WP2-D-1

Using Anomalous Data to Foster Conceptual Change in Security Awareness

Yuen-Yan Chan
Faculty of Education, The University of Hong Kong, Pokfulam Road, H. K., Hong Kong SAR
E-mail: yychan8@hku.hk

Abstract— **Users are often regarded as the weakest link in an information system. To this, information security awareness nowadays gains much attention in organizations, schools, and universities. Since the practice of safe computing involves individual perception, effective pedagogy that can deliver a proper message about security awareness is vital for information security education. This article reports an experiment conducted on 102 university students which determined if anomalous data can provoke conceptual change, and whether anomaly can affect the perception of information security of the students. With evidences found from the experiment, it is concluded that conceptual change fostered by anomalous data is an effective pedagogy for information security education.**

I. INTRODUCTION

One important goal for information security education is to make learners be aware of information security threats and be compliant with security rules and regulations [1], [2]. However, whether the learners practice safe computing in a long run depends much on their perception towards information security. Conceptual change, a process that changes an existing conception of an individual, can therefore be applied in this situation. In this paper, the author suggests applying conceptual change as a pedagogy of information security education. In particular, anomalous data that deviates from learners' original expectation was used to foster the occurrence of conceptual change. An experiment was performed on 102 students of an information security lecture at a university in Hong Kong, with 66 of them being in the experimental group and 36 of them in the control group. The experiment design, students' responses, and interpretation of the results are reported in this paper.

The rest of the paper is organized as follow. Section 2 briefs the related theories and the previous works in conceptual change, anomalous data, and information security education. Section 3 describes the details of the experiment, including its design, implementation, and the results. Section 4 discusses the findings in the experiment and suggests ways for further improvements. Lastly, the paper is concluded in Section 5.

II. LITERATURE REVIEW

A. Conceptual Change

According to Davis [3], conceptual change is a learning process that changes an existing conception such as belief, idea, and way of thinking. Premonitory works of conceptual change include Piaget's genetic epistemology [4] and Kuhn's paradigm shift and incommensurability [5]. One can see diSessa's [6] recent survey on conceptual change research. A formal model of conceptual change is given by Posner, Strike, Hewson, and Gertzog [7] and is summarized in [8]. According to Posner et al.'s theory, conceptual change occurs in learners when:

1. they became dissatisfied with their prior conceptions
2. the new conception is intelligible
3. the new conception appears initially plausible; and
4. the new conception appears fruitful for future exploration.

A number of teaching models and strategies for conceptual change were developed, including those proposed by Chinn and Brewer [9], Cosgrove and Osborne [10], and Champagne, Gunstone, and Klopfer [11]. These models exhibit the following structure proposed by Nussbaum and Novick [12]:

1. reveal student preconceptions
2. discuss and evaluate preconceptions
3. create conceptual conflict with those preconceptions; and
4. encourage and guide conceptual restructuring

Indeed, the above model aligns with Piaget's stages of cognitive development, assimilation and accommodation [13]. The latter two stages respectively involve processing new information in a way to fit the existing cognitive framework and to modify the cognitive structure so as to make it consistent with the new information.

A. Anomalous Data

Anomalous data are those that deviate from what were expected. According to Posner et al. [7], it is a main source of dissatisfaction of existing conceptions. In an instructional method for science education proposed by Chinn and Brewer [9], anomalous data were used to foster conceptual change. This is possible because learners will experience cognitive disequilibrium when they cannot explain the anomaly; therefore, they eventually learn or invent the new conceptions [14], [15].

B. Information Security Education

We are now situated in an information and communication technology (ICT)-rich society in which computer and World Wide Web are essential in our daily lives. System vulnerabilities can cause huge lost to individuals and organizations, information security awareness therefore gains much attention in many organizations [1], [2]. No matter how careful a computer system is designed, many of the security

978-1-4244-5016-9/09/$25.00 ©2009 IEEE

threats are caused by the end users [16]. Therefore one important goal for information security education is to make learners be aware of potential threats and be compliant with security rules. The desirable learning outcome of information security user education is therefore to change any incorrect perceptions of information security and make them be aware of the security issues in computer and network usage. Conceptual change pedagogy has been applied in security education [17], [18], this article reports a different instance of the experiment.

III. The Experiment

The experiment was conducted in December 2007. In the experiment, first year students from a university in Hong Kong received lectures in World Wide Web security issues, including Secure Socket Layer (SSL), encryption, and network security. They were asked to indicate their level of agreement with safe computing practice before and after the lecture. The experiment included two conditions: the presence of anomalous data (the experimental condition) and the absence of anomalous data (the control condition). If conceptual change occurs, students should indicate a different level of agreement with computing safety after the lecture. Furthermore, if such change is towards a desirable direction, the level of agreement should increase.

A. Method

The participants came from a university in Hong Kong. They were taking a course titled "Information Security" in which World Wide Web security is one of the topics. The subject contents taught to the 4 classes were identical. 2 of the classes (n = 66) were in the experimental group, and the remaining classes (n = 36) was in the control group. They participated in the experiment during a regularly scheduled lecture in the course. The assignment of classes to either condition was done by convenience.

For both groups, the students were asked about their perception of information security before the start of the lectures. In particular, the following question was asked:

Q1. We must always pay attention to security issues when using the World Wide Web.

And the answers would be provided in a 5-point Likert scale, with 5 (highest) indicating "strongly agree" and 1 (lowest) indicating "strongly disagree".

For both groups, the instructor then delivered subject contents including Secure Socket Layer (SSL) and related technologies such as Public Key Infrastructure (PKI), digital certificates, encryption, and decryption, and how SSL provides encryption to the data transmitted between two computers over the Internet. For the experimental group, they would observe a demonstration on packet sniffing (the action of capturing and analyzing the packets over the network) with a network analysis tool, WireShark™ [19]. Before the demonstration, they were asked with the following two questions:

Q2.When we log-in to the webmail website, the login information (user ID, password) can be read by the eavesdroppers.

Q3. When we send and receive emails at the web mail website, the email contents can be read by the eavesdroppers.

The answers would be given in one of the followings: *Yes*, *No*, and *I don't know*. Then they observed the demonstration of packet analysis using the WireShark™ packet analyzer, which captures and displays packet data over the network (Fig. 1). Therefore, it is possible for the others to examine the packets that one sends to and receives from the computer networks by using a packet analyzer.

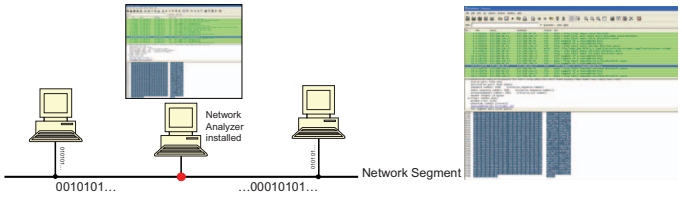

Fig. 1 Network analyzer examines the packets transmitting through the host computer.

Since the login page of webmail website (Fig. 2a) is encrypted by the SSL, the packet payload would appear to be encrypted ciphertexts (i.e. random, meaningless codes, Fig. 2b).

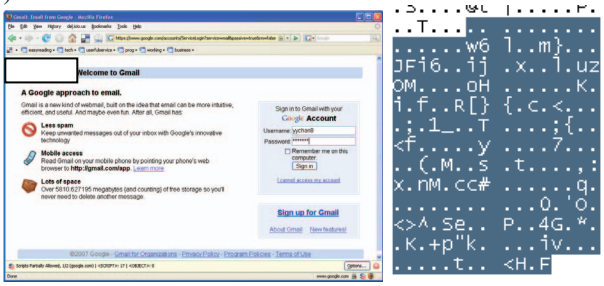

Fig. 2a and 2b. The webmail login page (left) and corresponding packet contents which are encrypted by SSL (right).

However, for the email contents page (Fig. 3a), as it is not encrypted by SSL, email contents ("This is a secret message and is confidential" as in the demonstration) could therefore be seen in plaintexts (Fig. 3b).

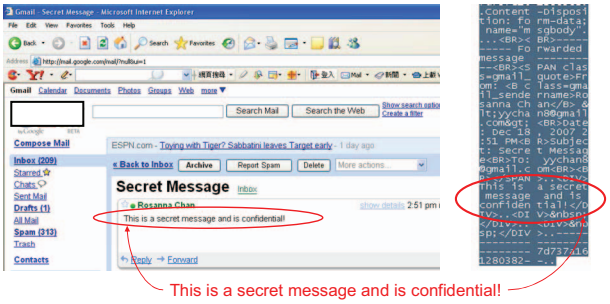

Fig. 3a and 3b. The web mail contents page (left) and packets contents which can be displayed in plaintexts by a network analyzer (right).

After observing the packet sniffing demonstration, the experimental group participants were further asked with the following two questions:

Q4.When we log-in to the web mail website, the login information (user ID, password) can be read by the eavesdroppers.

Q5. When we send and receive emails at the web mail website, the email contents can be read by the eavesdroppers.

For the control group, the instructor also demonstrated the network sniffing experiment with Ethereal™ and directly explained to students that web contents without SSL encryption can be read by eavesdroppers. The instructor performed packet sniffing at several SSL protected websites as well as those without SSL protection and compared their differences. However, the instructor did not explicitly tell nor demonstrate to the students that contents in the Webmail email page (without SSL) can be read using packet sniffing technique. In the end of the lecture, both groups were asked the following question:

Q6. We must always pay attention to security issues when using the World Wide Web.

This question was exactly the same as Q1. Here, Q1 and Q6 were respectively the pretest and posttest questions, measuring the participants' level of agreement with a safe practice in information security and World Wide Web usage. If the instruction was effective, an increase in the average posttest score should be shown. Furthermore, if the pedagogy adopted in the experimental group is effective, an ANCOVA (Analysis of Covariance) statistical analysis would indicate a significant difference between the experimental group and the control group. This will be discussed in next section.

It was assumed that the experimental group participants would initially believe contents in both login page as well as the email message page could not be eavesdropped. That is, they would answer No in both Q2 and Q3. Therefore, if they gave a Yes in Q5, this implies that the network analyzer demonstration was anomalous to them. Therefore, for those who answered No in Q3 and Yes in Q5, they were classified as the subgroup having observed the anomalous data. Further studies and discussions will be made to this subgroup of participants. Q2 and Q4 were another pretest-posttest question pairs to fulfill the completeness of the question set.

B. Results

According to the answers of Q3, of the 66 participants in the experimental group, 17 of them (25.8%) predicted that the email contents can be read by the eavesdroppers, 41 of them (62.2%) predicted that the email contents cannot be read, and 8 of them (12%) indicated that they did not know the answer. This shows that majority of the participants had a misconception that the email contents in A web mail is kept confidential over network transmission, which in fact is not the real situation. Q5 tests the conception of the participants after observing the demonstration. 50 (75.8%) of them answered that the email contents can be eavesdropped, 12 (18.2%) answered that the contents cannot be eavesdropped, and 4 (0.6%) answered not know. These results are shown in Figure 4. Among the 66 participants, 37 of them had observed the anomalous data according to the coding system described in previous section.

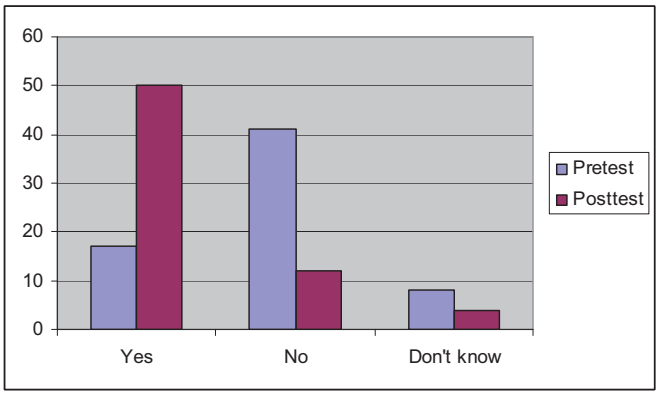

Fig. 4. Comparison between prediction (Q3) and observation (Q5) on the confidentially of email contents of the experimental group participants. Since the login page of webmail website.

The mean scores for Q1 (pretest) and Q6 (posttest) of experimental group and control group are given in table 1. In particular, the mean scores for the subgroup that had observed anomalous data are further broken down and listed in the table.

TABLE I
MEANS SCORE FOR Q1 (PRETEST) AND Q6 (POSTTEST) BY GROUPS TYPE SIZE FOR PAPERS

	N	Q1	Q6
Experimental	66	4.106	4.530
Experimental (Having observed anomalous data)	*37*	*4.035*	*4.757*
Control	38	4.166	4.251

The experiment conditions (experimental and control) were tested for their impacts on the treatment. Analysis of covariance (ANCOVA) was applied on the data to study such impacts in the posttest score (Q6). Table 2 presents the results of an ANCOVA on pretest and posttest results with Group as fixed variable (experimental = 66, control = 36). Although the experimental group exhibited a greater difference between the posttest and pretest scores than the control group (0.424 for experimental group and 0.085 for control group respectively), however, it is not statistically significant ($p > 0.1$).

TABLE 2
SUMMARY FOR TEST OF BETWEEN-SUBJECTS EFFECTS ON EXPERIMENT CONDITION

Source of Variance	Sums of squares	df	Mean square	F-ratio	Sig.
Regression	1.857	1	1.857	2.912	.091
Residual error	63.122	99	.638		
Total	2068.000	102			

The experimental group results were further analyzed to determine the impact of whether anomalous data had been observed. Table 3 presents an ANCOVA on pretest and posttest results with the fixed variable being whether anomalous data have been observed (not observed = 29, observed = 37). Here, significant difference ($p < 0.005$) is recorded (Table 3).

TABLE 3
SUMMARY FOR TEST OF BETWEEN-SUBJECTS EFFECTS WITHIN EXPERIMENTAL GROUP ON WHETHER ANOMALOUS DATA HAD BEEN OBSERVED

Source of Variance	Sums of squares	df	Mean square	F-ratio	Sig.
Regression	4.647	1	4.647	9.353	.003
Residual error	31.304	63	.497		
Total	1391.000	66			

IV. DISCUSSION

A. Learning Outcome

The key learning outcome of the lecture is to make students be aware of World Wide Web security. Quantitative measurement on the level of agreement with the importance of security issues of World Wide Web usage was used to determine whether the learning outcome has been achieved. From the ANCOVA results, significant difference is found between the subgroup that had observed anomalous data and those that had not. Here, we can conclude that the conceptual change fostered by anomalous data is effective in achieving the learning outcome in the information security lecture.

B. Conceptual Change and Anomalous Data

Results show that conceptual change happened in both experimental and control groups after the lecture, with the mean posttest scores higher than the mean pretest scores in both groups. However, the difference between the experimental group and control group was not significant. But when we further investigate the subgroup that had observed the anomalous data and compare their scores with those that had not, significant difference was found which shows that anomalous data is a factor that causes the difference. From the data, one can expect an even larger significant difference between the subgroup having observed the anomalous data and the control group. Such finding suggests that conceptual change fostered by anomalous data is effective in the teaching of information security in our experiment.

According to Posner et al. [7], anomaly is a major source of dissatisfaction with the existing conception, and the possible responses including realizing the needs for fundamental revisions or a rejection. In our experiment, despite the explicit demonstration and explanation, there were still a minority of participants (16 out of 66, of 18.8%) reported the email contents could not be read by third party. For these participants, they may either have a rejection of the anomaly or preventing the new information from conflicting with their original belief (Posner, et al., 1982; Shiu 2007 : 3). Further investigations can be performed on these participants.

C. Further Improvements

Further improvements for this research are suggested as follow:

1. The level of agreements with the importance of information security was only measured by one question, which was relatively rough. One should take this research as a pilot study and further design a set of benchmark questions on information security practices for the measurement purpose.
2. According to Chinn and Malhotra [15], the psychological processes in evaluating anomalous data involve four stages, namely observation, interpretation, generalizing, and retention. Further investigation on how participants react to the information security anomalous data in each stage can be made.
3. Further investigation on the subgroup that reported not having observed the anomalous data can be performed to determine why such observation is impeded.
4. Only the quantitative data was collected and analyzed, it is suggested that qualitative data such as participant interviews as well as instructor observation and self-reflection can be included in further research.

V. CONCLUSIONS

In this paper, the author described how conceptual change approach had been adopted in the teaching of information security to university students. In particular, anomalous data were used to foster the conceptual change. This paper narrated what have been done, discussed the experiment results, students' response, as well as the learning outcome. Further improvements for the current research design were also suggested. From the paper findings, it is concluded that anomalous data is effective in fostering conceptual change in information security education; and such change bring the students towards the desirable learning outcome of information security awareness.

REFERENCES

[1] B. Endicott-Popovsky, I. Orton, K. Bailey, and D. Frincke, "Community security awareness training,". in *Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop*, 2005, pp. 373 – 379.

[2] D. Frincke and M. Bishop, "Joining the security education community," in *IEEE Security & Privacy Magazine*, vol. 2, no. 5, 2004, pp. 61 – 63.

[3] J. Davis, "Conceptual Change," Dec. 15, 2008. [Online]. Available: http://projects.coe.uga.edu/epltt/. [Accessed : Oct. 15, 2009]

[4] J. Piaget, *Genetic Epistemology (E. Duckworth, Trans.)*. New York: Columbia University Press, 1970.

[5] T. Kuhn, T. *The Structure of Scientific Revolutions*. Chicago: University of Chicago Press, 1970.

[6] A. A. diSessa, "A history of conceptual change research: Threads and fault lines," *Cambridge Handbook of the Learning*

Sciences, R. K. Sawyer Ed. UK: Cambridge University Press, 2006, pp. 265 – 281.

[7] G. J. Posner, K. A. Strike, P. W. Hewson and W. A. Gertzog, "Accommodation of a scientific conception: Toward a theory of conceptual change," in *Science Education, vol. 66*, 1982, pp. 211 – 227.

[8] L. P. Shiu, "Theoretical background of conceptual change". in *Lecture Notes, EDM 6501*, Hong Kong: The Chinese University of Hong Kong, 2007.

[9] C. A. Chinn and W. F. Brewer, "The role of anomalous data in knowledge acquisition: A theoretical framework and implications for science instruction," in *Review of Educational Research, vol. 63, no. 1*, 1993, pp. 1 – 49.

[10] M. Cosgrove and R. Osborne, "Lesson frameworks for changing children's ideas," in *Learning in Science: The Implications of Children's Science*, R. Osborne and F. P. Freyberg Eds., Portsmouth, NH: Heinemann, 1985, pp. 101-111.

[11] A. B. Champagne, R. F. Gunstone and L. E. Klopfer, "Effecting changes in cognitive structures among physics students," in *Cognitive Structure and Conceptual Change*, L. West and A. Pines Eds., Orlando, FL: Academic Press, 1985, pp. 163-188.

[12] J. Nussbaum and N. Novick, "Alternative frameworks, conceptual conflict, and accommodation: Toward a principled teaching strategy," in *Instructional Science, vol. 11*, 1982, pp. 183 – 200.

[13] J. Piaget, The construction of reality in the child. New York: Basic Books, 1954.

[14] J. Piaget, *The Equilibrium of Cognitive Structures: the Central Problem of Intellectual Development (T. Brown & K. J. Thampy, Trans.).* Chicago: University of Chicago Press, 1985. (Original work published 1975).

[15] C. A. Chinn and B. A. Malhotra, "Children's responses to anomalous scientific data: how is conceptual change impeded?" in *Journal of Educational Psychology, vol. 94, no. 2*, 2002, pp. 327 – 343.

[16] M. Bishop. *Computer Security: Art and Science*. Boston, MA: Addison-Weslesley Professional, 2002.

[17] Y. –Y. Chan and V. K. Wei, "Teaching for conceptual change in security awareness," in *IEEE Security & Privacy, vol. 6, no. 6*, 2008, pp. 67 – 69.

[18] Y. –Y. Chan and V. K. Wei, "Teaching for conceptual change in security awareness: A case in higher education," in *IEEE Security & Privacy, vol. 7, no. 1*, 2009, pp. 68 – 71.

[19] Combs, Gerald, et al., WireShark, 2007, "WireShark: Go deep," [Online]. Available: http://www.wireshark.org/ [Accessed: Oct. 15, 2009].