APES

Anonymity and Privacy in Electronic Services

Claudia Diaz, Joris Claessens, Bart Preneel

APES is a project supported by the Flemish government aimed at developing tools and techniques for adding anonymity and pseudonyms to on-line services. The project is tackled both from a technical and from a legal standpoint. This paper presents the major research issues of the project.

Ir. Claudia Diaz

Ph.D. Student at the K.U.Leuven.

E-Mail: cdiaz@esat.kuleuven.ac.be

Dr. Ir. Joris Claessens

Postdoctoral researcher at the K.U.Leuven

E-Mail: joris.claessens@esat.kuleuven.ac.be

Prof. Dr. Ir. Bart Preneel

Professor at the K.U.Leuven

E-Mail: bart.preneel@esat.kuleuven.ac.be

Introduction

The APES project is part of the Flemish STWW program (http://www.iwt.be/), which is a collection of projects that try to bridge the gap between the research world on the one side and society on the other side. The project started in October 2000 and will carry on until October 2004.

The goal of the project is to develop basic building blocks that provide anonymity in a wide variety of applications. The idea is to develop technologies which add anonymity to communication infrastructures, but also to more sophisticated interactions such as payment, elections, contract signing, peer-to-peer systems, etc.

The research consortium consists of three partners from the K.U.Leuven, each bringing their own expertise in this project:

Coordinator research group COSIC, Department of Electrical Engineering-ESAT;

Research group DistriNet, Department of Computer Science;

Research group ICRI, Faculty of Law.

The consortium is backed up by a user group consisting of the following members: Data4S, Ubizen, Utimaco Safeware, HyperTrust, the Belgian Privacy Commission and ISPA Belgium.

1 Research

During the first two years of the project, we have focused our attention on tools and applications that require unconditional anonymity. In the next two years, we will study and develop systems with conditional anonymity requirements.

The documentation of the research that has been carried out for this project can be found on our website https://www.cosic.esat.kuleuven.ac.be/apes/

We present below a summary of this work.

1.1 Anonymity requirements for different applications

During the first six months of the project, we have surveyed the state-of-the-art in anonymity systems; we have studied the applications that require anonymity; and the specific anonymity requirements of each application. The obtained results can be found in the deliverable D2, "Application requirements" [D2].

For applications such as electronic voting and electronic payments, anonymity and privacy are strictly necessary. In a democratic society public elections will be held anonymously and citizens have a fundamental right to privacy, for example when buying goods or subscribing to services.

However, current technologies such as databases, online connections and mobile communications may lead to an increased erosion of privacy. For the time being no widespread communications and payment technologies are available to provide on-line shopping without giving away a substantial amount of personal information. Applications like email, publishing and web browsing are widely accepted, yet sensitive personal information is commonly being disclosed in these applications too. Deliverable D2 of the project describes the anonymity requirements of a variety of applications in which anonymity and privacy play an important role: anonymous connections, which can be used for all applications; email; web publishing; web browsing; online payments; on-line elections and finally on-line auctions.

In the deliverable we provide a general model that can be used to describe the anonymity properties of the applications we studied. Firstly the notions of 'privacy', 'anonymity', 'identity' and 'pseudonymity' are briefly set out (for anonymity we adopt the definition of Pfitzmann and Köhntopp in [1]). Secondly, an abstract and application-independent terminology (roles) is derived for the different entities that actively participate in the application, such as for example 'initiator' and 'responder', '(un)informed' provider, and 'trustee'. Anonymity properties should always be seen relatively to specific roles. Finally different types of anonymity (for example one-time anonymity and persistent anonymity) are described.

The remainder of the deliverable describes in detail the anonymity requirements for the selected applications. For all these applications we start with a short overview of their functionality and the different entities that participate in that application, together with a mapping of these entities to the abstract roles described in the model. Next, the anonymity related requirements and properties of the application are described in more detail. Some examples of anonymity requirements are: untraceability of communication, untraceability and unlinkability of electronic payments, voter anonymity, bidder anonymity, etc.

> Each application has its own specific requirements and, at first glance, a general solution for all applications seems unlikely.

This provides the justification for providing the abstract model. If the entities in different applications map to the same abstract roles in the model, it is likely that the solutions for these applications will be similar. A short overview is presented of the existing solutions to provide anonymity and privacy to these applications. We include a number of possible legal issues that will be further examined in the deliverable on legal aspects of anonymity.

1.2 Overview of technologies

The second phase of the project consisted of an exhaustive study of the available tools that may be used to add anonymity to a variety of applications. The results are presented in our deliverable D3, "Technologies: overview" [D3].

We present the first step towards a more solid foundation for the analysis, design and implementation of anonymity technologies. Anonymity techniques are often composed of several subcomponents that are each responsible for a particular anonymity aspect. In deliverable D3, we focus on these basic building blocks. In this way, we will increase the understanding in the exact execution of existing anonymity techniques and enable a more uniform evaluation process.

In order to structure the description of basic building blocks, we first present a block taxonomy, which is mainly based on the distinction between connection vs. application-level blocks. For each block, we then describe its functionality and various other properties, such as requirements, anonymity type and performance. We also evaluate its correctness and security in an informal way.

In the remainder of the deliverable, we present the composition of basic building blocks, which is the key to build more powerful anonymity services. As an advantage, block composition often results in additional anonymity properties. We describe composition requirements, dependencies and how it can be achieved using different composition strategies. A case study of Onion Routing[1] illustrates

[1] P. Syverson, D. Goldschlag and M. Reed, 'Anonymous Connections and Onion Routing', IEEE, Journal on Selected Areas in Communications, vol. 16 no. 4, May 1998, pp. 482-494.

this process for connection-level building blocks. Furthermore, some advanced cryptographic schemes are decomposed into several application-level building blocks.

1.3 Tools for technologies and applications

During the second year of the project, we have selected two applications, developed a set of tools to add anonymity to these systems and implemented a demonstrator. The results are described in the deliverable D5, “Tools for technologies and applications” [D5].

In deliverable D5 the appropriate privacy-enhancing technologies are chosen and incorporated in two different applications:

- privacy-preserving targeted advertising through web banners, and
- anonymous peer-to-peer networking.

New tools and technologies are also presented. A methodology to provide anonymity services is described.

A solution for *privacy-preserving targeted advertising* through web banners is proposed. The solution allows users to make a balance between the exposure of their privacy and the personalization of the advertisement. The key idea of the solution lies in dynamically associating users with profiles according to their interests and/or demographics instead of to individual identifiers. The user’s profile is hereby under full control of the user and is not maintained at the banner’s side. Furthermore, the solution relies on an infrastructure for anonymous communication to provide anonymity at the connection-level.

Secondly, an *architecture for anonymous P2P networking* was proposed. The architecture is application-independent and is independent of the P2P model. The architecture separates peer-level and connection-level services and hides the implementation of the anonymity functionality.

> Anonymity is not a black-or-white issue. A *model to measure the degree of anonymity* is therefore developed.

A specific model for applications such as the web banner system, as well as a generic model for anonymous communication, is presented. The degree of anonymity depends on the probabilities of having sent a message, and is measured with respect to a particular attacker. The model is based on the information theoretical concept of entropy. By analyzing (and maybe actively modifying) the traffic flow of an anonymous communication system (such as Crowds[2], for instance), an attacker can assign to the users different probabilities of having sent a particular message. The proposed model takes as input these probabilities and outputs the degree of anonymity provided by the system. This degree of anonymity takes high values when users appear as senders of the message with evenly distributed probabilities (the attacker does not obtain much information about the sender with the attack); when a user (or a reduced set of users) have a high probability of having sent the message, then the system is providing a low degree of anonymity (the attacker is obtaining a fair amount of information about the identity of the sender).

A *mix network*[3] forms the core of an anonymous communication infrastructure. A new theoretical mix design was proposed that uses randomness in order to make message tracing more difficult, and that provides better resistance against the blending attack (also called *n-1 attack*). This is a very powerful active attack against a mix that allows tracing a message that goes through the mix. The attack is deployed as follows: first, the attacker fills the mix with his own messages; then, he lets the target message in (so the target message is mixed with messages known to the attacker). The details of the attack depend on the type of mix and so does the effort of the attacker. In the proposed mix design the success of the attacker is probabilistic.

Finally, a *proof-of-concept* of both the web banner application and the P2P architecture has been implemented. The targeted advertising demonstrator can be downloaded from our website for testing purposes, and we are currently improving it in order to provide a service that blocks the access to banner servers with privacy-invading policies.

2 Future work

In the next two years, we will focus on applications for which uncontrolled anonymity is not suited. The specific requirements of how the anonymity should be controlled will be studied. A taxonomy of different ways to revoke anonymity will be made, and the requirements for such revocation will be investigated.

Similarly to the process followed with unconditional anonymity in the first two years of the project, we will evaluate the existing technologies for controlled anonymity.

Finally, our goal is to develop new tools and technologies that implement anonymity control, both at a theoretical and practical level.

3 Events

The APES project has organized three open workshops. The first APES Workshop took place on April 19, 2001; the second one on November 11, 2001; and the third one on November 5, 2002.

The goal of our workshops is to present to the scientific community the results of our research. We also invite external speakers that are working in the privacy and anonymity field. The workshops are open for anybody interested in this research topic and no registration fee is asked to the attendants.

Conclusion

This article presented the research project on Anonymity and Privacy

[2] www.research.att.com/projects/crowds/.

[3] See ‘Gateway’ in this issue.

in Electronic Services (APES). Within this project, we have first studied the anonymity requirements of different applications. Then, we have examined the available technologies that can be used to add anonymity to these applications. Finally, we have developed new tools and implemented some of these in a demonstrator. While during the first two years of the project we have worked on unconditional anonymity, in the next two years we will focus on conditional anonymity.

Acknowledgements

Claudia Diaz is supported by the IWT STWW project on Anonymity and Privacy in Electronic Services (APES). The three authors are supported in part by the Concerted Research Action (GOA) Mefisto-2000/06 of the Flemish government.

References

[1] A. Pfitzmann and M. Köhntopp, 'Anonymity, Unobservability and Pseudonymity – A Proposal for Terminology.' In Hannes Federath (Ed.), Designing Privacy Enhancing Technologies, Lecture Notes in Computer Science, LNCS 2009, pp. 1-9, Springer-Verlag, 2001.

As stated above, the results of our research are described in a number of deliverables publicly available through our website:

https://www.cosic.esat.kuleuven.ac.be/apes/.

[D2]C. Diaz, S. Seys, J. Claessens, C. Goemans, B. de Win, V. Naessens, B. Preneel, J. Dumortier, B. De Decker, 'Deliverable D2 of the APES project: Requirement study of different applications', May 2001, 73 pages.

[D3] C. Diaz, S. Seys, J. Claessens, C. Goemans, B. de Win, V. Naessens, B. Preneel, J. Dumortier, B. De Decker, 'Deliverable D3 of the APES project: Technologies Overview', November 2001, 93 pages.

[D5]C. Diaz, S. Seys, J. Claessens, C. Goemans, B. de Win, V. Naessens, B. Preneel, J. Dumortier, B. De Decker, 'Deliverable D5 of the APES project: Tools for technologies and applications', December 2002, 85 pages.

The research papers published by the team members include:

C. Diaz, S. Seys, J. Claessens, B. Preneel, 'Towards Measuring Anonymity,' Privacy Enhancing Technologies 2002, San Francisco, in print, Springer-Verlag, April 2002.

C. Diaz, J. Claessens, S. Seys, B. Preneel, 'Information Theory and Anonymity,' Proceedings of the 23rd Symposium on Information Theory in the Benelux, B. Macq and J.-J. Quisquater Eds., pages 179-186, May 2002.