

Delivery and Management Systems for Digital Contents and Their Security Verification

Project Leader	Toru Fujiwara	Graduate School of Information Science and Technology Osaka University
Investigator	Yasunori Ishihara	Graduate School of Information Science and Technology Osaka University
	Maki Yoshida	Graduate School of Information Science and Technology Osaka University

Abstract

Delivery and management systems for digital contents and their security verification are studied. In this report, we present the outlines of some of our results on an interactive drama delivery system and the security problem against inference attacks on object-oriented databases.

1 Introduction

This year, we have studied several problems on delivery and management systems for digital contents and their security verification. For the delivery and management systems, we have proposed an interactive drama delivery system for environments including mobile phone, where an intermediary exists. We have also proposed a digital contents consignment system protecting marketing information. For the security verification, we consider the security problem against inference attacks on object-oriented databases, and have obtained results on the decidability. We have also proposed a formal method for finding the lowest cost attack on cryptographic protocols.

In this report, we present the outlines of some of our results on the interactive drama delivery system and the security problem against inference attacks on object-oriented databases.

2 An Interactive Drama Delivery System Suitable for Mobile Phone

2.1 Interactive drama delivery problem

Mobile Internet services have become popular lately. Because of a narrow communication channel and the poor memory of a mobile phone, a contents provider (e.g., a web site) often divides contents into several component contents to deliver to a mobile phone user. For some contents, e.g., an interactive drama, the order of the delivered component contents is important. When delivering an interactive drama, a contents provider prefers that the order of delivered component contents follow one of the several possible story plots. We show an example of an interactive drama in Fig. 1. This drama has three plots, $1 \rightarrow 2 \rightarrow 4$, $1 \rightarrow 2 \rightarrow 5$ and $1 \rightarrow 3 \rightarrow 5$. Therefore, any user who viewed component contents 1 and 2, can view one of the component contents 4 and 5, however cannot view component content 3. If the user desires to view component content 3, then the user must view component content 1 again.

Delivery control for an interactive drama is focused in [1, 2], but the protection of users' privacy is not considered. User concerns over privacy have become stronger lately. Thus a delivery system needs to prevent even contents providers and mobile phone carriers from identifying the history of choices made by the user because a contents provider can prepare an interactive drama such that the history is indicative of some character of the user. For the interactive drama shown in Fig 1, there is a possibility that the contents provider will regard the user who selects $1 \rightarrow 2 \rightarrow 4$ as easy mark because the hero (i.e., the

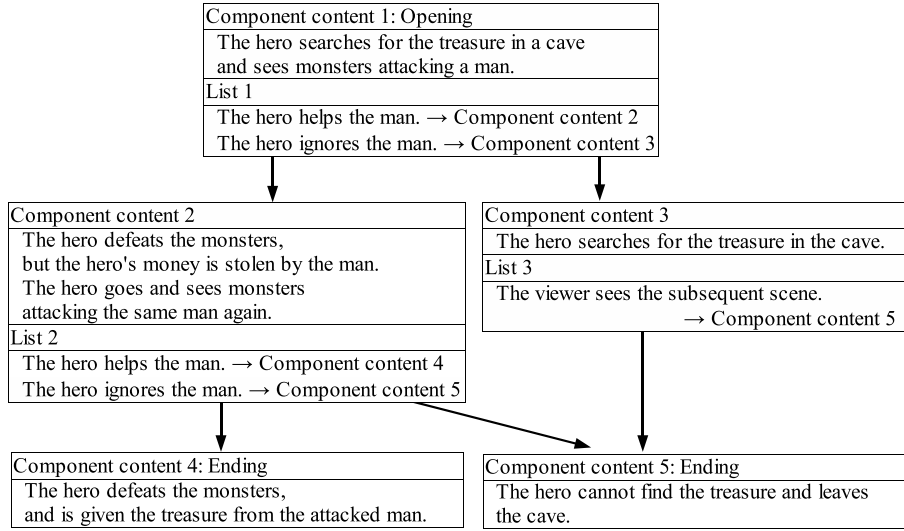


Figure 1: An example of an interactive drama.

user) helped the same man again despite the fact that the hero had had his money stolen by the man before.

In the communications infrastructure, a mobile phone carrier is involved as an intermediary. A mobile phone carrier relays data between contents providers and mobile phone users, charges each mobile phone user for component contents delivered through the carrier, and pays revenue to each contents provider. Therefore, a mobile phone carrier and a contents provider need to prove the accuracy of prices charged for delivered component contents. The type of charges structure we assume for an interactive drama is the pay-per-scene charges. In pay-per-scene charges, each component of the content is priced separately and each mobile phone user is charged the total price of component contents delivered to him or her. We propose a delivery system which satisfies the security requirements (the secrecy of the user's history of choices and the accuracy of charges) while enabling a contents provider to control delivery.

2.2 Main results

For an interactive drama, we have defined a plot graph PG , which represents all the possible plots, as a labeled directed graph (N, L, E) , where

- $N = \{c_1, \dots, c_n\}$ is the set of component contents, where c_i with $1 \leq i \leq n$ is a component content numbered i and c_1 is the *opening component content*;
- $L = \{a_1, \dots, a_l\}$ is the set of choices, where a_j with $1 \leq j \leq l$ is the choice numbered j ;
- $E \subseteq N \times N \times L$, and $(c_i, c_j, a_k) \in E$ if and only if a_k is assigned to a component content c_i and c_j is the next component contents of c_i when the choice a_k is made by a viewer.

The opening component content is the component content viewed first. Some component contents are assigned one or more choices, and others are assigned no choice. If choices are assigned, for each choice, it is decided which component content is delivered next. If no choice is assigned, there is no next component content. We call a component content assigned no choice an *ending component content*. A sequence of component contents on each path from the opening component content to some ending component content corresponds to one of the possible plots.

We have proposed a delivery system which satisfies the following requirements on the assumptions that the used cryptographic schemes are secure.

Requirement 1 (the accuracy of delivery control): For any coalition \mathcal{C} of viewers, after every delivery to any viewer in \mathcal{C} , if \mathcal{C} has been delivered the opening component content c_1 k times with $k \geq 1$,

there are k paths of PG from c_1 to some component contents, where the set of component contents on the k paths is equal to the set of component contents obtained by \mathcal{C} .

Requirement 2 (the accuracy of charges): For each delivery via an intermediary \mathcal{I} , \mathcal{I} can know the price of the component content delivered to the viewer \mathcal{V} , and can obtain the necessary evidence that \mathcal{V} agrees on the price. The contents provider \mathcal{P} can know the price of component content delivered to \mathcal{V} , and can obtain the evidence that \mathcal{I} agrees on the prices \mathcal{V} will pay.

Requirement 3 (the secrecy of choices against an intermediary): An intermediary \mathcal{I} cannot know which component contents and choices are sent through \mathcal{I} except the following trivial cases. (Case 1) Only one component content exists. (Case 2) \mathcal{I} knows a price p_i of a component content c_i and no component content other than c_i is priced at p_i .

Requirement 4 (the secrecy of choices against a contents provider): For every pair of choices sent to a contents provider \mathcal{P} , \mathcal{P} cannot decide whether the choices are made by the same viewer except the following trivial cases. (Case 1) Only one viewer exists. (Case 2) \mathcal{P} colludes with all viewers except for the target viewer. (Case 3) Two choices are assigned to two component contents that are included in the same path on which component contents are delivered to only one viewer.

Notes on the definitions of the requirements:

Generally, a contents provider \mathcal{P} tries to deliver component contents so that any viewer \mathcal{V} obtains a set of component contents on k paths of PG from the opening component content c_1 to some component contents if c_1 is delivered k times to \mathcal{V} . Some viewer colludes with other viewers to obtain such a set of component contents that there is no set of paths to obtain the set of the component contents, e.g., to obtain all ending component contents by obtaining c_1 only once. By satisfying Requirement 1, a collusion of viewers has no advantage.

Even if a contents provider \mathcal{P} shows a lower price than the actual price, only \mathcal{P} loses. Hence, such case is unlikely. The same is true for an intermediary. Therefore, it is sufficient to satisfy Requirement 2 to guarantee the accuracy of charges.

It is known that the history of each viewer's choices forms a set of paths from the opening component content in the plot graph. Moreover, if the prices of some component contents are known, then it is known from the price of a delivered component content that the component content is one of the component contents which have the same price. Therefore, Requirements 3 and 4 prevent a contents provider and an intermediary from obtaining any additional information. These definitions are defined considering the infrastructure.

3 Type Inferability and Decidability of the Security Problem against Inference Attacks on Object-Oriented Databases

3.1 Security problem against inference attacks on object-oriented databases

In recent years, various authorization models for object-oriented databases (OODBs) have been proposed and studied. Among them, the method-based authorization model [3, 4] is one of the most elegant models since it is in harmony with the concept that “an object can be accessed only via its methods” in the object-oriented paradigm. In the model, an authorization A for a user u can be represented as a set of rights $m(c_1, \dots, c_n)$, which means that u can *directly* invoke method m on any tuple (o_1, \dots, o_n) of objects such that o_i is an object of class c_i with $1 \leq i \leq n$. On the other hand, even if $m(c_1, \dots, c_n) \notin A$, u can invoke m *indirectly* through another method execution in several models, e.g., protection mode in [5]. Although such indirect invocations are useful for data hiding [5], they may also allow *inference attacks* in some situations.

Example 1 Consider the following database schema: *Employee*, *Host*, and *Room* are classes representing employees, hosts, and rooms, respectively. Method *computer* returns the host which a given employee uses, method *location* returns the room in which a given host is placed, and method *office*, which returns the room occupied by a given employee, is implemented as $office(x) = location(computer(x))$.

Now suppose that the physical computer network is top secret information. In this case, an authorization for a user u may be the one shown in Figure 2, where a solid (resp. dotted) arrow denotes an

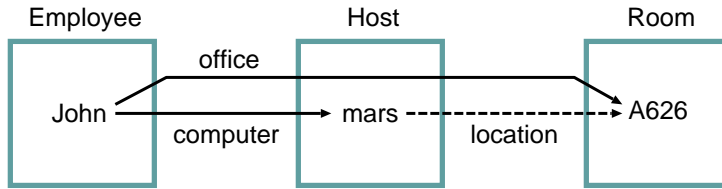


Figure 2: An example of an inference attack.

authorized (resp. unauthorized) method to u . Assume that u has obtained that $\text{computer}(\text{John}) = \text{mars}$ and $\text{office}(\text{John}) = \text{A626}$ using the authorized methods. Also assume that u knows the implementation body of office as its behavioral specification. Then, u can infer that $\text{location}(\text{mars}) = \text{A626}$, although executing $\text{location}(\text{mars})$ is prohibited.

The *security problem* is to determine whether the execution result of a given method (or, more generally, query) can be inferred under some database instance of a given database schema S and a given authorization A . In the above example, query $\text{location}(x)$ is not secure at class `Host` under the schema and the authorization. In [6], the security problem is formally defined under a model of OODBs (called *method schemas* [7, 8]) with the following limitations:

- The returned value of a method execution is a single object.
- All the information available to the user is
 - the execution results of authorized methods, and
 - the implementation bodies of authorized methods.
- User’s inference is based on equational logic using the above information.

In [6], the security problem is shown to be decidable for a subclass of method schemas called monadic schemas. In the decision algorithm, the technique of type inference is used, where type inference means deriving the classes to which the possible results of the method execution belong. Type inference is possible for monadic schemas, and the user’s inference is exactly simulated using the result of type inference. It has also been shown that for general schemas, the security problem is undecidable [6] and type inference is impossible [8]. It has shown some results on the decidability of the security of negative information, which are similar to that of positive information. However, the relationship between the type inferability and the decidability of the security problem has not been addressed so far.

3.2 Main results

This year, we have clarified the relationship between type inferability and decidability of the security problem (see also Table 1). We have focused on the linearity of queries, which is a popular notion of the field of term rewriting. A query (i.e., a term with variables) q is *linear* if no variable in q appears more than once. A schema S is *linear* if all the implementation bodies of the methods in S are linear. Clearly, monadic schemas are linear. We have shown that type inference is possible for linear queries under linear schemas, but impossible for non-linear queries even if the queries are security-decidable (Table 1(a)). Also, we have shown that the security is decidable for linear queries under linear schemas, but undecidable for non-linear queries even if the queries are type-inferable (Table 1(b)). These results imply that type inferability and decidability of the security problem are incomparable.

We discuss “logical” inference in OODBs in the sense that the result of the inference is always true. The inference in statistical databases [10] is a kind of logical inference. Ref. [11] focuses on logical inference in OODBs. Besides inferability of the result of a method execution, the article introduces the notion of controllability, which means that a user can control (alter arbitrarily) an attribute-value of an object in a database instance. We do not consider controllability since our query language does not support update operations for database instances. However, since our query language supports recursion while the one

Table 1: This year’s results.

(a) Type inferability.					(b) Decidability of the security problem.				
schemas	queries				schemas	queries			
	unary	linear	security- decidable but non-linear	general		unary	linear	type- inferable but non-linear	general
monadic	Y[8]	–	–	–	monadic	Y[6]	–	–	–
linear	Y	Y	N	N	linear	Y	Y	N	N
general	N[9]	N[9]	N	N[8]	general	N[6]	N[6]	N	N[6]

in [11] does not, detecting inferability in our formalization is not trivial. On the other hand, some of the recent research concentrates on “statistical” inference, i.e., inference with some statistical assumptions. For example, [12] discusses the inference based on Bayesian methods. In [13], a quantitative measure of inference risk is formally defined.

References

- [1] M.T. Kelso, P. Weyhrauch, and J. Bates: “Dramatic presence,” Technical Report CMU-CS-92-195, School of Computer Science, Carnegie Mellon University, 1992.
- [2] M. Mateas: “Interactive drama, art and artificial intelligence,” Technical Report, CMU-CS-02-206, School of Computer Science, Carnegie Mellon University, 2003.
- [3] E.B. Fernandez, M.M. Larronodo-Peritrie, and E. Gudes: “A method-based authorization model for object-oriented databases,” OOPSLA-93 Conference Workshop on Security for Object-Oriented Systems, pp.135–150, 1993.
- [4] H. Seki, Y. Ishihara, and M. Ito: “Authorization analysis of queries in object-oriented databases,” The Fourth International Conference on Deductive and Object-Oriented Databases, LNCS 1013, pp.521–538, 1995.
- [5] E. Bertino and P. Samarati: “Research issues in discretionary authorizations for object bases,” OOPSLA-93 Conference Workshop on Security for Object-Oriented Systems, pp.183–199, 1994.
- [6] Y. Ishihara, T. Morita, and M. Ito: “The security problem against inference attacks on object-oriented databases,” Research Advances in Database and Information Systems Security, Kluwer, pp.303–316, 2000. (A full version can be found at <http://www-infosec.ist.osaka-u.ac.jp/~ishihara/papers/dbsec99.pdf>).
- [7] S. Abiteboul, R. Hull, and V. Vianu: Foundations of Databases, Addison-Wesley, 1995.
- [8] S. Abiteboul, P. Kanellakis, S. Ramaswamy, and E. Waller: “Method schemas,” Journal of Computer and System Sciences, **51**, pp.433–455, 1995.
- [9] Y. Ishihara, S. Shimizu, H. Seki, and M. Ito: “Refinements of complexity results on type consistency for object-oriented databases,” Journal of Computer and System Sciences, **62**, pp.537–564, 2001.
- [10] D.E.R. Denning: Cryptography and Data Security, Addison-Wesley, 1982.
- [11] K. Tajima: “Static detection of security flaws in object-oriented databases,” The 1996 ACM SIGMOD International Conference on Management of Data, pp.341–352, 1996.
- [12] L. Chang and I.S. Moskowitz: “Bayesian methods applied to the database inference problem,” Database Security XII, Kluwer, pp.237–251, 1999.
- [13] K. Zhang: “IRI: A quantitative approach to inference analysis in relational databases,” Database Security XI, pp.279–290, 1998.

Research Results

Publications

- Toru Fujiwara: “Security Verification of Cryptographic Protocols”, IEICE, Handbook of Information Security (Chapter 3, Section 3), Ohmsha, 2004 (in Japanese).
- Shingo Okamura, Maki Yoshida, and Toru Fujiwara: “Unlinkable Delivery System for Interactive Dramas”, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E88-A, No. 1, 2005 (to appear).
- Shingo Okamura, Maki Yoshida, and Toru Fujiwara: “An Interactive Drama Delivering System Suitable for Mobile Phone”, 5th Workshop on Information Security Applications (Pre-Proceedings), pp.391-398, 2004.
- Yasunori Ishihara, Yumi Shimakawa and Toru Fujiwara: “Type Inferability and Decidability of the Security Problem against Inference Attacks on Object-Oriented Databases”, 6th International Conference on Information and Communications Security, pp.145-157, 2004.
- Akira Fujiwara, Shingo Okamura, Maki Yoshida, and Toru Fujiwara: “A Digital Contents Consignment System Protecting Marketing Information”, 2004 International Symposium on Information Theory and Its Applications, pp.468-473, 2004.
- Kunihiro Okamoto, Takayuki Ueno, Maki Yoshida, and Toru Fujiwara: “A Method to Ensure Reliability of a Detection Result for Correlation Based Watermark Detection Schemes”, 2004 International Symposium on Information Theory and Its Applications, pp.299-304, 2004.
- Shingo Okamura, Maki Yoshida and Toru Fujiwara: “Unlinkable Delivery System for Interactive Dramas Including Conditional Choices”, 2004 International Symposium on Information Theory and Its Applications, pp.474-479, 2004.
- Akira Fujiwara, Shingo Okamura, Maki Yoshida, and Toru Fujiwara: “Reducing Frequency of Communication on the Consignment Delivering System Protecting Marketing Information”, IEICE Technical Report, ISEC2004-34, 2004.
- Akira Fujiwara, Shingo Okamura, Maki Yoshida, and Toru Fujiwara: “An Off-line Consignment Delivery System Protecting Marketing Information”, Computer Security Symposium 2004, Volume II, pp.469-474, 2004 (in Japanese).
- Kunihiro Okamoto, Takaaki Fujita, Maki Yoshida, and Toru Fujiwara: “Correlation Based Watermark Detection Ensuring Given False Positive Error Probability for Video Using Inter-Frame Similarity”, Computer Security Symposium 2004, Volume I, pp.163-168, 2004.
- Takane Umayama, Maki Yoshida, and Toru Fujiwara: “A Formal Method for Finding the Lowest Cost Attack on Cryptographic Protocols”, IEICE Technical Report, ISEC2004-87, 2004 (in Japanese).
- Maki Yoshida, Shigeo Mitsunari, and Toru Fujiwara: “Time-Capsule Encryption”, IEICE Technical Report, 2004 (to appear).
- Satoshi Nakayama, Akira Fujiwara, Maki Yoshida, and Toru Fujiwara: “A Private Data Retrieval Protocol with Consistent Results and Its Applications”, 2005 Symposium on Cryptography and Information Security, 2005 (to appear).
- Takaaki Fujita, Kunihiro Okamoto, Maki Yoshida, and Toru Fujiwara: “The Evaluation of Inter-Frame Similarity to Ensure Given False Positive Error Probability for Correlation Based Video Watermarking”, 2005 Symposium on Cryptography and Information Security, 2005 (to appear).