Teaching for Conceptual Change in Security Awareness

A Case Study in Higher Education

Yuen-Yan Chan
The University of Hong Kong

Victor K. Wei
The Chinese University of Hong Kong

In educational psychology, conceptual change is a process that revises a student's understanding of a topic in response to new information. Conceptual change pedagogy is particularly effective for security awareness education because instructors must deliver concepts to people who primarily just use computer networks and information systems rather than display expertise in the underlying technology.[1]

In the last issue,[2] we described conceptual change and its pedagogical application. In this issue, we take the discussion one step further by describing a real-life case study: the implementation of a conceptual change pedagogy in security awareness education for nonengineering undergraduates at the Chinese University of Hong Kong.

Background

The Chinese University of Hong Kong launched its Student Information Technology Competency Program in 1999. It requires all students to attend and pass an information technology proficiency test before graduation. This test consists of eight sections, including one about information security that assesses students' knowledge about various concepts, as well as their ability to manipulate antivirus software. To promote security awareness in students' daily computer usage and to help them pass the test, the university offers multiple sessions of a three-hour training class. In this class, students learn various concepts related to information security, including computer viruses, electronic communication security, computer safety, Web security, and public-key infrastructures.

Overview of the Experiment

To learn whether conceptual change pedagogy is effective in information security awareness education, we performed an experiment in four sessions from September 2007 to June 2008. Each class had 20 to 30 students; we used two sessions as the control group and the other two as the experimental group.

We derived our experiment's design from Clark Chinn and Betina Malhotra's work,[3] which used anomalous data such as the same falling speed of heavy and light objects and the identical readings of two thermometers (one wrapped in wool and the other not) to foster conceptual change in fourth-, fifth-, and sixth-graders attending science classes. In our experiment, 102 students (45 male and 57 female) used a six-point Likert scale to rank their pre-instructional agreement with eight statements about information security beliefs:

- World Wide Web security is important for business.
- World Wide Web security is important for general computer users.
- We must pay attention to security issues when surfing the World Wide Web.
- When we use Internet banking services, we should make sure the connection is SSL-enabled.
- We must install and enable antivirus software.
- We must update antivirus software regularly.
- We must scan our computers for viruses regularly.
- We must always enable firewall protection.

The participants then attended a lecture covering Web security, computer safety, and network security. One version of the lecture took a conceptual change teaching approach, with anomalous data in security presented to the participants (the experimental condition), and a different version didn't (the control condition). In particular, the instructor intentionally guided the experimental group to create conceptual conflicts in their beliefs about network data confidentiality. This was a formal experimental design in which students in both the

experimental group (55 people) and the control group (47 people) answered identical questionnaires consisting of eight questions in security awareness both before and after the lecture. Our hypothesis was that if conceptual change occurred, the participants would indicate a different level of agreement with the statements before and after the lecture. Furthermore, if such change were effective, the level of agreement with the statements should increase.

Creating Conceptual Conflicts

To reveal participants' preconceptions in daily security issues and encourage them to discuss and evaluate such preconceptions, we guided the experimental group's participants to predict and observe an event that demonstrated the network data confidentiality of popular webmail services—specifically, they observed a demonstration of packet sniffing in a popular webmail application. To create the conceptual conflict, the instructor first accessed the webmail login page, typed in a username and password, and then showed the corresponding "sniffed" network packets. This helped the students see that all packet payloads were encrypted (because the webmail login page was SSL-protected), so we asked the participants a predictive question (Q1): "When we send and receive emails via [the webmail application, name of service provider removed], it's possible for eavesdroppers to read the messages' content. Is this true? (yes, no, I don't know)."

The instructor then introduced some core conceptual change principles to effect fundamental changes:[4] she first discussed the participants' preconceptions and agreed that most computer users expect an email message's contents to be encrypted, but she pointed out that there were exceptions. Next, the instructor created conceptual conflicts by demonstrating that the network traffic payloads of a few popular webmail services aren't, in fact, entirely encrypted. Specifically, she showed the participants that parts of the webmail service's Web site aren't SSL-protected and that they could see a message's contents in plain text (see Figure 1). This experiment proves that we can use such a demonstration as anomalous data for fostering conceptual change.

After the packet-sniffing demonstration, we asked the experimental group participants to answer Q1 again (for clarity, we call this Q2 in the remainder of the article).

For the control group, the instructor demonstrated network sniffing and directly explained to students that eavesdroppers can read Web contents not protected by SSL encryption. She demonstrated packet sniffing on several SSL-protected Web sites as well as several without SSL protection and compared the differences. However, the instructor didn't explicitly create conceptual conflicts. At the end of the lecture, we asked both groups to again rank their responses to our initial eight statements.

When asked Q1, 37 experimental group participants (67.27 percent) said that eavesdroppers couldn't read email content, and 8 (14.55 percent) indicated that they didn't know the answer; only 10 (18.18 percent) said that email content could be read. This shows that most participants mistakenly believed that email content is kept confidential in network transmissions. Q2 tested the participants after observing the demonstration—41 (74.55 percent) said that email content could be read, 8 (14.55 percent) said that the contents were unreadable, and 6 (10.91 percent) didn't know.

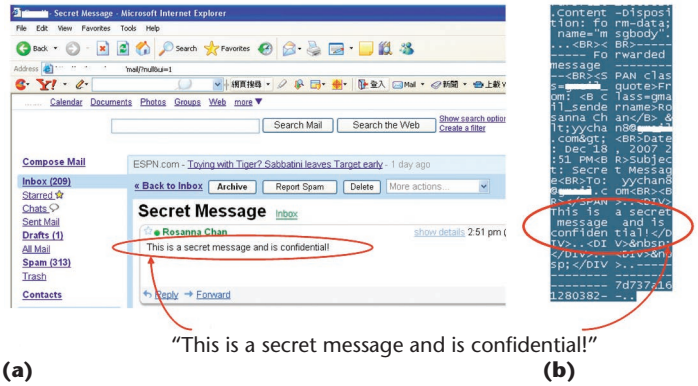

Figure 1. Webmail security. As demonstrated from an experiment performed in December 2007, (a) the webmail interface appears secure, but (b) a network analyzer can display packet contents in plain text.

New Department Editor

Cynthia E. Irvine is a professor of computer science at the US Naval Postgraduate School. Her research interests include high-assurance trustworthy systems, hardware-based security support, multilevel security, and cybersecurity education. Irvine has a PhD in astronomy from Case Western Reserve University. She is a member of the IEEE, the IEEE Computer Society, the ACM, and the Astronomical Society of the Pacific. Contact her at irvine@nps.edu.

Table 1. Mean scores for each group before and after the experiment.

	EXPERIMENTAL (N = 55)		EXPERIMENTAL SUBGROUP; OBSERVED ANOMALOUS DATA (N = 32)		CONTROL (N = 47)	
	PRE-TEST	POST-TEST	PRE-TEST	POST-TEST	PRE-TEST	POST-TEST
World Wide Web security is important for business	4.845	5.064	4.844	5.375	4.840	5.011
World Wide Web security is important for general computer users	4.936	5.173	4.938	5.344	4.968	5.031
We must pay attention to security issues when surfing the World Wide Web	4.736	5.009	4.750	5.219	4.734	4.913
When we use Internet banking services, we should make sure the connection is SSL-enabled	4.518	5.074	4.438	5.313	4.565	4.819
We must install and enable antivirus software	4.700	5.027	4.625	5.219	4.717	4.926
We must update antivirus software regularly	4.536	4.955	4.438	5.125	4.543	4.734
We must scan our computers for viruses regularly	4.630	4.955	4.625	5.063	4.628	4.968
We must always enable firewall protection	4.611	5.009	4.531	5.156	4.628	4.840
Overall average	4.689	5.033	4.648	5.227	4.703	4.905

We further classified those who at first predicted email content couldn't be read but saw later that, in fact, the reverse is true as the subgroup that observed anomalous data. Among the 55 experimental group participants, 32 of them fell into this category.

The Experimental Condition

A Cronbach's alpha value of 0.818 indicates that our initial set of eight statements was a reliable instrument for measuring participants' preconceptions about information security. Table 1 shows the mean scores for each group's pre- and post-test results.

We applied analysis of covariance (Ancova) to the data to study the experiment's impact on the average post-test score. In Tables 2 and 3, we adopted standard statistical notations in which p and *Sig.* denote the probability that the two groups are the same, df denotes the degree of freedom, and the F-ratio reflects whether the two comparing groups are approximately equal. Two equal groups give an F-ratio of value 1. Table 2 shows the results on both pre- and post-test results where the group is the fixed variable (experimental = 55, control = 47). Although the experimental group exhibited a greater difference between the pre- and post-test scores than the control group (0.344 for experimental group and 0.202 for control group, respectively), it isn't statistically significant ($p > 0.1$).

We further analyzed the experimental group results to determine the impact of whether the participant had observed anomalous data. Table 3 presents an Ancova on pre- and posttest results, where the fixed variable is whether the participant observed anomalous data (not observed = 23, observed = 32). Here, there is a significant difference ($p < 0.05$).

Our findings show that conceptual change pedagogy, an approach proven effective in science education, is also effective in security awareness training for nonengineering undergraduates. The set of eight statements tested quantitatively how well the participants could transfer their learning from the security awareness training class to various aspects of information security practices. Our results showed that the mean post-test scores were higher than the mean pre-test scores in both the experimental and control groups (Table 1), but the difference between them wasn't statistically significant (Table 2). However, when we added the subgroup that observed the anomalous data and compared their scores with those who hadn't, we found a significant difference (Table 3). This suggests that conceptual change fostered by anomalous data is effective in teaching information security awareness, and that participants could transfer

Table 2. Statistical test of differences between experimental group and control group.*

VARIANCE SOURCE	SUMS OF SQUARES	DF	MEAN SQUARE	F-RATIO	SIG.
Regression	.424	1	.424	.523	.417
Residual error	80.390	99	.812		
Total		2609.856	55		

**Sig.* denotes probability that the two groups are the same, *df* denotes the degree of freedom, and *F-ratio* reflects whether the two comparing groups are approximately equal.

Table 3. Statistical test of differences between experimental group participants who observed anomalous data and those who didn't.*

VARIANCE SOURCE	SUMS OF SQUARES	DF	MEAN SQUARE	F-RATIO	SIG.
Regression	3.239	1	3.239	4.681	.035
Residual error	35.983	52	.692		
Total		1434.626	55		

**Sig.* denotes probability that the two groups are the same, *df* denotes the degree of freedom, and *F*-ratio reflects whether the two comparing groups are approximately equal.

their new perceptions about webmail services' confidentiality to a range of daily security practices.

Indeed, according to Clark Chinn and William Brewer,[1] observing anomalies can cause subjects to substantially reconsider their existing preconceptions and thus promote conceptual change. In our experiment, despite the explicit demonstration and explanations, a minority of participants (8 out of 55, or 14.55 percent) reported that a third party couldn't read email content. These participants might have either rejected the anomaly or prevented the new information from conflicting with their original preconceptions. Further investigations could help us modify our teaching to encourage the observation of anomalous data so as to best implement conceptual change as a tool in teaching information security. Overall, we conclude that conceptual change fostered by anomalous data is an effective pedagogy for security awareness. □

References

1. C.A. Chinn and W.F. Brewer, "The Role of Anomalous Data in Knowledge Acquisition: A Theoretical Framework and Implications for Science Instruction," *Rev. Educational Research*, vol. 63, no. 1, 1993, pp. 1–49.
2. Y.-Y. Chan and V.K. Wei, "Teaching for Conceptual Change in Security Awareness," *IEEE Security and Privacy*, vol. 6, no. 6, 2008, pp. 67–69.
3. C.A. Chinn and B.A. Malhotra, "Children's Responses to Anomalous Scientific Data: How Is Conceptual Change Impeded?" *J. Educational Psychology*, vol. 94, no. 2, 2002, pp. 327–343.
4. J.E. Ormrod, *Educational Psychology: Developing Learners*, 6th ed., Prentice Hall, 2008.

Yuen-Yan Chan *is a postdoctoral fellow in the Faculty of Education at the University of Hong Kong and an adjunct assistant professor in the Department of Information Engineering at the Chinese University of Hong Kong. Her research interests include learning sciences, engineering education, cryptography, and security education. Chan has a PhD from the Chinese University of Hong Kong, with a doctoral dissertation focused on cryptography. She's the founding chair of the IEEE Education Society, Hong Kong Chapter, and is a US National Academy of Engineering Center for the Advancement of Engineering Education new faculty fellow. Contact her at yychan@ie.cuhk.edu.hk.*

Victor K. Wei *is a professor in the Department of Information Engineering at the Chinese University of Hong Kong. His research interests include cryptography, provable security, and coding theory. Wei is an IEEE fellow. Contact him at kwwei@ie.cuhk.edu.hk.*