Phishing scenario start with Google

(b) Phishing scenario start with Gmail

(c) Phishing scenario start with yes123

Figure 18. An example of generated phishing scenario

For convincing adaptive learning mechanism, we label each generated phishing scenario S by (M ,P ,PT) where M is the mission number of the corresponding legitimate scenario, P is the page number of the start phishing page and PT is the corresponding phishing attack type.

For example, a phishing “Go to 104 Find Job” scenario, shown in Figure 19, is labeled as (“Go to 104 Find Job”, “Gmail”,”homograph”) because users start this phishing “Go to 104 Find Job” mission by receiving a phishing mail with “Homograph” technique in Gmail. In the next chapter, we will utilize this labeling system and generated game mission to propose our adaptive learning strategies.

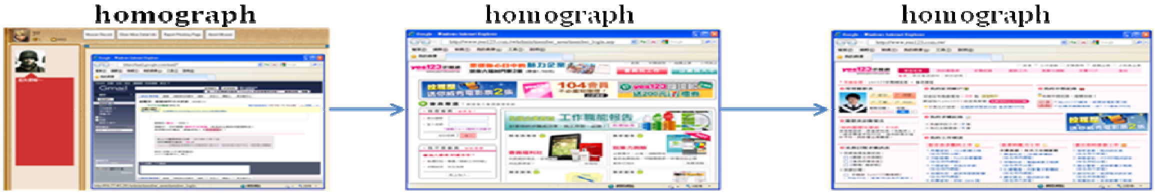


Figure 19. A labeling example of “Go to 104 Find Job” scenario

.

Chapter 5 Adaptive Learning Approach

In the chapter, we propose our adaptive strategies. First, we use phishing concept hierarchy for adjusting learning goal and plan. Contrast strategy is further applied to help users to converge the recognition of certain phishing attacks, while analogy strategy is used to improve the users' knowledge transfer ability.

5.1 Adaptive learning based on phishing concept hierarchy

Learning security is usually not a primary goal of users in Internet and the time of users spending in anti-phishing educations vary. Therefore, it is important to design different learning plans according to distinct learning periods. Phishing concept hierarchy in Chapter 3 is proposed to organize phishing attack knowledge. Figure 20 shows an example of phishing concept hierarchy. The higher concept consists of more phishing attack knowledge but rougher. For example, "Homograpgy" is phishing attack that spoof users by using mimic URL. However there are many techniques to construct a mimic URL such as "Add Word", "Delete Word" and "Replace Similar Word". These techniques are described more detailedly than "Homograpgy". Thus, "Add Word", "Delete Word" and "Replace Similar Word" is the sub-domain of "Homograpgy". We can construct a hierarchy between detailed concept of "Homograpgy"and its sub-concept.

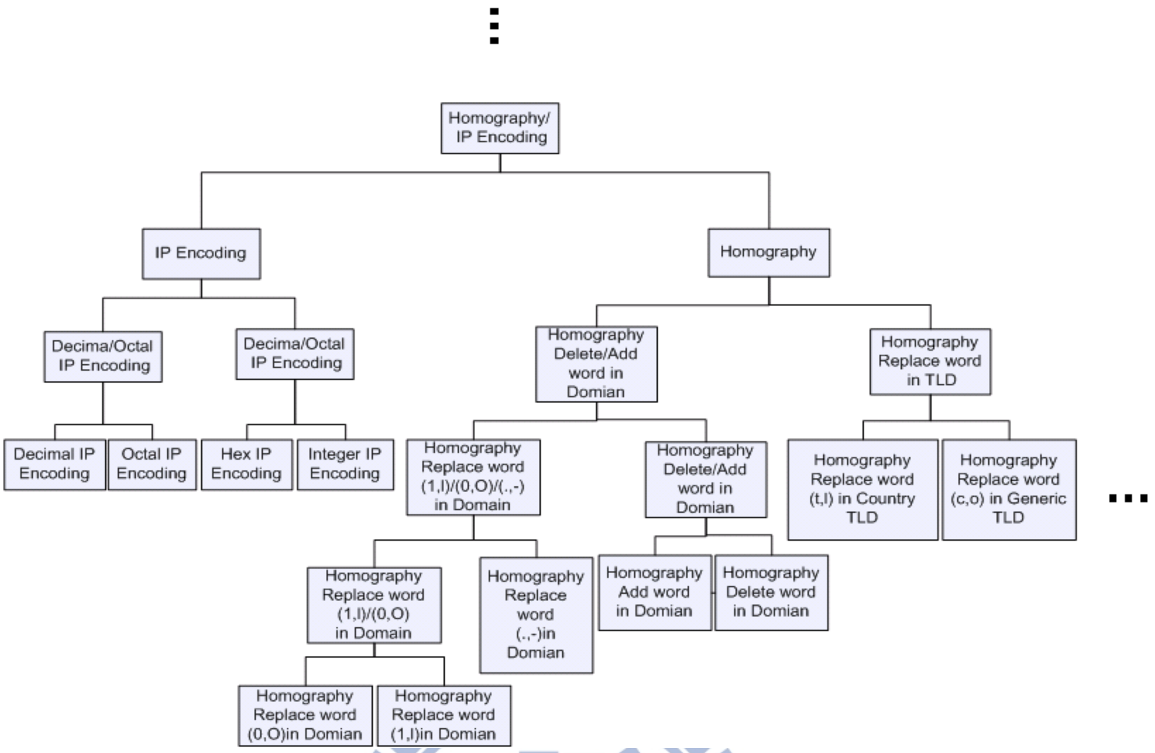

Homography/ IP Encoding
IP Encoding
Homography
Decima/Octal IP Encoding
Decima/Octal IP Encoding
Homography Delete/Add word in Domian
Homography Replace word in TLD
Decimal IP Encoding
Octal IP Encoding
Hex IP Encoding
Integer IP Encoding
Homography Replace word (1,l)/(0,O)/(.,-) in Domain
Homography Delete/Add word in Domian
Homography Replace word (t,l) in Country TLD
Homography Replace word (c,o) in Generic TLD
...
Homography Replace word (1,l)/(0,O) in Domain
Homography Replace word (.,-)in Domian
Homography Add word in Domian
Homography Delete word in Domain
Homography Replace word (0,O)in Domian
Homography Replace word (1,l)in Domian

Figure 20. Phishing Concept Hierarchy

Before introducing our adaptive ideas, we first define user learning portfolio. A user learning Portfolio UP is a set of $UP_i = (M_i, AP_i, A_i, T_i)$ where M_i is the current mission number, AP_i is the current visiting page, A_i is the action record and T_i is the current time. For example, user in mission M=(1,1, homograph) clicks a phishing link, then the user learning portfolio UP records ((1,1, homograph) ,(1,1) , ‘click’ ,’14:00:00’). According to different learning periods, our system will adjust different learning goal (different level in concept hierarchy). The basic idea is that users learned this phishing concept if they have learned certain instances of this concept. Therefore, in a limited time period, we first introduce the overview of phishing attack knowledge. As time goes by, the detailed phishing attack techniques will continue to be introduced. Example 2 show we adjust learning plans in different time period.

Example 2

According to the concept hierarchy and user portfolio in Figure 18, if the number of phishing attacks users can identify is more than a threshold, than we assume that users have finished in learning the sub-concept. If the number of finished sub-concept more than a threshold, we assume that users have finished learning the concept. At the first five minutes, we train user with the highest level concept, in this period, for example, to teach to avoid "Homograpgy" without classifying what technique use in "Homograpgy"; thus, if users have finished learning "Homograpgy" than we assume that users have finished in learning. In the next period, we will teach more detailed phishing attack in next level of concept hierarchy, users need to finish learning these detailed phishing attack.

5.2 Adaptive Learning Strategies

Although phishing concept hierarchy can be used to adjust learning plan, the users' learning abilities are still critical. If users cannot understand phishing concepts in time, designed learning may not be achieved. Hence, our idea is to speed up learning phishing concept by providing legitimate page. This strategy is so-called the contrast strategy. By comparing phishing page and legitimate page, users can observe the difference between them easier. This difference is indeed a phishing attack technique presented via the phishing features. The following example shows how the contrast strategy works.

Example 3

In Figure 20, the mission is "Find Job by yes123 mail", users need to go to Gmail to receive mail sent by "yes123", than go to "yes123" and login. There are three pages in the mission, "Gmail", "yes123 login" and "yes123 home". And we use this mission to teach user "Homography" shown in Figure 21.(a). If users can not identify "Homography" in page "Gmail", then will restart the mission with the scenario that the page "Gmail" is legitimate shown in 21.(b). Thus, user can compare phishing page and legitimate page.

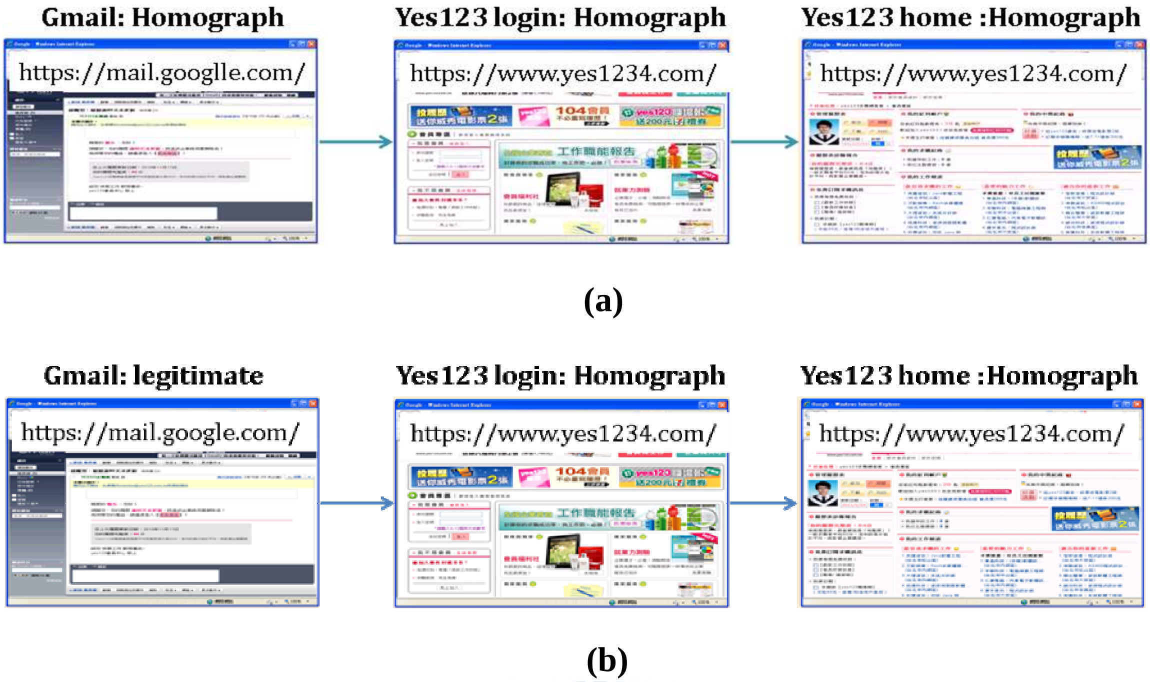
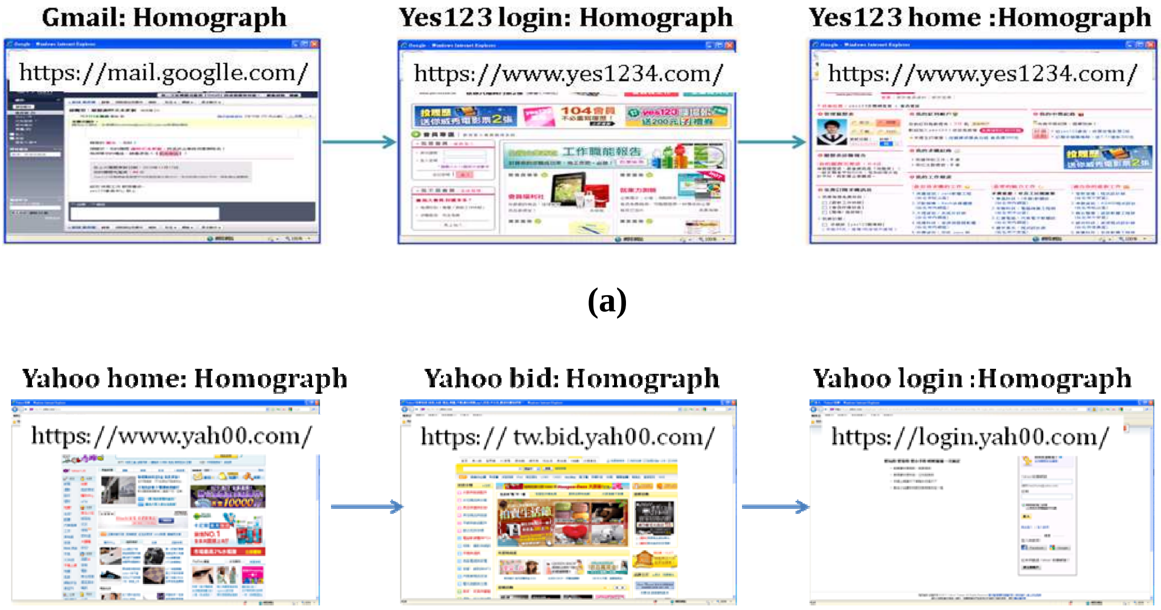


Figure 21. Contrast strategy in Adaptive Game Content Selection

The most important goal of anti-phishing educations is to teach users how to prevent phishing attacks in their daily life. Therefore, the knowledge transfer abilities of users which are to apply phishing knowledge to detect phishing pages with different scenarios are essential. Our idea of improving the knowledge transfer ability is to provide different phishing pages with the same phishing attack. This is so-called the analogy strategy. By previous experiences, user can understand how this phishing attack works easier. Example 5 shows the analogy strategy in our proposed system.

Example 5

In Figure 21, the mission is “Find Job by yes123 mail”, users need to go to Gmail to receive mail send by “yes123”, than go to “yes123” and login. If users can identify phishing attack in this mission shown in Figure 22.(a). We will select another mission shown in Figure 22.(b) with the same phishing attack to test the knowledge transfer ability of users.



(a)

(b)

Figure 22. Analogy strategy in Adaptive Game Content Selection

In our proposed system, adaptive strategy based on phishing concept hierarchy is prior to the contrast strategy and the analogy strategy. After learning whole phishing concepts, the analogy strategy is then applied to improve the knowledge transfer ability. Once users misjudge a phishing page, the contrast strategy is applied to help users to understand this embedded phishing attack knowledge. In the next chapter, we will propose our system containing knowledge acquisition module, mission generation module and adaptive game engine. The experiment results are also provided in the next chapter.

Chapter 6 System Implementation and Experiment

6.1 System Implementation

For evaluating our proposed approach, we implement a three-phase prototype system including Knowledge Acquisition Phase, Game Mission Generation Phase and Adaptive Game Content Selection Phase. The system architecture is shown in Figure 23.

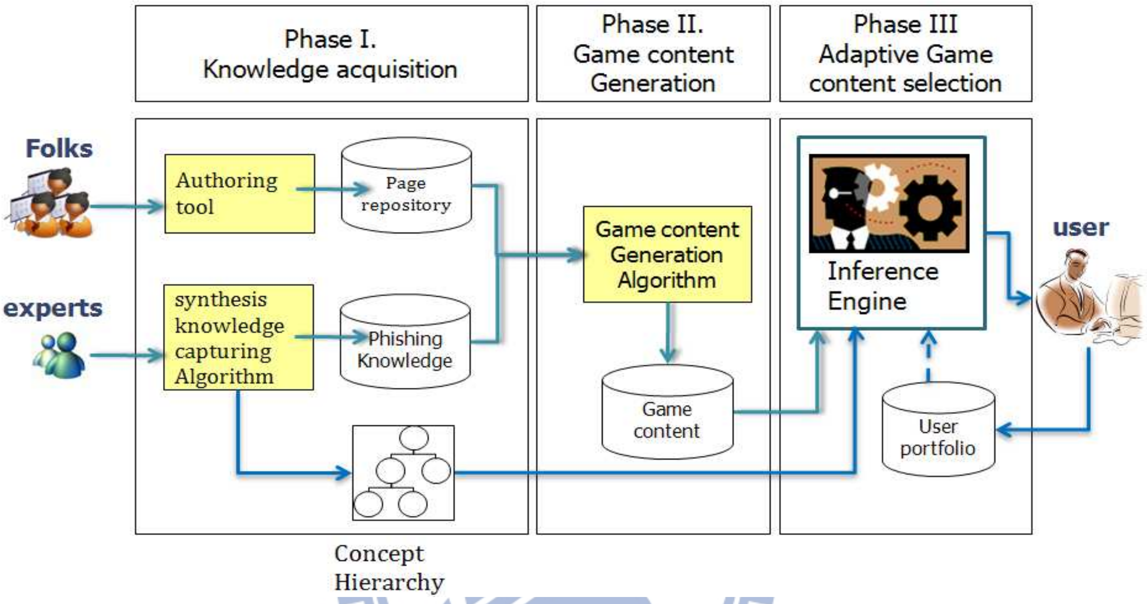
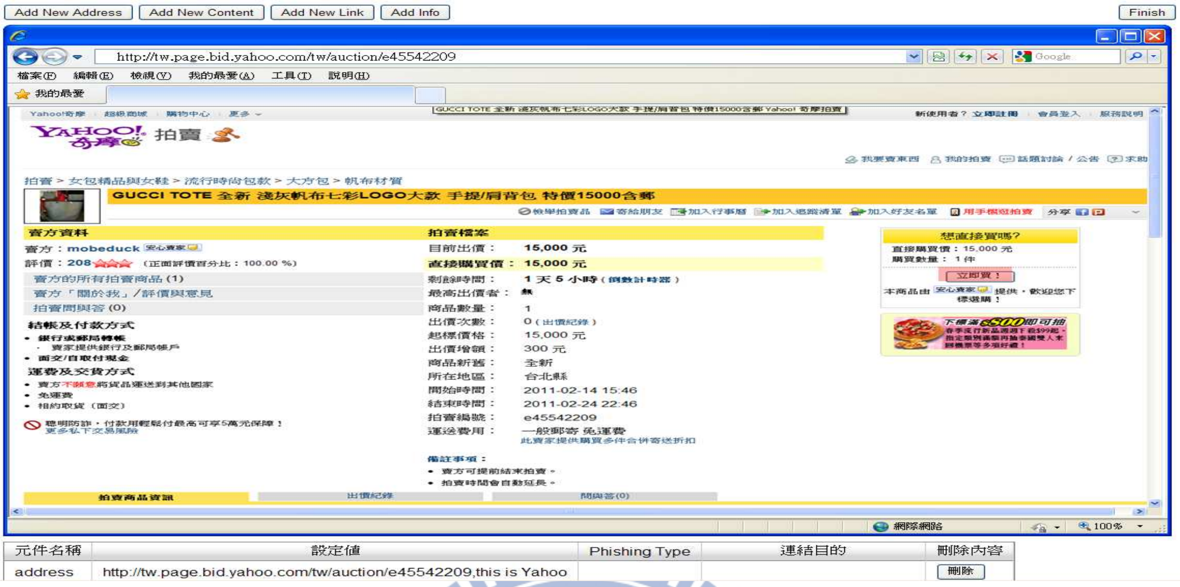


Figure 23. Intelligent Mission Management System Architecture

In knowledge acquisition phase, phishing knowledge is acquired from experts via the synthesis knowledge capturing algorithm. In the meanwhile, folks can provide page scenario by the proposed authoring tool. In Phase II, the stored page scenarios and phishing knowledge are further used to generate game missions for anti-phishing education game. While users start playing anti-phishing education, the inference engine selects phishing page adaptively based on users' portfolio and phishing concept hierarchy.

The screen shot of authoring tool is shown in Figure 24. Folks firstly provide the address of this page and then edit new page scenario of the phishing attack technique. If the existing phishing features are insufficient to describe the phishing attack techniques, folks can click the "add new info button" to extend the frame by inserting new phishing feature. Therefore, anti-phishing education game can be flexible for educating evolving phishing attack knowledge.


Add New Address
Add New Content
Add New Link
Add Info
Finish
http://tw.page.bid.yahoo.com/tw/auction/e45542209
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
Yahoo!奇摩 | 超級商城 | 購物中心 | 更多
新使用者？ 立即註冊 | 會員登入 | 服務說明
YAHOO!奇摩 拍賣
我要賣東西 我的拍賣 話題討論 / 公告 求助
拍賣 > 女包精品與女鞋 > 流行時尚包款 > 大方包 > 帆布材質
檢舉拍賣品 寄給朋友 加入行事曆 加入追蹤清單 加入好友名單 用手機逛拍賣 分享
拍賣商品資訊 出價紀錄 問與答(0)
網際網路 100%

GUCCI TOTE 全新 淺灰帆布七彩LOGO大款 手提/肩背包 特價15000含郵

賣方資料

賣方：mobeduck 安心賣家

評價：208 (正面評價百分比：100.00 %)

賣方的所有拍賣商品 (1)

賣方「關於我」/評價與意見

拍賣問與答 (0)

結帳及付款方式

- 銀行或郵局轉帳
  - 賣家提供銀行及郵局帳戶
- 面交/自取付現金

運費及交貨方式

- 賣方不願意將貨品運送到其他國家
- 免運費
- 相約取貨（面交）

聰明防詐，付款用輕鬆付最高可享5萬元保障！
更多私下交易風險

拍賣檔案

目前出價：	15,000 元
直接購買價：	15,000 元
剩餘時間：	1 天 5 小時（倒數計時器）
最高出價者：	無
商品數量：	1
出價次數：	0（出價紀錄）
起標價格：	15,000 元
出價增額：	300 元
商品新舊：	全新
所在地區：	台北縣
開始時間：	2011-02-14 15:46
結束時間：	2011-02-24 22:46
拍賣編號：	e45542209
運送費用：	一般郵寄 免運費 此賣家提供購買多件合併寄送折扣

備註事項：

- 賣方可提前結束拍賣。
- 拍賣時間會自動延長。

想直接買嗎?

直接購買價：15,000 元

購買數量： 1 件

立即買！

本商品由 安心賣家 提供，歡迎您下標選購！

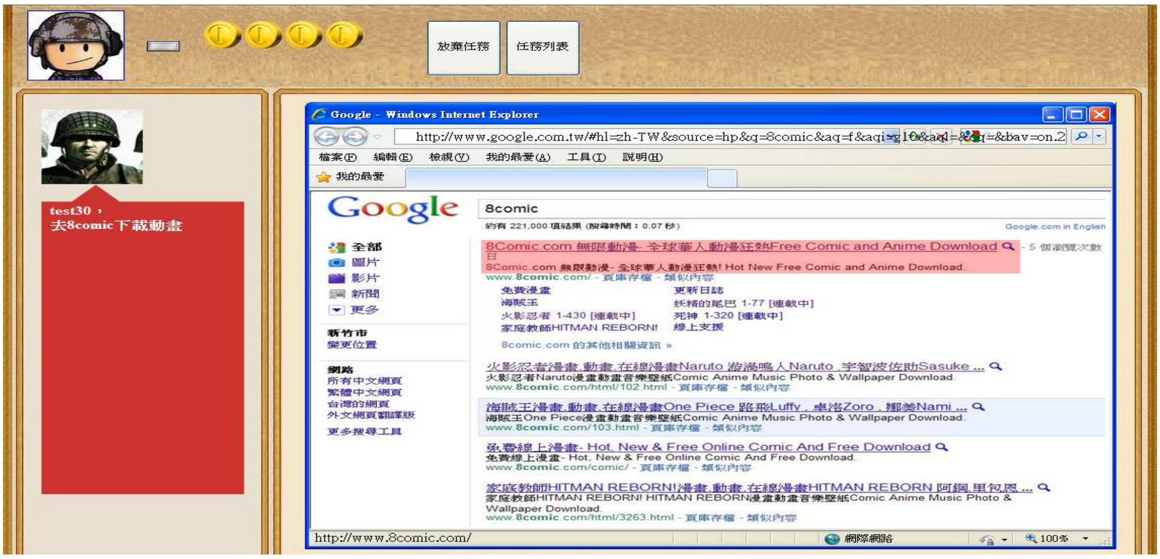
下標滿$800即可抽 春季流行新品週週下殺$99起，指定類別滿額再抽泰國雙人來回機票等多項好禮！

元件名稱	設定值	Phishing Type	連結目的	刪除內容
address	http://tw.page.bid.yahoo.com/tw/auction/e45542209,this is Yahoo			刪除

Figure 24. Page scenario authoring screen shot

The screen shot of game is shown in Figure 25. The main character of the game is a soldier John, where John has to complete the missions from his commander, but has to avoid phishing attacks. In mission, John can determine whether each desiring hyperlink is phishing or not. The other character, John’s commander, helps John out by providing tips on how to identity phishing page, shown in Figure 25.

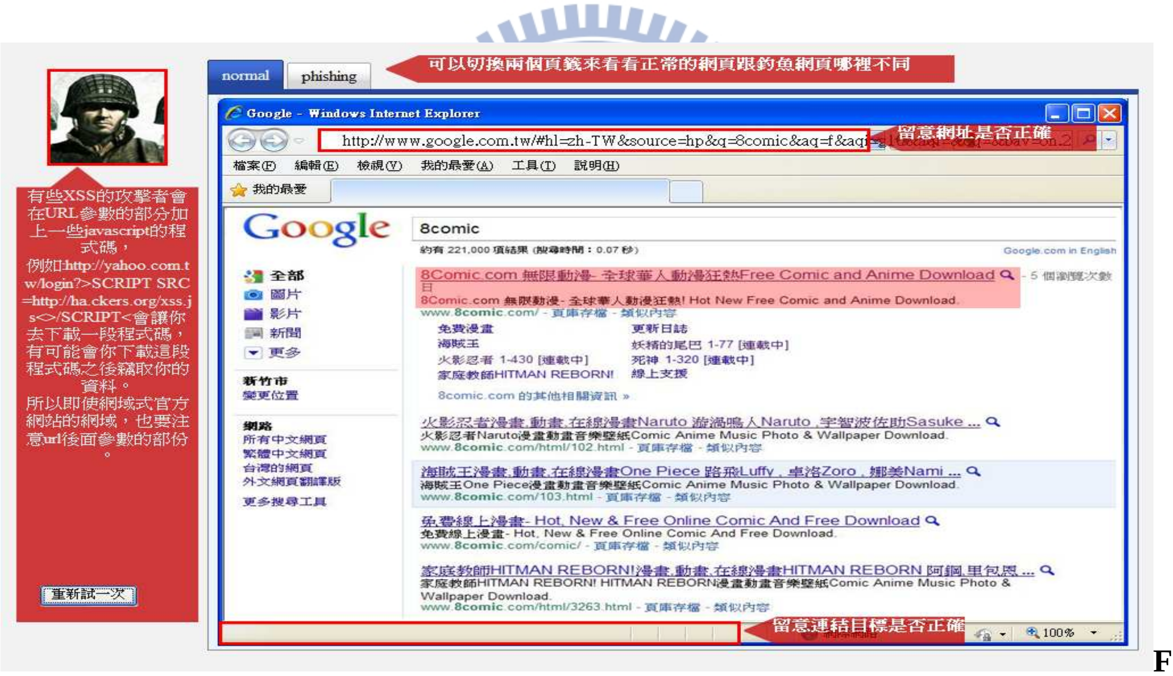
In this immediate feedback, the left column is an introduction of this phishing attack technique. The main frame shows the user’s misjudged phishing page, the phishing features are highlighted for reminding users. The corresponding legitimate page is also provided for recognizing this phishing attack knowledge.



放棄任務
任務列表
Google - Windows Internet Explorer
http://www.google.com.tw/#hl=zh-TW&source=hp&q=8comic&aq=f&aqi=g10&aql=&oq=&gs_rfai=&bav=on.2
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
8comic
全部
圖片
影片
新聞
更多
8Comic.com 無限動漫- 全球華人動漫狂熱Free Comic and Anime Download
http://www.8comic.com/
網際網路
100%

test30，
去8comic下載動畫

Figure 25. Screen shot of ASAPEG



normal
phishing
Google - Windows Internet Explorer
http://www.google.com.tw/#hl=zh-TW&source=hp&q=8comic&aq=f&aqi
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
我的最愛
8comic
全部
圖片
影片
新聞
更多
8Comic.com 無限動漫- 全球華人動漫狂熱Free Comic and Anime Download
重新試一次
100%

可以切換兩個頁籤來看看正常的網頁跟釣魚網頁哪裡不同

留意網址是否正確

有些XSS的攻擊者會在URL參數的部分加上一些javascript的程式碼，例如:http://yahoo.com.tw/login?>SCRIPT SRC=http://ha.ckers.org/xss.js<>/SCRIPT<會讓你去下載一段程式碼，有可能會你下載這段程式碼之後竊取你的資料。所以即使網域式官方網站的網域，也要注意url後面參數的部份。

留意連結目標是否正確

Figure 26. Screen shot of immediate feedback

In the evaluation, we consult several experts in security domain and education domain. Security experts consider phishing attack knowledge as the implementation techniques. From this viewpoint, advanced phishing attack techniques such as DNS cache poison and XSS attack cannot be completely represented by our proposed anti-phishing education game. However, our goal is to train users how to avoid phishing attack instead of training phisher. In contrast, security experts consider that phishing features provided by anti-phishing education game can describe nowadays phishing attacks. Education experts are satisfied with most functions of anti-phishing education game excepting game scenarios. In general, most experts agree that anti-phishing education game is convenient for educating users about phishing attack and improving users' ability of distinguishing phishing page in real life.

6.2 Experiment Design

In this experiment, we evaluated the learning achievement and learning motivation of participants. First, 20 Web pages are given, and participants were asked to determine whether each page is phishing or not and the confidences of their judgments. After 10 minutes training, 20 Web pages are given, and participants were asked to determine 20 more Web pages which were phishing. Finally, a questionnaire based on Technology Acceptance Model (TAM) was provided for evaluating learning motivation. The experiment flow is shown in Figure 27.

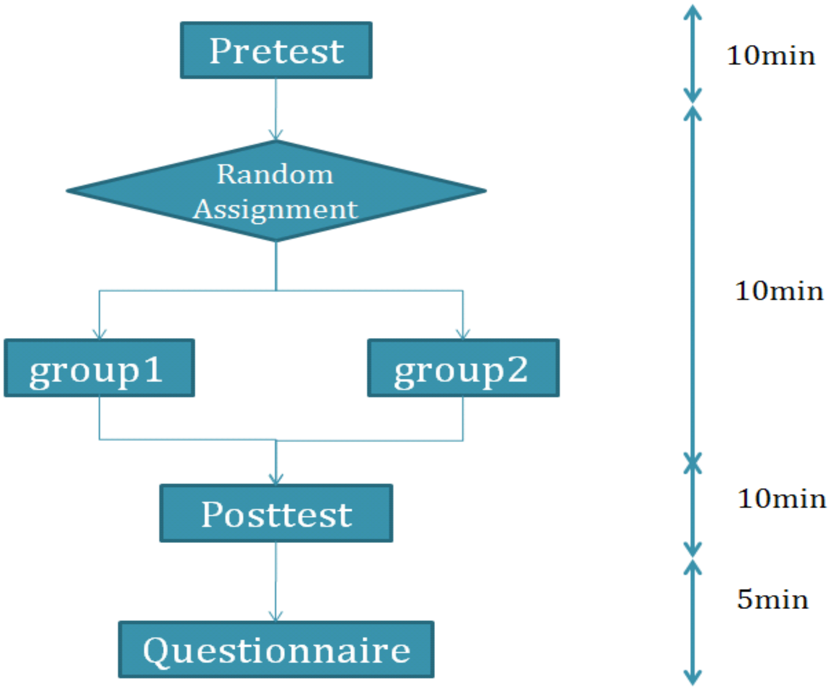


Figure 27. Experiment of APEG flow

We used a between-subjects experimental design to test two training conditions:

Existing training material condition: In this condition, participants were asked to spend ten minutes reading online anti-phishing material.

Adaptive Game condition: In this condition, participants played the adaptive Anti-Phishing Education Game for ten minutes.

After taking posttest, participants were asked to complete a TAM-based satisfactory questionnaire. The Technology Acceptance Model (TAM), shown in Figure 28, is an information systems theory that models how users come to accept and use a technology. In this questionnaire, we evaluate perceived usefulness, perceived ease of use, attitude toward using, and behavior intentions to use of ASAPEG

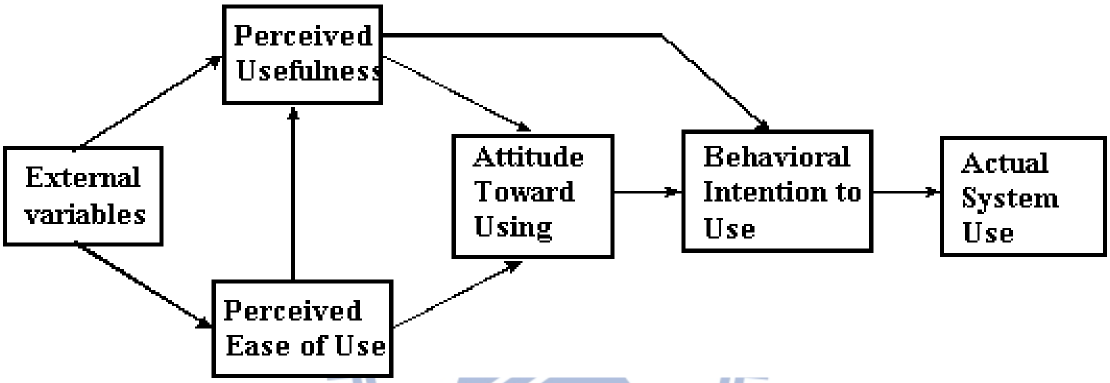


Figure 28. Technology acceptance model to measure APEG

6.3 Experiment Result

In this experiment, we recruit 62 online folks via PTT which is the greatest BBS station in Taiwan as participants. There are 44 males and 18 females involved in this experiment. The average time of participants in Internet is around 5 hours per day. Table 2 compares the learning achievements of experimental and control groups by Pair T-test. The corresponding standard deviations are represented in parentheses. There are significant learning achievements in experimental and control groups ($p<0.0001$ and $p=0.001$, respectively). This indicates that users can improve their phishing-detection abilities if they are willing to learn.

Table 2. Learning achievements of experimental and control groups

	Pretest	posttest	P-value
Experimental group	37.5483 (14.1941)	57.6935 (15.6964)	<0.0001
Control	37.0806 (17.047)	47.3870 (19.0729)	0.001

Table 3 compares the mean scores of control and experimental groups in pretest and posttest by Two Sample T-test. There is no significant difference in pretest (p=0.906). This indicates that participants in both groups have similar prior knowledge on detecting phishing pages. However, after anti-phishing training there reveals significant difference in posttest (p=0.0021). This result shows that our proposed approach performs better than traditional one.

Table 3. Test Score Comparison of experimental and control groups

	Experimental group	Control group	P-value
Pretest Score	37.5483 (14.1941)	37.0806 (17.047)	0.906
Posttest Score	57.6935 (15.6964)	47.3870 (19.0729)	0.0021

We further compare the score gained of two groups in One-way ANOVA, shown in Table 3. There is significant difference between experimental and control groups (p=0.0208). The average gained scores of experimental group and control group are around 20 points and 10 points, respectively, shown in Table 2. Therefore, experimental group performs significantly better than control group.

Table 4. One-way ANOVA

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1500.403	1	1500.403	5.6412	0.0208
Within Groups	15958.44	60	265.9739		
Total	17458.84	61			

We evaluate the users' satisfaction via TAM-based questionnaire. We collect the satisfaction of the participants for their comments in APEG After they finished anti-phishing training, they filled a TAM-based satisfaction questionnaire. 5 scale is used to evaluate the degree of participants' satisfaction, from very agree (1) to very disagree (5). The results of questionnaire in each group are shown in Table 4.

Question	Satisfaction Degree
Q1 我覺得操作這個遊戲很容易	3.72
Q2 我覺得操作說明可以幫助我操作這個遊戲	4.13
Q3 我覺得這個遊戲可以幫助我判斷釣魚網站	4.34
Q4 這個遊戲有教會使用工具來判斷釣魚	3.94
Q5 我覺得這個遊戲很有趣	3.99
Q6 我覺得這個遊戲有提高我去瞭解釣魚網站的動機	4.10
Q7 有需要的話我會去玩這個遊戲	4.07
Q8 我將來還會繼續使用玩這個遊戲	3.69
Q9 任務中的錯誤提示有幫助我判斷釣魚網站	4.26
Q10 我從遊戲中學到如何觀察釣魚網站的特徵	4.31

Table 5. Questionnaire of Control group

In Table 5, Q1 measure perceived ease-of-use (PEOU) in APEG. The result shows that participants believe that APEG would be free from effort. And Q2 measures perceived usefulness (PU) in APEG. Participants believe that using APEG would enhance their performance in anti-phishing. As a consequence, APEG with a high level of PU and PEOU is more likely to induce positive perceptions.

Chapter 7 Conclusion

In our thesis, we first extend KAME by Phishing Knowledge Combination Method. And then, we model the phishing page by decomposing into the phishing attack knowledge frame and page scenario repository. Next, we generate game content in APEG for adaptive learning. The main contributions of this paper are building game-based anti-phishing training and proposing a phishing knowledge combination approach to combine phish knowledge into new phishing knowledge.

The posttest and pretest result shows that there is a conspicuous difference between tradition anti-phishing education and game-based anti-phishing education. And the questionnaire shows that participants accept APEG in anti-phishing training.

In the near future, we will continue to increase game feature of anti-phishing education game for making anti-phishing education game more attractive.

REFERENCE

[1] Phishing Scams: Understanding the latest trends, June 2004

[2] Tsung-Ju Lee , et al., "Game-based Anti-Phishing Training", TWELF, 2010.

[3] Ponnurangam Kumaraguru, et al., "Teaching Johnny not to fall for phish", ACM Transaction on Internet Technology, 2007.

[4] Mingxing He, et al., "An efficient phishing webpage detector" Expert Systems with Applications, pp12018-12027, 2011

[5] Kuan-Ta Chen, et al., "Fighting Phishing with Discriminative Key point Features", Internet Computing, pp56 - 63 ,2009.

[6] Hossain Shahriar, Mohammad Zulkerninea. "Trustworthiness testing of phishing websites: A behavior model-based approach", Future Generation Computer Systems , Feb 2011.

[7] Maher Aburrous, et al., "Intelligent phishing detection system for e-banking using fuzzy datamining", Expert Systems with Applications, pp7913-7921, December 2010.

[8] Anthony Y. Fu. "Detecting Phishing Web Pages with Visual Similarity Assessment Based on Earth Mover's Distance (EMD)", Dependable and Secure Computing, pp301 – 311, Oct. 2006.

[9] Pablo Moreno-Gera, et al., "Educational game design for online education", in Computers in Human Behavior, pp.2530-2540, 2008

[10] Ponnurangam Kumaraguru, et al., "Protecting people from phishing: the design and evaluation of an embedded training email system", in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'07), 2007

[11] Ferguson, A. J. "Fostering E-Mail Security Awareness: The West Point Carronade", EDUCAUSE Quarterly , pp. 54-57, 2005.

[12] eBay, http://pages.ebay.com/education/spooftutorial

[13] Microsoft, Microsoft. Consumer awareness page on phishing. http://www.microsoft.com/ athome/security/ email/phishing.mspx.

[14] DimeNOC, http://www.dimenoc.com/antiphish/

[15] Bank Safe Online, http://www.banksafeonline.org.uk/phishing_explained.html

[16] ABA, http://www.aba.com/ABAEF/033104PHISH.htm

[17] OnGuardOnline, http://www.onguardonline.gov/games/phishing-scams.aspx

[18] S. A. Robila , Ragucci, J. W., "Don't be a phish: steps in user education”, Proceedings of the 11th Annual SIGCSE Conference on Innovation and Technology in Computer Science Educatio, 2006.

[19] Gorling, S, "The Myth of User Education”, in Proceedings of the 16th Virus Bulletin International Conference, 2006.

[20] Anandpara, et al. "Phishing IQ tests measure fear, not ability”, Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security, 2007.

[21] Marina Papastergiou, “Digital Game-Based Learning in high school Computer Science education:Impact on educational effectiveness and student motivation” , Computers & Education, pp 1-12, January 2009.

[22] Martin Ebnera, Andreas Holzingerb. “Successful implementation of user-centered game based learning in higher education: An example from civil engineering”, Computers & Education, pp873-890, Nov 2007.

[23] Wilfried Admiraala, et al., “The concept of flow in collaborativegame-basedlearning”, Computers in Human Behavior, pp1185-1194, May 2011.

[24] Ching-Chiu Chao, “An Investigation of Learning Style Differences and Attitudes toward Digital Game-based Learning among Mobile Users”, Wireless, Mobile and Ubiquitous

Technology in Education, pp. 29 – 31, Nov. 2006.

[25] Daniel Burgos, et al., “Re-purposing existing generic games and simulations for e-learning”, in Computers in Human Behavior, pp. 2656-2667, 2007.

[26] Wen-Hao Huang, “Evaluating learners’ motivational and cognitive processing in an online game-based learning environment”, Computers in Human Behavior, pp694-704, March 2011.

[27] Steve Sheng, et al., “Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish”, Symposium On Usable Privacy and Security (SOUPS), July 2007.

[28] Paypal Quiz, https://www.paypal.com/au/cgi-bin/webscr?cmd=xpt/Marketing/security
center/antiphishing/CanYouSpotPhishing-outside

[29] PhishMe, http://www.phishme.com/cyber_monday.php

[30] VeriSign, https://www.phish-no-phish.com/default.aspx

[31] A Study of Adventure Game Design for Disaster Prevention Education

[32] Kenneth J. Klassen , Keith A. Willoughby, "In-Class Simulation Games: Assessing Student Learning", Journal of Information Technology Education, 2003.

[33] Deane, and Kathleen, “Automatic Item Generation via Frame Semantics : Natural Language Generation of Math Word Problems”, Annual Meeting of the National Council on Measurement in Education. p. 28, 2003.

[34] Zualkernan, et al. ”Automatic Generation of Just-in-time Online Assessments from Software Design Models”, Educational Technology & Society, pp. 173–192, 2009

[35] S. Kim, J. A. Clark and J. A. McDermid, “The regorous generation of Java mutation using HAZOP”, Proceedings of the 12 the International Conference on Software and Systems Engineering and Their Applications (ICSSEA '99), 1999.

[36] Z. Branko, S. Stankov, M. Rosic and A. Grubisic, “Dynamic test generation over ontology-based knowledge representation in authoring shell,” Expert Systems with Application, pp. 8185-8196, 2009.

[37] Behram Beldagli, Tufan Adiguzela. "Illustrating an ideal adaptive e-learning: A conceptual framework", Procedia - Social and Behavioral Sciences, 2010.

[38] Louis Cohen, "Research Methods in Education", 2009.

[39] Crowther, et al. ” Using repertory grids for knowledge acquisition for spatial expert systems”, Intelligent Information Systems, pp.14 – 17, Nov 1996.

[40] Gwo-Jen Hwang, “A knowledge acquisition approach to developing Mindtools for organizing and sharing differentiating knowledge in a ubiquitous learning environment” Computers & Education, pp1368-1377, August 2011.

[41] Shian-Shyong Tseng, Shun-Chieh Lina. “VODKA: Variant Objects Discovering Knowledge Acquisition”, Expert Systems with Applications, pp2433-2450. March 2009,

[42] G. J Hwang. “Knowledge acquisiton for fuzzy expert systems.”, International Journal of Intelligent Systems, p541-560,1995.

[43] S.H Huang. “Dimensionality reduction in automatic knowledge acquisition: a simple greedy search approach”, Knowledge and Data Engineering, p1364 – 1373, Nov. 2003.

[44] Castro-Schez, et al. “Fuzzy repertory table: a method for acquiring knowledge about input variables to machine learning algorithm”, Fuzzy System, p123 – 139, Feb. 2004.

[45] Gwo-Jen Hwang, “New Knowledge Elicition Method for Construct Expert System”, Doctor of Philosophy, National Chiao Tung University, 1991.

[46] The Phishing Guide , http://www.technicalinfo.net/papers/Phishing.html