Table of Contents

Invited Papers

Regular Short Papers

Regular Long Papers

On Mobile Agents Resistance to Traffic Analysis

Kamil Kulesza[1] Zbigniew Kotulski[2]

Institute of Fundamental Technological Research
Polish Academy of Sciences, Warsaw, Poland

Konrad Kulesza

Rhodes University, Grahamstown, South Africa

Abstract

This paper will concern itself with a formulation of traffic analysis problem for mobile agents. It is an interesting theoretical problem as well as a critical feature when using agents on a massive scale in decision making systems. The decision making systems are applied to demanding and complex environments such as stock markets. The mobile agents used are a natural targets for attacks, because they provide information for decision making. The resulting information can have a value measured in millions of dollars and information of such a high value attracts potential attacks. An efficient way to attack the user of decision making systems is to learn her strategy and respond in kind. In this respect even passive observation of agents can provide useful data, namely what information they are gathering. A common first defense is to provide anonymity for mobile agents. However, what happens when anonymity is gone? What information then becomes available and what steps will the user take? Yet, the problem has not been previously formulated for such a framework. We formulate it in terms of various factors used for traffic analysis. These factors originate from different side channels that provide information on the operating agents. At the end we state a paradox, which links an excessive use of countermeasures against traffic analysis with weakening system security.

Key words: mobile agents security, security protocols, traffic analysis, side channel attacks

[1] Email: kkulesza@ippt.gov.pl

[2] Email: zkotulsk@ippt.gov.pl

This is a preliminary version. The final version will be published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

1 Introduction and Motivation

"Program a map to display frequency of data exchange, every thousand megabytes a single pixel on a very large screen. [...] Up your scale. Each pixel a million megabytes. At a hundred million megabytes per second, you begin to make out certain blocks in midtown Manhattan, outlines of hundred-year-old industrial parks ringing the old core of Atlanta."

William Gibson in [1]

1.1 Preliminaries

Mobile agents were at their peak in the late 90's, which was closely correlated with the Internet boom. Now, when the preoccupation with the agents decreased, why it is worthy to bother with the mobile agents systems?

The main reason for disappointment with the mobile agent technology is, that it failed to meet the expectations. It is true, that individuals do not use mobile agents on a massive scale, for instance to shop for the lowest airlines fares [5]. One of the reasons was certainly the economy. But were mobile agents a case of failed technology or too high expectations? Or maybe mobile agents were put aside by new concepts in IT technology, e.g. grid computing? These are topics of ongoing dispute, which are far from being resolved.

We deal with mobile agents security because of two reasons:

- they are a fascinating and challenging theoretical concept (we also have a strong feeling that mobile agents will have their great comeback);
- there are applications for mobile agents, which are security critical.

Mobile agents benefit simultaneously from remote code execution, coupled with autonomy and adaptation to a changing environment. Mobile code offers a new paradigm in computing, which is well suited for increasingly interconnected environments. This paradigm opens new opportunities, but simultaneously creates new threats.

Mobile agents are excellent vehicles for modern decision making systems, see [2]. In the same paper another agents' feature is discussed: close similarity to a real life solutions and situations. In fact, we witness the situation that an increasing number of concepts, characteristic to real life, migrate into cyberspace. This process is well visible in the field of security protocols [3]. Mobile agents based decision making systems may be perceived as a collection of protocols for distributed information acquisition and analysis. Reality and cyberspace enter into a feedback.

Intelligent mobile agents are the most refined form of decision systems that we have yet created. The agent systems can be considered as not only an effective, but also a user-friendly information technology tools, easy to accept by non-professional users [4].

In the modern world mobile agents are applied in the most demanding and complex environments, for instance stock markets. The resulting information can have a value measured in millions of dollars. When such high stakes are on a table, they always attract potential attackers. An efficient way to attack the user of such a system is to learn her strategy and respond with one's own. The mobile agents are a natural target for the attack, because they provide information for decision making.

While the mobile agent technology has been created for the users' convenience and improvement in decision systems' performance, it has introduced new risks into the process—the decision process can now be observed and influenced by the competitors.

The purpose of this paper is to present a new source of risk. It arises from the agent systems potential vulnerabilities and leads to a perceived or acknowledged business risk that may need to be contained. As far as we know, the problem was not investigated from such an angle. To be able to formulate it, first we need to provide some information on mobile agent security. This will allow us to make security assumptions needed for more precise description of the problem.

1.2 Mobile Agent Security

Mobile agents security falls into a set of problems with mobile security, which were nicely outlined by Roger Needham in [6]. In the paper he presents the development of security methods from a historical perspective. At first security was designed for immobile environments, next mobile technologies (e.g. agents) appeared and a security gap was created. Although great efforts have been made to close the gap, the major problem is in the paradigm. The historical foundation was good as long as "nothing move[d]", see [6]. Hence, it is not surprising that currently mobile agent security is an active field of research, with many challenges still ahead, see [7,8]. The most recent survey on mobile agents' security can be found in [21].

The problems with security protocols involving mobile agents, prompted Volker Roth to write about programming Satan's agents [9], in the fashion similar to Ross Anderson's Satan's computer [10]. Roth's article shows the seriousness of the situation. However, since mobile agents security is still a young discipline, it is assumed that in time, many of the problems will be resolved. Therefore, this paper will make two assumptions: (1) protocols used are secure and (2) the agents outside trusted hosts do not leak any other information, than possibly about their presence.

However, even with both assumptions in place, one should still be cautious. The paper discusses how to perform successful traffic analysis in such an environment. Moreover, any effort to increase a level of protection against traffic analysis can result in opening windows of opportunity for some side channel attack. Before outlining these concepts in Section 3, first a few remarks about traffic analysis itself.

2 Traffic Analysis

"Thus, what is of supreme importance in war is to attack the enemy's strategy. Next best is to disrupt his alliances by diplomacy. The next best is to attack his army."

Sun Zi in [11]

2.1 Remarks on Traffic Analysis in Security

In the networking world there are many schemes using different techniques in order to enhance resistance to traffic analysis. Yet, a majority of them share one common assumption about the network: a topology consisting of point-to-point links. This approach works nicely for the cable networks. However, when it comes to mobile security it fails miserably, due to lack of point-to-point links. Although the problem of resistance to traffic analysis has been around for some time (e.g. [12,13]), only recently Matt Blaze *et al.* have managed to formulate it for the wireless environment, see [14].

A majority of the schemes first and often only line of defense is anonymity (e.g. [7,15]). Although there is whole continuum for degrees of anonymity (see [16]), to simplify the model it is assumed that for a mobile agent it is a binary value and can be lost only once (see [17]).

However, what is the situation when the anonymity is gone? In such a situation, what remains to be protected is information accessed, collected and analyzed by decision making systems. The way to handle traffic analysis may be derived from drawing conclusions from real world cases.

2.2 Traffic Analysis in the Real World

This section serves the purpose of introducing traffic analysis in a wider context, and to draw attention to a more general, strategic agenda. Also, it can be nicely translated into a very precise language of game theory.

Passive observation seems to be as old as espionage itself, which claims to be the second oldest profession. The case of traffic analysis for intelligence agents was described in detail by Peter Wright in "Spycatcher: The Candid Autobiography of a Senior Intelligence Officer" [18]. In the book he describes how Russian agents were performing successful traffic analysis on British counterintelligence services in London during the Cold War. There are also accounts of the technical side of the story, traffic analysis depended heavily on monitoring radio transmissions between counterintelligence officers.

The accounts given in the book concerned a multi-layer traffic analysis. The first level traffic analysis provided information on what data was being collected by the opponent. The second level analysis employs strategy. When data was gathered over a long period of time, it permitted the Soviets to draw conclusions on what information had been acquired by counterintelligence. This, together with the knowledge of their own operations, developed an accurate picture about British secret services' *level of knowledge and strategy.* It also allowed for estimating what the other party does not know, to find a so-called *knowledge complement.* Such a reasoning seems at first to be very complicated, but it serves the ultimate goal "to attack the enemy's strategy".

3 Mobile Agents Traffic Analysis

In the previous chapter we described the state of art in traffic analysis. First, we discussed it in the context of cyberspace (data security). Next, we recalled cases from the real world. As was stated earlier, we witness situations where reality and cyberspace enter into a feedback. Joining both realms and applying them to mobile agents will allow us to present the main contribution of this paper. This is a good place to recall our assumption on mobile agents' security: (1) protocols used are secure and (2) the agents outside trusted hosts do not leak any other information, than possibly about their presence.

Now we are ready to formulate the traffic analysis problem for mobile agents. We focus on the specific situation when agents are used on a massive scale, for instance to acquire information for decision making systems. In the proposed framework, where large numbers of free roaming mobile agents are employed in the complex network (possibly the whole Internet), traffic analysis of the agents resembles a case for the wireless environment. Hence, we advocate using an approach proposed by Matt Blaze *et al.* in [14].

3.1 The System and Threat Models

The owner of agents has a simple goal, to collect data without leaking information about itself. The owner, during the process, can encounter two adversary types: *listening adversary* and *Byzantine adversary.* The adversary goals are more complex:

- Collecting the data on the opponent's (owner) level of information;
- Collecting information on opponent's knowledge complement (Section 2.2);
- Collecting information of the opponent's patterns of behavior and the reactions to certain stimulus;
- Collecting information on the opponent's strategy (ultimate goal).

Knowing that agents are under constant surveillance, an owner may develop countermeasures. For instance, various strategies can be employed to increase the volume of traffic, with an artificial increase in random and non-meaningful traffic (so-called "white noise").

In another example, agents drop information only at secure locations and are not in regular contact with the owner. Usually, mobile agents generate traffic in two ways, they exchange data with their owner and proliferate themselves through the network. This results in multi-layer traffic analysis (Section 2.2). In the real world the best agents do not communicate with the owner. They act autonomously, because information exchange is the most vulnerable element of any intelligence operation (e.g. [18]). Instead agents should exchange information only in secure locations, ideally at the owner's own host.

Unfortunately, there is always a price to pay for the countermeasures (see [19]). It comes either in system security or performance and accuracy. For instance, a traffic volume big enough to prevent traffic analysis might be unfeasible in terms of other constraints (e.g. cost, bandwidth available). However, a really serious threat follows the observation, that overdoing countermeasures might enable side channel attacks.

3.2 Side Channel Attacks

A side channel attack uses some secondary data about the object investigated to deduce its main properties. An excellent example is a whole class of attacks on the smartcards based on the power analysis (e.g. [20]). In this case cryptographic functions performed by the smartcard are not attacked directly (e.g. by breaking algorithms). The power consumption of the device is measured and on this basis the statistical information about "the patterns" in the smartcard operations are obtained. This attack has recently proven to be quite successful, see [20].

Each side channel makes use of a different measure of some patterns resulting from the main activity of the systems under attack. For the agents' mode of operation described, let us provide a few possible side channels:

- Time spent at the host by the agent;
- Power or resources used by the agent;
- Changes in visible agent's characteristics (e.g. the size of the traveling agent);
- Host communication with the agent's owner, for instance billing for the information used.

It can be shown that many of these originate from the countermeasures against traffic analysis. This leads to the paradox that some side channel attacks may result from excessive use of countermeasures. As was the case when smartcards with build-in countermeasures against power analysis attacks were tested for electro-magnetic emission (e.g. [20]).

Yet, another side channel example occurs due to the earlier countermeasure by owners to require agents to drop information at secure locations. This requirement forces mobile agents to carry all the collected information with them. As the agent acquires data, his size will change. Although all information is encrypted, it will provide data that the host database was used.

In summary; in order to protect oneself against traffic analysis one needs to avoid any "patterns". The type of sideline pattern can be very difficult to predict in advance. Hence, the owner has to "submerge" the activity (e.g. information requested) into the ocean of statistically non-distinguishable activities, for instance see [15]. Still, there is no guarantee that some unexpected attack resulting from a newly found sideline would not appear. The more countermeasures against traffic analysis are used, the greater the chance for more side channels. The lesson learned is that an increasing supply of privacy may benefit the attacker and hence be counterproductive. We hope that in this short paper, we were able to sketch the problem in the way, which makes it an interesting topic for further investigations.

Acknowledgement

The paper is dedicated to the memory of Konrad Kulesza (1979-2003)—researcher, philosopher and warrior. The ideas presented originate from Konrad and Kamil discussions during Kamil's visit to Rhodes University, Grahamstown, South Africa.

The authors want to thank Lynn Moses for editing the manuscript.

References

[1] Gibson, W., "Neuromancer", Ace Books, New York, 1984.

[2] Kulesza, K., and Z. Kotulski, *Decision Systems in Distributed Environments: Mobile Agents and Their Role in Modern E-Commerce*, in: A. Łapińska, ed., Informacja w Społeczeństwie XXI Wieku, Wyd. UW-M, Olsztyn, 2003.

[3] Bella, G., S. Bistarelli, and F. Massacci, *A protocol's life after attacks*, to appear in post-Proceedings of the 11th Cambridge International Workshop on Security Protocols (IWSP'03), LNCS, Springer-Verlag, Berlin.

[4] Schumacher, P., "HCI-Aspekte von Softwareagenten", GMD Research Series No.3/1999, 1999.

[5] Anderson, R., private communication, february 2004.

[6] Needham, R., *Keynote Address: Mobile Computing versus Immobile Security*, in: B. Christianson *et al.*, eds., Security protocols, LNCS **2467**, Springer-Verlag, Berlin, 2002, 1–3.

[7] Jansen, W., and T. Karygiannis, "Mobile Agent Security". National Institute of Standards and Technology, Special Publication 800-19, August 1999.

[8] Greenberg, M.S., J.C. Byington, and D.G. Harper, *Mobile Agents and Security*, IEEE Communications Magazine **36, 7**, July 1998, 76–85.

[9] Roth, V., *On the robustness of some cryptographic protocols for mobile agent protection*, Proceedings of the 5th International Conference on Mobile Agents, LNCS **2240**, Springer-Verlag, Berlin, 2002, 1–14. Revised version of "Programming Satan's agents".

[10] Anderson, R., and R. Needham, *Programming Satan's computer*, in: Computer Science Today, LNCS **1000**, Springer-Verlag, Berlin, 1995, 426–441.

[11] Zi, S., Art of War—Chinese manuscript dated about 500 BC. The english translation Prof. Zhang Huimin, comments Gen. Xie Guoliang, publisher Panda Books, Beiging, 2001.

[12] Menezes, A.J., P. van Oorschot, and S.C. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton, 1997.

[13] Pieprzyk, J., T. Hardjono, and J. Seberry, "Fundamentals of Computer Security", Springer-Verlag, Berlin, 2003.

[14] Blaze, M., J. Ioannidis, A. Keromytis, T. Malkin, and A. Rubin, *Protocols for anonymity in wireless networks*, to appear in post-Proceedings of the 11th Cambridge International Workshop on Security Protocols (IWSP'03), LNCS, Springer-Verlag, Berlin.

[15] Beimel, A., and S. Dolev, *Buses for anonymous message delivery*, Journal of Cryptology **16** (2003), 25–39.

[16] Reiter, M.K., and A.D. Rubin, *Crowds: anonymity for Web transactions*, ACM Transactions on Information and System Security **1, 1** (1998), 66–92.

[17] Wang, C., F. Zhang, and Y. Wang, *Secure Web Transaction with Anonymous Mobile Agent over Internet*, Journal of Computer Science and Technology **18, 1** (2003), 84–89.

[18] Wright, P., "Spycatcher: The Candid Autobiography of a Senior Intelligence Officer", Viking, New York, 1987.

[19] Acquisti, A., R. Dingledine, and P. Syverson, *On the Economics of Anonymity*, to appear in Proceedings Financial Cryptography (FC'03), LNCS, Springer-Verlag, Berlin.

[20] Jaffe, J., *Taking Side-Channel Cryptoanalysis to its Limits: The State of the Art of Differential Power Analysis*, in: "Quo vadis cryptology ?", Proceedings Enigma 2003, Warsaw, 2003.

[21] Kulesza, K., "Mobile agents security", Proceedings Enigma 2004, Warsaw, 2004.