On Mobile Agents Anonymity; formulating traffic analysis problem

KAMIL KULESZA[1], ZBIGNIEW KOTULSKI[1], KONRAD KULESZA[2]
[1]*Institute of Fundamental Technological Research, Polish Academy of Sciences*
ul.Świętokrzyska 21, 00-049, Warsaw, Poland, e-mail: {kkulesza,zkotulsk}@ippt.gov.pl
[2]*Rhodes University, Grahamstown, South Africa*

Abstract: In the paper we are concerned with resistance to the traffic analysis for mobile agents. This feature is especially important while using agents on massive scale in decision-making systems. In modern world such systems are applied in the most demanding and complex environments, for instance stock market. The resulting information can have value measured in millions of dollars. When that high stakes are on the table, they always attract potential attackers. Efficient way to attack the user of such system is to learn her strategy and respond with own. The mobile agents are natural target for the attack, because they provide information for decision-making. In this respect even passive observation of the agents can provide useful data, namely what information they are gathering for they master. Anonymous agents are much more difficult to target or trace, in other words anonymity enhance resistance to traffic analysis. Even when the anonymity is gone, traffic analysis still can be prevented or at least made difficult. We propose a new area of research by formulating the problem in terms of various factors that can be used for traffic analysis. These factors originate from different side-channels that can provide information on the operating agents. In the discussion we try to stick as close as possible to real world, supporting the view that the future modes of operation for Mobile Agents originate from there.

Key words: mobile agents, distributed computing, cryptography, data security, econometrics of security

1. INTRODUCTION

"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 "Neuromancer" (see [10])

Mobile Agents are very promising concept in modern information technology. In fact as they counterparts in the real world, they are employed to perform various tasks for their masters. One of the most popular is gathering of the information. The information can be used in many ways, quite often to support decision-making. Mobile Agents are fine vehicles for modern decision making systems, as described in [15]. In the same paper the other of their features is discussed: close similarity to real life solutions and situations. The agent systems can be considered as not only effective, but also user-friendly information technology tool, easy to accept by non-professional users [25]. However, while the agent technology and, in particular, mobile agent technology has been created for the users' convenience and improving decision systems performance, it introduced new risk into the process. Information transmission and the agent relocations put the decision process is under competitors' watching eyes. Thus, we face the usual paradox in cryptography: convenience & reliability versus secrecy & security (see [17], [13]). The purpose of this paper is to present this new source of risk. It arises from the agent systems vulnerabilities and leads to the business risk that needs to be contained.

In order to be more formal we start from the definition provided by Reilly (see [23]): *"Mobile agents are agents that can physically travel across a network, and perform tasks on machines that provide agent hosting capability. This allows processes to migrate from computer to computer, for processes to split into multiple instances that execute on different machines, and to return to their point of origin. Unlike remote procedure calls, where a process invokes procedures of a remote host, process migration allows executable code to travel and interact with databases, file systems, information services and other agents."*

The following quote refers to Java mobile agents (aglets) but the characteristics mentioned are common to all mobile agents:

- "Mobility: Aglets can carry their code or data execution state with them from one computer to another across the network.
- Autonomy: Algorithms implemented in the code of aglets enable them to make local decisions on what to do, where to go and when to go.
- Concurrency: Multiple aglets can be dispatched simultaneously to accomplish various parts of a task in parallel.
- Local interaction: Mobile aglets interact with local entities, such as databases, file servers and stationary aglets through method invocation, while interaction with remote entities is by message passing.
- Flexible routing: The route traversed by an aglet can be predetermined, but it can also be modified dynamically by the aglet as it discovers additional information during its journey.
- Rapid response: An aglet can visit several sites, negotiating with local software at each site, and can return to its home base in only a few seconds" (see [7])

As we can see from the quote it is already implied that mobile agents poses some degree of operational freedom and wisdom, but one important characteristic should be added, namely:

- Intelligence: Ability to make decisions driven by the concern of own survival. Powered by genetic algorithms and the will to survive.

Adding this characteristic, we arrive at Intelligent Mobile Agents. The development of these agents has been a breakthrough for two main reasons:

Firstly, mobility is something that suits the network environment. Whilst all previous systems have been built with stand-alone machines in mind, agents are built with networks in mind. The development of agents responds to an ever-increasing need to modernize the way in which we think of solving problems on the network.

The second reason refers to their intelligence. Intelligent mobile agents are the most refined form of decision systems that we have yet created. Their main goal is to collect information for their owner; their very survival depends on their ability to do so. In [15] the argument liking the intelligence with evolutionary development is presented. The authors see agent's survival instinct as the breath of life inside them. In such framework the agent may has a personal interest in making things happen. He will do anything to survive: he will evolve, find the shortest path through the network, lie to you or fight his way with other agents. Such philosophy closely mirrors the real world. In fact, we witness the situation that more and more concepts that are characteristic to the real life migrate into the cyberspace. This process is very well visible in the field of security protocols, for instance see [5]. Actually one may think about Mobile Agents based decision-making system as collection of protocols for distributed information acquisition and analysis, for instance see [24]. A good example is multi-agent approach to supply chain dynamics (e.g.: [28], [31]).

Mobile Agents can be seen very much the same as agents working for some organization in the real world. Mobile Agents, like the real ones, can perform other activities apart from information gathering. A good example consists of problems with the malicious mobile code and agent misuse (e.g.: [11], [30]).

In the context of resistance to traffic analysis intelligence can give Mobile Agents additional advantage. Kevin Mitnick has shown that security of many systems can be compromised by means of psychological attack, which explores rather human than technological weaknesses (see, [19]). US National Security Agency (NSA) maintains policy that the best-known protection is user security awareness and intelligence (e.g.: [3]). The intelligence can be used to make separate agent from the owner and create autonomous agent. The owner would be fed with the data, while not being aware about the particulars of agents operations.

In the Section 2, we discuss selected security issues for Mobile Agents. While many problems can be handled with modern cryptographic tools like secure multiparty computations (see: [9] for problem formulation and [18], [22] for general reference), some still remain ([24], [30]). We restrict our considerations to issues relevant to anonymity and traffic analysis. This is especially important for mobile agents that par excellence are used for information gathering.

In the Section 3 traffic analysis method is outlined, while the Section 4 describes problem of traffic analysis for mobile agents. The conclusions and final remarks are presented in the Section 5.

2. ON THE AGENT SECURITY

Security for the Mobile Agents falls into set of problems with mobile security, which were nicely outlined by Roger Needham in [20]. In the paper he presents development of security methods in historical perspective. At first security was

designed for immobile environment, next mobile technologies appeared (e.g. agents) and security gap was created. Although great efforts have been made to close the gap, the major problem is in the paradigm. The foundation was good as long as "nothing moves", see [20]. Certainly, there are some good practical, software engineering solutions. The Mobile Agents security often boils down to Java security considerations (e.g. [21]), together with the security of underlying primitives.

In this paper we are not going to address these issues in detail. We also omit problems related to misuse involving Mobile Agents falling into the following categories: damage, denial of service, breach of privacy, harassment, social engineering (see, [11]). Same applies to event-triggered attacks and compound attacks, which result from composition of various attack techniques (see, [11]).

We rather focus on selection of some techniques protecting Mobile Agents and their masters. In our model we have the following parties: the owner/master for the agents, the Mobile Agents, the hosts (locations visited by the agents), the adversary. In the security model that we consider:

- Agents that can move free between hosts;
- In public agents travel in encrypted form, same applies to the data acquired by the agent. For this purpose slicing encryption can be used, see [11];
- Hosts are secure locations, which means that adversary cannot compromise hosts security.

These requirements can be handled with modern cryptographic tools like secure multiparty computations (see: [24], [30] for protocol descriptions in the Mobile Agent context). Authors are aware that available solutions are not perfect (see [24]), yet for the sake of discussion it assumed that above security model holds.

At the end of this section we want to comment on some legal aspects of Mobile Agents security. Since agents operate in global, public network in which there is no uniform jurisdiction, we have to assume that they have status of public information (e.g. [4]). So, all the information obtained from observing them, while in public network, is equivalent to accessing public information. Taking this argument further, one may try to show that traffic analysis is legal as much as any intelligence technique based on the public information. This leads to conclusion that resistance of the agent to these methods should be built by modifying its behavior in the way that it does not reveal "the pattern". In order to describe what is meant by "the pattern" we need to describe attack technique first. The patterns emerge from traffic data collected.

3. 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 Tzu (see [26])

3.1 General problem description

Anonymity of the agent is hard to maintain and can be lost only once. It is interesting to see what are the consequences. In our discussion we assume that compromised anonymity provides only identification for "the parties of the

protocol". This in turn allows passive observation of their behavior in the public places. Reasoning based on such monitoring has been around for a while and is known as traffic analysis. It is important to stress that traffic analysis can be successfully performed using publicly available information and as such can be classified as so-called "white intelligence".

We refer to real life cases, since passive observation seems to be as old as espionage itself, which claims to be second oldest profession. The case of traffic analysis for intelligence agents was described in the detail by Peter Wright in famous "Spycatcher: The Candid Autobiography of a Senior Intelligence Officer" ([32]). In the book he describes how Russian agents were performing successful traffic analysis on British counterintelligence services in London during the cold war. There is also account of technical side of the story since traffic analysis depended heavily on monitoring radio transmissions between counterintelligence officers. It took quite long time before the British uncovered the attack. Peter Wright describes the countermeasures that were undertaken once the problem was discovered.

Actually, the account given concerns multilayer traffic analysis. At first it started with standard surveillance practice of monitoring Soviet diplomatic posts in London by MI5. Some of the Soviet diplomats (suspected agents) were followed by the officers. Since it was pretty standard procedure, Russians decided to use it against British. Using counter-observation and monitoring of encrypted communication (which they did not decrypt), between British counterintelligence, they were able to determine which of their own people were under surveillance. It was first level of traffic analysis providing information on what data is being collected by the opponent.

The second one was trickier. When for the long time data were gathered, they permitted Soviets to draw conclusions on what information was collected by counterintelligence. This, together with the knowledge of their own operations, allowed building good picture about the British secret services' level of knowledge and strategy. It also allowed to estimate what the other party does not know, to find so- called *knowledge complement*. Very good description of such information games is given in "Russia House" by John le Carre ([16]). Although, at first, it seems to be complicated it serves the ultimate goal, quoted at the beginning of this section: "to attack the enemy's strategy".

Since we are mainly concerned with application from field of economic decision making it is time to get rid of espionage stories and provide business related example. An excellent account of this type of operations is given "Wall Street", the movie directed by Olivier Stone (see, [29]). The story is based on famous Ivan Boesky case in 80', when a stock market tycoon was nailed by SEC (Securities and Exchange Commission) with charges of insider trading. In the picture stock market tycoon Gordon Gekko (Michael Douglas) sends his young apprentice Bud Fox (Charlie Sheen) to observe Sir Larry Wildman (Terrence Stamp). The later is powerful British investor planning some deal in the US. Gekko wants to learn about the deal. Following Sir Larry Wildman for all day Bud Fox finds what investment banks Brit was talking to. He also found where to investor flew his jet after the talks. The apprentice is unable to get any detail of conversations, since these were carried out in secure locations. When Bud Fox came to his master to report, he was

apologizing for the poor results. But for Gordon Gekko it was enough information. Knowing the names of investment banks and people involved he was sure that Sir Larry Wildman was interested in some heavy industry enterprise. All these, combined with the Wildman's plane destination (some location in Pennsylvania) revealed his adversary the company itself - Anacott Steel. Such result was possible, since Gordon Gekko very well knew Sir Larry Wildman. He combined his knowledge with all the information obtained by the traffic analysis. As the result he derived and implemented strategy that allowed him to make millions of dollars on the stocks market.

It was not only matter of insider trading or greenmail operation; it was demonstration of the highest skills - successful attack on the enemy strategy.

3.2 Traffic analysis in security

Traffic analysis problem has been around for a while. It originated from analysis of command and control in the military, see [1]. Usually it has been connected with security of some operational practices in big organizations. Problem was also known to signal engineers and telecommunications specialists, with most recent applications in the information warfare, see [8]. In some of these fields there were attempts to approach problem more formally, for instance using conflict modeling methods (e.g. [1]). More formal treatment in the security was presented during Crypto'82 in [9] and found many applications in network security. One of the most important is in intrusion detection (e.g., [22]). Nowadays large part of network administrator job is to perform traffic analysis on the data passing through his site. It is true that this analysis is done in the different, rather defensive context (as long as system administrator does not have sideline hobby of users' surveillance).

In the networking world there are many schemes supporting anonymity, using different techniques to provide requested service. Yet, majority of them share one common assumption about network: the topology consisting of point-to-point links. This approach works nicely for the cable networks, but when it comes to mobile security it miserably fails (lack of point-to-point links). In addition new mobility related problems emerge, as discussed in [20]. Although, problem of resistance to traffic analysis has been around for a while (e.g., [22]), only recently Matt Blaze managed to formulate it for the wireless environment, see [6].

The Mobile Agents operating in the complex network very well approximate wireless environment. Hence, in this paper we propose to look at the problem using approach proposed by Matt Blaze in [6]. This is very new field of research, yet some characteristics can be made. In such framework resistance to traffic analysis can be seen in terms of:

a. Protecting identities or anonymity of the parties involved. If this is provided and assumptions stated in the Section 2 are maintained, it would be a perfect solution, since no traffic analysis is possible. Such solution is a very difficult to implement, below we discuss less demanding one;

b. When anonymity is gone, what remains to be protected is information accessed, collected and analyzed by decision-making system. This is very much like in the real world traffic analysis, as discussed in the Section 3.1.

4. MOBILE AGENTS TRAFFIC ANALYSIS

"*Foreknowledge cannot be gotten from ghosts and spirits, cannot be had by analogy, cannot be found out by calculation. It must be obtained from people, people who know the conditions of the enemy." Sun Tzu (see [26])*

Resistance to traffic analysis is specially important while using agents on the massive scale, for instance, to acquire information for decision making systems. The best way to attack user of such system is to attack his strategy. As described in the Section 3.1, in order to be successful one has to learn the opponent strategy. This can be done with help of traffic analysis. On the opposite side, the owner of agents wants to collect data without leaking information about herself.

The adversary goals can be more complex:

a. Collecting the data on the agents' owner level of information;
b. Collecting information on opponents knowledge complement (Section 3.1);
c. Collecting information of the agents' owner patterns of behavior and the way of responding to certain situations;
d. Collecting information on the owner's strategy.

At this point it is good to recall our assumptions for security model:

- Agents that can move free between hosts;
- In public agents travel in encrypted form, same applies to the data acquired by the agent;
- Hosts are secure locations, which means that adversary cannot compromise hosts' security.

These assumptions mirror real life situation, where agents can operate from the diplomatic post using diplomatic status as additional protection (e.g. [32], [27]). We have to make same assumptions as made by intelligence services, that agents are under constant surveillance (recall legal remark from the Section 2).

The Mobile Agents generate traffic in two ways, they can exchange data with their owner and proliferate themselves through the network. Such situation creates great opportunities for traffic analysis, since not only each of the ways can be separately analyzed, but also their interactions can be investigated. This would result in multilayer traffic analysis, which example was given in the Section 3.1. Again, we follow analogy with the real world that the best agents do not communicate with the masters. They act autonomously, because information exchange is the most vulnerable element of any intelligence operation (e.g. [27]). Instead we propose mechanism that agents exchange information only in secure locations, ideally at the owner's own host.

4.1 Core problem

We start from obvious observation, that once all parties are anonymous the successful traffic analysis is not possible. Only, when at least one of the requirements is compromised window of opportunity appears.

4.1.1 Adversary models

We discuss two situations:

1. Only movements of the agents are observed. This is very much the case discussed in the Section 3.1. It permits multilayer analysis (e.g. [32]), but only agents' movements are taken into consideration. Data can be collected by:

- Following the agents through the network;
- Tracing agent's route backwards;
- Observing some key nodes (e.g. database hosts).

As the result the volumes of data are collected from which activity patterns can be extracted. In addition it is always good to have some extra information, which can speed up the analysis. The case from "Wall Street" is a good instance.

2. Movements of the agents are observed; in addition the agent can be captured and interrogated. In cyberworld agents consist of bits, which can be freely copied. Although protection techniques are available (for instance see [8], [2]), they have serious limitations. Hence we consider situation that agents can be captured. This can be done simply by copying or replicating the agent, the process that neither agent's owner nor the agent himself be aware about. This is major difference in respect to the real world, where usually master knows that agent was captured. In cyberworld it is left to the adversary to decide whether she would disclose the fact of agent capture (e.g. by making traceable use of acquired information).

Once adversary has the agent (or technically speaking the copy of the agent), she can interrogate him. The main goal is to learn all information that agent posses. However sometimes it is more feasible to manipulate agent for own advantage. In such situation agent can be used as the medium to obtain more information from the agent's master. A very good instance concerning assessing level of knowledge and knowledge complement was provided in [16].

4.1.2 Agent in captivity

The detailed classification of interrogation levels can be copied from the reality (e.g. [32], [27]). For the purpose of this paper two ways of interrogation are proposed. We also outline some of possible countermeasures.

1. Hardcore approach. Breaking the agent and extracting all information available. The first line of defense would be to use cryptographic tools, like encrypted data manipulation (see [11]). Such tools are not easy to corrupt; yet sometimes attack might be feasible. Apart from the cryptographic layer is good to introduce more layers of protection.

One protection can be "need to know principle" used by all intelligence services. It can be nicely illustrated by the old saying: "The less information you have, the shorter is your interrogation time". For Mobile Agents in can be implemented within SPECNAZ framework as proposed in [15].

Other layer may include protection against reverse engineering in form of code obfuscation ([11]). This is especially efficient when joint with black box security approach [18].

2. Soft approach. Confusing the agent by creating false environment turning agents, etc. This approach, compared to the first one, is more sophisticated method.

Again, the minimal goal is to extract information from the agent. However this times no violent methods, like breaking are used. The interrogation concentrates on

convincing the agent that he can release information. For instance fake owner host, with full corresponding environment can be produced. The game can be carried out much further, since agent may be fed with the data and released in order to mislead his owner. Also the information that he provides can be correct, but aiming to provoke some action. Because problem is fuzzy, hence technical countermeasures are difficult to design. One of the methods would be to use state appraisal functions ([11]), which make sure that agent's data are not tampered with.

The general defense method should copy real life and use agent's intelligence. Intelligent Mobile Agents can be more difficult to confuse, but they are also more difficult to control. If you are intelligent, you can lie in convincing way. Survival driven Agents evaluate their situation in the context of own best interest, see [15]. This makes them efficient, but also increases certain risks (double agents, turning agents and so on).

4.1.3 Countermeasures

Although this paper is dedicated to the problem formulation, not to the protection against traffic analysis, we summarize section 4.1 with description of general countermeasures.

- Cryptographic tools, specially ones supporting anonymity and distributed multiparty computations, see [22];
- Anonymity servers infrastructure and routing via multiple proxies (e.g. [8], [2]);
- Adapting trail obscuring techniques ([11]), which were invented to prevent agent tracking;
- Various strategies for increasing volume of the traffic, with artificial increase in random and non-meaningful traffic (so-called "white noise").

Since "there is no free lunch", it is not surprising that countermeasures cost:

- Econometrics of security (e.g. [2]). Since traffic generated has to be orders of magnitude higher, which in turn may prove to be quite expensive;
- New attack possibilities. It is a paradox, that increasing level of the protection allows for the new side channel attacks, as discussed in the next section.

4.2 Side channel attacks

The first use of the term "side channel attack" appeared in early stages of the cryptography development and is difficult to trace. Some argue that many of the concepts in cryptanalysis are indeed equivalent to some type of side channel attack. Informally speaking side channel attack uses some secondary data (resulting from side channel) about the object investigated to deduce it's main properties. An excellent example is whole class of attacks on the smartcards based on the power analysis (e.g. [12]). In this case cryptographic functions performed by the smartcard are not attacked directly (e.g., by breaking algorithms concerned). 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 type of attack has recently proven to be quite successful, see [12].

More formally speaking each side channel makes use of different measure of some patterns resulting from the main activity of system the under attack.

For the reasons stated later in this section, it is rather impossible to list all possible side channels. Nevertheless, following agents' mode of operation described so far, let us provide a few:
- Time spent at the host by the agent;
- Power or resources used by the agent;
- Changes in visible agent characteristics (e.g. the size of traveling agent);
- Way that agent was hosted (priorities, status, security level, etc.). For instance in the case described in the Section 3.1 only intelligence services communications were encrypted, while all other (e.g. police, fire services) were in plaintext, which allowed to separate them from the data stream;
- Communication with agent's owner, for instance billing for the information used.

It is interesting to note that almost all the attacks result from the countermeasures described towards the end of the Section 4.1. The side channels are used to make the countermeasures transparent, like they were never in place.

In practice it is very difficult to anticipate in advance all possible side channels. This would require complete knowledge of all the system parameters in every state of operation. Such requirement can be easily brought to much more philosophical question: will our understanding of Nature ever be complete? In addition there is paradox that some of side channel attacks can result from excessive use of countermeasures. That was the case when smartcards with build-in countermeasures against power analysis attacks were analyzed for electro-magnetic emission (e.g., [12]). In case of Mobile Agents, one of the opportunities would emerge from the fact that agents do not exchange information with the owner. As the result they have to carry all the information with them. When agent acquires data, her size will change. As stated above this is a side channel, since although all information is encrypted, it will provide data that the host database was used, possibly with the measure of the information acquired.

To summarize, in order to protect against traffic analysis one needs to avoid any "the patterns". The type of sideline pattern can be very difficult to predict in advance. Hence, the owner has to "submerge" her activity (e.g., information requested) in to the ocean of statistically non-distinguishable activities. While statistical measures can be built and implemented for this purpose, there is no guarantee that some unexpected attack resulting from newly found sideline would not appear.

5. CONCLUDING REMARKS

"So only a brilliant ruler or a wise general who can use the highly intelligent for espionage is sure of great success." Sun Tzu (see [26])

In the paper we described problem of traffic analysis. We based our description on the real world and tried to stick to it as close as possible. Problem is formulated, but much still remains to be done:

1. Development of countermeasures. This is hard, because one has to foresee type of attack in order to describe the pattern that should be avoided. As discussed in the Section 4.2, although general solution might be out of reach, it is good to test new attacks possibilities.

2. Building more complex adversary models. So far, we assumed passive adversary that only observes the agents action. In the Section 4.1 we outlined opportunity of agent capture and interrogation. Model of the adaptive adversary interacting with the agents, for instance by feeding them with the information, and playing "the game" with the owner, is still to be built.
3. Introducing more parameters into the model. Following proposed approach the inspiration should come from real-life situation and scenarios, for instance:
   - Some hosts (databases) can leak information, cooperating with the attacker;
   - Allowing information exchange between agents and the owner by means of broadcast, so limitations stated at the beginning of the Section 4.1 can be lifted;
   - Double agents, etc.
4. Mathematical formulation of traffic analysis for Mobile Agents. The toolbox can include:
   a. Mathematical methods of AI, e.g. using fuzzy sets/logic to build traffic analysis expert systems ;
   b. Abstract algebra;
   c. Graph theory methods (see, [14]), e.g.:
      - movement graphs/networks
      - graph knowledge presentation
      - graph grammars

ACKNOWLEDGEMENT

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

REFERENCES

[1] Thomas B. Allen. 1989. 'War Games'. Mandarin Paperback, London
[2] Ross J. Anderson. 2001. 'Security Engineering: A Guide to Building Dependable Distributed Systems'. John Wiley & Sons.
[3] 'The NSA Security Manual' , anonymous source, available from Ross Anderson Webpage at: http://www.cl.cam.ac.uk/ftp/users/rja14/nsaman.pdf
[4] Janusz Barta, Ryszard Markiewicz. 1998. 'Internet a prawo', TAiWPN Universitas.
[5] Giampaolo Bella, Stefano Bistarelli, Fabio Massacci. 2003. 'A protocol's life after attacks'. To appear in LNCS, post-proceedings of the 11th Cambridge International Workshop on Security Protocols, Sidney Sussex College , 2-4.04.2003
[6] Matt Blaze, John Ioannidis, Angelos Keromytis, Tal Malkin, Avi Rubin . 2003.' Protocols for anonymity in wireless networks'. To appear in LNCS, post-proceedings of the 11th Cambridge International Workshop on Security Protocols, 2-4.04.2003
[7] Dasgupta, P., Narasimahan, N., Moser, L.E., and Melliar-Smith, P.M. 1999. 'MAgNET: Mobile Agents for Networked Electronic Trading'. Department of Electrical and Computer Engineering University of California, Santa Barbara, CA 93106
[8] Dorothy E. Denning. 1998. 'Information Warfare & Security'. Addison-Wesley.

[9] Danny Dolev , Agi Widgerson. 1982. 'On the security of multi-party protocols in discributed systems'. LNCS , (Advances in Cryptology – CRYPTO'82)
[10] William Gibson. 1984. 'Neuromancer '. Ace Books, New York
[11] Michael S. Greenberg, Jeniffer C. Byington, David g. Harper. 1998. 'Mobile Agents and Security'. IEEE Communications Magazine , July 1998 pp.76-85
[12] Joshua Jaffe. 2003. "Taking Side-Channel Cryptoanalysis to its Limits: The State of the Art of Differential Power Analysis". In: 'Quo vadis cryptology ?', Enigma 2003.
[13] Zbigniew Kotulski. 2002. 'Modern information technologies: data security', M. Kleiber [ed.], *Tech. Scien at the Beginning of XXI Century*, IFTR PAS, Warsaw, pp. 181-210
[14] Kamil Kulesza, Zbigniew Kotulski. 2003. 'Graphs in cryptography, proposal for new optics', Eurocrypt 2003, Warsaw, rump session.
[15] Konrad Kulesza, Zbigniew Kotulski. 2003. '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
[16] John Le Carre. 1989. 'The Russia House' Hodder & Stoughton General.
[17] Ueli Maurer. 2000. 'Cryptography 2000±10'. In: Informatics - 10 Years Back, 10 Years Ahead, Lecture Notes in Computer Science, Springer-Verlag, vol. 2000, pp. 63-85.
[18] Menezes A.J., van Oorschot P. and Vanstone S.C. 1997. 'Handbook of Applied Cryptography'. CRC Press, Boca Raton.
[19] Kevin Mitnick, William Simon. 2002. 'The Art of Deception:Controling the human Element of Security', John Wiley & Sons, 2002.
[20] Roger Needham. 2002. 'Keynote Address: Mobile Computing versus Immobile security'. In: Christianson B. et al. (Eds.): Security protocols, LNCS 2467 pp.1-3 ,Springer-Verlag, Heidelberg.
[21] Scott Oaks. 2001. 'Java Security'(2nd Edition). O'Reilly & Associates.
[22] Pieprzyk J., Hardjono T. and Seberry J. 2003. 'Fundamentals of Computer Security'. Springer-Verlag, Berlin.
[23] David Reilly. 1998. 'Mobile Agents – Process migration and its implications'.Avalable at: http://www.davidreilly.com/topics/software_agents/mobile_agents/
[24] Volker Roth. 2001. 'On the robustness of some cryptographic protocols for mobile agent protection'. LNCS 2240 (Proc. Mobile Agents 2001). Revised version of "Programming Satan's agents". Springer-Verlag
[25] Patrick Schumacher. 1999. 'HCI-Aspekte von Softwareagenten', GMD Research Series, No.3/1999.
[26] Sun Tzu. 'Art of War' – Chinese manuscript about 500 BC. The english translation Prof. Zhang Huimin, comments Gen. Xie Guoliang, publisher Panda Books, Beiging 2001.
[27] Wiktor Suworow. 2002.'Akwarium', Wydawnictwo Adamski i Bieliński
[28] Jayashankar Swaminathan, Stephen .F. Smith, Norman M. Sadeh. 1998 'Modeling Supply Chain Dynamics: A Multi-Agent Approach', Decision Sciences, Vol 29
[29] 'Wall Street', the movie , directed by Olivier Stone, Twentieth Century Fox , 1987.
[30] ChangJie Wang, FangGuo Zhang and YuMin Wang. 2003.'Secure Web Transaction with Anonymous Mobile Agent over Internet'. J. Comp. Sci.&Tech., Vol.18, No.1, pp.84-89
[31] Michael P. Wellman, William E. Walsh 2000. 'Distributed Quiescence Detection in Multiagent Negotiations'. In: Fourth International Conference on Multiagent Systems pp. 317-324
[32] Peter Wright. 1987.'Spycatcher: The Candid Autobiography of a Senior Intelligence Officer'. Viking, New York