

# **The fifth EWU-IPU International Exchange Program In Computer Science 2012**

A 3D-rendered globe with a blue ocean and orange/yellow landmasses, primarily showing North and South America. The globe is set against a background of faint, overlapping binary code (0s and 1s).

## **CSIEP 2012**



Sponsored by Informatics Society

Publication Office

Informatics Laboratory

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

Publisher

Tadanori Mizuno, President of Informatics Society

ISBN: 978-4-902523-34-8

**General Co-Chairs:**

Paul Schimpf, Eastern Washington University  
Yoshitaka Shibata, Iwate Prefectural 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  
  
Masakatsu Nishigakki, Shizuoka University  
Yoshia Saito, Iwate Prefectural University  
Yoshikazu Watanabe, Iwate Prefectural University

**Local Chair:**

Catherine Dixon, Eastern Washington University

**Local Supporters:**

Geancarlo Palavicini, MS Student, Eastern Washington University  
Kyle Gwinnup, MS Student, Eastern Washington University

**Publishing Chair:**

Yoshia Saito, Iwate Prefectural University

**Web Chair:**

James Lamphere, Eastern Washington University

## Contents

Preface	1
Keynote: “Disaster Communications Issues” <i>Yuko Murayama</i>	2
An Experiment of Reconstruction Watcher in Disaster Area <i>Yoshia Saito and Yuko Murayama</i>	7
Construction of Anshin model about information security for online shopping <i>Dai Nishioka, Yoshia Saito and Yuko Murayama</i>	9
Wide Area Monitoring System from a Balloon with Omni-Directional Cameras <i>Sanetaka Arimura, Koji Hashimoto and Yoshitaka Shibata</i>	11
Analysis of Backscatter from Chipless RFID Using Metal Patches <i>Kyohei Chiba and Goutam Chakraborty</i>	13
Privacy Protection by using masquerade pointer in Android OS <i>Harunobu Agematsu, Junya Kani, Kohei Nasaka, Hideaki Kawabata, Takamasa Isohara, Keisuke Takemori, Masakatsu Nishigaki</i>	15
Gamified CAPTCHA <i>Junya Kani, Harunobu Agematsu, Masakatsu Nishigaki</i>	17
Fuzzy Signature scheme for Biometric Digital Signature <i>Yuta Yoneyama, Kenta Takahashi, Eisei Honbu and Masakatsu Nishigaki</i>	19
Studies on the efficiency of delivery methods in P2P streaming using BitTorrent <i>Takanori Kashiwagi, Jun Sawamoto, Eiji Sugino and Norihisa Segawa</i>	21
Examining the effectiveness of using GPS information to enhance the prediction model of Japanese-language input systems for mobile phones <i>Ken Tarusawa, Jun Sawamoto, Eiji Sugino and Norihisa Segawa</i>	23
Optimization and Instrumentation - Measuring machine impact on program implementation <i>Daniel McDermott</i>	25
Malware Hooking <i>Geancarlo Palavicini Jr</i>	31

## **Preface**

It is our great pleasure to have the fifth workshop of the Eastern Washington University (EWU)- Iwate Prefectural University (IPU) International Exchange Program in Computer Science published by the Informatics Society. The exchange program started in the summer of 2008 after an administrative meeting the previous year. Since then, the workshop has been held every year.

This year as the fifth workshop, we had the keynote speech by Yuko Murayama from Iwate Prefectural University, followed by eleven presentations by the faculty members and graduate students from Iwate Prefectural University and Eastern Washington University. Those presentations span a wide variety of topics in computer science, networking, security, human aspects of technology and disaster communications

We had five graduate students joined from Iwate, this year, as well as three more students from Shizuoka University. 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.

July 2013

General Co-Chairs: Yoshitaka Shibata and Paul Schimpf

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

## Disaster Communications Issues



Yuko Murayama  
Faculty of Software and Information Science Iwate  
Prefectural University  
[www.go-iwate.org](http://www.go-iwate.org)

## Outline

1. Iwate Disaster IT Support Project activities
  - Support required at disaster
  - Support organization
  - Some results from our experience
2. Issues of disaster communications
  - trust issues
  - distrust issues
3. Future work



Sept. 6, 2012

Disaster Communications Issues

2

## Damage caused by the 3.11 disaster



- Tohoku Region:
  - Deaths: 15,806
  - Missing: 2,906
  - Injured: 4,669
- Iwate: 15,278.40 km²
  - Deaths: 4,671
  - Missing: 1,214
  - Injured: 201

Reference:  
1. National Police Agency  
<http://www.npa.go.jp/archive/keibi/biki/higaijokyo.pdf>  
July 11, 2012

Sept. 6, 2012

Disaster Communications Issues

3

## Support for Iwate



Iwate is large:

- Iwate: 15,278.40 km² (5,899.02 sq mi)  
[http://en.wikipedia.org/wiki/Iwate\\_Prefecture](http://en.wikipedia.org/wiki/Iwate_Prefecture)
- Connecticut: 14,357 km² (5,543 sq mi)  
<http://en.wikipedia.org/wiki/Connecticut>

Sept. 6, 2012

Disaster Communications Issues

4

## Technical Support required at Disaster

1. Information acquisition and provision:
  - People search: safety information: on-line, cell phone, off-line
  - Visualizing Lifeline information:
    - road condition, transport, electricity, water supply etc.
  - radioactivity, shopping and daily-life-related
  - portal sites of disaster information: [www.go-iwate.org](http://www.go-iwate.org)
    - No. of access: 5,892 (as of 12:30 Mar. 2, 2012)
2. Networking for information infrastructure:
  - internetworking with communication links
  - IT environment with PCs and printers
3. Shelter information management for a local government
  - List of people in a shelter: name/age/family/address
  - An information system for food and goods distribution
4. Volunteer Support
  - Tohno Volunteer Center:
    - local information for visitors

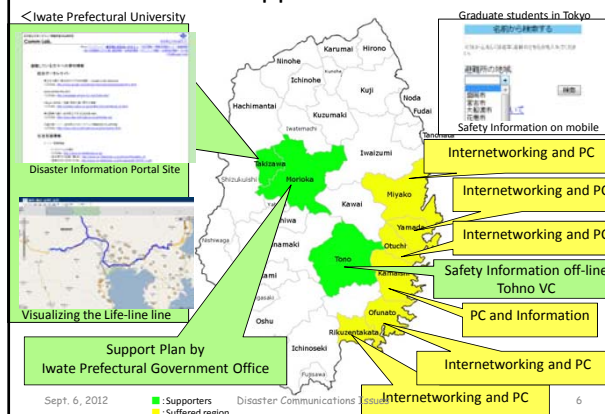


Sept. 6, 2012

Disaster Communications Issues

5

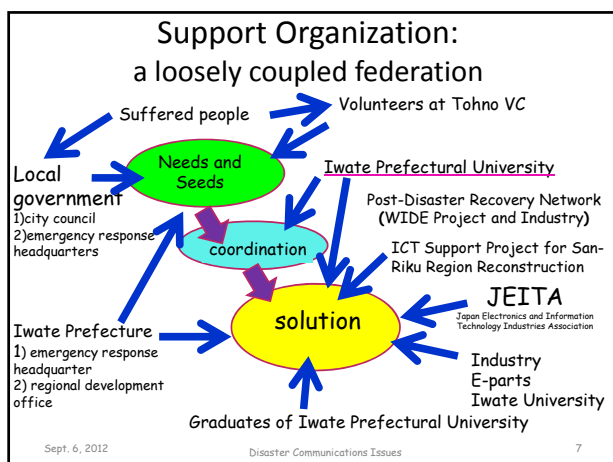
## Our Support Activities



Sept. 6, 2012

Disaster Communications Issues

6



- Issues from the experience:  
ICT was not required so desperately**
1. Providers' viewpoint:  
    - IT should be required
  2. Need to understand the real need  
    - Supporters and Cars, first
    - And then, ICT
  3. Organizational Protocols  
    - Hierarchy and independence of local governments
      - e.g.) convincing the need for networking
        - Prefectural offices: 1) emergency 2) normal
        - Local government offices: a) emergency b) normal
- Sept. 6, 2012 Disaster Communications Issues 8

**Disaster Communications**

**Risk Communications**  
vs.  
**Disaster Communications**

Sept. 6, 2012 Disaster Communications Issues 9

- Disaster Communications**
- ✓ Risk Communications (e.g. nuclear plant, disaster prevention)
    - ✓ residents
    - ✓ specialists
  - ✓ Disaster Communications
    - ✓ sufferers
    - ✓ volunteers
    - ✓ Administrative offices
    - ✓ Supporters:
      - organizations
      - individuals
- 
- Sept. 6, 2012 Disaster Communications Issues 10

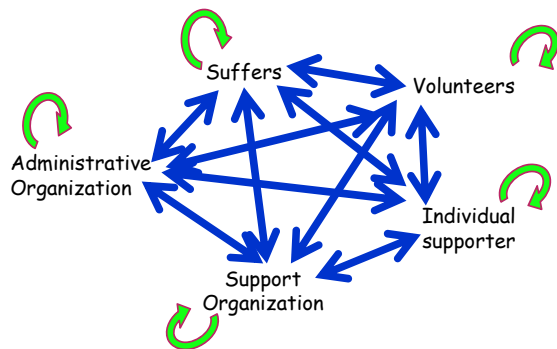
- Nature of Disaster Communications**  
*the same purpose but hard to cooperate*
- ✓ Heterogeneity of people
    - Background, tired, fatigue, volunteer vs. business
  - ✓ Most of us are novices
    - Need to deal with the matters without experiences
  - ✓ Communications with unknown people
    - Easy to misunderstand
  - ✓ Need for decision-making in changing circumstances
    - No best optimized solution
  - ✓ None knows the true needs
    - ICT is only a small part of solution
  - ✓ Don't expect appreciation
    - No time; things keep happening one after another
    - Multiple issues to deal with at the same time
  - ✓ No workflow available including volunteers
- Sept. 6, 2012 Disaster Communications Issues 11

**What is needed  
for disaster communications**

speed  
rhythm  
trust

Sept. 6, 2012 Disaster Communications Issues 12

## Trust required in Disaster Communications



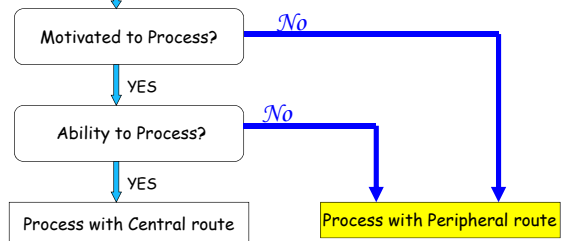
Sept. 6, 2012

Disaster Communications Issues

13

## Elaboration Likelihood Model (ELM)

Persuasive Communication (Message and Information from the others)



Petty, R. E., & Cacioppo, J. T. :Attitudes and persuasion: Classic and contemporary approaches. Dubuque, IA: William C. Brown 1981

Sept. 6, 2012

Disaster Communications Issues

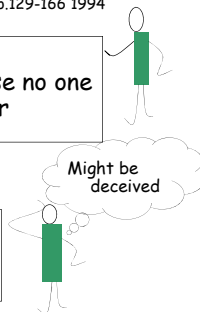
14

## Anshin vs. Trust

Yamagishi, T. & Yamagishi, M.: Trust and commitment in the United States and Japan, *Motivation and Emotion* 18(2), pp.129-166 1994

the community with Anshin:  
there is no need for trust because no one  
is supposed to deceive the other

the community with Trust :  
judge the others based on the  
information



Sept. 6, 2012

Disaster Communications Issues

15

## What we need is Trust

### Basic Factors of Cognitive Trust:

1. Competence
2. Integrity
3. Benevolence

Sept. 6, 2012

Disaster Communications Issues

16

## the asymmetry principle of Trust

trust building  
vs.  
trust destroying

Slovic, P. :Perceived risk, trust, and democracy.  
*Risk Analysis*, 13, 675-682 1993

Sept. 6, 2012

Disaster Communications Issues

17

## Distrust

✓antonym of Trust:

- Absence of Trust
- Not Distrust

✓cognitive trust vs. emotional trust

✓Distrust is emotional part of trust



Sept. 6, 2012

Disaster Communications Issues

18



## Distrust in Disaster Communications

- ✓ Easy to get distrust
- ✓ Need to have trust-processing
- ✓ Collaboration with the Salient Value Similarity (SVS) model



Sept. 6, 2012

Disaster Communications Issues

19

## Related Work: Emergency Management

- **History:** the Office of Emergency Preparedness (OEP) in the Executive Office of the President
  1. a prototype Delphi System (1970)
  2. Emergency Management Information System for the Wage Price Freeze (EMISARI) (1971)
    - 200 to 300 users to exercise coordinated response to crisis situations
    - the companion PREMIS system: for collaborative actions
- **Crisis management:**
  - a highly flexible but also structured group communication system is required

Murray Turoff: Past and future emergency response information systems, Comm. of the ACM Vol. 45 No. 4, April 2002

Sept. 6, 2012

Disaster Communications Issues

20

## User of SNS for Emergency Management

- **Facebook:**
  - Information Systems for Crisis Response and Management (ISCRAM),
  - The Humanitarian Free and Open Source Software (hFOSS) Project
  - Arkansas Tech University Department of Emergency Administration and Management
  - Emergency Awareness at the University of Maryland
- **LinkedIn:**
  - Emergency Management and Homeland Security Officials,
  - Professionals in Emergency Management,
  - American College of Emergency Physicians (ACEP)
  - Firefighter, Rescue & EMS Network
  - the International Association of Emergency Managers (IAEM)
  - IAEM EUROPA
  - Community Emergency Response Teams (CERT)

Connie White, Linda Plotnick, Jane Kushma, Starr Roxanne Hiltz, Murray Turoff: An online social network for emergency management. International Journal of Emergency Management, Vol. 6, No. 3-4 pp. 369-382 2009

Sept. 6, 2012

Disaster Communications Issues

21

## from Short-term restoration to Long-term reconstruction

- ✓ **Disaster Information System**
  - **Short term:** safety information, lifeline, shelter, volunteer activity, goods distribution
  - **Long term:** care, jobs, housing, community, transport
  - **ICT environment**
    - From shelters to temporal housing
    - Local governments
    - Public transport
- ✓ **From infrastructure to applications**
  - education,
  - Reconstruction watcher
- ✓ **Sustainable support:** new business models, new collaboration
  - Welcome to Project Fumbaro Eastern Japan
  - Amazon: wish list
  - OpenStreetMap
  - Safecast

Sept. 6, 2012

Disaster Communications Issues

22

## Reconstruction Watcher (Yamada and Kamaishi)



Sept. 6, 2012

Disaster Communications Issues

23

## Setting a PC and a web camera



Sept. 6, 2012

Disaster Communications Issues

24

## Disaster Information System

*Different from a normal-time use*

- ✓ Need a standard format
  - Safety information
  - Information on sufferers: family, shelter
  - Shelter
  - Good Distribution: never be well-planned
  - Medical information: the disaster weak
  - donation: traceability
- ✓ Open Source + Global Community of Software Developers
  - Sahana[1] and Ushahide
- ✓ Global collaboration over the net
  - Open street map and Safecast
- ✓ Need a well-known interface
- ✓ Killer Application for Cloud Computing!

[1] Paul Currian, Chamindra de Silva and Bartel Van de Walle: Open source software for disaster management, Comm. of The ACM, Vol. 50, Issue 3, pp.61-65 2007

Sept. 6, 2012

Disaster Communications Issues

25

## Iwate Disaster IT Support Project

[www.go-iwate.org](http://www.go-iwate.org)



Sept. 6, 2012

Disaster Communications Issues

26

# An Experiment of Reconstruction Watcher in Disaster Area

Yoshia Saito\* and Yuko Murayama\*

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

**Abstract** - The Tohoku Region Pacific Coast Earthquake and its Tsunami caused serious damage to the Pacific coast in northeastern Japan. One year has passed since the Earthquake and the reconstruction is being gradually advanced. However, it takes long time for the reconstruction. We suggest it is important to share the serious situation in the disaster area to gain sustainable public understanding and support. To solve this issue, we have proposed Reconstruction Watcher which lets people share reconstruction progress visually to gain sustainable public understanding and to support the disaster area. This paper reports system design and implementation of the Reconstruction Watcher besides our challenges and findings. We also analyzed an access log operating the implemented prototype system.

**Keywords:** Disaster, Reconstruction

## 1 INTRODUCTION

The Tohoku Region Pacific Coast Earthquake hit northeastern Japan on Mar. 11, 2011. Tsunami created by the earthquake caused serious damage along the Pacific coast. We looked for ways to contribute disaster relief applying information technology to help our community and found that most people did not really know what the damage was like as well as the reconstruction progress. Presumably it is important to make people aware of the damage and the effort towards reconstruction for getting public understanding and support. News media serves filtered, sensational and short-term information of the disaster. However, the reconstruction spans long periods of time and information for the reconstruction support should be in the raw and long-term to gain understanding from potential supporters.

Meanwhile, we have been researching Internet broadcasting technologies [1, 2]. Since we can transmit information visually with Internet broadcasting, we tried to apply it to present the disaster damage as well as the reconstruction progress. Typical post-disaster system mainly aims for management of disaster supporting information and support for victims intended for government and supporters [3, 4]. Meanwhile, Japanese government could not provide enough information to people in this disaster because of a flood of information. We believe it is necessary to get support from private individuals. Even after the Tsunami, some private individuals in the disaster area could use 3G Internet connection and communicate to the others by Twitter. It compensated for the lack of information from the government. Public participation is said to be important in disaster [5].

We have proposed Reconstruction Watcher which aims for public participation intended for people all over the world to gain public understanding and to support the disaster area. People in the disaster area send videos and pictures to the Reconstruction Watcher via the Internet. The people in the other area can receive them and be aware of what the damage is like and the efforts made for reconstruction. The Reconstruction Watcher also maintains the videos and the pictures for a long time so that the general public can grasp reconstruction progress on a long-term basis. It could produce historical records for future generations.

## 2 IMPLEMENTATION

We implemented a prototype system of the Reconstruction Watcher to operate it in disaster area. The implemented Reconstruction Watcher could take a photograph at intervals of one hour or so that we would consume neither communication bandwidth nor storage for records. This way, it would be easier to keep records over several years and users can see all photographs and understand reconstruction progress. Figure 1 presents the system architecture of the prototype system. Our new system is composed of an uploader, a server and a client.

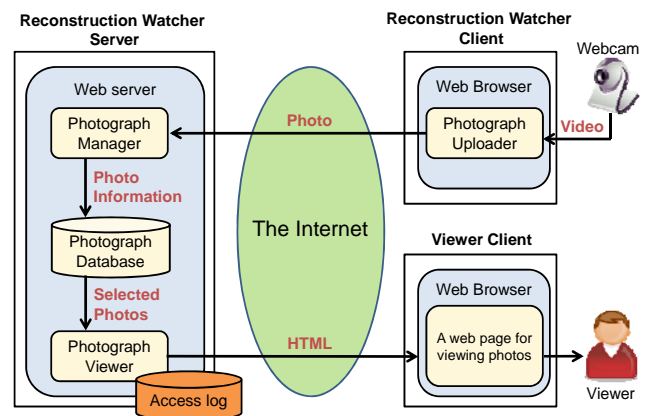


Figure 1: System Architecture

The Reconstruction Watcher client has a web camera and executes a web application for uploading photographs taken. The web application can be downloaded by accessing a URL on the Reconstruction Watcher server, and it creates a photograph captured by the camera. The photograph is compressed in JPEG and sent to the Reconstruction Watcher server.

The server receives the photograph and creates its thumbnail. A photograph and its thumbnail are put on web server so that they can be accessed via the Internet. The

URLs of the photograph and its thumbnail, the uploaded time are stored in a photograph database.

When a user wants to see the photographs, he or she can make an access to a website of the Reconstruction Watcher with a web browser.

## 2.1 User Interface

The Reconstruction Watcher client is implemented as a Flash application. Figure 2 shows the user interface for an uploader. The uploaders can periodically take a photograph and send the compressed photograph to the Reconstruction Watcher server on their web browsers without installing any proprietary software. When a viewer accesses to the server by a web browser, samples of photographs for each date are displayed in a calendar style as shown in Figure 3a. Then, the viewer can select a date from the calendar and a list of photographs in the selected date is appeared as shown in Figure 3b. At last, the viewer can select a photograph and see the high-quality photograph.

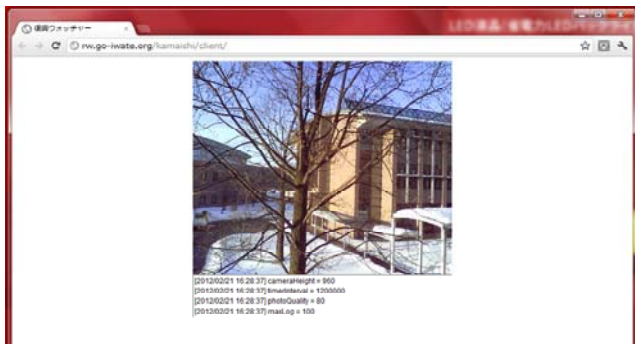


Figure 2: User Interface for an Uploader

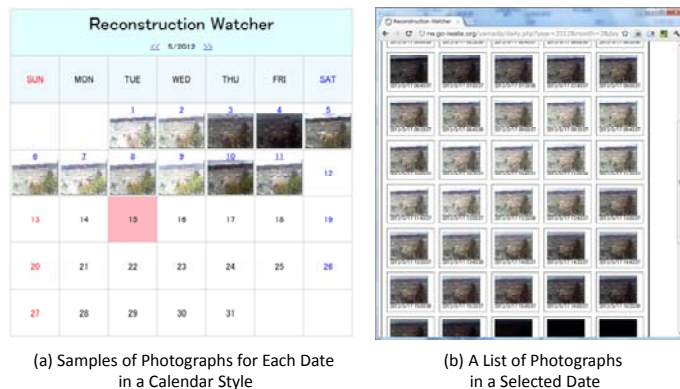


Figure 3: User Interface for a Viewer

## 3 EXPERIMENT

We conducted an experiment with the prototype system at Yamada-machi in Iwate, Japan. We made the prototype system available to the public from Mar. 12, 2012 and recorded the access log. The access log consists of the accessed time, the IP address and the kinds of the accessed page. We analyze the access log from Mar. 12 to May 11, 2012. Figure 4 shows the result. 48 people without relevant researchers and search robots accessed to the prototype system. Of those, 27 people accessed up to the calendar page as in Figure 3a and 6 people up to selected date as in

Figure 3b. The remaining only people viewed high-quality photographs. These people viewed the photographs which were taken at intervals of around 2 hours continuously or a few days and months. From these results, we find there are a lot of redundant photographs and it can reduce the communications traffic to save precious network bandwidth in disaster area.

Furthermore, we found difficulty to operate the system in disaster area. Since electric power in disaster area is not stable, the prototype system was frequently shut down. The system in disaster area should be sustainable and maintenance-free one for practical purposes.

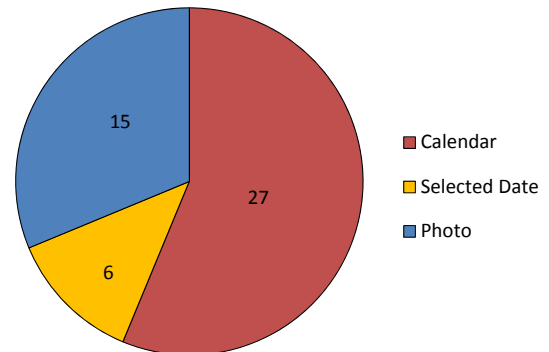


Figure 4: Trends in users' page access

## 4 CONCLUSION

We implemented a prototype system of the Reconstruction Watcher to operate it in disaster area and conducted an experiment. From the result of the experiment, we found trends in users' page access and issues of the system operation in disaster area. For the future, we will improve the prototype system and deploy it widely in disaster area.

## REFERENCES

- [1] Saito, Y. and Murayama, Y., "A Proposal of an Interactive Broadcasting System for Audience-driven Live TV on the Internet", *Journal of Information Processing*, 18, pp.26-37 (2010).
- [2] Saito, Y. & Murayama, Y., "An Experiment for an Interactive Internet Live Broadcasting System with a High-Quality Snapshot Function", *IWIN 2010*, pp.152-157 (2010).
- [3] Paul Currier, Chamindra de Silva, Bartel Van de Walle, "Open source software for disaster management", *Communications of The ACM*, Vol. 50, Issue 3, pp.61-65 (2007).
- [4] Margit Kristensen, Morten Kyng, Leysia Palen, "Participatory design in emergency medical service: designing for future practice", *CHI'06*, pp.161-170 (2006).
- [5] Leysia Palen, Sophia B, "Citizen communications in crisis: anticipating a future of ICT-supported public participation", *CHI'07*, pp.727-736 (2007).
- [6] Reconstruction Watcher at Yamada-machi, <http://rw.go-iwate.org/yamada>

# Construction of Anshin model about information security for online shopping

Dai Nishioka<sup>\*</sup>, Yoshia Saito<sup>\*\*</sup> and Yuko Murayama<sup>\*\*</sup>

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

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

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

{y-saito, murayama}@iwate-pu.ac.jp

**Abstract** - Anshin is a Japanese term that indicates the sense of security. Traditional researches on security have been based on the assumption that users would feel Anshin when provided with objectively secure systems. In this research, we investigate construction of users' subjective Anshin model.

**Keywords:** Anshin, Anshin model, Trust, Factor analysis, SEM

## 1 INTRODUCTION

Traditional researches on security have been based on the assumption that users would feel Anshin when provided with objectively secure systems. However, it is not always true that users feel Anshin with the secure systems. In previous work, we produced questionnaire to reflect the feedbacks from these users.

In this paper, we conducted a Web survey with 888 subjects and extracted the factors of Anshin. As the result of the factor analysis, we found four factors: "Perceived benevolence", "Perceived competence and Integrity", "User's Imagery" and "Reputation of the company from a third party". We report the construction of an Anshin model for users without technical knowledge about information security based on these factors.

## 2 RELATED WORK

In information security technologies, it is important to survey on human aspects. One of the representative examples is social engineering [1]. Social engineering is a technique for attacks which exploit a non-technical aspect of information technology relied on human interaction to break security procedures. In western countries, the similar concept of Anshin is trust, and it has been studied in the fields of psychology, philosophy, economics and sociology. Riegelsberger [2] describes a basic trust model in which "Trustor" is a person to trust and "Trustee" is a trusted person. Trustor decides, based on trustee's ability and motivation, whether to trust the trustee. In addition, internalized norms and benevolence are included in trustee's motivation. Trustor judges to trust trustee using trustee's temporary information, social information and institutional information. Although these surveys reported on the subjective factors, they did not elucidate the subjective factors and models sufficiently.

In our first survey [3], we conducted a questionnaire survey on Anshin with 452 students when they use a security system or service on the Internet. Most subjects

were computer science students and the only hundred ones were non-computer science students. As the result of the analysis, we had six factors. With the later survey [4], we conducted a survey with users who did not have the technical knowledge, and the five factors were found. With those surveys, we used a questionnaire which was produced based on the preliminary survey with the computer science students. Since ordinary people using information security do not necessarily have the technical knowledge, we wished to conduct a survey on Anshin about information security for the ordinary people. We needed a questionnaire to reflect feedbacks from the users without technical knowledge. We created the questionnaire which was introduced ideas of these users [5].

## 3 MAIN SURVEY

We conducted a user survey using the new questionnaire through a web survey. The survey was conducted on 888 subjects from 22 to 24 February, 2011. We asked for their ideas about Anshin in online shopping. We asked knowledge and experience of the users to create an Anshin model. As questions about the knowledge, we asked eight questions about security risks and security measures.

As questions about experience, we asked the frequency of the use of online shopping from the subjects. Factor analysis with the maximum-likelihood method and the promax rotation derived four factors.

Factor one is Perceived benevolence. This factor means when users feel benevolence from company's responses in "the trouble occurred by the user's mistake" and "the user's query", users feel Anshin. Factor two is Perceived competence and integrity. This factor means when users feel the company possesses competence not to let personal information leak out and the company performs personal information management with integrity, the users feel Anshin. Factor three is User's imagery. This factor means users assess Anshin from "instinct" and "experience". Factor four is Reputation of the company from a third party. This factor means users assess Anshin based on information from a third party.

## 4 ANSHIN MODEL

We clarified four Anshin factors with the users without technical knowledge. In this section, we report our trial on the construction of an Anshin model based on these four factors. The extracted factor one and factor two show cognitive trust. The cognitive trust is trustor's rational assessment on trustee's competence, benevolence and integrity [6]. We define factors one and two as the cognitive trust into Anshin model. In addition, it is reported that



user knowledge and experience affect trust. We introduce the concepts of the user knowledge and experience into Anshin model. However, it is not clear which factors affect user's knowledge and experience [7]. Therefore, we temporarily define that the user knowledge and experience are related to all factors.

In order to verify the model, we conducted Structural Equation Modeling (SEM). SEM is a statistical technique for causal modeling. It is a hybrid technique that includes confirmatory factor analysis, path analysis and regression. We constructed a high-order factor model using AMOS 18. We surveyed which factors affect user's knowledge and experience.

As the result of SEM, the user knowledge was related with factor three and four. The user experience was related with factor four. However, we found that the overall fit of the models are not acceptable with GFI (0.839), CFI (0.870), RMSEA (0.112). The models have a close fit by the criteria indicated: RMSEA below 0.08, CFI and GFI above 0.9.

Therefore, we needed to improve the Anshin model. We used modification index for the improvement of Anshin model. The modification index is an index to determine whether we add a path newly. We added four paths. The first is a path from question item 19 to 20. The second is a path from question item 22 to 23.

The third is a path from Anshin factor to question item 19. The fourth is a path from Anshin factor to question item 22. As a result, the overall fit of the model turns out to be acceptable with GFI (0.957), CFI (0.971), RMSEA (0.054). The improved Anshin model is shown in Figure 1.

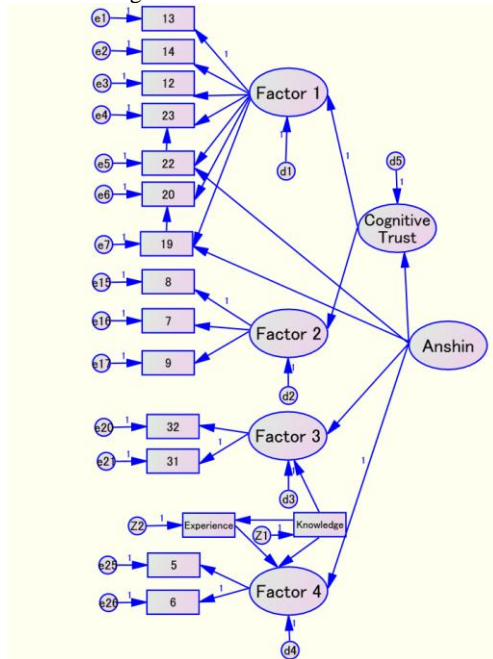


Fig 1. Anshin model

## 5 DISCUSSION

With our Anshin model with the four Anshin factors as well as user knowledge and experience, we found that the four question items were related to Anshin. This result shows the possibility of a new factor. These question items represent usability. This factor represents not only usability from the viewpoint of information technology but also the one in terms of online shopping as a whole. Two question items show operability of online shopping system. The other two question items show how the company responds to the users' queries.

We discussed the relationship between user's knowledge and the Anshin factor. As a result, the user knowledge was related to the factors three and four as well as user experience. This result shows the possibility that the factors three and four are Anshin factors for the users without information knowledge. Moreover, this result indicates that the Anshin factors might affect not only the user knowledge but also user experience.

However, the relationship between user's knowledge, user's experience and Anshin is not yet clear. Therefore, we will survey the difference in tendency to attach a high value to Anshin factor by the difference of user's knowledge level and experience level using Multivariate analysis of variance and multiple comparison. These are techniques to determine whether there would be a difference between specific groups.

## 6 CONCLUSION

In this work, we produced a new questionnaire for the survey on Anshin, which reflected feedbacks from users without technical knowledge of information security. After a survey conducted on 888 subjects with the new questionnaire, we extracted four factors for Anshin with factor analysis. We reported the construction of an Anshin model based on those four factors as well as user knowledge and experience. As a result, the model was acceptable. We have found that the four question items are related to Anshin. They are the usability factor.

We discussed the user's knowledge related to user's experience and Anshin. As a result, we showed the possibility that factor three and four were Anshin factors for users without information knowledge. In addition, we showed the possibility that only the user experience does not affect the Anshin factors. However, the relationship of user's knowledge and user's experience is yet to be clear. As the future work, we need to identify how the Anshin factors would be related to user knowledge and experience using multi-variate analysis of variance and multiple comparison.

## REFERENCES

- [1] The Knightmare: Secrets Of Super Hacker, Loompanics Unlimited, (1994)
- [2] Riegelsberger, M., J., Sasse, A., McCarthy, D. J., The mechanics of trust: a framework for research and design, International Journal of Human-Computer Studies, vol. 62, pp381-422, (2005).
- [3] 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
- [4] Fujihara, Y., Yamaguchi, K., Y., Murayama, Y., A Survey on Anshin of the Users without Technical Knowledge on Information Security, Information Processing Society of Japan Journal Vol.50 No.9, pp2207-2217, 2009
- [5] Nishioka, D., Murayama, Y. and Y. Fujihara: Producing a Questionnaire for a User Survey on Anshin with Information Security for Users without Technical Knowledge, 45th Hawaii International Conference on System Sciences (HICSS-45), pp.454-463 (2012)
- [6] Mayer, R.C., Davis, J.H. and Schoorman, F.D. "An Integrative model of organizational trust." Academy of Management Review, Vol.20, No3, pp709-734, (1995).
- [7] Tim, K., Eamonn, O., Chris, B., Vassilis, K., Danae, S.F., Tim, J., Measuring Trust in Wi-Fi Hotspots, Proc of the 26th annual SIGCHI conference on Hum

# Wide Area Monitoring System from a Balloon with Omni-Directional Cameras

Sanetaka Arimura<sup>\*</sup>, Koji Hashimoto<sup>\*\*</sup> and Yoshitaka Shibata<sup>\*\*</sup>

<sup>\*</sup>Graduate School of Software and Information Science, Iwate Prefectural University, Japan  
g231k003@s.iwate-pu.ac.jp

<sup>\*\*</sup>Faculty of Software and Information Science, Iwate Prefectural University, Japan  
{hashi, shibata}@iwate-pu.ac.jp

**Abstract** - Japan has many disasters such as earthquake and tsunami. Immediately after the disaster, we will be required to provide information quickly to collect disaster. We propose a monitoring system from the sky with a moored balloon. It will be able to remotely monitor the affected areas by this system. And solar panels and wireless LAN router omnidirectional camera is equipped with a balloon. It is compact and lightweight balloon than conventional systems thereby.

**Keywords:** Disaster, Emergency, Omnidirectional camera, Shooting from a high level, Balloon.

## 1 INTRODUCTION

More than 70% of the land in Japan is mountains. Therefore laying of infrastructure such as the Internet is difficult. In addition, Japan happen disasters such as earthquakes and tsunamis are frequent. Hence, may be an isolated village disaster occurs. Great East Japan Earthquake that occurred in March 2011, Japan suffered large. Immediately after the disaster, we will be required to provide information quickly to collect disaster. By the earthquake and tsunami, information such as the "division of the road", and "collapsed houses," and "isolated village" is very important in promoting the rescue operations. However, we cannot go to the stricken area because of the tsunami and the earthquake.

Make the design of the balloon to allow shooting from the sky, sky transferred using a fish-eye lens to the camera of Power over Ethernet, in this paper, we propose a system that allows you to monitor a wide area.

## 2 SYSTEM OVERVIEW

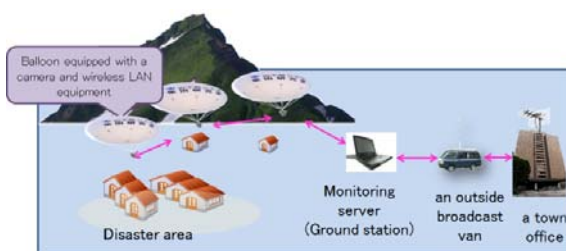


Figure 1: System overview

In this paper we propose a system for remote monitoring by sending the video to the monitoring server using the wireless LAN from the balloon equipped with omnidirectional camera. The System we to build are composed of several moored balloons and monitoring server to the image processing on the ground. The balloon is equipped with a "wireless LAN router" and "film-type solar panels" and a "lightweight compact omnidirectional camera" balloon. As shown in Figure 1, this system covers a wide area by more than one captive balloon.

Balloons communicate with each other by forming an ad-hoc multi-hop network.

It sends to the server to monitor the video of each balloon.

The camera uses device Power over Ethernet (PoE).

Necessary power is supplied to the PoE and Wireless LAN router using the film-type solar panels mounted on the balloon. Omnidirectional camera which is mounted on each balloon is sent to the monitoring server with the wireless network the image of the RGB24bit. Monitoring server performs processing such as processing and expanding panorama.

## 3 SYSTEM ARCHITECTURE

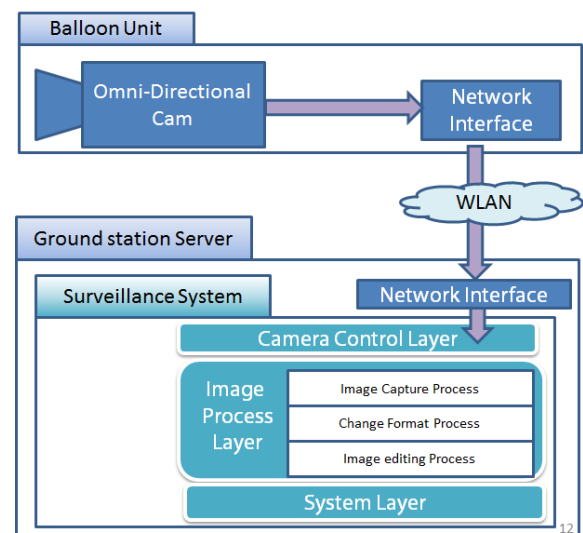


Figure 2: System Architecture

Figure 2 shows the system architecture of the monitoring system. Camera Control Manager provides functions such as connection management and configuration of the omnidirectional camera. Image Process Layer is related to image processing, such as the deployment process

omnidirectional retrieve or store images from the camera, processing and format conversion. System Manager is a general processing system for processing events in the system, such as is performed.

## 4 DEPLOYMENT PROCESS



Figure 3: Image taken by the camera

Figure 3 is a picture of the omnidirectional camera fitted with a fisheye lens. This system uses this camera. It is possible to shoot an image of 360 ° around by adopting a fisheye lens. In addition, PAL lens is a blind spot underneath, as shown in Figure 4 fisheye lens does not make a blind spot.



Figure 4: Fish-eye image



Figure 5: The panoramic image which unfolded in middleware

Panorama processing is used to customize the omni-directional middleware has been developed in our laboratory. Figure 5 is a panoramic image that is deployed in the middleware. Do not appear directly below the camera and processing panoramas. Therefore, I have implemented functions to enlarge and display the image features beneath the camera. Figure 6 shows the beneath the camera image and Enlarge image.



Figure 6: Beneath image(left), Expanded image(right)

## 5 BALLOON CONFIGURATION

Balloon used in this system is a flat type. Balloon type flat surface area is smaller than the ball type. Resistance can be reduced thereby. In addition, the balloon also increases stability by lift. Case of the sphere, horizontal to the wind drag is 0.2. On the other hand, a flat type (1:1.8) is 0.08. By filling a gas, the balloon takes advantage of the buoyancy of about 1.5 times the total weight of the role[1]. Part of the balloon

Mooring is a combination of multi-point Mooring and Mooring one point[2]. Power supply method assumes a disaster. Therefore, commercial power is not available. This system uses a photovoltaic film. And, for the downsizing of the balloon, the communication from omnidirectional cameras to the ground uses the wireless LAN.

## 6 MULTI-HOP COMMUNICATION

I assume a stricken area; the setting of the node above the ground is not possible. However, some balloons and monitoring server is far. Therefore, the balloons communicate with each other by forming an ad-hoc multi-hop network. By using multi-hop, the monitoring server can see the image of the balloons that cannot communicate directly.

## 7 MAP MONITORING

Of the balloon position and image of the panoramic image beneath camera is displayed on the map of the monitoring server. You can register the location and settings of the camera, a monitor on the map to make it easier to recognize.

## 8 PROTOTYPE

This system uses a network of PM-510's camera Arecont Vision. Resolution of the camera is  $2592 \times 1944$  pixel. The camera can be captured by using a HTTP connection 1FPS. The camera is equipped with a fisheye lens that's FJ06-2K OPTART. Film-type solar panels using the KT1500's Konarka. Development of the system language is C++ (Microsoft Visual C++ 2008), image processing using Open Source Computer Vision Library[3] (OpenCV1.1)

## 9 CONCLUSION

In this paper, we propose wide Area Monitoring System from Balloons with Omni-Directional Camera. We can by this system, to monitor the wide area of the affected areas and mountainous areas that are difficult to limits in the event of a disaster. Furthermore, the system can manage it by using the film type photovoltaic power generation panel even if there is not a commercial power supply.

Future, I Conduct actual experiments using the balloon prototype and study on the method of multi-hop communication and development of a system that maps the image on the map

## 10 REFERENCE

- [1]Ministry of Public Management Tohoku Bureau of Telecommunications, Study group of balloon wireless network system for disaster recovery
- [2]Masahiko ONOSATO, Moored balloon type information for disaster Information "Development of InfoBalloon"
- [3] <http://opencv.willowgarage.com/wiki>



# Analysis of Backscatter from Chipless RFID Using Metal Patches

Kyohei Chiba<sup>\*</sup>, Goutam Chakraborty<sup>\*\*</sup>

<sup>\*</sup>Graduate School of Software and Information Science, Iwate Prefectural University, Japan  
g231j027@s.iwate-pu.ac.jp

<sup>\*\*</sup>Faculty of Software and Information Science, Iwate Prefectural University, Japan  
goutam@iwate-pu.ac.jp

**Abstract** - The main reasons hindering the wide spread deployment of passive RFID tags are high cost and limited range. The present work focuses on developing a sub-cent RFID capable of operating from a reasonable distance, though with some compromise on the information content. Defined by poles and zeros depending on the dimensions of the patch, such resonating structures can be used to create tags with a purpose of storing information in the various resonant frequencies. The challenge is to retrieve these resonant frequencies in the presence of clutter from surrounding objects without the use of any nonlinear elements. We have used an Artificial Neural Network to analyze the nature of the clutter signal.

**Keywords:** Patch Antenna, Chipless RFID, Backscatter, Soft-computing techniques, Artificial Neural Network

## 1 INTRODUCTION

Radio frequency identification (RFID) is used in numerous applications to identify and track object or living beings.

1. RFIDs using semiconductor chips hit a cost wall.
2. Creating an RFID at the end user's premises, as is done with printed bar code labels, is still not practical.
3. The operating range for passive backscatter tags is relatively short.

Once the above restrictions are lifted, read-only RFID is expected to see a significant increase in deployment. The motivation of the present work is premised on constructing metallic structures (ideally lossless), that would scatter all the energy incident on a structure without the need for powering a chip. In the absence of clutter, such a structure provides backscatter whose amplitude independent of frequency of illumination (assumed continuous wave), but the backscattered signal suffers discernible change in phase as resonance is approached. Such resonances are the mechanism to code the information. As the technique uses phase rather than amplitude to detect resonance, there is more room to operate in real-life environments containing clutter. Furthermore, being a frequency domain technique, it could use small detection bandwidth and therefore be capable of operating with very little transmitted power. At the same time, it could use a large operating bandwidth to create range gating and thereby reduce the effect of clutter.

## 2 BASIC PRINCIPLE

Figure 1 depicts a rectangular patch antenna as a scattering structure - one of the kinds of RFIDs we propose. This one

has three layers of conducting metal patches, separated by dielectric. When the upper patch resonates, the middle patch acts as a ground plane. Similarly, when the middle patch resonates, the bottom patch acts as a ground plane [1]. Depending on the dimensions of the two upper layer patches, we will have two resonance frequencies in the fundamental mode if patches are assumed to be square [2]. The transmit signal is a swept continuous wave signal. As the frequency sweeps, the phase (and therefore group delay) undergoes significant changes at resonance frequencies.

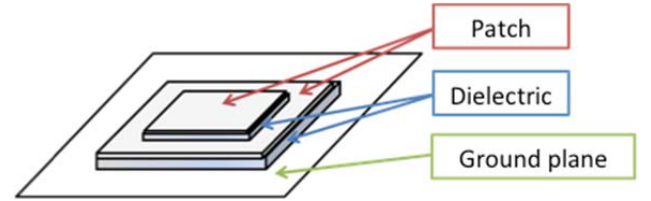


Figure 1: Stacked rectangular patch antenna

## 2.1 Set-up to Measure Backscatter

Two identical linearly polarized log periodic antennas were connected to the ports of a Vector Network Analyzer (VNA) and the signal between them was measured. As discussed in [2], the transfer function of the patch antenna will be described by the following equation:

$$H_{\omega i} = A_m \times \exp(-j \cdot \omega_{ch} \cdot \tau) \times \prod_{i=1}^N \frac{(-j \cdot \omega_{ch} - z_i)(-j \cdot \omega_{ch} - z_i^*)}{(-j \cdot \omega_{ch} - p_i)(-j \cdot \omega_{ch} - p_i^*)} = \Re + j \cdot \Im \quad (1)$$

Where  $N$  is the number of patches,  $i$  is the index for different poles and zeros,  $p$  and  $z$  are the  $i^{th}$  pole and zero respectively,  $p^*$  and  $z^*$  denoting the complex conjugate, ( $i \cdot \omega_{ch}$ ) is the complex swept signal frequency,  $A_m$  is the scale factor or normalization factor. From the structure, we know that the number of poles is equal to the number of zeros. With two layers of patches above the ground plane, we will give two poles and two zeros. For an ideal all-pass network, as the patch antenna would, the poles and zeros are exactly mirror images about the imaginary axis.

## 3 ANALYSIS OF THE SIGNAL

In this section, we discuss the three-step algorithm to analyze the backscatter signal.

### 3.1 Removing the periodic humps

Different frequency components of a swept signal experience different phase shifts for the  $\exp(-j \cdot \omega \cdot \tau)$  term in Eq. 1, the backscatter signal looks like a periodic sinusoidal except at resonant frequencies. In real situations, in the presence of noise, the shape is further distorted as in Figure 2. To get the actual pole zero, we first need to estimate  $\tau$  and eliminate its effect. The easiest way is to multiply the scattered signal with  $\exp(j \cdot \omega \cdot \tau)$  which is reciprocal of  $\exp(-j \cdot \omega \cdot \tau)$ . As the estimation of  $\tau$  is only approximately correct, this may not eliminate the delay effect totally. At present, we eliminate the delay effect by multiplying the scattered signal with  $\exp(j \cdot \omega \cdot \tau)$ . Though the result is reasonably good, it is not perfect due to small error in delay estimation.

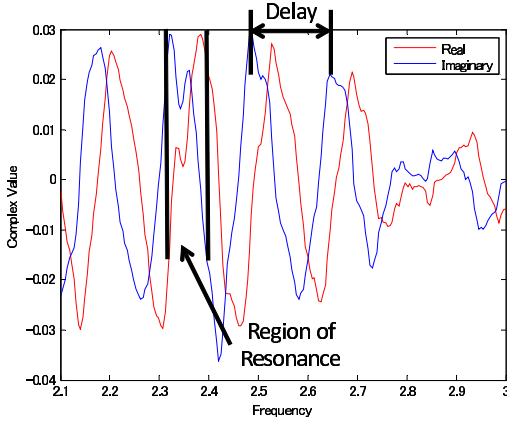


Figure 2: Scattered signal in the presence of significant clutter.

### 3.2 Identifying the Region of Resonance

Once the scattered signal is preprocessed to eliminate the delay effect, the only point where the real and imaginary value crosses with opposite slope is near the resonance. But, it is not the exact point of resonance. This is because, due to structural imperfections, pole and zero are nearly symmetric but not exactly so. The clutter do not have any symmetric poles and zeros. As the aim is to find the extract value of resonance frequency, we extract signal around the resonance.

### 3.3 Analysis of Artificial Neural Network

We used Artificial Neural Network (ANN) of multi-layer perceptron type trained by error-back propagation. [3]

## 4 ANALYSIS AND RESULT

As shown in Figure 3, the ANN used in our work has 30 input nodes, 15 representing real values of the scattered signal and 15 imaginary values. The real-imaginary crossing point is the middle data. In addition, 7 values from lower frequencies and 7 values from higher frequencies are used in the input. The two outputs represent the imaginary parts of pole and zero. 5000 artificially created data were generated, out of which 4000 were used for training the ANN and the remaining 1000 used for testing the

performance of the trained neural network. Using the MLP in Figure 3, we trained the ANN 10,000 times (learning rate is 0.001).

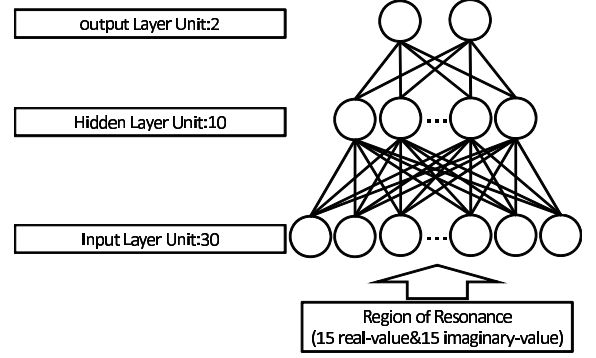


Figure 3: Artificial Neural Network architecture.

## 4.1 Experimental Result

We present two results, one showing the stability of the detected resonant frequency with respect to different trials, varying the experimental environment. These results are shown in Table I. All results are with one ground plane and two patches above it, the three patches being separated by dielectric. All scattered signals are from the lowest mode of resonance. The consistence, i.e., low standard deviation of the results ensures stability of the system.

Table 1: The Resonance Frequency - Its Answer and Average and Standard Deviation

	Two Patches	Single patches
Answer	3.60	4.40
Average	3.63	4.44
Std.Dev	0.05	0.07

## 5 CONCLUSION

We proposed a novel way to realize implementation of chipless RFID using layered thin metal patches. The size of the patch, which is its signature information, could be read from the resonating frequency of the backscatter when a swept signal is incident. We also proposed an Artificial Neural Network based algorithm for real-time reading of the scattered signal, even in the presence of noise. The accuracy of the result and its low standard deviation ensures the possibility of its use in real world environments. We are continuing work on the following to enhance the accuracy and robustness of the system.

## REFERENCES

- [1] Bancroft R. Microstrip and Printed Antenna Design, Noble Publishing Corporation 2004
- [2] Somnath Mukherjee and Goutam Chakraborty, ``Chipless RFID using stacked multilayer patches``, IEEE International Conference on Applied Electromagnetics, Kolkata, Dec., 2009.
- [3] Christopher M. Bishop, Neural Networks for Pattern Recognition, Oxford University Press, 1995.

# Privacy Protection by using masquerade pointer in Android OS

Harunobu Agematsu<sup>1</sup>, Junya Kani<sup>1</sup>, Kohei Nasaka<sup>1</sup>, Hideaki Kawabata<sup>2</sup>,  
Takamasa Isohara<sup>2</sup>, Keisuke Takemori<sup>2</sup>, Masakatsu Nishigaki<sup>3</sup>

1 Graduate school of Informatics, Shizuoka University  
3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011 Japan  
{gs11002,cs08028,gs10041}@s.inf.shizuoka.ac.jp

2 KDDI R&D Laboratories, Inc.  
2-1-15 Ohara, Fujimino, Saitama, 356-8502 JAPAN  
{kawabata, ta-isohara, takemori}@kddilabs.jp

3 Graduate school of Science and Technology, Shizuoka University  
3-5-1 Johoku, Naka, Hamamatsu, Shizuoka, 432-8011 Japan  
nisigaki@inf.shizuoka.ac.jp

**Abstract**— Security of smart phone is considered as important. Especially the number of leakage of privacy information, incorrect billing, and one-click billing fraud has been increasing recently, and they cause many problems. This paper proposes a new security measure to protect privacy information; “security manager” and “masquerade pointer”. The security manager returns the reference pointer for the privacy information, instead of the privacy information itself, when any Android application sends a request for it to the OS.

**Keywords**—component; Android smartphone; malicious Android application; security manager

## 1 INTRODUCTION

The number of Android phone (smartphones equipped with the Android OS) users has exploded in recent years.

Some famous markets such as Google Play Store [1] take steps to check all applications and remove malicious ones. However, “untrusted” market places exist, in which malicious applications pretending to be safe applications infiltrate the market. These malicious Android applications (One-Click ware[2], Geinimi[3]) called Trojans cause many problems. Once installed, it leaks personal information to an external server. Its behavior appears normal from the user’s perspective, thus hiding the leak.

In this paper we introduce a “security manager” module for the Android OS, to handle personal information in a safer manner. Under standard Android OS operations, when an application requires personal information, (i) it sends a request to the OS (ii) the OS returns the information to the requesting application. The proposed module is implemented into the Android OS between an application and the OS. Under the proposed solution, when an application requests personal information, (i) it sends the request to the “security manager” module, (ii) the “security manager” returns a reference pointer to the data instead of the data itself.

## 2 RELATED WORK

Enck et al proposed “TaintDroid”, a system-wide dynamic taint tracking system, in which multiple sources of sensitive data are tainted and the taint is used as a marker capable of real-time tracking of sensitive data [4]. They implemented “TaintDroid” and the evaluation result said that the overhead time for taint tracking was about 29% at most.

## 3 ANDROID OS

The following is an overview of the standard API call flow in Android OS, when an application requests personal information for displaying on smartphone screen (Figure 1)  
Step1) The application calls the API, which retrieves the personal information.  
Step2) The OS returns the personal information to the application.  
Step3) The application calls the display API with the data received from OS.  
Step4) The OS displays the personal information on smartphone screen.

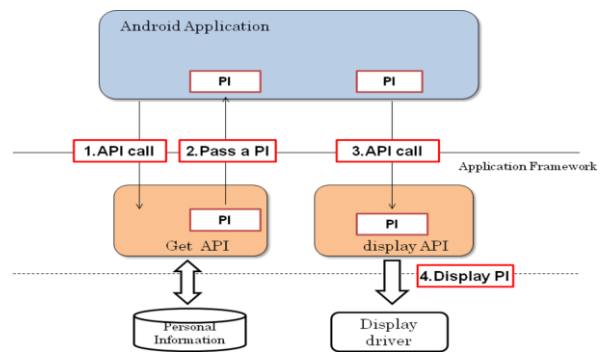


Figure1. The management of personal information in Android OS

The problem here is that the Permission request (Figure2) at time of installation is very abstract for ordinary users. It is difficult to determine what the application will do, and it is also hard to judge exactly what kind of information the applications will access. Due to this, it could be hard for most users to understand an application's potential threat. Once such an application is installed, it can cause multiple problems, since smartphones maintain a considerable amount of personal information.

## 4 PROPOSED METHOD

In this paper, we develop the reference pointer (masquerade pointer) and security manager. The security manager manages the personal information and reference pointer in Android OS.

The security manager returns a reference pointer instead of personal information to a requesting application, and inserts it into the security manager table. When an application outputs the personal information, the security manager automatically decides whether to retrieve the personal information from reference pointer or not. If the output is within the resources managed by OS (for example, the screen for display), it is automatically retrieved. If the output falls outside of the OS (for example, send it to other phone or write it in phone's SD card), the security manager asks for confirmation from the user. It retrieves the data only when permission is granted by the user.

If the user grants read permission (ex. READ\_PHONE\_STATE) to a malicious application, any personal information is replaced with reference pointers when the application reads it. The malicious application never gets the data itself, thus it cannot leak it. Access to the sensitive data by a non-malicious application is unaffected, since the security manager automatically retrieves the information. In section 3.1, we gave an overview of the series of API calls (Figure 1) made by an application requesting personal information. Implementation of our proposal (Figure 2) changes the flow of API calls as follows:

Step1) The Application calls the API, which retrieves the personal information.

Step2) The security manager generates a descriptor (the reference pointer), it pairs the data with the descriptor, and inserts them into the table.

Step3) The OS returns the reference pointer to the requesting application.

Step4) Application calls the display API with reference pointer.

Step5) The security manager refers to the table and retrieves the personal information from the reference pointer and passes it to the OS.

Step6) The OS displays the personal information on smart phone screen.

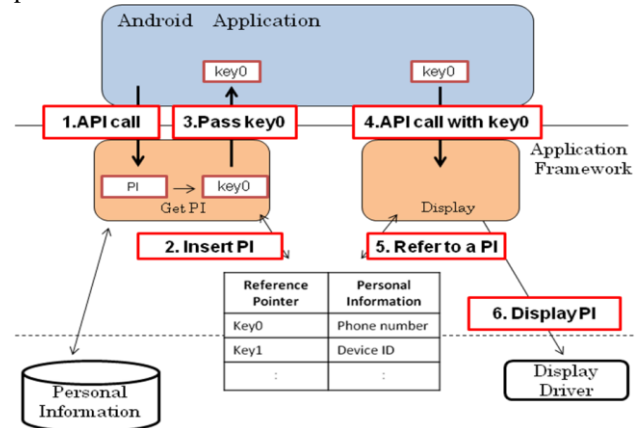


Figure2. Management of personal information by security manager

When the application simply displays the information to the screen (Figure 2), the user is not required to confirm access to the data in step 5. However, when the application attempts to send the data externally, the called API is changed to Send API (instead of Display API) at step 4 and step 6. In this case, the user receives a confirmation dialog at step 5.

## 5 CONCLUSION

In this paper, we proposed a solution to the problem of information leak. We implemented that solution through the security manager module, and masquerade pointer, which masks the personal information at the application level. Android users can prevent many forms of leak of information by implementing the security manager module into the Android OS. The next step is to deal with the issue arising from masking the data to allow processing of personal information in non-malicious applications. As well as solving the limitations when dealing with premium rate abuse, and bot attacks. A proposal for a countermeasure against the wrong use of root authority should be formulated.

## REFERENCES

- [1] Google Play Store:  
<https://play.google.com/store>
- [2] TrendLabsSecurityBlog:  
[http://blog.trendmicro.co.jp/archives/4714\(in japanese\)](http://blog.trendmicro.co.jp/archives/4714(in%20japanese))
- [3] Yomiuri Online "Appearance bots to the Android terminal":  
<http://www.yomiuri.co.jp/net/security/goshinjuryutsu/20110107-OYT8T00678.htm> (in japanese)
- [4] William Enck, Peter Gilbert, Byung-Gon Chun, Landon P. Cox, Jaeyeon Jung, Patrick McDaniel, Anmol N. Sheth : "TaintDroid: An Information - Flow Tracking System for Realtime Privacy Monitoring on Smartphones", Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI'10), Canada, 2010



# Gamified CAPTCHA

Junya Kani<sup>\*</sup>, Harunobu Agematsu<sup>\*</sup>, Masakatsu Nishigaki<sup>\*\*</sup>

<sup>\*</sup>Graduate School of Informatics, Shizuoka University, Japan  
{gs12012, gs11002}@s.inf.shizuoka.ac.jp

<sup>\*\*</sup>Graduate School of Science and Technology, Shizuoka University, Japan  
nisigaki@inf.shizuoka.ac.jp

**Abstract** –We propose a Gamified CAPTCHA that uses movie-based quizzes to prevent malicious automated attacks by employing the human capability to recognize the “strangeness” of a short movie story.

**Keywords:** CAPTCH, Entertainment-Security, strangeness, quiz

## 1 INTRODUCTION

With the expansion of web services, denial-of-service (DoS) attacks by malicious automated programs (e.g., bots) are becoming a serious problem. Thus, the Turing test is becoming a necessary technique to discriminate humans from malicious automated programs and the CAPTCHA [1] system developed by Carnegie Mellon University has been widely used. The simplest CAPTCHA presents distorted or noise added text (Figure.1) to a user. If the given text is read correctly, the CAPTCHA decides the user is a human; otherwise malicious automated programs (bots).

However, researchers have recently pointed out security problems with conventional CAPTCHA [2]. We therefore need to adopt even more advanced human cognitive processing capabilities to enhance CAPTCHA to overcome this problem.

But, proving whether one is human can be an annoying to the users. We must make the CAPTCHA systems user friendly.



Figure.1 CAPTCHA used by Google

## 2 FOUR-PANEL CARTOON CAPTCHA

Focusing on the human cognitive capability to “recognize strangeness”, and “understand humor”, we proposed the “four-panel cartoon CAPTCHA” [3].

This CAPTCHA presents the four randomly rearranged panels. And if the user sorts the panels in the correct order, it decides the user is a human. For a computer, however, it would be a difficult task to sort the four panels in the right order unless it is able to understand humor. Because reading cartoons is fun and entertaining for humans, a four-

panel cartoon CAPTCHA will most likely be seen as an agreeable and enjoyable Turing Test; thus it does not adversely affect the users.

## 3 IMPROVEMENT OF USABILITY

For enhancement of safety, we employ the advanced human cognitive processing capability.

For enhancement of usability, we focus on the novel ability of human “quiz” for improvement of CAPTCHA. When a human challenges a difficult quiz, he/she feels engaged and eager to solve the problem. We developed a CAPTCHA that makes use of fun activities, which is different from the existing CAPTCHA systems.

## 4 GAMIFIED CAPTCHA

We propose a new CAPTCHA that combines two human capabilities (1) to recognize “strangeness” and (2) to solve “quizzes”.

### 4.1 Example of authentication procedure

Step1. Randomly select one of the movies from the movie database.

Step2. For some of the scenes of the movie is selected, perform the swapping process or the deletion process.

Step3. Play the movie to the user.

Step4. The user clicks on the screen as soon as he/she feels strangeness in the sequence of the movie scenes.

Step5. If the user clicks at the right moment, the user is a human. Otherwise, a malicious automated program.

### 4.2 Strangeness about the movie

Strangeness can be introduced by a swapping or deletion of the scenes in the movie. This strangeness would be difficult to recognize for malicious automated programs.

#### 1). Swapping

We chose two scenes and swap them. A human should be able to point out find the scenes that have been swapped.

## 2). Deletion

A scene is deleted from the movie. A human should be able to find the location of the deleted scene. If the user has trouble finding location of the deleted scene, the deleted scene is presented as a hint.

## 5 BASIC EXPERIMENT

The purposes of this experiment are: 1) to determine if the proposed system is usable by humans, 2) to investigate the entertainment value of the proposed method.

The subjects in this experiment were ten volunteer students from the department of information and the department of engineering of Shizuoka University. We played the movie that had two scenes swapped or a scene deleted. The subjects were instructed to suspend the movie when they recognized strangeness. The movie was played without sound to avoid clueing the malicious automated programs in to “skipping” in the movie with audio cues. The movies were to satisfy the two criteria:

- Easy to understand the story without voice.
- Fun to watch.

We chose the “Tom and Jerry” cartoon movie for the experiment.

The user can watch the movie as many times as needed. However, the number of clicking to pause is limited to three times. The subjects were given three CAPTCHA tests, Text CAPTCHA (2 questions), Swapping CAPTCHA (2 questions), and Deletion CAPTCHA (2 questions). In the case of the deletion, the subjects were allowed to see the hint.

After finishing all CAPTCHA tests, we asked the following questionnaire.

- Did you enjoy sorting the CAPTCHA? (Fun)
- Is it user friendly? (User-friendly)
- Is it easy to sort the movie? (Easy-sort)
- Are you happy when you are correct? (Happy)
- Did you want to do it one more time? (One-more-time)

Each question is scored by the subjects on a 1-5 point scale, 1 meaning definitely no, 5 meaning definitely yes.

Table 1 shows the percentage of correct clicking. The high percentage indicates the users were recognized the “strangeness”.

Table 2 shows the average score of questionnaire responses. As for “Fun”, “Happy”, “One more time”, the averages of Gamified CAPTCHA exceed 4 point. As for “User-friendly”, the average of Gamified

CAPTCHA is 2.6 points, which is almost the same as the text recognition based-CAPTCHA.

Table1. Percentage of correct clicking

CAPTCHA	Percentage
Swapping CAPTCHA(1question)	90%
Swapping CAPTCHA(2question)	100%
Deletion CAPTCHA(1question)	100%
Deletion CAPTCHA(2question)	100%

Table2. Result of questionnaire

	Text	Swapping	Deletion
Fun	1.9	4.3	4.4
User-friendly	2.7	2.7	2.5
Easy-sort	3.1	3.1	2
Happy	1.8	4.4	4.5
One-more-time	1.2	4.3	4.4

## 6 CONCLUSION

From the experiment result we conclude it is easy to recognize the strangeness that the Gamified CAPTCHA presents. The table 2 shows the increased level of “Fun”, “Happy”, and “One-more-time”, with moderate sacrifice in User friendliness.

## 7 FUTURE WORK

We plan to use a better statistical method including a larger population and controlled experiment. We will analyze the safety against brute-force-attacks, and improve the usability by reducing the user time required for the Gamified CAPTCHA, and automating the movie creation process.

## REFERENCES

- [1]The Official CAPTCHA Site,  
<http://www.captcha.net> <http://www.captcha.net>.
- [2] PWNtcha-Captcha Decoder  
<http://caca.zoy.org/wiki/PWNtcha>
- [3] Tokuichiro Suzuki, Takumi Yamamoto, Masakatsu Nishigaki:Proposal of Four-panel CARTOON,SCIS,3D3-3(CD-ROM),2009

# Fuzzy Signature scheme for Biometric Digital Signature

Yuta Yoneyama<sup>1</sup>, Kenta Takahashi<sup>2,3</sup>, Eisei Honbu<sup>1</sup> and Masakatsu Nishigaki<sup>4</sup>

<sup>1</sup>Graduate School of Informatics, Shizuoka University, Japan  
{gs12040, gs11042}@s.inf.shizuoka.ac.jp

<sup>2</sup>Graduate School of Information Science and Technology, The Universe of Tokyo, Japan

<sup>3</sup>Technology Laboratory, Hitachi Ltd., Japan  
kenta.takahashi.bw@hitachi.com

<sup>4</sup>Graduate School of Science and Technology, Shizuoka University, Japan  
nisigaki@inf.shizuoka.ac.jp

**Abstract** -In this paper, we built a fuzzy signature scheme by fusing functionally in the Schnorr signature and fuzzy commitment in the integral lattice space. It allows variance in the inputted value of the private key. Thereby we realize a biometric digital signature which outputs the verifiable signature given only plain text and biometric information.

**Keywords:** Digital Signature, Biometrics

## 1 INTRODUCTION

A digital signature is a scheme for verifying the authenticity of a digital message and the sender. Digital signatures are necessary for the safety of financial transactions. Digital signature provides functions of authentication and non-repudiation.

A digital signature scheme is typically formulated as a function that generates the signature when given plain text and a private key. The private key which is needed to generate the signature is important information as a trust point. So traditionally the private key must be stored in an IC card, and the problem is, they can be lost or stolen and IC cards are less convenient.

In contrast, using biometric information as the private key is expected that avoids these problems. However, biometric information is generally processed as analog values and due to read errors the values may differ. Since current cryptosystem is usually based on number theory, it is difficult to realize a digital signature scheme that allows the error in the value of the private key.

To solve this problem, biometric key generation techniques that commit random values using the biometric information based on biometric encryption has been studied [4, 5]. In the biometric encryption, it can restore the random numbers, if given only a biometric information near enough to the one used when committing the random number. Digital signature using biometric information is realized by using this random number as a secret key. But in this scheme, it is necessary that the user is required to present commitment to the system. Thus, it is needed for the user of that query to request from the server which manages the commitment, or possession of the commitment in an IC card. So far as we know, a function to achieve fuzzy signature: given only plain text and biometric information which

corresponds to the private key and outputs a signature, have not been developed.

In this paper, we built a fuzzy signature scheme by fusing functionally in the Schnorr signature [1] and fuzzy commitment in the integral lattice space [2], and thereby realized a biometric digital signature.

## 2 DEFINITIONS

In this chapter, we define the digital signature and biometric digital signature and the requirements needed to realize this proposal.

### 2.1 Definition of Digital Signature

A digital signature scheme typically consists of three algorithms:

**Key generation algorithm G:**  $gen(1^k) \rightarrow (K_s, K_p)$

Select a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

**Signing algorithm S:**  $sig(K_s, M) \rightarrow \sigma$

Given a message and a private key, produces a signature.

**Verifying algorithm V:**

$ver(m, K_p, \sigma) \rightarrow \text{ACCEPT or REJECT}$

Given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

These algorithms require two main properties as following.

**Legitimacy:** legitimate user can make verifiable signature.

**Security:** illegitimate users cannot forge a legitimate signature.

### 2.2 Definition of Biometric Digital Signature

In this paper, we define that a digital signature scheme that uses biometric information to generate a digital signature is biometric digital signature. A biometric digital signature scheme consists of three algorithms.

**Key generation algorithm BG:**  $gen_b(1^k, b) \rightarrow K_p$

Given a security parameter  $k$  and user biometric information, outputs a public key corresponding to user biometrics called the public template.

**Signing algorithm BS:**  $sig_b(b', M) \rightarrow \sigma$

Given a message and a user's biometric information, produces a signature. We note that biometric information

used as a template, generation is slightly different from the one used at signing corresponding to the signing key extracted by the same user. This is due to minor errors in biometric information scanning.

#### Verifying algorithm BV :

$ver_b(m, K_p, \sigma) \rightarrow \text{ACCEPT or REJECT}$

Given a message, public template and a signature, either accepts or rejects the message's claim to authenticity.

Because the biometric digital signature is a form of digital signature, shown in Section 2.2 will be taken over directly as requirements that must be met even in the biometric digital signature. However, in each requirement, we must consider the threshold of variance in biometric information as a signature generation key (private key).

### 3 FUZZY SIGNATURE SCHEME

In This chapter describes the fuzzy signature scheme that meets the definitions and requirements of biometric digital signatures shown in the previous section.

#### Preparation

P1 Let biometric feature  $n$ -dimensional real vector, distance of between biometric features  $X$  and  $X'$   $L_\infty$  distance i.e.

$$d(X, X') = \max_i |x_i - x'_i|$$

If  $d(X, X') < t$  then  $X$  and  $X'$  are matching.

P2 Let large prime  $p$ , generator  $g \in \mathbb{Z}_p^*$ , security parameter  $K$ , set of grid points  $\mathcal{L}(K)$  as follow:

$$\mathcal{L}(K) = \{Y = (y_0, \dots, y_n - 1) | y_i \in \mathbb{Z}, 0 \leq y_i < K\}$$

and function  $int: \mathcal{L} \rightarrow \mathbb{Z}$  be common parameter on the system.

#### Key generation

Inputs: biometric feature vector  $X$

Outputs: public template  $T$

G1 Choose integral vector  $Y \in \mathcal{L}(K)$  at random.

G2 Let  $s = int(Y)$ ,  $h = g^{-s} \bmod p$ .

G3 Let fuzzy commitment  $C = X + 2t \cdot Y$ , and outputs  $T = (h, C)$ .

#### Signing

Inputs: plain text  $M$ , biometric feature vector  $X'$

Outputs: signature  $\sigma$

S1 Choose integral vector  $Y' \in \mathcal{L}(K)$  at random.

S2 Let  $s' = int(Y')$ ,  $h' = g^{-s'} \bmod p$ .

S3 Generate Schnorr signature  $\hat{\sigma}$  of  $M$  using  $s'$  as private key. Then  $h'$  is public key to verify  $\hat{\sigma}$ .

S4 Let  $C' = X' + 2t \cdot Y'$ , and outputs  $\sigma = (\hat{\sigma}, h', C')$ .

#### Verifying

Inputs:  $M, \sigma, T$

Outputs: ACCEPT or REJECT.

V1 Verify  $\hat{\sigma}$  using  $M$  and  $h'$  in manner of Schnorr's scheme, if invalid outputs REJECT and quits.

V2 Compute  $s_d$  as follow:

$$s_d = int\left(\left\lfloor \frac{1}{2t} \cdot (C - C' + t \cdot \mathbf{1}) \right\rfloor + K \cdot \mathbf{1}\right)$$

where  $V = (v_0, \dots, v_n) \in \mathbb{R}^n$ ,  $[V] = ([v_0], \dots, [v_n]) \in \mathbb{Z}^n$  and  $\mathbf{1} = (1, 1, \dots, 1)$ .

V3 Compute  $h_d$  as follow:

$$h_d = \frac{g^{-int(K \cdot \mathbf{1})} h}{h'} \bmod p$$

V4 If  $h_d = g^{-s_d} \bmod p$  then outputs ACCEPT or return REJECT.

In step V2,  $s_d$  is equal to  $s - s'$  only when  $d(X, X') < t$ . So, verifier can confirm that  $X$  and  $X'$  are nearing enough and signature is valid by matching  $s_d$  and exponent of  $h_d$  in step V3.

### 4 EVALUATION

About legitimacy, if the signer is a person having biometric information included in the public templates, it can be expected that  $d(X, X') < t$ . Therefore, if the signature is generated by an owner of the public template, it is possible to pass verifying.

About security, Schnorr signature is proven of CMA-EUF (existentially unforgeability against adaptive chosen-message attack) under the assumption of discrete logarithm problem hardness and random oracle [3]. Therefore  $s'$  is necessary to forge the signature. However, it is difficult that guess  $s$ ,  $s'$ ,  $x$  or  $x'$  by signature, public template or calculation of  $s - s'$  and  $x - x'$  under the assumption same as Schnorr signature. So, fuzzy signature is as difficult to forge as Schnorr signature.

### 5 CONCLUSIONS AND FUTURE WORK

In this paper, we built a fuzzy signature scheme by fusing functionally in the Schnorr signature and fuzzy commitment in the integral lattice space that allow variance in the inputted value of private key. Thereby realizing a biometric digital signature which avoids risks of being stolen, lost and is more convenient.

Future work is more research in security, implement and evaluate the accuracy and verify experiments.

### REFERENCES

- [1] C. P. Schnorr, "Efficient identification and signatures for smart cards", CRYPTO'89, LNCS 435, pp.239-252. Springer-Verlag, 1990.
- [2] G. Zheng, W. Li, and C. Zhan, "Cryptographic key generation from biometric data using lattice Mapping", In 18th International Conference on Pattern Recognition, 2006.
- [3] Pointcheval D. and J. Stern, "Security proofs for signature schemes", Proceedings of EUROCRYPT '96, LNCS 1070, pp.387-398, Springer-Verlag, 1996.
- [4] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", IEEE International Symposium on Information Theory, pp.408, 2002.
- [5] A. Jules and M. Wattenberg, "A fuzzy commitment scheme", In Proc. ACM Conf. Computer and Communication Security, pages 28-36, 1999.



# Studies on the efficiency of delivery methods in P2P streaming using BitTorrent

Takanori Kashiwagi<sup>\*</sup>, Jun Sawamoto<sup>\*\*</sup>, Eiji Sugino<sup>\*\*</sup> and Norihisa Segawa<sup>\*\*</sup>

<sup>\*</sup>Graduate School of Software and Information Science, Iwate Prefectural University, Japan  
g231j009@s.iwate-pu.ac.jp

<sup>\*\*</sup>Faculty of Software and Information Science, Iwate Prefectural University, Japan  
{sawamoto, sugino, sega}@iwate-pu.ac.jp

**Abstract** – Here in we describe a method for improved streaming content delivery over P2P networks using BitTorrent. We present an improvement on the established methods of BiToS and RarestFirst.

**Keywords:** Networks, Streaming, Peer to Peer, BitTorrent, Content delivery

## 1 INTRODUCTION

Streaming large files such as video and audio content from the internet has become an increasingly common practice with users and content providers [1]. Content delivery presents serious challenge for content providers, with the increased cost of hosting and transmitting large video files, the existing client server system is experiencing problems. The high server load of incurred by the client model is costing hosts considerable resources.

Peer to Peer (P2P) technology alleviates some of these problems by distributing transfer work among multiple hosts (peers). P2P works by sending and receiving data directly with other peers that are participating in the network. It distributes resources and load across the network. This can solve the problem of the client server system resource overload.

The purpose of this research is to propose a method which is suitable for streaming using P2P and solves the problem of client server system resource overload. The work hopes realize stable video streaming, low latency playback, and reduction of the number of breaks due to buffering.

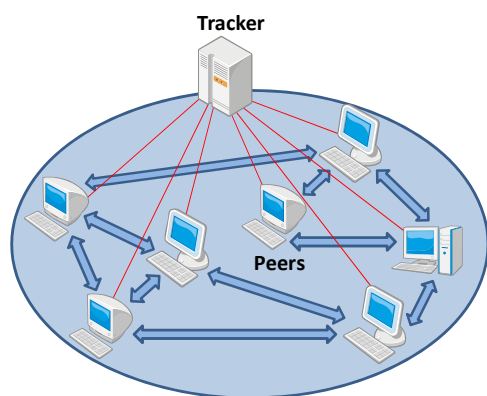


Figure 1: BitTorrent

## 2 BACKGROUND

BitTorrent is one of the most popular P2P protocols [2]. Holding, sending, and receiving of all content is performed by only the peers. The tracker manages information about peers in the swarm, it co-ordinates initial connections and keeps a table of connected hosts. File transfer operates by splitting the file into many pieces.

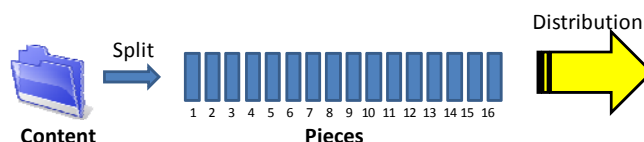


Figure 2: File transfer operates

Peers transfer the pieces out of order in a distributed fashion then re-assemble the original file. This distributed method is suitable for large-capacity content delivery.

The order of the pieces transferred is determined by the RarestFirst algorithm. This algorithm tells peers to send the least common pieces amongst the swarm first, causing convergence faster. RarestFirst transfer makes P2P very efficient when compared to the random out of order method. However, it is bad for streaming because pieces are transferred out of order and it is hard to predict the next piece. Streaming requires in-order transfer for smooth playback. The method proposed in this paper aims to provide more predictable transfer to allow for smooth playback.

BiToS(Enhancing Bittorrent for Supporting Streaming Applications) was a previous attempt to solve the streaming P2P problems [3]. It was research to reduce the number of breaks when streaming using BitTorrent. The BiToS method changed from RarestFirst so that pieces near playback mark have higher priority than later pieces. This allowed somewhat smoother playback, but there were still pauses. BiToS method works by assigning a priority to two groups of pieces. If the probability of selecting a piece from the high priority group is "p" then low priority group probability is "1-p". Within each priority group we simply use RarestFirst method.

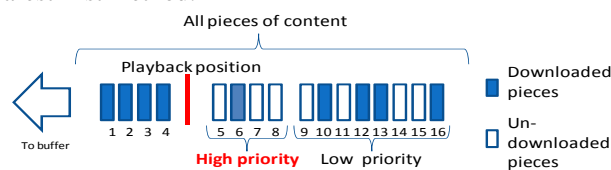


Figure 3: BiToS method

The number of pieces in the group changes depending on the playback position. Using BiToS we receive pieces closer to the playback position sooner. This is more suitable for content delivery than pure RarestFirst method.

However within each group the RarestFirst method is still used, so there may be breaks if the priority group is next to the playback position. This means pieces are still sent out of order within each priority group. This causes gaps in playback when the playback position reaches an un-downloaded piece.

### 3 PROPOSED SOLUTION

To propose a method which is suitable for streaming using P2P, emphasis must be placed on reduction of the number of breaks in playback. To this end, we must do something different if there is a gap in download pieces between our playback position and the next available piece.

Improved peer and piece selection methods, such as special priority for pieces near playback position may hopefully alleviate the problems with BiToS and RarestFirst. Specifically, if the piece closest to the playback position is not yet downloaded then the proposed method will set an emergency priority. Within the high priority group we must request missing pieces from the peer with the fastest connection.

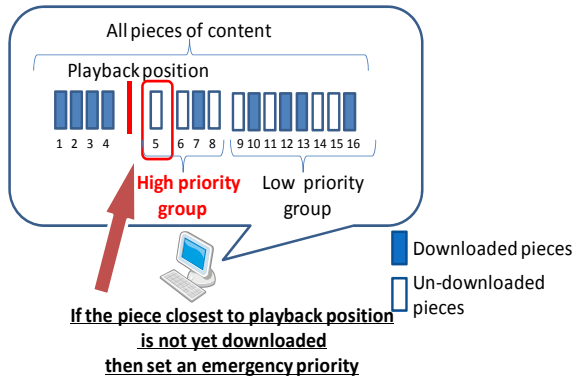


Figure 4: emergency priority

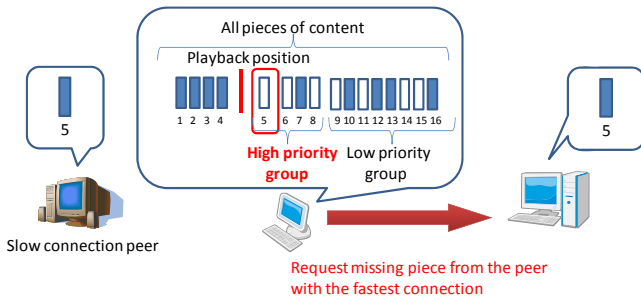


Figure 5: peer selection

If there is enough buffered content then the new method may download pieces from a lower priority group using simple RarestFirst. Thus it is still possible to contribute to the distribution of rare pieces on low priority groups and improve convergence speed.

The proposed method solves the problem of BiToS where pieces close to playback are not always chosen. This leads to a more stable delivery and smooth playback.

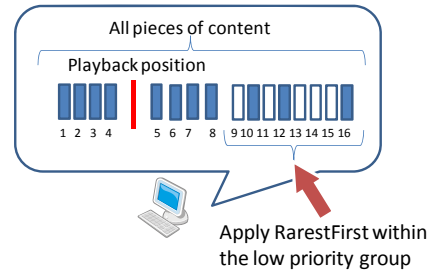


Figure 6: enough buffered content

### 4 PLANNED EXPERIMENTS

In order to verify the proposed method's effectiveness when compared to the established methods of RarestFirst and BiToS, it is necessary to perform simulations and experiments. One such proposed experiment is to provide a peer that implements each method on a software simulator.

The simulation begins with one peer joining the network with a complete copy of the content in advance. Following at 10 second intervals a peer will join the network and start downloading content. The simulation ends when all the peers have downloaded all the content. The sample content will be a 900MB file comprising about 3600 seconds of video. The file will be split up into 1MB pieces, about 4 seconds each. The total number of pieces should be 900. Video playback shall commence once the first piece of content has been completely downloaded.

Multiple peers will download a piece of content and performance results will then be compared. Comparison metrics will include total time of playback, the number of playback failures, and the number of times the playback is interrupted due to un-downloaded pieces.

### 5 SUMMARY

The purpose of this research is to propose a method which is suitable for streaming using P2P while solving the problem of client server system resource overload in the content delivery market. The research has proposed a new method of peer and piece selection in a P2P streaming environment using BitTorrent. The proposed simulations examine the effectiveness of the new methods for improving on the established BiToS and RarestFirst methods. It is the research's sincerest hope that the proposed method alleviates some of the current challenges facing streaming content delivery.

### REFERENCES

- [1] Cisco®, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update 2011–2016, (2012).
- [2] BitTorrent Inc., BitTorrent, <http://www.bittorrent.com>
- [3] A. Vlavianos, M. Iliofotou, and M. Faloutsos, BiToS: Enhancing Bittorrent for Supporting Streaming Applications, Proc. Conf. 25th IEEE Computer and Communications Societies, pp.1–6, (2006).

# Examining the effectiveness of using GPS information to enhance the prediction model of Japanese-language input systems for mobile phones

Ken Tarusawa\* Jun Sawamoto\*\* Eiji Sugino\*\* Norihisa Segawa\*\*

\*Graduate School of Software and Information Science, Iwate Prefectural University, Japan  
g231j026@s.iwate-pu.ac.jp

\*\*Faculty of Software and Information Science, Iwate Prefectural University, Japan  
{sawamoto, sugino, sega}@iwate-pu.ac.jp

**Abstract** –Adding location based Japanese language input prediction to android.

**Keywords:** Android, location information, input prediction, mobile phone, language input.

## 1 INTRODUCTION

Mobile phones are now very familiar for us. Usage expands every year. The use of e-mail function became very popular, outstripping the call function on the present mobile phones.[1] And Japanese text input function became a critical factor.

In this paper, the character input is sped up by strengthening the predictive accuracy of input. Research has been done recently that changes the prediction candidate according to the situation. There is an existing system that generates the prediction candidate from position information.[2][3] However, it is not so widespread because it is very time-consuming to make a dictionary. Moreover, the possibility of a "Character related to the place" that is the "Character that the user wants to input" is low.

The purpose of this research is to display that a character frequently input in the present place is a highly ranked prediction candidate, and that input efficiency improves. In our research, the character with the highest frequency input in the present place in the past is displayed to the prediction candidate. Moreover, the amount of read data is kept to the minimum.

## 2 SYSTEM CONFIGURATION

Japanese is a language that needs many characters compared with other languages. For example, there are 83 hiragana and 86 katakana along are used. First of all, if the user wants to input a Chinese character, katakana is input and the user pushes the conversion button. Then, words are displayed in order of probability that the user will choose it in the conversion candidate field. Prediction candidates are displayed early if the system has a smart algorithm. However, when the algorithm is bad, the user's word is not displayed on the screen.

This research is to display the character that the user wants to input with high probability. This research is composed of two systems. One is the Japanese-language input system "CocoIME" on the Android platform. The other one is the dictionary automatic generation system "KNDS" on the server.

### 2.1 The character input system and the dictionary automatic generation system

CocoIME adds the function that the prediction conversion candidates are displayed according to the present place in the standard Japanese-language input system. When the user inputs the character with CocoIME, "Position information" and "Input word" are output as a log. Logs are regularly uploaded to KNDS which examines whether there are relations in "Position information" and "Input word". The dictionary is automatically generated as a result. CocoIME regularly downloads new dictionaries.

### 2.2 Relation of position information and words

First, we draw lines on the earth by the spacing of latitude and longitude at 0.0005 degrees, we call this work "Gridding". From this grid, we make trapezoid shapes which we call pieces. Our system can make dictionaries up to the number of pieces stored in the mobile phone.

Next, we explain the flow that registers words to dictionaries. The system gets latitude and the longitude at the present place using GPS. The user inputs the character string, and the input character is saved. At this time, the system preserves the position information and input character string as a log, which is regularly uploaded to the KNDS server.

The default update timing is one minute. The reason this initial value was set is that it was thought that this value fit best according to the "Speed a man walks" and the "Specifications of this system". The speed on foot is 4.8 kilometers per hour according to a government survey. The distance between two pieces is about 55 meters. The time necessary for this movement and for the mobile phone to be taken out, and time until the mail screen is opened, it is about one minute.

### 2.3 Decision of priority

When a character is input, CocoIME finds the present place using GPS, and looks at dictionaries of nearby pieces. When the dictionary on KNDS is newer, CocoIME acquires the newer dictionary. As a result, CocoIME can read pieces' dictionaries within about a 1.1 kilometer radius of the device at any time.

When the user inputs a character, the system uses the dictionary in the device. The system regularly measures the present place, and reads pieces' dictionaries corresponding to the present place and radius. In this thesis, the system only reads 13 pieces. Words and the frequency values (the value of how frequently a word is input) are registered in dictionaries. The system displays the prediction candidate words with a ratio of 1.0 or more between the frequency value and a constant. The constant decreases for pieces further from the user. Figure 2.1 shows the priority and the constant value of the piece.

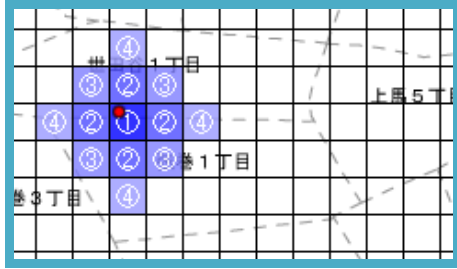


Figure 2.1 Priority in Gridding and Prediction

## 2.4 Dictionary automatic generation

KNDS makes new dictionaries from logs of CocoIME automatically. When the dictionary is made, it uses words that a lot of users input. As a result, CocoIME can display words that other people input in prediction candidate. In this thesis, because it is an experiment only on CocoIME, a detailed explanation of KNDS is omitted.

## 3 EXPERIMENT

### 3.1 Experiment method

This study used only one device.  
The experimental conditions are as follows.

- The subject inputs Japanese E-mail of about 50 characters of mixed writing of kanji and kana.
- The subject inputs 50 mails on a trip, and 50 mails from home.
- The subject inputs 100 E-mails without using the function to display the word prediction from position information. Afterwards, the test was repeated with a position information on.
- The input method is to cycle through Japanese syllables until the correct character is selected.

During both test a count of the number of key strokes was kept with both the position information off and on to find which was more efficient.

### 3.2 Experimental result

Table 3.1 shows the result of the experiment. We found that predicting words by using position information was the

most efficient. However, input efficiency did not improve in all mail, and decreased in some.

Table 3.1 Comparison of Numbers of Key Strokes

		Home mails	Travel mails	All mails
Average(times)	Position information off	133.7	138.7	136.2
	Position information on	123.2	122.0	122.6
Standard deviation	Position information off	13.50	16.49	15.20
	Position information on	21.24	27.97	24.72

## 3.3 Experimental result

It was expected that this system would be effective when a word that is related to the place was input. Travel mails correspond to it. Similarly, it was expected that it would have the opposite result with home mails. However, the system was found to be effective with both travel mail and home mail. It is thought that the reason it is less effective for home mail is the content of the home mail. It is expected that as the contents of mail becomes varied, and the amount of time the subject spends at home increases, the efficiency of prediction will decrease.

The number of key strokes has been decreased greatly for travel mails. The reason is because there are a lot of proper nouns.

Words predicted by the proposed technique are usually more likely to be what the user wants.

## 4 SUMMARY

With many users it is thought that input efficiency can be improved greatly.

It is predicted that input efficiency will improve further if the position information function can be turned on and off according to the situation.

Also, there is a problem with inconstant sizes of pieces made from gridding. To improve this problem, the authors should change how to delimit the longitude in proportion to latitude.

The authors will aim at a further improvement of input efficiency by advancing the improvement of CocoIME at the same time as conducting the experiment that introduces KNDS in the future.

## REFERENCES

- [1] iSHARE co. (2009, 12 22). *Report of the research on the most frequently used functions on the mobile phone*. Retrieved from <http://release.center.jp/2009/12/2201.html>
- [2] Tsuchida, M. (2007, 3 15). *Patent No. 2007-65906*. Japan.
- [3] ArakawaYutaka, SuematsuShinji, DendoShigeaki, FukudaAkira. (2011). *Dynamic Cictionary Genaeration Method for Contextaware Input Methdo Editor*. IPSJ Journal Vol.52 No.3.

# Optimization and Instrumentation

Measuring machine impact on program implementation

Daniel McDermott  
Eastern Washington University  
September 5, 2012

## Outline

- 1 Motivation
- 2 Background / refresher
- 3 Naive Matrix Multiplication
- 4 Measuring programs
- 5 Optimizing Matrix Multiplication
- 6 Selected topics

## Outline

- 1 Motivation
- 2 Background / refresher
- 3 Naive Matrix Multiplication
- 4 Measuring programs
- 5 Optimizing Matrix Multiplication
- 6 Selected topics

## Something to read

### *What Every Programmer Should Know About Memory*

A fairly comprehensive paper about CPU, memory, and cache written by Ulrich Drepper, lead maintainer of Gnu C, in 2007. Available for free online.

This talk is largely inspired by, and borrows a lot from, his work.

This talk will be geared towards applications in C for Linux on modern commodity x86 hardware.

## Motivation

Modern hardware is complex and rapidly changing. Many programmers do not have a clear view of what is occurring within the machine.

**“...the limiting factor for most programs is now, and will be for some time, memory access”**  
– Ulrich Drepper, 2007

Understanding the machine, and how to measure performance accurately, is critical to designing systems software, real time systems, and massive computing applications.

## Two quotes

Albert Einstein

“In theory, theory and practice are the same.  
In practice, they are not.”

Donald Knuth

“In established engineering disciplines a 12% improvement, easily obtained, is never considered marginal and I believe the same viewpoint should prevail in software engineering.”

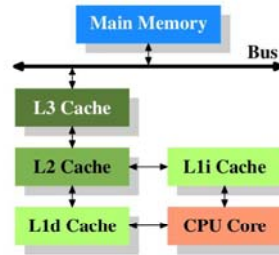
## Outline

- 1 Motivation
- 2 Background / refresher
- 3 Naive Matrix Multiplication
- 4 Measuring programs
- 5 Optimizing Matrix Multiplication
- 6 Selected topics

## Refresher

### A quick refresher:

- Register, cache, memory hierarchy

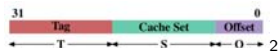


- Recall that there is *virtual* memory and *physical* memory.
- Harvard vs. Von Neumann architecture (L1 vs. L1d+L1i)

<sup>1</sup>borrowed from Drepper, 2007

## Refresher (cont.)

- Cache associativity (fully vs. set, direct map)



$O = \log_2$  cache line size,  $S = \log_2$  number of sets

A cache is divided into sets, each set has a number of lines called its *associativity*, each line has a size (in bytes). Thus the size of the cache will be line size  $\times$  associativity  $\times$  number of sets.

- Write caching policy (writeback vs. writethrough), write combining

In some intuitive sense, a set associative cache behaves like a hash table with limited chain length. When chains (sets) are full, entries are evicted.

<sup>2</sup>borrowed from Drepper, 2007

## Costs

### Hit/Miss costs Pentium M <sup>2</sup>

To where	Cycles
Register	$\leq 1$
L1 data	$\approx 3$
L2	$\approx 14$
Main Memory	$\approx 240$

**Keep in mind:** "Accessing memory is not an arbitrarily fast process." It can be influenced and even controlled through careful use of built-in functions and macros, thoughtful program flow, and data layout.

## Outline

- 1 Motivation
- 2 Background / refresher
- 3 Naive Matrix Multiplication
- 4 Measuring programs
- 5 Optimizing Matrix Multiplication
- 6 Selected topics

## Recall matrix multiplication

The  $ij$ th element of the product of two  $N \times N$  matrices  $A$  and  $B$  is:

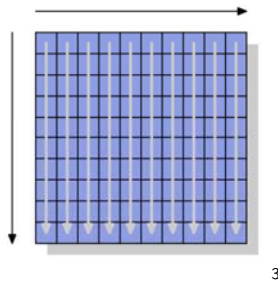
$$(AB)_{ij} = \sum_{k=0}^{N-1} a_{i0}b_{0j} + a_{i1}b_{1j} + \dots + a_{i(N-1)}b_{(N-1)j}$$

When implemented straightforward, the time complexity is  $O(N^3)$ . There are other algorithms with slightly better time costs, but for another talk.



## Matrix multiplication, naive access

```
for (i = 0; i < N; ++i)
  for (j = 0; j < N; ++j)
    for (k = 0; k < N; ++k)
      res[i][j] += mul1[i][k] * mul2[k][j];
```



<sup>3</sup>borrowed from Drepper, 2007

Daniel McDermott (EWU)

Optimization and Instrumentation

September 5, 2012

13 / 32

## Why is this bad anyways?

- 1 In sequentially accessed memory, the processor automatically prefetches data into the cache.
- 2 Memory design / timing. Example: **5 - 5 - 5 - 15**
  - CAS - Column Access Strobe aka Column Latency, how long it takes to access a column.
  - $T_{RCD}$  - Row to Column Delay, time between opening a row and addressing a column.
  - $T_{RP}$  - Row to Row Precharge delay, the minimum time before opening a **new** row after opening a row.
  - $T_{RAS}$  - Row Activate Time, how long it takes to open a new row.

**It takes a long time to select new rows in memory**

Daniel McDermott (EWU)

Optimization and Instrumentation

September 5, 2012

14 / 32

## First attempt

Get rid of random access. Notice that `mul2` is accessed many times in the innermost loop. It's possible that finding some re-arrangement of `mul2` may improve performance?

**Transpose of a matrix:** The  $i$ th row,  $j$ th column element of  $A^T$  is the  $j$ th row  $i$ th column of  $A$ .

$$[A^T]_{ij} = [A]_{ji}$$

**Notice:**

$$(AB)_{ij} = \sum_{k=0}^{N-1} a_{i0}b_{0j} + a_{i1}b_{1j} + \dots + a_{i(N-1)}b_{(N-1)j}$$
$$(AB)_{ij} = \sum_{k=0}^{N-1} a_{i0}b_{j0}^T + a_{i1}b_{j1}^T + \dots + a_{i(N-1)}b_{j(N-1)}^T$$

Daniel McDermott (EWU)

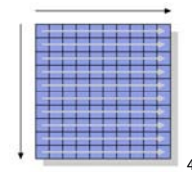
Optimization and Instrumentation

September 5, 2012

15 / 32

## New implementation

```
double temp[N][N];
for (i = 0; i < N; ++i)
  for (j = 0; j < N; ++j)
    temp[i][j] = mul2[j][i];
for (i = 0; i < N; ++i)
  for (j = 0; j < N; ++j)
    for (k = 0; k < N; ++k)
      res[i][j] += mul1[i][k] * temp[j][k];
```



<sup>4</sup>borrowed from Drepper, 2007

Daniel McDermott (EWU)

Optimization and Instrumentation

September 5, 2012

16 / 32

## Outline

- 1 Motivation
- 2 Background / refresher
- 3 Naive Matrix Multiplication
- 4 Measuring programs
- 5 Optimizing Matrix Multiplication
- 6 Selected topics

Daniel McDermott (EWU)

Optimization and Instrumentation

September 5, 2012

17 / 32

## Introduction to Linux `perf`

Perf is a powerful subsystem in the Linux kernel available for profiling and gathering performance statistics. It is implemented via CPU model-specific performance measurement units (PMUs).

The `perf` command is available as part of the **linux-tools** package on most Linux distributions.

`perf` has a "git-like" invocation, i.e.

`perf <subcommand> [options] <arguments>`

Daniel McDermott (EWU)

Optimization and Instrumentation

September 5, 2012

18 / 32

## Try it out

Lets compare sequential and random access matrix multiplication

## Outline

- 1 Motivation
- 2 Background / refresher
- 3 Naive Matrix Multiplication
- 4 Measuring programs
- 5 Optimizing Matrix Multiplication
- 6 Selected topics

## Problem

Lets revisit the original **problem**: `mu12[k][j]` and `mu12[k][j+1]` are in the same cache line, however by the time `j` is incremented in the middle loop, this line has already been evicted from L1d by loads in the inner loop.

Note that the order in which additions are performed in computing **each element** of the resulting matrix is **not important**.

**Basic idea**: We will solve sub sections of the problem which are more local in L1d by using the above property, along with some tricks.

## Cache aligning and loop unrolling

**Specifically**: we will handle two iterations of the middle loop together so that we can access `mu12[k][j]` and `mu12[k][j+1]` with good locality.

This will halve the number of L1d cache misses and decrease the number of main memory row selections that may need to be performed.

**Let's look at the code**

## Prefetching

By default, the processor uses complex algorithms to try to figure out where data will probably be coming from next.

We can give it hints using `emmintrin.h`

**Specifically**: `_mm_prefetch(void*, hint_level)`

There are 4 hint levels:

- `_MM_HINT_T0` pre-fetch into all cache levels
- `_MM_HINT_T1` pre-fetch into L2 only
- `_MM_HINT_T2` pre-fetch into L3 only (if one exists)
- `_MM_HINT_NTA` Non Temporal Aligned - put this into L1d only **and** do *not* push to a higher level when evicted, push directly to main mem.

## Vectorized Load and Store

Intel SSE instructions. SSE = "Streaming SIMD"

SMID = "Single Instruction Multiple Data" operations.

Many modern processors support processing of 2, 4, 8, or even more values at a time. These are usually called *vectorized* operations.

Intel processors have SSE2 instructions that can handle two doubles in one operation.

The functions which expose these operations are also in `emmintrin.h`



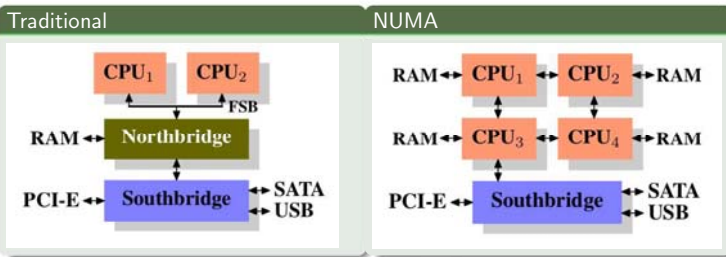
## Lets look again

A quick demo of all four: naive, transposed, sub-matrix cache aligned, and fully optimized matrix multiplication

## Outline

- 1 Motivation
- 2 Background / refresher
- 3 Naive Matrix Multiplication
- 4 Measuring programs
- 5 Optimizing Matrix Multiplication
- 6 Selected topics

## Non-uniform Memory Architecture



- Memory is not uniformly accessible from all CPUs anymore. Thread affinity and scheduling plays a role, but also virtual memory "allocation strategy" across CPUs.
- Default strategy is to stripe allocation across all processors, that way a thread can be migrated freely.
- This can be controlled or overridden with libNUMA, a C library available for Linux.

## Critical word load

Memory access is **"bursty"**.

Memory typically transfers data to the cache 64bits at a time, while modern caches have a line size of 64 or 128bytes. This means it can take 8 or 16 transfers to fill a cache line.

Each transfer usually takes about 4 cycles.

If the data you want is somewhere near the end of the line, it can take a long time before it arrives.

However, data can be used the moment it *does* arrive...

**Solution:** Create structures with the most frequently used members at the beginning. Access elements in the order in which they were defined, whenever possible.

## Instruction Cache

Optimizing instruction cache (L1i) is generally easier because instruction data is generated by compilers, and compiler writers know what they're doing.

Help your compiler by:

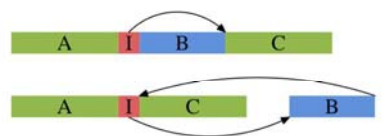
- Making the code footprint as small as possible.
- Making code execution as linear as you can (reduces "bubbles").
- Aligning code using compiler options (see Drepper pp. 57-58)
- Help it help the Branch Predictor

## Inlining and Branch Prediction

Inlining functions can cause code duplication, which makes code larger. However, it can also help the branch prediction unit make better decisions.

- `inline void foo();`
- `void foo() __attribute__((always_inline));`
- `__builtin_expect(long EXP, long C);`

These three work together to create this effect, where *C* is the more likely to be executed code block, and *B* is less often executed.



<sup>5</sup>borrowed from Drepper, 2007

## How to query the architecture information

- SysFS: A virtual file system provided by Linux which exports various system information.
  - `/sys/devices/system/cpu/cpu*/index*` Cache meta information, like type, level, and which CPUs share the cache.
  - `/sys/devices/system/cpu/cpu*/topology` The topology for NUMA, which CPU's are core siblings and thread siblings.
  - See pp. 44-45 of Drepper for details on how to read this information.
- `/proc/cpuinfo` contains CPU capabilities.
- `getconf -a` is a command which lists a variety of system configuration variables and their values. Among them will be cache sizes, line sizes, and associativities.
- `sysconf()` is a C function from `unistd.h`. It does roughly the same thing as `getconf`, except for C programs during runtime.

## Further Resources

- *What Every Programmer Should Know About Memory* by Ulrich Drepper, 2007, Red Hat Inc.  
[www.akkadia.org/drepper/cpumemory.pdf](http://www.akkadia.org/drepper/cpumemory.pdf)
- Linux manpages for `perf_3.2`
- Oprofile, an alternative to `perf`.
- Google `perf-tools`, another alternative (more for C++ applications profiling).
- `valgrind` with `massif` and `callgrind` - memory usage profiling tools.

### Questions?

These slides were made using the L<sup>A</sup>T<sub>E</sub>X beamer package and Vi Improved.

Geancarlo Palavicini Jr,  
OSCP/CCSE/MCSE  
9/6/2012

## Malware Hooking

### Overview

- Define Hooks
- Define Malware Hooking
- Systems Background
- IAT/EAT Hooks
- IDT/MSR Hooks
- SSDT Hooks
- Inline API Hooks
- IRP Hooks
- Defenses

### Hooks

- A hook is a point in the system message-handling mechanism where an application can install a subroutine to monitor/process the message traffic in the system before they reach their target procedure. (MSDN)

### “Legitimate” Hooking

- Debuggers
- System Monitoring
- Computer-Based Training Applications
- Malware Analysis
- Extend Functionality
  - A/V Applications
  - Firewalls

### Malware Hooking

- A technique that replaces a legitimate system call's function pointer from a system call table with a malicious routine's address, with the intent to hijack the execution flow into a malicious routine.

### General Idea

- Identify a call table
- Save an existing entry in the table
- Swap in a new address to replace the existing entry
- Restore the old entry when you're done

## Hooking Rewards

- Block calls made by certain applications (a/v, anti-spyware)
- Alter or replace the original routine
- Monitor the system by intercepting input parameters
- Filter output parameters (deceive other system components)
- Steal CPU cycles and then call the original routine

## Background

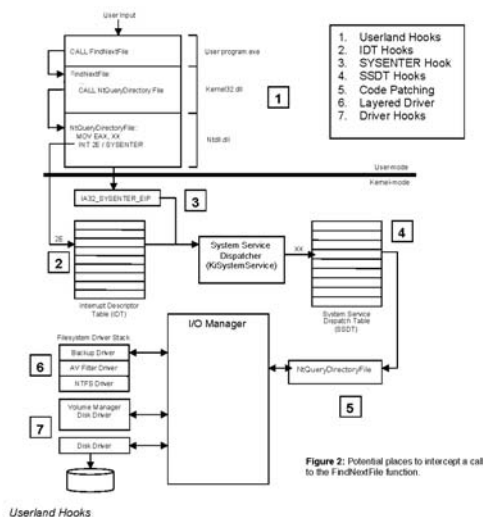
- Windows architecture has a layered design.
- 2 Ring architecture for memory protection
  - User-Mode (Ring 3)
  - Kernel-Mode (Ring 0)
- Windows Loader uses Portable Executable (PE) images on disk to load binaries into memory

## DLL Layering

- Layering is implemented through subsystem Dynamic Linked Libraries.
  - These libraries "export" the documented interface to a particular subsystem.
  - Expose subset of executive services
  - Applications do not call system services directly, but go through one or more subsystem DLLs.

## Driver Layering

- Drivers Stacked
  - Provide flexibility
  - Extend functionality
- Drivers are implemented in Ring 0.
  - Device drivers are kernel-mode modules
  - only way to add user-written kernel-mode code to the system



## Portable Executables

Binary images that are fed to the Windows loader for insertion into memory.

- 3 types of PEs:
- EXE (Applications)
  - DLL (Subsystem)
  - SYS (Device Drivers)

## IAT

### ■ Import Address Table

- Data structure that exists in PE images used by the loader for library linking
- Stores the addresses of the library routines that an application imports from the system DLLs.

## EAT

### ■ Export Address Table

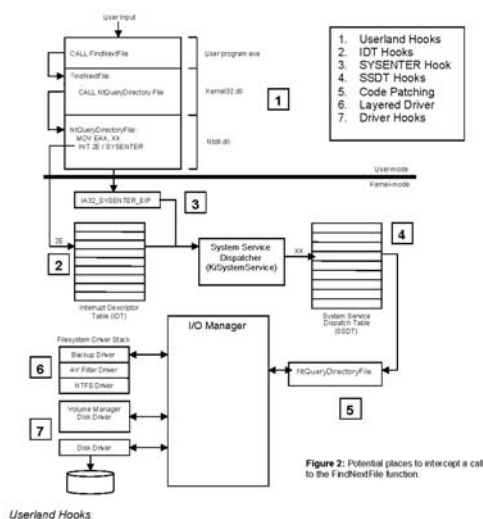
- Data structure in exportable DLL's PE
- Stores the names of the functions exported by a particular DLL, and the Relative Virtual Address (offset within the DLL where the function can be found)
- The RVA is relative to the base address of the DLL when it is loaded into memory

## IAT/EAT Hooking

- Injects a DLL into the target process
- Injected DLL parses through the PE's header looking for:
  - IAT/EAT data structure
  - Pointer for the desired function to hook.

## IAT/EAT Hooks

- Once it finds the location of the pointer:
  - overwrites it with a pointer to an attacker supplied function
- IAT - Forces the process to call malicious code, instead of the legitimate API.
- EAT – Hijacks the flow of execution to malicious DLL on legitimate API calls.



## IDT Hooks

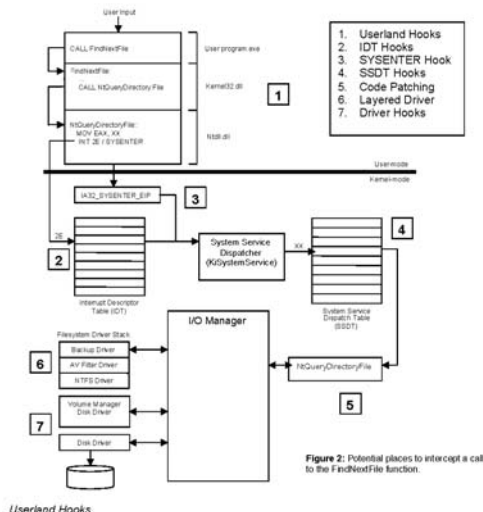
- Interrupts
  - User/Kernel Gateway
  - Interrupt 2E instruction causes the processor to transfer the flow of execution into the routine pointed to by the 0x2E slot of the IDT.
- Overwrite 0x2E entry in IDT
  - Intercepts every call across user-kernel boundary

## MSR

- Machine Specific Registers.
  - IA32\_SYSENTER\_CS
  - IA32\_SYSENTER\_EIP
  - IA32\_SYSENTER\_ESP
- Do Not reside in memory.
- Registers are loaded once a process invokes the SYSENTER instruction
  - Which handles the jump between user-mode and kernel-mode (much like 2E in older systems)

## MSR Hooking

- Read MSR EIP address
- This call `nt!FastCallEntry`, this is the code we replace with our hook
  - Place address of our code in the MSR\_EIP register
- MSR can only be modified from within the kernel-space.
  - Remember that Device Drivers are kernel-mode modules
  - stackable



## SSDT

- System Service Dispatch Table stores pointers to a system service rather than to an interrupt handling routine.
- System service refers to native functions in the Windows OS that are callable from user mode

## SSDT Hooks

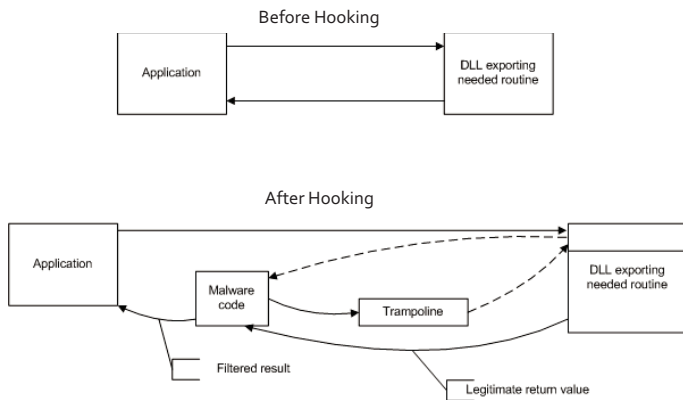
- In order to intercept every call to a particular system service, simply replace the table entry for the system service with the address of the malicious code.
- After executing the malicious code, we can call the original system service and modify the returned data or skip calling the legitimate service and return bogus data.

## Inline Hooking (patching)

- Trampoline or detours
- Does not overwrite any pointers
- Disassembles routine's instructions, and write to the process in memory
- Injects a JMP instruction in the prologue (1<sup>st</sup> 5 bytes of a function call) of legitimate function to force process into an attacker supplied malicious DLL.

## Inline Hooking

- Rogue DLL calls “trampoline” function
- Trampoline calls the original function
- On completion of legitimate function, it returns to the detour function (caller) to alter results.
- Every time the hooked function is called, the calling process will be forced to execute the malicious code



## IRP

- I/O Request Packet
  - Data structure created by I/O system to store information it needs to process an I/O request
  - It includes a code to identify the desired operation (read, write, create), and buffers for any data to be read or written by the driver.
- Applications in Windows communicate with drivers by sending IRP packets.
- Each driver maintains an IRP function table or major function table.

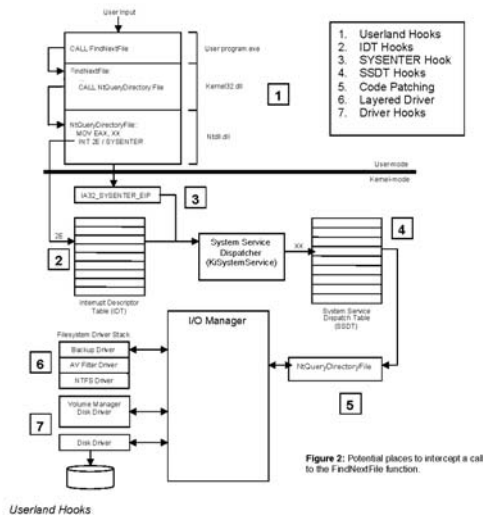


Figure 2: Potential places to intercept a call to the FindNextFile function.

## IRP Hooking

- Modifies entries in a driver's IRP function table, pointing them to malicious code, generally residing outside of the driver's memory segment.
- Ex. By hooking the IRP\_MJ\_WRITE function in a driver's IRP table, one can inspect a buffer before it is written to disk or across the network.

## Defenses

- Inspect call tables
  - Verify function point inside DLL's address space
- Disassemble first instructions of function looking for JMP or CALL instructions
- Inspect IRP major function pointer
  - Verify they point inside DLL's address space

## Discussion

## References

### Books

- Practical Malware Analysis
- Malware Analyst's Cookbook and DVD
- The Rootkit Arsenal 1<sup>st</sup> & 2<sup>nd</sup> Edition
- The Shellcoders Handbook 2<sup>nd</sup> Edition
- Windows Internals 5<sup>th</sup> Edition

### Papers

- An Online Cross View Difference and Behavior based Rootkit Detector
- Inside Windows Rootkits
- A Comparative Analysis of Rootkit Detection Techniques
- API\_Hooking\_Revealed
- Rootkit attacks and protection: a case study of teaching network security
- Windows Rootkits: Attacks and Countermeasures

### Web

- <http://msdn.microsoft.com>