

# **The third EWU-IPU International Exchange Program in Computer Science 2010**



**CSIEP 2010**



Sponsored by Informatics Society

Publication Office

Informatics Laboratory

3-41, Tsujimachi, Kitaku, Nagoya 462-0032, Japan

Publisher

Tadanori Mizuno, President of Informatics Society

ISBN: 978-4-902523-24-9

**General Co-Chairs:**

Yoshitaka Shibata, *Iwate Prefectural University*

Paul Schimpf, *Eastern Washington University*

**Program Co-Chairs:**

Carol Taylor, *Eastern Washington University*

Kosuke Imamura, *Eastern Washington University*

Yuko Murayama, *Iwate Prefectural University*

**Program Committee:**

Paul Schimpf, *Eastern Washington University*

Yoshitaka Shibata, *Iwate Prefectural University*

Kousuke Imamura, *Eastern Washington University*

Tim Rolfe, *Eastern Washington University*

Yoshia Saito, *Iwate Prefectural University*

Masanori Takagi, *Iwate Prefectural University*

Brian Kamp, *Eastern Washington University*

Atsushi Inoue, *Eastern Washington University*

**Local Chair:**

Lauri McLaughlin, *Eastern Washington University*

**Publishing Chair:**

Yoshia Saito, *Iwate Prefectural University*

**Web Chair:**

James Lamphere, *Eastern Washington University*

## Contents

Preface	1
Keynote: “Critical Infrastructure Cyber Security: Trust and Decision Making” <i>C. Hauser</i>	2
An Analysis on Teaching Methods Using a WBT System “CollabTest” Enabling Students to Create Quizzes Collaboratively <i>M. Takagi, K. Yamada, J. Sasaki, T. Kaneko, M. Mochizuki and Y. Teshigawara</i>	5
Enhancement of Questionnaire on Anshin <i>D. Nishioka, Y. Fujihara and Y. Murayama</i>	7
Evaluation and Agendas of Wireless Input Device for Tiled Display Desktop Environment <i>A. Sakuraba and Y. Shibata</i>	9
Self-Powered Independent Communication Network System for Emergencies <i>T. Suzuki and Y. Shibata</i>	11
Internet Connection Over Challenged Network for Disaster Information System <i>Y. Sasaki and Y. Shibata</i>	13
Content Grouping on P2P Network <i>T. Sasaki and J. Sawamoto</i>	15
An Experimental Study on TOR Traffic Analysis Attacks <i>R. Hoeflin, C. Taylor and K. Imamura</i>	17
Design and Implementation of an Interactive Live Broadcasting System with a High-Quality Snapshot Function on the Internet <i>Y. Saito and Y. Murayama</i>	19
Social Engineering Awareness in a Financial Institution <i>R. Long and C. Taylor</i>	21

## **Preface**

It is our great pleasure to have the workshop of the third EWU-IPU International Exchange Program in Computer Science published by the Informatics Society. The exchange program started in the summer of 2008 following the administrative meeting in the previous year. The workshop was held at the end of the program every year since that time.

This year, we had the keynote speech by Dr. Carl Hauser from Washington State University in Pullman, followed by seven presentations by the faculty members and graduate students from Iwate Prefectural University as well as two presentations by a faculty member and a graduate student from Eastern Washington University. Those presentations span a wide variety of topics in computer science, networking, security and human aspects of technology.

We hope that the workshop is a good basis for more participants in this international research exchange program and leads to further research collaboration.

Finally, but not least, we appreciate the Informatics Society for publishing the proceedings from this summer workshop.


September 2010

General Co-Chairs: Yoshitaka Shibata and Paul Schimpf

Program Co-Chairs: Carol Taylor, Kosuke Imamura and Yuko Murayama

WASHINGTON STATE UNIVERSITY  
World Class. Now for Real.

School of Electrical Engineering and Computer Science



**Critical Infrastructure Cyber Security: Trust and Decision Making**

Carl Hauser  
Associate Professor  
Electrical Engineering and Computer Science

September, 2010

1

WASHINGTON STATE UNIVERSITY  
World Class. Now for Real.

**Motivation**

- We work on communication infrastructure to support power grid monitoring and control
  - "Smart Grid" craze
  - => large numbers of "intelligent devices" deployed in the grid
  - => increasingly automated control
  - What about security?
- Control decisions rely on good data
- Must only act on the basis of authenticated commands
- Scale:  $n \times 10^5$  devices,  $m \times 10^3$  owning organizations

2

WASHINGTON STATE UNIVERSITY  
World Class. Now for Real.

**CIA Cyber-Security Model**

- Confidentiality
- Integrity
- Availability
- C&I typically provided using encryption technology
  - Example: digital signatures using public-key cryptography
    - Send( $M$ , Sign( $M, K$ )) –  $K$  is signer's private key
    - Check( $M$ , Sign( $M, K$ ),  $K^{-1}$ ) --  $K^{-1}$  is signer's public key

3

WASHINGTON STATE UNIVERSITY  
World Class. Now for Real.

**The real world**

- Problems – even if *encryption* is perfect ...
  - How does recipient know sender can be relied on?
    - Experience?, Authority?,
    - (Considerable motivation for dishonesty)
  - How does recipient know association of  $K^{-1}$  and a particular device?
    - Something told it – PKI? (Authority)
    - How trustworthy is the authority? (The problem is recursive!)
- In infrastructure-scale systems we cannot assume perfect reliability of devices and authorities – must deal with uncertainty

4

WASHINGTON STATE UNIVERSITY  
World Class. Now for Real.

**Asking the right questions ?**

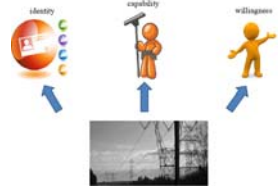
- "Secure" or "Not Secure" ?
  - If we are honest, the answer must be "not secure"
  - But this is not helpful! Life goes on
- "How secure" ?
  - Requires that we confront uncertainty that exists in the real world – one form of *risk*
  - Requires security *metrics*
  - How would we use such metrics?
    - To make decisions

5

WASHINGTON STATE UNIVERSITY  
World Class. Now for Real.

**So, what do we measure?**

- Technical parameters of encryption – key size, years to break, ...
  - Yes, but it's not enough
- Automate
  - Evidence gathering and processing
  - Decisions
- In addition to *identity* must have ways to talk about confidence in the *capability* and *willingness* of other parties
  - That is, "Trust"
  - Evidence-based
  - Useful in making decisions



6

**WASHINGTON STATE UNIVERSITY**  
*World Class. Never Stagnant.*

## Trust is ...

- For us, *only* of interest for how it affects decisions
  - Ignoring “emotional trust”
- Predictive about the real world
  - Therefore uncertain
- Context dependent
  - By purpose
  - By time
- Subjective
  - Different trustors, given same evidence, may evaluate trust metric differently

7

**WASHINGTON STATE UNIVERSITY**  
*World Class. Never Stagnant.*

## Decision Theory

- Choose particular decision from some space of possible decisions to minimize the *expected* cost
  - For each possible outcome there is a cost
    - This is the decision maker’s subjective *penalty function*
    - Example:
 

	Rain	Clear
Picnic	+50	-50
Indoor	0	+25
  - For each decision there is a distribution on the possible outcomes, determined from evidence
    - Also, in general, subjective: depends not only on the evidence but the decider’s prior distribution for the outcomes
    - Example: if it’s cloudy, I might predict 75% rain chance and you might predict 25% rain chance

8

**WASHINGTON STATE UNIVERSITY**  
*World Class. Never Stagnant.*

## Trust Metrics

- A trust metric should be
  1. Based on evidence
    - a) Trustor’s experience with trustee
    - b) Maybe, the experience of others (do we *trust* their recommendations?)
  2. Formulated for use in a decision procedure
  3. Assessable: does its use result in objectively better decisions?
- Much of the computational trust research to date
  - Ignores goals 2 and 3
  - Uses arbitrary mappings of experience to the metric
    - Which you can do if you ignore goals 2 and 3

9

**WASHINGTON STATE UNIVERSITY**  
*World Class. Never Stagnant.*

## Example: Credit Reporting


- Credit reporting system
- Lenders report their experience with borrowers to credit reporting agency
- Agency gives potential lender a summary of borrower’s past behavior
- Lender decides: to make loan or not; what terms to offer
  - Lender assesses the ability and willingness of borrower to repay
  - Also considers things like collateral offered
  - Assessment is based on lender’s experience with borrowers having similar credit reports

10

**WASHINGTON STATE UNIVERSITY**  
*World Class. Never Stagnant.*

## Example: Credit Scoring

- As in the previous example, except
- Credit agency calculates a credit score based on the credit report evidence (a single number)
- Lender uses credit score in place of detailed evidence in its decision making
- Credit scoring is itself a decision-making process



11

**WASHINGTON STATE UNIVERSITY**  
*World Class. Never Stagnant.*

## Why does this work?

- Lots of experience data – not just for individuals but for whole population
- Observed positive correlation of experience data with loan performance
- Risk pooling: lender really cares about penalty for whole pool of “similar” borrowers, not any single borrower
- System is resilient against failure of appreciable number of loans
- Was the sub-prime mortgage crisis of 2008 an example of failure of this system?

12

## Will this work for CI Security?

- Maybe
  - “Secure” or “not secure” doesn’t work
  - Decision theory is applied successfully in many domains to get objectively better decisions
- However,
  - Success requires gathering the right evidence and correctly interpreting it
  - Also need appropriate penalty functions
  - Credit system is very tolerant of failures, which occur frequently
  - Security failures in CI systems are potentially disastrous

13

## Conclusion

- CI systems at the scale of the power grid must face up to uncertainty of cyber security
- Even robust techniques like digital signatures are at the mercy of potentially untrustworthy participants
- The “trust” concept seems to appropriately capture important notions of prediction and uncertainty
- This must be coupled with decision making processes to be useful
- Making it work will take a lot of data and experience

14



# An Analysis on Teaching Methods Using a WBT System “CollabTest” Enabling Students to Create Quizzes Collaboratively

Masanori Takagi<sup>\*</sup>, Keizo Yamada<sup>\*</sup>, Jun Sasaki<sup>\*</sup>,  
Tetsuya Kaneko<sup>\*\*</sup>, Masamitsu Mochizuki<sup>\*\*\*</sup>, and Yoshimi Teshigawara<sup>\*\*\*\*</sup>

<sup>\*</sup> Faculty of Software and Information Science, Iwate Prefectural University, Japan

<sup>\*\*</sup> Center for Excellence in Teaching and Learning, Soka University, Japan

<sup>\*\*\*</sup> Faculty of Business Administration, Soka University, Japan

<sup>\*\*\*\*</sup> Faculty of Engineering, Soka University, Japan

{takagi-m, k-yamada, jsasaki}@iwate-pu.ac.jp, {ktetsuya, mochi, teshiga}@soka.ac.jp

**Abstract** - In this paper, we propose a teacher support function in order to reduce the load to use our developed system named “CollabTest”. In addition, we report methods for effective utilization of the system by using feedback obtained from teachers via questionnaires and interviews.

**Keywords:** Problem Posing, Peer Review, Online Test

## 1 INTRODUCTION

Recently, e-learning systems which enable learners to independently create quizzes have been actively studied [1, 2]. We previously developed a web-based learning system named “CollabTest” that enables learners to acquire knowledge by creating quizzes and sharing them with their peers [3]. A noteworthy feature of our system is the collaborative environment for quiz creation. Moreover, we have employed this system continually since 2002 at educational institutions. As a result, CollabTest has been used in a total of 158 courses over 8 years, and 7856 learners and 53 teachers have used the system. In addition, learners have created 21165 quizzes and posted 50890 comments. From these practical studies, we have demonstrated that CollabTest has the potential to improve study time effectively and students who have actively used it have improved their test scores.

However, educational models or methods to improve the educational effects using CollabTest are still unclear. For this reason, the outcomes of using the system differ widely among teachers. For example, because the system provides many functions, it is difficult for teachers to determine which functions they should use and how to use them in order to achieve their course objectives. In order to solve this problem, we propose a teacher support function which displays a guideline of CollabTest<sup>1</sup>.

## 2 PROPOSAL AND OBJECTIVE

Figure 1 shows an outline of our proposed function. First, a teacher selects a desired effect. And then, the minimum functions to need to achieve the effect will be selected

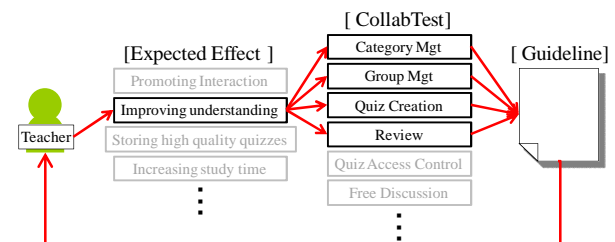


Figure 1: Guideline Function

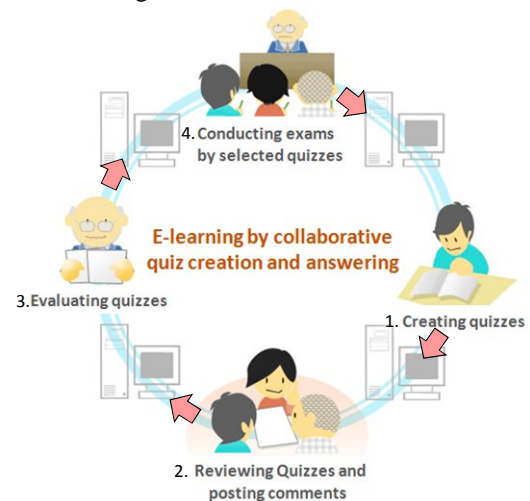


Figure 2: CollabTest Basic Learning Procedure

automatically. Next, CollabTest will automatically display a guideline showing ways of using the loaded functions. Teachers use our system referring to the guideline.

The purpose of this study is to determine the models and methods for using CollabTest effectively. In addition, the related studies have not clarified them. We intend to develop a guideline for teachers that describes the procedures and precautions for promoting learning through quiz creation and peer review et al. In this paper, we issued questionnaires and conducted interviews with teachers to analyze how CollabTest has been used in their classes.

## 3 COLLABTEST

Figure 2 shows the learning procedure for creating, reviewing, and taking quizzes as performed by learners:

- I. Create quizzes with explanation of quiz content.
- II. Review the quizzes collaboratively in a group.

<sup>1</sup> The work reported in the paper was supported in part by Grant-in-Aid for Scientific Research (B) (No.21300315) from the Ministry of Education, Culture, Sports, Science and Technology of Japan.

- III. Submit quizzes to their teacher.
- IV. Take student- or teacher-created quizzes to test their comprehension.

This procedure is conducted during or after class. When learners register a quiz, they must select a category item registered by their teacher as all quizzes are managed using category items. After learners start using the system, teachers need to assess the quizzes created by their students, post comments, and create tests.

## 4 DATA COLLECTION AND ANALYSIS

We investigated the effective methods for utilization of the CollabTest system by questionnaires and interviews. The investigation was conducted from the semester beginning in September 2007 to the semester beginning in April 2010.

### 4.1 Questionnaires

We asked Teachers: "What did you do to use the CollabTest system effectively?" Then we analyzed responses from teachers who had used it effectively. From these results, we identified that clarifying the quiz theme and the number of quizzes which students had to create, and giving learners time to create quizzes during a class are effective methods when teachers ask students to create quizzes. Moreover, the results show that setting deadlines for submitting or answering tests is important to ensure that these tasks are done. In addition, we confirmed that reorganizing the group periodically is an effective strategy.

### 4.2 Interviews

We interviewed some teachers to investigate the effective educational methods of the CollabTest system. From the results, we confirmed the following 4 methods.

#### (1) Quiz Creation and Peer Review during Class

In the course "Information System Theory and Engineering", taught at Iwate Prefecture University, a teacher effectively conducted tests and quiz creation during classes. He conducted a test during the first 30 minutes of the class to assess the comprehension level of the contents of previous lessons. The test items were produced by correcting and integrating quizzes created in previous classes. First, students answered the test on paper. Next, each student marked another student's test. Then the teacher explained each quiz to the class. Thereafter, he taught new contents for 30 minutes and finally encouraged learning by asking students to create a quiz on the new course content.

#### (2) Cooperative Reuse in Two or More Courses

In the "TOEIC Intermediate Course", taught at Soka Women's College, students did not create any quizzes. However, the teacher conducted online tests during each class using quizzes created in the similar course "Seminar A", in which English language instruction was the objective. In "Seminar A", 16 students created 770 quizzes throughout the first semester. This was the most active course in which CollabTest has ever been used. The teacher provided thorough instructions for describing the explanations in detail and evaluated all quizzes. As a result, the quizzes received favorable comments such as "the explanations were

written in more detail than any commercial reference books" and "the explanations were easy to understand."

### (3) Integration of CollabTest Learning and Classroom Learning

A teacher used the CollabTest system in a classroom which had no PC. In the course "Teaching Method", taught at Soka University, he effectively integrated learning in CollabTest with learning in the classroom. He also adopted face-to-face workgroups in each class. The flow of this course is shown below.

- I. Students create more than 3 quizzes each.
- II. Each student answers all quizzes created by their group members, then posts more than 5 comments for each quiz.
- III. Students select 2 quizzes from their group and submit them to their teacher.
- IV. The teacher opens all quizzes submitted by students as online tests in the course.
- V. The teacher selects appropriate quizzes from those submitted and conducts class tests.

In the above-mentioned tests, the teacher placed each quiz on a MS PowerPoint slide and displayed it to the students with a projector. Students responded to the quizzes using a clicker, which is an audience response method. Students took the test twice; first, they answered the test on their own, then they answered it as a group.

### (4) Other Methods for Using CollabTest

At the Kyushu Institute of Technology, our system has been used by a teacher and TA to create and store quizzes which are used in the "Information Processing" course. The teacher and the TA were both registered as student users, then they created quizzes and reviewed them interactively. From this practice, we could confirm that our system is also capable of providing an environment for teachers or TAs to create quizzes.

## 5 CONCLUSION

In this study, we proposed a teacher support function which displays a guideline of CollabTest. In addition, we analyzed the effective uses and teaching methods of the CollabTest system from the questionnaires and interviews. In the future, we will analyze the relationship between these methods and functions provided by CollabTest. We will also create guidelines for each teaching method.

## REFERENCES

- [1] M. Barak and S. Rafaeli, On-line question-posing and peer-assessment as means for web-based knowledge sharing in learning, *International Journal of Human-Computer Studies*, Vol.61, No.1, pp.84-103 (2004).
- [2] Fu-Yun Yu, Yu-Hsin Liu and Tak-Wai Chuan, A web-based learning system for question posing and peer assessment, *Innovations in Education and Teaching International*, Vol.42, No.4, pp.337-348 (2005).
- [3] M. Takagi, M. Tanaka, and Y. Teshigawara, A Collaborative WBT System Enabling Students to Create Quizzes and to Review Them Interactively, *Transactions of Information Processing Society of Japan*, Vol.48, No.3, pp.1532-1545 (2007).

# Enhancement of Questionnaire on Anshin

Dai Nishioka\*, Yasuhiro Fujihara\*, and Yuko Murayama\*

\*Graduate School of Software and Informatics, Iwate Prefectural University, Japan

d.nishioka@comm.soft.iwate-pu.ac.jp

{ fuji, murayama }@iwate-pu.ac.jp

**Abstract**—We have conducted the user survey on Anshin of the users for the information security technology by questionnaire and factor analysis. However, those question items in the questionnaire might not be enough to extract Anshin factors correctly, because we did not review those items scientifically. From this viewpoint, we used brainstorming and KJ method to review the questionnaire. As a result, we come up with two new types of question items. This paper reports on our findings.

**Keywords:** Questionnaire, Brainstorming, KJ method, Web survey

## 1 INTRODUCTION

Anshin is a Japanese term that indicates the sense of security and safety. The concept of trust is investigated as the research which is similar to Anshin in the Europe and USA [1][2][3]. Trust has been researched sociology, psychology and economics. Deutsch introduced to look forward to others as confidence about the trust [4][5]. Marsh proposed the computational trust model with trust values of -1 to +1[6]. We have identified that Anshin is the emotional part of trust [7]. We are currently working on Anshin to derive the factors of Anshin [8][9]. We conducted the user survey with a questionnaire and perform a factor analysis on the survey responses. The original questionnaire was produced based on the responses from free description on a questionnaire for the students from Department of Software and Information Science in our university; a question looked like "What makes you have Anshin?" This is a popular way to produce a questionnaire. One may wonder, due to their intuitive nature, whether those questions are enough to extract Anshin factors. We presume that producing a good questionnaire would be critical to extract Anshin factors successfully. In this research, we try and improve the questionnaire so as to obtain enough questions for comprehensive coverage of Anshin factors. In this research, brainstorming [10] and KJ method [11] are considered as our research methods. The brainstorming is used for idea generation by group instead of individuals. Therefore the brainstorming is preferred over free style idea generation. KJ method is an information organization method. Matching words as well as phrases in this process is based on semantics but not letter.

## 2 THE REVIEWING OF QUESTIONNAIRE

### 2.1 Research Method

In this research, we created a questionnaire using the techniques such as brainstorming and KJ method. Brainstorming is used for generating ideas with a group of

people rather than with an individual. Brainstorming has 4 rules as follows:

1. **Focus on quantity**
2. **Without criticism**
3. **Welcome unusual ideas**
4. **Combine and improve ideas**

The first rule is "Focus on quantity". As for Brainstorming, the quantity is more important than the quality. The participants of the brainstorming are required to provide a lot of ideas. The second rule is "Without criticism" The participants do not allow denying the ideas which the other participants provide. The third rule is "Welcome unusual ideas." Unusual ideas are welcomed. The participants are required not to deny their ideas. The fourth rule is "Combine and improve ideas" Ideas are combined to form a single better good idea.

KJ method is bottom up clustering. A process of the KJ method consists of the following *processes*:

1. **Card making process**
2. **Grouping and naming**
3. **Chart making process,**
4. **Explanation**

Card making process is to write ideas on individual cards. At grouping and naming process, we find similar cards and put them into one group, and give a label for each group. If we have ten or more groups as a result, these steps are iterated until we obtain less than about ten groups. At chart making process, we make chart that contains relations of each group on a large sheet of paper. Explanation process is to determine description of findings throughout the previous stages

### 2.2 Investigation on question items

We conducted the brainstorming users' images of Anshin. We asked the subjects what makes them feel Anshin when they use the credit card at on-line shopping. Also, the author didn't participate in the discussion and had done him/her investigation only in the examinees. As a result of the brainstorming, we had in total 46 items. Next, we organized 46 items using KJ method. As a result of KJ method, 46 items into the seven groups. We reviewed the new questionnaire generated as a result of this new approach. We compared questions in the new and old questionnaires. As a result, 22 questions appeared in both, and 24 appeared only in the new one. There are 28 questions in the old one. And we compared the extracted opinions and group of the KJ method. The Result of comparison, 24 opinions were not included in the previous questionnaire, and, those items are in two groups of KJ method. This result, we introduced items of two groups in the new questionnaire

Group 1. Third Party

Sample opinions: third-party intervention as a negative opinion, compensation benefits by credit card companies, hidden/implicit involvement of the third-companies in commerce

Group 2. Knowledge other than information technology

Sample opinions: company profile (e.g. location, capitals, executive officers, history), product information presented on the web site, hidden/implicit involvement of the third-companies in commerce, prompt announcement of product recalls.

### 2.3 Make the questionnaire

We created the new questionnaire which was created a result of brainstorming and KJ method. The new questionnaire would consist of 52 items. (Previous questionnaire: 28 items, this survey: 24 items) However, we thought that the number of questions is too many. So, we reduced the number of question items to 36. (Previous questionnaire: 24 items, this survey: 12 items). We organized a question items using the KJ method and decreased these to 36 question items. In the new questionnaire, we use a 7-point scale of preference, ranging from strongly agree (1) to strongly disagree (7).

## 3 WEB SURVEY

### 3.1 Result of Web Survey

We conducted a new survey using the new questionnaire. The specification of this investigation is as follows:

**Purpose:** The correction of sentences of the question items

**Assumption:** Subjects uses on-line shopping with the credit card

**Schedule:** 22 and 23, July, 2010

**Number of Subjects:** 103

We conducted some statistical analysis. We focused at seven types to consider.

1. ceiling effect,
2. floor effect
3. The absolute value with high skewness kurtosis
4. The absolute value with high kurtosis
5. The value with high median
6. Cronbach's alpha coefficient

This result, we have 3 question items whose floor effects is problem, 2 question items whose kurtosis is high (over 2), 1 question items whose median is high (over 4), 5 question items whose Cronbach's alpha coefficient is problem. Therefore, these question items need to be further studied. We conducted factor analysis. We focused at one type to consider.

1. The value with low commonality

Explanatory Factor Analysis with Maximum Likelihood method and Promax rotation is used. We used PASW Statistics Base 18. As a result of this investigation, we have 6 question items whose commonality is low (under 0.4). Next, we did Explanatory Factor Analysis without 6 items. As a result of this investigation, we have 4 question items whose commonality is low (under 0.4).

## 3.2 Discussion

We have 16 problem items from statistical analysis and factor analysis. 3 items are in the 'Knowledge other than information technology' group, out of 8 totals. 4 items are in the 'Third party' group. That is the entire group. The other problem items are previous question items. Therefore, it is necessary to correct the problem items in the 'Knowledge other than information technology' group. Also, the entire 'Third party' group needs reviewing. We have 10 problem items from Evaluation of KJ method. Study is necessary to use the KJ method. This subject did not have the knowledge of the KJ method. Consequently we were thought that subjects may have chosen different groups. Therefore, we have to consider changing these items to semantic. We should consider to correct the problem items by semantic.

## 4 CONCLUSION

We have investigated the brainstorming and KJ method to make a better questionnaire for Anshin investigation. We extracted seven factors based on personal information exclusively about the online shopping. Also, we found new two factors. Two factors are "Third Party" and "Knowledge except information technology".

We conducted a preliminary case study on online shopping users using a questionnaire produced via this novel approach. In the future works, we further refine those question items and investigate using the correcting questionnaire.

## REFERENCES

- [1] Xiao, S. and Benbasat, I.: Understanding Customer Trust in Agent-Mediated Electronic Commerce, Web-Mediated Electronic Commerce, and Traditional Commerce, Information Technology and Management, Vol.4, No.1- 2, Kluwer Academic Publishers, pp. 181-207 (2004).
- [2] Xiao, S. and Benbasat, I.: The formation of trust and distrust in recommendation agents in repeated interactions: a process-tracing analysis, Proc. of the 5th international conference on Electronic commerce (ICEC'03), pp. 287-293 (2003).
- [3] D. Gambetta: Can we trust trust?, Making and Breaking Cooperative Relations, electronic edition, Department of Sociology, University of Oxford, chapter 13, pp. 213-237 (1988).
- [4] Deutsch, M.: Trust and Suspicion, The Journal of Conflict Resolution, Vol. 2, No. 4, pp.265-279 (1958).
- [5] Deutsch, M.: The effect of motivational orientation upon trust and suspicion, Human Relations, 13, pp.123-139 (1960).
- [6] S.P. Marsh: Formalising trust as computational concept, PhD Thesis, Department of Mathematics and Computer Science, University of Stirling (1994).
- [7] Murayama, Y., Hikage, N., Fujiwara Y. and Hauser, C.: The structure of the sense of security, Anshin, Proc. of CIRITS2007 pp.85-96 (2007)
- [8] Hikage, N., Hauser, C. and Murayama, Y. : A Statistical Discussion of the Sense of Security, Anshin Information Processing Society of Japan Journal Vol.48 No.9 pp.3193-3203 (2007)
- [9] Fujihara, Y., Yamaguchi, K., Y., Murayama, Y. : A Statistical Discussion of the Sense of Security, Anshin Information Processing Society of Japan Journal Vol.50 No.9 (2009)
- [10] Alex F. Osborn: YOUR CREATIVE POWER, Motorola Univ Pr; abridged edition (1948)
- [11] Kawakita, J.; "*KJ method - a scientific approach to problem solving*," Kawakita Research Institute, 1975.

# Evaluation and Agendas of Wireless Input Device for Tiled Display Desktop Environment

Akira Sakuraba\* and Yoshitaka Shibata\*

\*Faculty of Software and Information Science, Iwate Prefectural University, Japan  
g231i015@s.iwate-pu.ac.jp, shibata@iwate-pu.ac.jp

**Abstract** - Many tiled display environments are proposed as a visualization tool, presently interaction between user and systems is using generic mouse and keyboard. These generic devices are causing interaction burden for users because it is not intuitive. We developed a wireless interactive pointing device system on a tiled display desktop environment. The aim of this system would be alternative mouse and keyboard input method. In this paper, we evaluate the performance of the prototype system feature in real configuration. Finally we discuss some agendas in further development from the results of evaluation.

**Keywords:** Tiled display, Human-Computer Interaction, Input devices

## 1 INTRODUCTION

Ultra high-definition displays are very effective devices for large amounts of data processing tasks and used for tele-immersion, visualization and geographic information systems. Those tasks need viewing function of high resolution content without resizing, especially down scaling, because many applications using those systems require high-definition display devices for representation or analytical results by scientific computations. On the other hand, PC clustering technology is a prevailing one using low-cost PC and high speed networks. For the applied technology of PC clustering for representation, tiled display technology is proposed. The tiled display is a high-definition display system which uses clustering hosts to organize a display environment. Tiled displays can be realized with low initial cost and high scalability.

There are issues for tiled display environments as a tool for visualization device systems. For instance, most of the tiled display systems do not equip dedicated input interface devices.

However these generic input devices have some problems between the display space and interaction space. In other words, ordinary mice used by horizontal operations on the desk. Meanwhile, almost all tile displays are set up vertically. This difference forces burden of mismatch of interaction against the user of these visualization system.

In this paper, we propose a wireless interactive input device system for tiled display systems operated on desktop environments. This method allows interaction with desktop environments intuitively and liberates user location restriction. As an input device, users grip a video game controller to interact with the application. The aim of this system is to provide high application independent and

intuitive interaction for users of the application on tiled displays. We use some infrared markers to discern the display position, which are placed on top of the display wall. Then we evaluate system configurations and develop several agendas based on results, to further develop the system.

## 2 RELATED WORK

Scalable Adaptive Graphic Environment (SAGE) [1] is a high-scalability display system. SAGE is able to deal with many different applications as videos, digital images, and 3DCG objects. However, the operation of the SAGE user interface cannot directly pass the input events to the applications. The other issue is that the conventional mouse and keyboard are still used as interaction devices.

Chiba et al. proposed a Windows based desktop tiled display system [2]. In this system, pixel data as desktop images are received through a virtual display driver from Application Host. However, a conventional mouse and keyboard are still used for user interaction the same as the Windows PC environment.

Human computer interactions for all of these tiled displays are delivered using generic mouse and keyboard, the instinctive and direct operations and functions for the contents by this device are very low and provide inconvenience for user interactions.

## 3 DETAIL SYSTEM

In order to resolve those problems, we propose a new interactive system for tiled display environment, DETAIL (Direct input Environment for Tiled display with Active Infrared Lighting). DETAIL System provides an alternative mouse operation method in desktop space on tiled display and hotkey input feature.

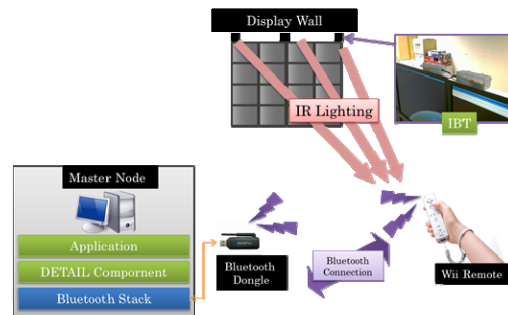


Figure 1: Configuration of DETAIL System.

This proposal system is organized by, DETAIL Component as software component on the master node,

hand-held human interface device and IR lighting devices which are placed on the top of display wall. Figure 1 shows system configuration of DETAIL.

At the system setup, a Bluetooth dongle is connected to the master node and establishes a connection channel between the master node and input device to send input device status. This status includes the current values of the internal sensors, the status of each button whether pushed or no. Among the status parameters of the human interface device, we use the button status to perform hotkey input functions and CMOS IR sensor image to estimate the position which is pointed to on tiled display wall. We use a single Wii Remote [3] for an interface device.

Pointing position estimation requires some IR markers to define display location on DETAIL System. For available pointing estimation, the system requires at least 2 units of Infrared Beam Thrower (IBT), which are placed on the top of the tiled display wall. There is another conformable device in the previous study as a middleware on a collaborative virtual environment interface device, we use the button status to perform hotkey input functions and CMOS IR sensor image to estimate the position which is pointed to on the tiled display wall.

We designed an arc-shaped alignment of IR LEDs on board as a unit of IBT in Figure 2. On each IBT, there are 3 subunits which are mounted by 3 IR LEDs. Figure 3 shows the area which they are able to light from top view.

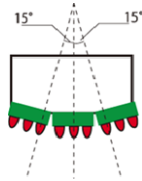


Figure 2: Arrangement of IR LEDs on a single IBT

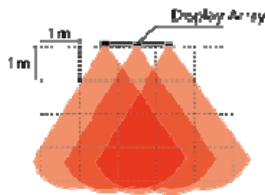


Figure 3: Estimated lighting area with 3 IBTs from the top view.

## 4 EVALUATION AND AGENDAS

In the first evaluation experiment, we measure identified points of received IR light from each IBT while Wii Remote was paused. Figure 4 shows the result of this evaluation. Compared to the lighting device in [4], it is possible to receive in a larger area.

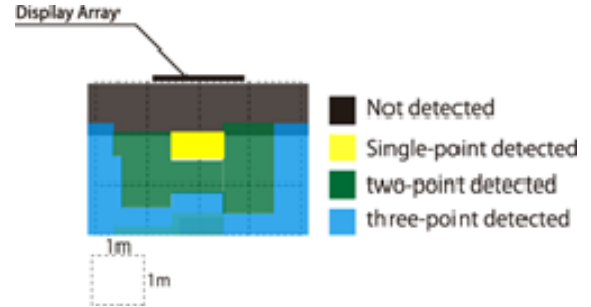


Figure 4: Received number of signals from IBTs from the top view.

Another evaluation measures the ability of point-able coverage area from user's position of located in front of display wall. We did some trials from points which cover nearly all area of display wall. In this experiment, we cannot calculate pointed position because the Wii Remote did not receive signal from IBTs while Wii Remote is fast-moving. Another reason is caused by angle of view of CMOS camera within the Wii Remote.

We have several agendas by result of these evaluations for further development, using the acceleration and Gyro sensor within the Wii Remote and append identity feature of IBT to the system.

## 5 CONCLUSION

In this paper, we proposed a wireless input device system for tiled display desktop environments using the Wii Remote. In this system, conventional mouse operation can be realized using multiple IR markers on top of a display wall to estimate the pointing locations. As future works, more scalable system independent to the installation of the display array will be considered. Also more high resolution method by measuring input resolution on the prototype system is considered.

## REFERENCES

- [1] Scalable Adaptive Graphics Environment (SAGE), <http://www.ev1.uic.edu/cavern/sage/index.php>
- [2] G. Chiba, T. Ishida and Y. Shibata: "High-Resolution Presentation Environment Using Multi Displays". ainaw, pp.1012-1016, 22nd Int'l Conference on Advanced Information Networking and Applications – Workshops, 2008.
- [3] "Wii Remote", [http://www.nintendo.co.jp/wii/features/wii\\_remote.html](http://www.nintendo.co.jp/wii/features/wii_remote.html)
- [4] K. Yatsu and Y. Shibata: "A Middleware System to Realize Virtual Reality on Tele-immersion Environment", waina, pp.560-563, 2009 Int'l Conference on Advanced Information Networking and Applications Workshops, 2009



# Self-Powered Independent Communication Network System for Emergencies

Toshihiro Suzuki\*, Yoshitaka Shibata\*

\*Graduate School of Software and Information Science, Iwate Prefectural University, Japan  
g231i023@s.iwate-pu.ac.jp, shibata@iwate-pu.ac.jp

**Abstract** - Recently, wireless LANs have spread rapidly. They are excellent at mobility, portability and easy installation. These advantages are suitable for use as disaster information networks. However, in the case of actual disaster, electric power lines are also damaged and those wireless LANs cannot function. In this paper, we introduce a power saving wireless LAN for disaster use with a solar panel, wind turbine, and battery combination, so that an autonomous wireless network can be established and provide normal network functionality even though the electric power and wired network are seriously damaged. In this paper, we designed a self-powered wireless disaster information network, and constructed a prototype system to evaluate the functional and performance.

**Keywords:** disaster information, wireless network, network engineering

## 1 INTRODUCTION

Japan is an island nation occupied more than 70 percent by mountainous districts. Moreover, in Japan, natural disasters are frequent occurrence, such as earthquakes, tsunami, typhoons, heavy rain, and snow. Once a large disaster happens, serious damages to communication base stations due to power failure are unavoidable [1]. For those problems, the usual information infrastructure cannot be used when the disaster occurs. Especially, since the stoppage of the information infrastructure causes the isolation of the entire region, a network for emergency cases which can be easily and quickly reconstructed to be used for disaster relief is strongly required. In this study, the wireless relay station system for disasters used under continuously running duty is constructed based on a self-power supply via the hybrid power generating system.

Moreover, by integrating this wireless system together with inter-vehicle communication and wireless balloon networks, a large independent telecommunication network system for disaster use can be realized. In this paper, a prototype system that performs the compositional and basic elemental functions as mentioned above is described.

## 2 SYSTEM CONFIGURATION

Our proposed system is composed of several components to establish the independent telecommunication network system for disasters. The actual network configuration for disaster use is shown in Figure 1. In this system, Self-Powered Wireless Base Stations are proposed [2].

### 2.1 Self-Powered Wireless Base Stations

The Self-Powered Wireless Base Stations consist of one or more wireless LAN access points, solar panels, a wind turbine, and battery, and an IP-based digital camera. Thus all electricity used in this station are self-supplied. Through this base station, wireless terminals nearby can communicate with each other and access the Internet since this base station also performs a gateway function to the Internet.

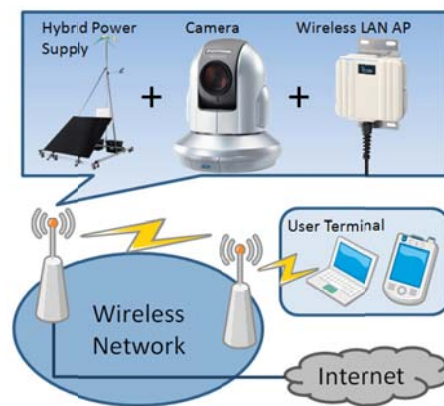


Figure 1. System Configuration

In electric power generation, using sunlight and the force of the wind, it is difficult to supply all of the energy required for the base station on continuous duty because the amount of power generation depends on natural conditions like sunshine and the velocity of the wind, etc. However, when the network infrastructure can work using only natural energy, any excess energy is accumulated to the battery, and, vice versa, the accumulated battery energy can be used when the natural energy is not enough to supply the total system. Additionally, an IP-based camera is equipped as a composition of the base station to watch the situation around the station by remote control, with pan/tilt/zoom operations from a remote site through the Internet over the wireless network as shown in Figure 1.

In this research, we designed our proposed system to be used in cases where the commercial power source cannot be used, such as in unfavorable geographical features such as in a canyon, or other cases where power failure has occurred because of a disaster. For this reason, this system includes a power generation system which is a combination of solar panels and a wind turbine because this is set up outdoors.

When the network in wireless LAN system is constructed at the base of a canyon, it is necessary to consider the conditions of land slope and obstacles such as trees in the forest. This network system also should be able to adjust the degree of the antenna direction to relay communication paths by multi-hopping the other base stations. In actual field operation, it is necessary to improve the antenna gain with strong directivity in the case where the amount of multi-hopping is increased to avoid the obstacles. Oppositely, the wide range of communication from the wireless LAN base can be preferable when there are obstacles around it.

For this reason, in our system, a wireless LAN access point built for outdoor use with exchangeable antenna was used to meet this requirement. As a result, the advantage of exchangeable antennas and changeable antenna positions and waterproof and dustproof facilities for wireless LAN equipment simply can be realized.

## 2.2 In-Vehicle Mobile Access Point

Self-Powered Wireless Base Stations will mainly be used in mountainous districts. In contrast, the In-Vehicle Mobile Access Point is designed for use in the vicinity of the foot of the mountains.

By setting up the wireless network equipment in a car, it becomes possible to move around the stricken area.

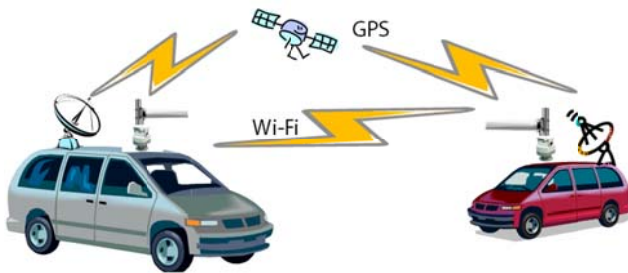


Figure 2. Inter-Vehicle Communication Network

This system uses the directional antenna to extend the communication distance, to enable contact with the mountainous region and other car nodes.

But directional antennas have narrow coverage, so this system has the ability to turn the antenna in the direction to be communicated with automatically.

GPS and a gyroscope are used for the measurement of the position of other communicants. The power never depends on an outside source because it is supplied by a gasoline generator. [3]

## 3 PERFORMANCE EVALUATION

### 3.1 Amount of power generation

This evaluation was to measure how the wireless LAN base station can work under a continuous duty load in both daylight and night by the hybrid power generation system. It is known that the combined power consumption of the wireless LAN access point and the network camera are about 207.6Wh and 211.2Wh, respectively

The transitional voltage of the accumulated electricity in the battery is shown in Figure 3.

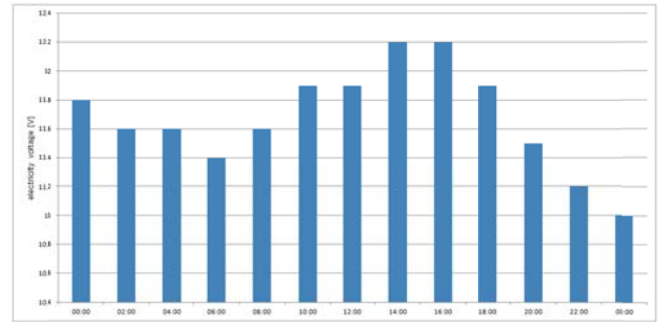


Figure 3. Transitional voltage of the accumulated electricity in battery

The weather on the evaluation day was mostly calm and cloudy: the total power generation was only 502Wh because the period of sunlight was under the average value. It is estimated that electric power was consumed from the battery without any electricity being accumulated the internal energy loss that occurred. As a result, voltage level of the battery became lower than at the beginning of the measurement period as can be seen from Figure 3. However, the final accumulation of electricity voltage was 11.0V and did not descend under 10.2V which is a critical level at which the feeding power system stops (as discovered through a preliminary experiment a priori to this evaluation).

## 4 CONCLUSIONS

In this paper, we proposed Self-Powered Wireless Base Stations for disaster use with a combination of solar panels, a wind turbine, and a battery for emergency use when the electric power and wired network are seriously damaged. Through the field operation, we confirmed that our suggested system could be used effectively in the mountainous districts as a wireless base station. Currently we are evaluating performance and various other functions such as control function for the energy-saving of the installing equipment based on acquired data and continue with the Inter-Vehicle Communication Network.

## REFERENCES

- [1] Daisuke Nakamura, Noriki Uchida, Hideaki Asahi, Kazuo Takahata, Koji Hashimoto, Yoshitaka Shibata "Wide Area Disaster Information Network and Its Resource Management System", AINA'03, March 2003.
- [2] Goshi Sato, Noriki Uchida Daisuke Asahizawa and Yoshitaka Shibata, "Power Saving Cognitive Radio LANs for Disaster Information", The 12th International Conference on Network-Based Information Systems, (NBIS2009), CD-ROM, August. 2009.
- [3] Daisuke Asahizawa, Yoshitaka Shibata, "Research on Automatic Directional Antenna Control System for Long Distance Wireless Network in Disaster Situation", DPS142, (in Japanese), March 2010



# Internet Connection Over Challenged Network for Disaster Information System

Yutaka Sasaki\* and Yoshitaka Shibata\*\*

\*Graduate School of Software and Information Science, Iwate Prefectural University, Japan

\*\*Faculty of Software and Information Science, Iwate Prefectural University, Japan

\*g231i018@s.iwate-pu.ac.jp, \*\*shibata@iwate-pu.ac.jp

**Abstract** –Our project is to build a disaster information system that can function even when Internet connection is disrupted. We have previously built the disaster information system as web application. However, the system becomes unusable when Internet connection is disrupted and when the base-station is become under a stress state. We apply the DTN (Delay Tolerant Networking) architecture to our new disaster information system in order for the system to communicate over challenged networks.

**Keywords:** DTN, application, disaster information system.

## 1 INTRODUCTION

For a long time, Japan has been exposed to the menace of the natural disasters such as earthquakes, typhoons, and tsunamis. We recently experienced large-scale earthquakes, Niigata-Chuetsu Naibu earthquake and Iwate-Miyagi Nairiku earthquake. In order to save the lives and protect the properties of residents, we need to prepare for the anticipated large earthquakes in the future.

We constructed a disaster information sharing system that was able to share disaster information on Web-GIS in our previous research [1]. We implemented the system as web application. The system functions as long as the clients are connected to the Internet. However, it will be ineffective on networks when the large-scale disaster occurs, because frequent disconnect to the Internet may occur. And, there will be some regions that lose communications due to physical destruction of the base stations.

We propose a new disaster information system that uses the DTN (Delay Tolerant Networking) [2] technology over challenged networks.

## 2 RELATED WORK

The research on routing using DTN to efficiently deliver data to a target place has been actively conducted [3][4]. However, the routing over challenged networks has not been researched adequately. Recently, some researches provide the application service over challenged networks [5][6]. These systems are enabled to exchange chat messages and mails over challenged network.

Our approach is to provide the disaster information services by an application level.

## 3 SYSTEM ABSTRACT

The system overview of current system and our proposed system are shown in Figure 1. In current system, these users can use the system normally when the Internet connection is

up. However, when a disaster strikes, the base-station becomes under a stress state and the Internet connection is disrupted. Our proposed system installs a DTN server and DTN clients in networks. The users have DTN client software, and the DTN mobile server is a gateway to the Internet. These users can use the system through the DTN server when the base station is under stress.

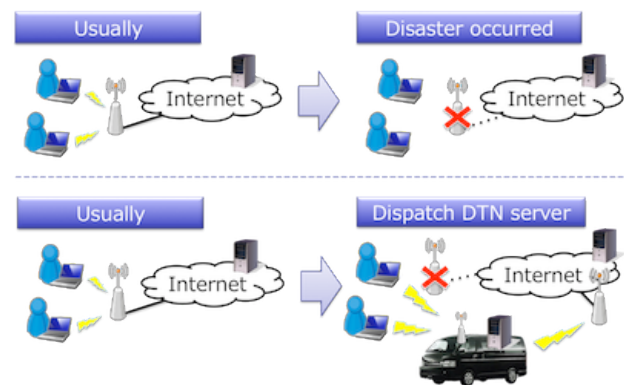


Figure 1: System overview.

### 3.1 DTN Architecture

We apply the DTN architecture that makes communication over challenged networks possible. The DTN architecture is originally developed for communication between planets. The DTN technology considers frequent disruption and delay. It is suitable communicating over challenged network. Store and forward scheme is used for the DTN clients and server communication when a neighbor node or the destination is detected. These nodes analyze communication situation in the background.

### 3.2 Disaster Information System

We previously implemented disaster information system as a web application. It provides stricken area information and safety information. Our new system will provide the same information as text-based messages to minimize the network traffic in challenged network.

## 4 PROPOSED SYSTEM

Our proposed system implements DTN functions using DTN2 [7]. The DTN2 is a freeware package and it has functions such as store and forward, neighbor node discovery, application data conversion into a bundle. We designed the DTN proxy to pass DTN2 data from the

application layer, to send and receive disaster information text messages and image types, and to monitor if the Internet access is possible.

#### 4.1 System Architecture

The system architecture of our proposed system is shown in Figure 2. The bundle layer is set up on the transport layer, and the DTN proxy is set up between DTN2 and the application layer. The DTN server has a web server and DBMS to provide disaster information over challenged networks. The DTN server is the Internet gateway. The DTN client has a web browser. The web browser and the DTN proxy communicate through own IP addresses in a loopback mode. The DTN proxy acts on behalf of the application browser. The DTN proxy's main function is to control the communication between web browser and DTN2, and to monitor the Internet connection situation in background, and to convert input data to XML file.

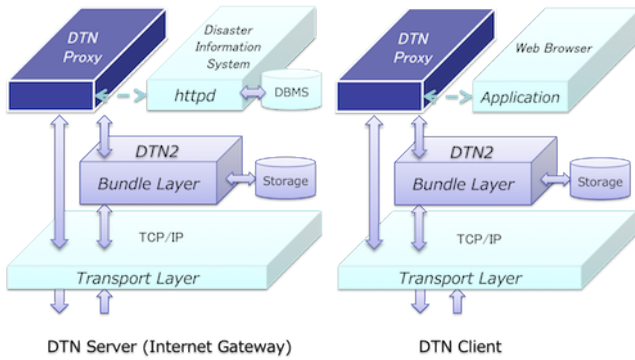


Figure 2: System Architecture

The system data flow when disaster information transmitted from a web browser of a DTN client is shown in Figure 3. First, a user inputs disaster information. Then, the web browser generates IP packets and sends to the network layer. The packets return to the DTN proxy through the route table. Then, the DTN proxy inquires its monitoring thread about communication situation. If communication situation is good, the packets are sent through TCP/IP over the Internet. If communication situation is bad, the packets are saved as XML file by the DTN proxy. The DTN proxy initiates the XML file transfer to the DTN server. Then, the XML file is converted into a bundle and stored in the storage. The stored bundles are transmitted to a neighbor node when detected.

## 5 SUMMARY

We proposed the disaster information system that can work even when network is challenged by broken base-stations. We use the DTN architecture to implement the disaster information system, using a mobile DTN server to maintain the Internet connection. The users can share the disaster information over challenged networks through the DTN server and the DTN client.

We have two design issues: (1) How can the server provides the disaster information over challenged networks

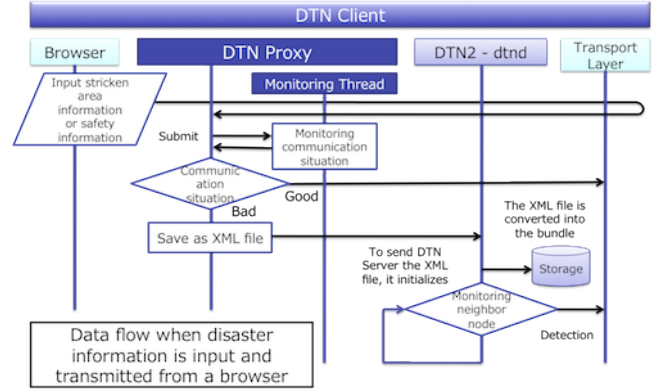


Figure 3: System Data Flow

(since the server is web-based). (2) How can information be synchronized between the DTN server and the Internet server.

## REFERENCES

- [1] Y. Sasaki, and Y. Shibata, A Disaster Information System by Unified Temporal Presenting Operation Facility, IPSJ, 3ZC-5 (2010).
- [2] Kevin Fall, A Delay-Tolerant Network Architecture for Challenged Internets, ACM SIGCOMM, pp27-34 (2003).
- [3] S. Jain, K. Fall, and R. Patra, Routing in a Delay Tolerant Network, ACM SIGCOMM, pp.145-157 (2004).
- [4] J. Ott, and D. Kutscher, Integrating DTN and MANET Routing, ACM SIGCOMM, pp.221-228 (2006).
- [5] R. Metzger, and M. Chuah, Opportunistic Information Distribution in Challenged Networks, ACM CHANTS, pp.97-104 (2008).
- [6] N4C Project, <http://www.n4c.eu/N4Cproject.php>
- [7] DTN2 Reference Implementation, <http://dtnrg.org/wiki/Code>

# Content Grouping on P2P Network

Takuya SASAKI\* and Jun SAWAMOTO\*

\*Iwate Prefectural University, Japan

g231i017@s.iwate-pu.ac.jp,sawamoto@iwate-pu.ac.jp

**Abstract** -In recent years, the diversification and ubiquitousness of information is rapidly advancing due to the development of information and communication technology. As for the usage of the information, it depends on the user. The attention to sharing information using P2P network rises, and it is increasingly being used in many fields. The distributed hash table (DHT) is one of the typical overlay networks on P2P. However, there is a problem of lacking of flexibility in the retrieval on a DHT. In this paper, to improve the convenience of the contents retrieval, we propose an efficient content retrieval method based on the grouping technique of the contents using the content access history and frequency.

**Keywords:** Network,Peer-to-Peer,clustering.

## 1 INTRODUCTION

In recent years information has become more diverse. Information is increasingly stored on the internet and communication technology has developed to give us more ways to access the internet. For example, at the shopping mall, goods information, inventory information, and campaign information is managed. More people search for information using the internet so, there is a larger load on the internet servers. Because P2P networks have smaller loads, more attention is being given to P2P networks.

The P2P network Model has smaller loads to the server than the Client Server Model. The address of a node is stored in an overlay network. In a P2P network, an overlay network exists as a network which manages node information. Each node uses a key and value for index information. An overlay network is divided into structured and un-structured. The DHT is stored in the structured part of the overlay network.

The DHT manages index information on the P2P network. It is possible to manage much more content information by using a DHT. Since a hash is applied to the content's name, a search will only return an exact match. As an example of representation of a distributed hash table, there are Chord [1] and Kademlia [2] and development of the algorithm of a distributed hash table is performed also in today. Various research and evaluations of the search engine in P2P structured networks using a DHT have already been performed[3].

When performing a search using a P2P network, my research aims at raising search efficiency. I suggest using a user's search history to group contents based on search frequency, and search group content based on the members of group.

### 1.1 Abstract

Unlike the client server model, the P2P network does not use the center server to search content. The P2P network manages content information by cooperation of each node.

There is research being done on other methods of grouping. There is research which performs grouping based on the vector of a Web page[4] and research which performs grouping based on the links of a Web page[5].

The user gets some content on one search then more Content is recommended from the grouping.

For example if a user searches for information on bookA. And bookA, B, C are grouped. The user will receive the information for bookA and links to bookB and bookC.

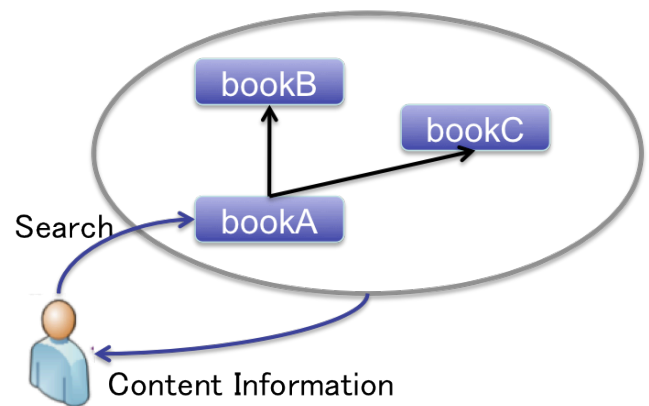


Fig 1 Content grouping

Grouping uses a lot of search histories from a server. An example of this would be Amazon's recommendation system. My suggestion is to use content grouping on P2P networks. When a node searches content information, the node circulates a relationship. Because node communication on p2p networks is distributed, my suggestion uses a smaller server load than the client server model.

It is judged whether contents are grouped based on how strong the relationship is between the content. Each node circulates how frequently it is searched. If a node is searched frequently a strong relationship is formed and it is added to the group. Content that is not searched is removed from the group.

## 1.2 NodeCommunication

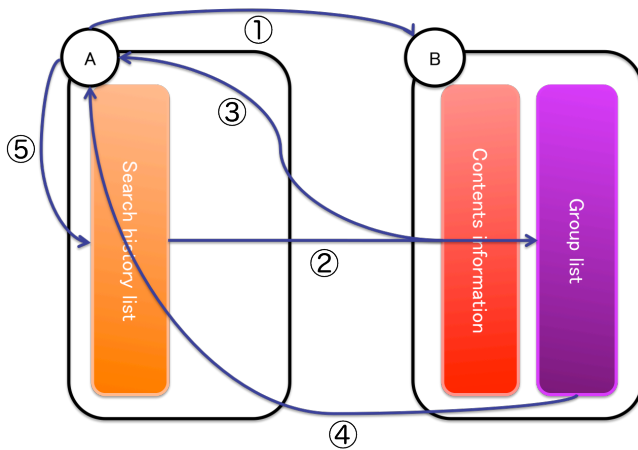


Fig 2 Node Communication

- ① First, if nodeA wants content information from nodeB, nodeA makes a request to nodeB. Then, at the same time as the search request,
- ② nodeA sends it's search history list to nodeB. NodeB receives the search request and the search history list from nodeA and returns the content information from nodeB. Then nodeB inserts the search history list into the group list.
- ③ The group list sorts the search history by the number of times an entry has been accessed.
- ④ At the same time nodeB returns it's content information it also returns it's GroupList to nodeA to notify nodeA of relevant group content.
- ⑤ Then nodeA updates it's search history.

## 2 CONSTRUCTION

### 2.1 Node construction

There are two kinds of nodes. They are Search Nodes and Provider nodes. The Search Node has a search history list and DHT. The Search history list contains the search history of the user.

The Provider node has the content's information, DHT, and a Group list. The Group List contains information on other nodes in the grouping.

### 2.2 System construction

Figure 3 shows the system construction. On the right is the search node. On the left is the provider node. When the provider node joins the network, the node registers its content in the DHT. When a user searches, a search node is created. A user searches for content information by using a word search on a user interface. The search node looks up the user's word in the DHT and finds the node that has the content information. A request is made to the provider node for the content information and the user node sends the Search History List to the provider node. The searched word is added to the Search History List.

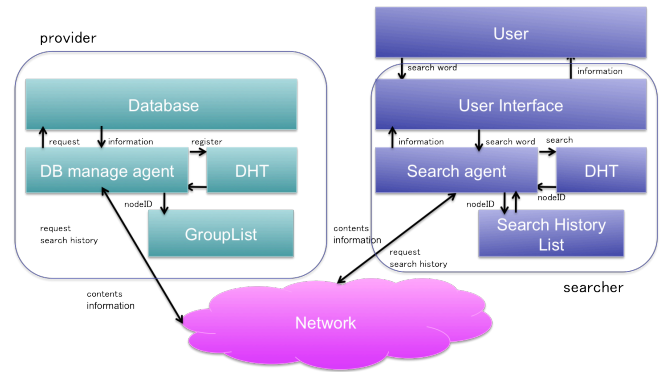


Fig 3 System Construction

## 3 CONCLUSION

I suggest grouping content on P2P networks. I will build a search system using P2P network content grouping. After the search system is built, it will need practical experiments and evaluation.

## REFERENCES

- [1]. Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, and Hari Balakrishnan. Chord: A scalable peer-to-peer lookup service for internet applications. In Proceedings of the ACM SIGCOMM '01 Conference, San Diego California, August 2001
- [2]. Petar Maymounkov, David Mazières, Kademlia: A Peer-to-peer Information System Based on the XOR Metric, In Proceedings of the 1<sup>st</sup> International Workshop on Peer-to-Peer Systems(IPTPS), March 2002.
- [3]. Sriram Ramabhadran, Sylvia Ratnasamy, Joseph M. Hellerstein, Scott Shenker: Pre-fix Hash Tree:An indexing data structure over distributed hash tables, Technical report, Intel Research, 2004.
- [4]. Keishi Tajima, Yoshiaki Mizuuchi, Masatsugu Kitagawa, and Katsumi Tanaka: "Cut as a Querying Unit for WWW, Netnews, and E0mail", Proceeding of 9<sup>th</sup> ACM Conference on Hypertext and Hypermedia, pp.235-244, (1998.6)
- [5]. Necip Fazil Ayan, Wen-Syan Li, Okan Kolak:"Automating Extraction of Logical Domains in a Web Site", In International Journal of Data and Knowledge Engineering, 43(2), Elsevier Science, pp.179-205, (2002.11)



# An Experimental Study on TOR Traffic Analysis Attacks

Ronnie Hoeflin, Carol Taylor, Kosuke Imamura

Eastern Washington University, USA  
{ctaylor, kimamura}@ewu.edu

**Abstract** - TOR is a free anonymous software system that improves users' privacy and security. However, TOR is not completely safe against traffic analysis. We embedded possible protective techniques within TOR and analyzed their effects under the traffic analysis attack. Our experiment suggests that a relay cell delay technique is promising.

**Keywords:** TOR, Anonymity, Traffic Analysis, Onion Routing, Privacy

## 1 INTRODUCTION

While the Internet has become necessity in our daily life, aversion to privacy and anonymity is becoming more common. A person's information about surfing habits, recent purchases, and IP address are all logged, data-mined, and sold to the highest bidder [1]. TOR improves users' privacy and security. However, TOR is not completely safe against traffic analysis attacks. We verify the traffic analysis attack performed by Murdoch and Danezis [2]. Then, we embed protective techniques in TOR and analyze the effects..

## 2 OVERVIEW OF ONION ROUTING

The onion routing is based on Chaum's mix cascades [3] and was introduced in 1996 [4]. An anonymous communication starts out with a connection to the application proxy. The application proxy connects to an onion proxy which is a gateway into the onion network. The onion proxy "defines a route through the onion routing network by constructing a layered data structure called an onion" [5].

## 3 TIMING ANALYSIS VERIFICATION

Fig. 1 shows our test environment. Zarathustra, Mininix, and Napoleon constitute the TOR network. Triton is the corrupt node used to monitor the latency of a relay in the TOR network. We use Puppetor, a Java TOR simulator [6].

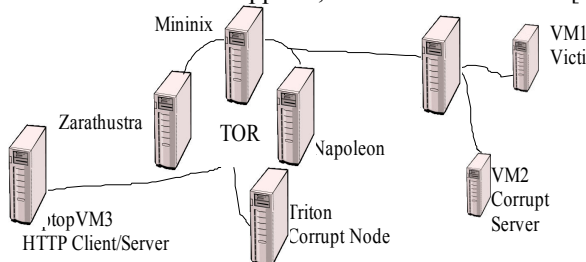


Fig. 1 Physical Test Environment Representation

A corrupt TOR node measures the traffic load of a TOR relay and the burst of traffic is sent as described in [2]. Fig. 2 shows the same type of characteristics as the original attack as [2]. Fig.3 shows the nodes which are not relaying CS's modulated traffic will not exhibit the timing characteristics.

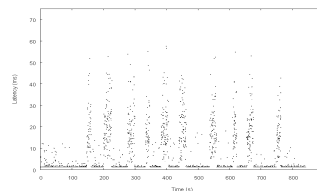


Fig. 2  
Latency Results From Flooding  
Attack

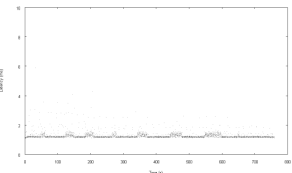


Fig. 3  
Latency with Corrupt Tor Node  
Not in Victim's Circuit Path

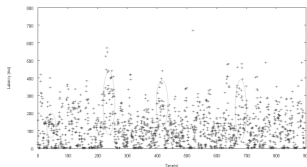
## 4 ATTACK SIGNIFICANCE

The attack does not seem to have much significance. After all, the victim's anonymity is never compromised. This attack is still useful especially in conjunction with other known attacks against TOR. Those attacks can be found in [7] [8] [9] [10] [11]. Determining how feasible the attack can be in conjunction with other attacks is left to future research.

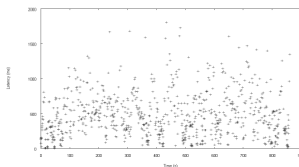
## 5 ATTACK PREVENTION AND ANALYSIS:

### 5.1 Dummy Packets

For this experiment VM3 is used to run a client/server program (virtual user). These virtual users flood the TOR network with traffic effectively acting as the dummy packet generator to thwart the timing analysis. The timing characteristics start disappearing with 20 and 40 virtual users in Fig. 4 and 5. However, the cost in latency alone is quite striking. Using the verification in Section 3 as a reference, the test environment requires a 1000% latency increase before the timing characteristics begin to blend in as background noise.



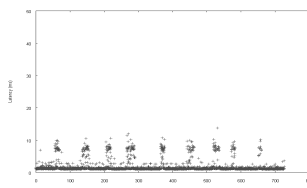
**Fig. 4**  
Dummy Packet Prevention with  
Twenty Virtual Users



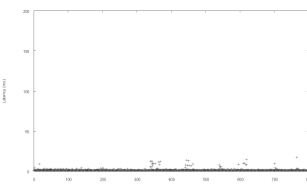
**Fig. 5**  
Dummy Packet Prevention with  
Forty Virtual Users

## 5.2 Cell Delay

Cell delay delays cells for a random amount of time between relay nodes. The upper bound delay times used for testing are: 20, 50, 100, and 200 milliseconds. The delay required to remove any timing characteristics is roughly 3000% with 400ms (Fig 6, 7) which will average 200ms.



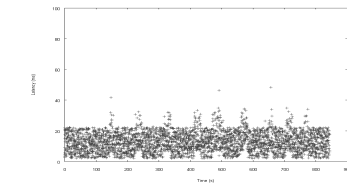
**Fig. 6**  
Flooding Attack with Relay Cell  
Delayed Up To 200 Milliseconds



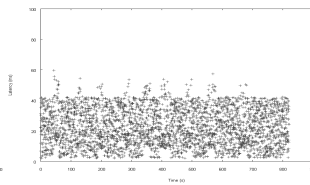
**Fig. 7**  
Flooding Attack with Relay Cell  
Delayed Up To 400 Milliseconds

## 5.3 Endpoint Delay

This strategy will delay all end point traffic with varying latencies. From Fig 8 and 9, delaying all endpoint cells doesn't fully remove the echoes of the flooding attack.

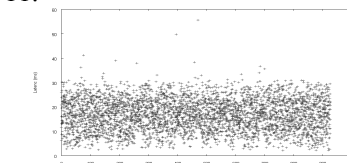


**Fig. 8**  
Flooding Attack with Endpoint Cells  
Delayed Up To 20 Milliseconds

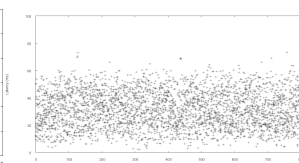


**Fig. 9**  
Flooding Attack with Endpoint Cell:  
Delayed Up To 40 Milliseconds

Looking at Fig. 8 and 9, there actually seems to be a pattern in how peaks and voids in the graph are appearing relative to the delay time selected. They both have an offset of about half the latency time used when the flooding attack is occurring vs. when it is not occurring. This observation allows us to modify this strategy to compensate for this offset and add it to the delay time when the attack is not occurring. The modification result is shown in Fig 10 and 11:



**Fig. 10**  
Flooding Attack with Endpoint  
Cells Delayed Up To 20  
Milliseconds (Modification)



**Fig. 11**  
Flooding Attack with Endpin  
Cells Delayed Up To 40  
Milliseconds (Modification)

## 6 CONCLUSION AND FUTURE RESEARCH

Dummy packets though having the potential to remove the flooding timing characteristic has undesired side effects: 1000% increase in latency from the baseline and the bandwidth that it would require from host computers. Relay cell delay, in particular the strategy used in Section 4.3 only increases the latency by 289%. At roughly 1/3 the latency of the other method, it looks promising. There is also the question of how to detect that an attack of this type is occurring. There are also several other preventative methods proposed [2] that were not explored in this paper. This too is still a venue for more research.

## REFERENCES

- [1] Liedtke, M. (2006, August 9). Google to Keep Storing Search Requests. Washington Post. Retrieved April 21, 2008, <http://www.washingtonpost.com/wp-dyn/content/article/2006/08/09/AR2006080901487.html>
- [2] Murdoch, S. J., Danezis, G. (2005), Low-cost traffic analysis of TOR, in 'Proceedings of the 2005 IEEE Symposium on Security and Privacy', IEEE CS.
- [3] Chaum, D. (1981). "Untraceable Electronic Email, Return Addresses, and Digital Pseudonyms". Communications of the ACM 24(2), 84-88.
- [4] Goldschlag, D.M., Reed, M. G. & Syverson, P.F. (1996), "Hiding routing information", in R. J. Anderson, editor, Information Hiding', Vol. 1174 of LNCS, Springer-Verlag, Cambridge, U.K., pages. 137-150
- [5] Syverson, P.F., Reed, M.G., Goldschlag, D.M. (1997). "Private Web Browsing". Journal of Computer Security Special Issue on Web Security, Volume 5, Number 3, 1997, pp. 237-248
- [6] Loesing, K. (2007, Oct 5). "Puppetor A Java-based TORsimulator User's Guide". Retrieved May 7, 2008 from <https://tor-svn.freehaven.net/svn/puppetor/trunk/doc/howto.pdf>
- [7] Hopper, N., Vasserman, E., Chan-Tin, E. (2007), How much anonymity does network latency leak?, in 'ACM Conference on Computer and Communications Security', pg 82-91.
- [8] Murdoch, S., Hot or Not: Revealing Hidden Services by their Clock Skew, in '13th ACM Conference on Computer and Communications (CCS)', 2006
- [9] Overlier, L., and Syverson, P (2006). Locating Hidden Servers. in 'Proceedings of 2006 IEEE Symposium on Security and Privacy', May 2006, IEEE
- [10] Abbot, Lai, Lieberman, and Price (web.mit.edu/tabbott/www/papers/tor.pdf),
- [11] Bauer, K., McCoy, D., Grunwald, T., Sicker, D., (2007).: Low-Resource Routing Attacks Against Anonymous Systems. In Proceedings of the 2007 Workshop on Privacy in the Electronic Society (WPES), 2007

# Design and Implementation of an Interactive Live Broadcasting System with a High-Quality Snapshot Function on the Internet

Yoshia Saito\* and Yuko Murayama\*

\* Faculty of Software and Information Science, Iwate Prefectural University, Japan  
{y-saito, murayama}@iwate-pu.ac.jp

**Abstract** –In this paper, we propose an Internet broadcast system with a high-quality snapshot function to improve user experience. While the proposed system delivers low-quality video to audience, it provides a high-quality snapshot function which enables the audience to take a snapshot of a desired and favorite scene anytime.

**Keywords:** Internet Broadcasting, Interactive TV

## 1 INTRODUCTION

Live video broadcasting by Internet users gets popular nowadays. A lot of Internet users broadcast their original live video contents using PCs and web cameras. It is expected that these video sharing and broadcasting services would become widely used much further and network traffic of the videos would grow more in the next couple of years.

The huge video traffic, however, causes a problem of communications expenses. Although most video sharing and broadcasting services run on income from advertisements on their websites, it is difficult to make profits because of its expenses more than its advertising income. Moreover, current online video services distribute videos with a few hundred kilobits per second (kbps). The video quality on the Internet does not come up to TV quality yet. While the video services should provide more high-quality videos, it is not easy to improve the video quality for the above reason.

In this paper, we propose an interactive internet live broadcasting system called *Photographable TV* which provides a high-quality snapshot function so that audience can take high-quality pictures of favorite scenes for their memories at any time watching live video. In case of graduation ceremony, parents of graduates can take ceremonial pictures remotely as if they were attending the ceremony. The pictures can be saved to local disks for their personal memory albums. Since the data size of still pictures is far small than that of video, the proposed system can improve user experience without increasing network traffic. To study the effectiveness of the high-quality snapshot function, we design and implement a prototype system. We also conduct an experiment in our graduation ceremony to evaluate how to use our system by audience and find issues.

## 2 RELATED WORK

Interactive television (iTV) [1] is a research area which provides interactive features to video contents in order to improve user experience. Ustream and Justin.tv which are typical services for live video broadcasting apply the iTV technologies to their system. In these services, live video viewers can communicate with broadcasters and other

viewers using chat and social communication tools watching live video contents. These interactive functionalities are attracting the attention of many Internet users despite low resolution and bit rate of the live videos.

For similar ideas to our high-quality snapshot function, there are several studies in educational system. Ichimura proposes Chalk Talks [2] which is a remote lecture system with high-quality pictures. While the Chalk Talks provides high-quality pictures at fixed intervals, the Photographable TV provides high-quality pictures when audience requests.

One of video sharing services, PANDORA.TV [3] provides a snapshot function to the viewers. In the service, there is an image capturing button on the video player and still pictures of favorite scenes can be captured in JPEG format watching videos. However, it does not provide high-quality pictures because resolution and quality of the pictures are same as that of videos. Our system offers high-quality pictures to the audience more than video quality.

## 3 PHOTOGRAPHABLE TV

Figure 1 shows the system model of the Photographable TV. This model consists of a broadcaster, its audience and the proposed system. Firstly, the broadcaster sends a high-quality video source to the system. The system receives and encodes the high-quality video storing the original source. The audience receives the compressed video from the system in real time over the Internet and also can send a picture request to the system anytime watching the video. When the system receives the picture request, a high-quality picture is made from the stored original video source and sent to the audience. The audience can see and save the high-quality picture.

There are several issues to realize the Photographable TV. The Photographable TV requires encode functions for video and pictures. Since quality of pictures is equivalent of the original video quality, the original video should be uncompressed and high-resolution so that high-quality pictures can be made from it. However, it is difficult to send the original video over the Internet because the data size of the uncompressed and high-resolution video is too large. This is an issue. The encode functions must be near the broadcaster side not to across the Internet. Besides video encoding, the broadcaster's PC has to extract a frame from the video and encode the frame to make a still picture. It is expected to consume CPU resource of the PC and we should take care of its load. Another issue is frequency of the high-quality picture requests from audience. The proposed system is available in accordance with an idea that picture traffic is much less than video traffic. If the audience frequently requests high-quality pictures, the picture traffic would be

considerable amount. We have to study how many times the audience requests the high-quality pictures and control the picture traffic not to exceed network capacity.

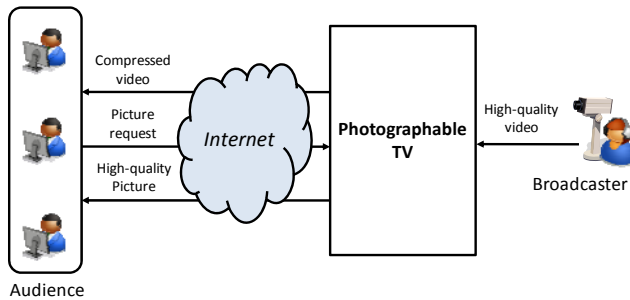


Figure 1. The model of Photographable TV

## 4 PROTOTYPE SYSTEM

The prototype system consists of four servers; an encode server, a streaming server, a management server and a picture server. The encode server has two functions. One is a video encode function and the other is a picture encode function. The video encode function receives an uncompressed video source from a camera and compresses the video for broadcasting. The uncompressed video source is also passed to the picture encode function. The picture encode function stores the uncompressed video so that high-quality picture could be made from the source.

The compressed video is sent to a video streaming function on the streaming server. The streaming server sends the video to each client by unicast when requested. The audience can send a picture request to a client management function on a management server watching the video through a user interface on the browser of the client when they would like to take pictures of specified scenes. The client management function keeps client IDs and forwards the picture requests with their client IDs to the encode server. When the picture encode function receives a picture request from the management server, it encodes high-quality picture from the uncompressed video. Since the picture data is compressed in JPEG format, it increases CPU load of the encoder server. If the clients frequently send picture requests to the encoder server, the picture generation would be aborted. To make matters worse, the frequent requests would cause huge network traffic between the encode server and the picture server even if the data size of the JPEG files is small. Therefore, we introduced periodic picture buffering scheme into the picture encode function. The picture encode function stores BMP data on the memory at fix intervals. In this implementation, we set the interval to 500 msec taking into account the server load. When a picture request is arrived, the encode function searches latest picture from the arrival time minus video buffering time of the client on the memory. The picture data is encoded in case it was not previously encoded. If the picture data has been already encoded, it does not process the picture encode and returns only the picture URL to the client.

The encoded picture is sent to a picture management function on a picture server. A thumbnail is made from the picture and they are stored in a database on the server. After that, a picture ready message is sent to the picture encode

function and it is forwarded to the client management function with the client ID and location information of the thumbnail and the picture. The client management function forwards location of the pictures based on the client ID. The client only downloads the thumbnail from the picture server to save network resource in case the audience does not like the shot. After the audience confirmed the thumbnail, the client downloads the picture from the picture server and displays it on the user interface. The audience can save the high-quality picture to the local disk on the client to enjoy the pictures after the broadcasting.

## 5 EXPERIMENT

We conducted an experiment in our graduation ceremony with the prototype system in order to evaluate how to use our system by audience and find issues. At first, we counted the number of the viewers through the broadcastings to study how many/long people used our system. The total number of unique viewers is 148. The maximum and average numbers of the viewers are 43 and 33 respectively. As a whole, the prototype system kept the number of viewers throughout the broadcast.

We also analyzed CPU load of the encode server and number of the photo requests per second to study its scalability. The CPU load was around 40% through the experiment. While the number of the photo requests per second constantly occurred, the prototype system could provide the snapshot function. Since the total number of the photo requests was 423, the viewers used the snapshot function frequently.

From the experiment, we found the prototype system could be used by several tens of viewers at least and load of the encode server was suppressed by the periodic picture buffering scheme. The prototype system could provide the snapshot function for small-scale live broadcasting.

## 6 CONCLUSION

In this paper, we proposed an Internet broadcast system with a high-quality snapshot function toward improvement of user experience. From the experiment, prototype system worked stably throughout the experiment even if more than 40 users watched the broadcasting simultaneously and the snapshot function was used 423 times. We confirmed the prototype system could provide the snapshot function if it is small-scale live broadcasting.

As future work, we will study how the Photographable TV improves user experience. We will also evaluate its scalability when audience increases more.

## REFERENCES

- [1] Ursu, M. et al, "Interactive TV narratives: Opportunities, progress, and challenges", ACM TOMCCAP, Vol. 4, Issue 4, 2008.
- [2] Ichimura, S., "Delivering Chalk Talks on the Internet", 40th Hawaii International Conference on System Sciences (HICSS), Collaboration Systems Track, IEEE CS Press, p.4-11, 2007.
- [3] PANDORA.TV: <http://www.pandora.tv>



# Social Engineering Awareness in a Financial Institution

Rebecca Long\*, and Carol Taylor\*\*

\*Graduate School of Computer Science, Eastern Washington University, USA

\*\*Faculty of Computer Science, Eastern Washington University, USA

[rebecca.long@eagles.ewu.edu](mailto:rebecca.long@eagles.ewu.edu), [ctaylor@mail.ewu.edu](mailto:ctaylor@mail.ewu.edu)

**Abstract** - This is a research proposal into social engineering within a financial institution. The goal of the research is to determine if user training or technology alone is a better means to defending against social engineering attacks.

The results of this study will help an institution determine where best to focus their resources on securing their system from this type of attack.

**Keywords:** Social engineering, security, awareness, training, human-factors.

## 1 INTRODUCTION

Security is a top concern for any institution. The term “security” includes many components including: physical security, technical or computer security, and user security. Each component is important in order to have the overall security of a system or infrastructure be effective. Any security professional will know this in theory, but putting it to practice and knowing the best methods to cover each component is often a challenge especially when it comes to “user security.”

Securing users is no easy task. Users are human, and as such, have a natural tendency to trust and want to help others. While this can be a good thing for those who deserve to be trusted and helped, it is a bad trait to have dealing with people who want to exploit that trust.

### 1.1 Social Engineering

The term used for people who exploit the trust of users is “social engineers.” Social engineers are masters of tricking users into handing over private data or performing unauthorized tasks. [1] Most of the time, users will never know they were a victim of a social engineering attack and will often walk away with a good feeling about the whole encounter. [2]

Social engineers typically use a basic cycle for performing an attack: [3, 4]

1. Information gathering
2. Developing relationships
3. Exploitation
4. Execution

As an example, if a social engineer wanted to attack Bank A, the first step would be to gather information on Bank A. Many techniques can be used for this step: reviewing the public Web site, finding flyers or advertisements, dumpster diving for thrown out non-shredded documents, phone book, etc.

They would then use the information attained to contact employees within Bank A such as a teller or someone on the help desk. This is the stage for developing relationships with legitimate employees and users of Bank A’s system. The social engineer may pretend to be a fellow teller from another branch location who is in need of assistance. The actual teller will naturally want to help the social engineer. The social engineer will start by requesting a small favor for help in order to not arouse suspicion. The social engineer may do this over the phone, and may call multiple times over a number of days or weeks asking for more favors. The favors could be just gathering more information or having the real employee perform some task for them.

Ultimately, the social engineer will have the employee hand over private information or perform some task that allows the social engineer access to their system. This exploits the trust built between the social engineer and the legitimate employee. It then allows the social engineer to perform their final attack. In the case of Bank A, it could be to transfer money out of accounts into the social engineers personal account or to gain access to a server and load a virus that destroys their system. Anything is possible once the system has been compromised.

### 1.2 Training vs. Technology

Securing users from the threat of social engineering is a difficult task for any security professional. There is a debate about which method is best for users: training or technology.

User training uses the idea that if users have the proper information and understanding, they will make good decisions regarding security. If a user knows what a phishing email is and the risk involved with clicking on a link from it, they will not click on any links and proceed with proper actions such as deleting the email or informing their IT department.

History has shown that even with proper training users do not always act accordingly. Users will still make bad decisions, seemingly forgetting any and all training regarding security. Because of this, there is a growing argument that user training is a waste of time and money; pushing the idea that users are “idiots” and cannot be trained. [5, 6]

The other side of this debate is in favor of using technology to control user actions. If technology is in place to prevent users from accessing the Internet or clicking on links from emails, the user cannot make bad decisions. With this theory, it doesn’t matter if users know anything about security or not because the technology will force them to behave in a safe and secure manner.

Both of these methods have pros and cons. User training can be cumbersome and repetitive, especially if the training courses need to be done annually. This could make the training less effective with every repeat course. And while technology can be effective, it can irritate and frustrate users. Users might look for means around the technology in order to do what they want to do (i.e. browse the Internet on their lunch break).

Neither method has really been tested or proven to be better than the other. [7] Both are in a theory phase in regards to the effectiveness and actual results. Both methods are currently being used in varying capacities in industry. Our goal here is to provide some scientific results to this argument and help institutions determine which method is better to focus their resources on

## 2 RESEARCH

This is a research project for a Master's thesis that began in 2007. We have partnered with an outside security firm and will be performing our research experiment on one of their affiliated banks (Bank #3). Two previous banks we were scheduled to work with were both phished and pulled out of our study.

### 2.1 Motivation

It is a well known fact that people are the weakest link in any security chain. It is just as important to secure the users of the system as it is to secure the technology. Unfortunately, since people can be easily tricked and manipulated, this is no easy task and needs further research in order to know how best to accomplish this.

### 2.2 Goals and Benefits

The goal of this study is to determine whether user training or technology alone is the better method to counter the threat of social engineering attacks to a secure system. Perhaps user training will prove to be effective and a good way to go for an institution. Or perhaps user training will end up being as useless as some security people have argued and technology is the best route to go. Or another option would be that the best method is to actually use both methods together to achieve the maximum benefit.

The results of this research will benefit any institution looking to secure itself from social engineers. Institutions rely on a limited amount of resources to operate: training resources, general IT and technological resources, and special security resources. Where and how to divvy up resources to most effectively defend from social engineering attacks is vital information for any institution. For example, if training turns out to be a waste of money, the institution can focus its efforts on the necessary technology to secure its system.

### 2.3 Proposed Methods

To test which method of securing users is best, we will be performing the following experiment on employees who work for Bank #3.

Half of all employees will receive special social engineering training. The training will conclude with a test to determine the level of knowledge retained from completing the training course. The training will be delivered to employees by Bank #3's training department along with their regularly scheduled training.

Two to three months following the completion of the training, a phishing email will be sent out to all employees. Half of the employees will be placed into a group where they will receive a notification message upon falling for the phishing email to inform them that they were just a victim of a phishing attack. Two to three months following the first phishing email, a second phishing email will be sent out to all employees.

The phishing emails will be delivered to employees via our partnered security firm. This will prevent any confidential bank data from being stored on University hardware.

### 2.4 Control Groups

There will be two control groups for this study: one for the training and one for the technological feedback notification.

	<i>Training</i>	<i>No Training</i>
<b>Technology</b>	Group #1	Group #3
<b>No Technology</b>	Group #2	Group #4

### 2.5 General Timeline

This study will begin with training being delivered to employees in November 2010. The first phishing email will be sent in late winter 2011 with the second phishing email to follow in spring 2011. Results should be ready in summer 2011.

### 2.6 Expected Results

We expect that Group #1 will have the best results since they will have both training on social engineering and receive the technological notification if they happen to fall for the phishing email.

The employees who fall for the first phishing email but get the notification should show the greatest improvement between the first and second phishing emails. The notification will let the employees know they fell for a phishing email and remind them what to do with a phishing email in the future. This reminder will come quickly while the first phishing email is fresh in their mind. This should help them to associate their mistake and remember it for the second phishing email.

## REFERENCES

- [1]. Schneier, B. (2004). *Secrets & Lies: Digital Security in a Networked World*. Indianapolis, Indiana: Wiley Publishing, Inc.

- [2]. Mitnick, K., & Simon, W. L. (2002). *The Art of Deception: Controlling the Human Element of Security*. Indianapolis, Indiana: Wiley Publishing Inc.
- [3]. Allen, M. (2007). *Social Engineering: A Means to Violate a Computer System*. SANS Institute.
- [4]. Twitchell, D. P. (2008). *Social Engineering and its Countermeasures*. In M. In Gupta, & R. Sharman, Handbook of Research on Social and Organizational Liabilities in Information Security (pp. 228-242). Idea Group Inc.
- [5]. Timmer, J. (2010). *Users are still idiots, cough up personal data despite warnings*. Ars Technica.  
<http://arstechnica.com>
- [6]. Timmer, J. (2008). *Fake popup study sadly confirms most users are idiots*. Ars Technica.  
<http://arstechnica.com>
- [7]. Sasse, M. A., Brostoff, S., & Weirich, D. (2001). *Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security*. BT Technol , 19 (3).