PRIVACY-INVASIVE SOFTWARE IN FILE-SHARING TOOLS

Andreas Jacobsson, Martin Boldt, and Bengt Carlsson
School of Engineering, Blekinge Institute of Technology, S-372 25 Ronneby, SWEDEN
{andreas.jacobsson;martin.boldt;bengt.carlsson}@bth.se

Abstract Personal privacy is affected by the occurrence of adware and spyware in peer-to-peer tools. In an experiment, we investigated five file-sharing tools and found that they all contained ad-/spyware programs, and, that these hidden components communicated with several servers on the Internet. Although there was no exchange of files by way of the file-sharing tools, they generated a significant amount of network traffic. Amongst the retrieved ad-/spyware programs that communicated with the Internet, we discovered that privacy-invasive information such as, e.g., user data and Internet browsing history was transmitted. In conclusion, ad-/spyware activity in file-sharing tools creates serious problems not only to user privacy and security, but also to network and system performance. The increasing presence of hidden and bundled ad-/spyware programs in combination with the absence of proper anti-ad/spyware tools are therefore not beneficial for the development of a secure and stable use of the Internet.

Keywords: Spyware, adware, peer-to-peer, privacy.

1. Introduction

As the Internet becomes more and more indispensable to our society, the issue of personal information is recognised as decisively important when building a secure and efficient social system on the Internet [3]. Also, in an increasingly networked world, where new technologies and infrastructures, from pervasive computing to mobile Internet, are being rapidly introduced into the daily lives of ordinary users, complexity is rising [15]. As a consequence, vulnerabilities in systems are more eminent and greater in number than ever before. At the same time, the business climate on the Internet is tightening; e-commerce companies are struggling against competitors and frauds. A powerful component in any business strategy is user/customer information. In general, the company with the most information about its customers and potential customers is usually the most successful one [19]. With respect to personal customer information, consumers generally want their privacy to be protected, but businesses, on the other hand, need reliable personal information in order to reach consumers with offers [13]. Undoubtedly, these demands must be satisfied to establish sound e-commerce, and a secure and well-functioning use of the Internet. However, these conflicting goals leave the control of user information at great risk, and a consequence may be that the users feel uneasy about sharing any personal information with commercial web sites. Human activity on the Internet will only thrive if the privacy rights of individuals are balanced with the benefits associated with the flow of personal information [13].

The problem of assuring user privacy and security in a computerized setting is not new, it has been a discussion for more than 30 years now [9]. However, there are some new aspects, that need to be highlighted. In this paper, we intend to explore privacy aspects concerning software components that are bundled and installed with file-sharing tools. Since file-sharing tools are used exclusively when connected to the Internet, users constitute a good foundation for online marketing companies to display customised ads and offers for users. The displayed contents of these offers are sometimes based on the retrieval of users' personal information. Usually, this kind of software operation is considered to be an invasion of personal privacy [8]. One of the most simple and clear definitions of privacy was first proposed in 1890 by Warren and Brandeis in their article "The Right to Privacy" [23], where privacy was defined as "the right to be let alone". In general, privacy is the right of individuals to control the collection and use of information about themselves [3]. In an Internet setting, the extraction of the definition by Warren and Brandeis has come to mean that users should be able to decide for themselves, when, how, and to what extent information about them is communicated to others [7]. Previous work has suggested that malicious software, or malware, set to collect and transmit user information and/or to display ads and commercial offers without the consent of users have been found bundled with file-sharing tools [11] [22]. There are two kinds of software programs that perform such actions: adware displays advertisements, and spyware goes further and tracks and reports on users' web browsing, keystrokes or anything else that the author of the software has some interest in knowing. In reality, this means that software can be adware and spyware at the same time. However, not all adware is spyware and most spyware is not easily detected by displaying ads [11].

Ad-/spyware has gained a lot of space and attention lately. According to the Emerging Internet Threats Survey 2003 [6], one in three companies have already detected spyware on their systems, while 60% consider spyware to be a growing and future threat. Also, 70% of the companies say that peer-to-peer (P2P) file-sharing is creating an open door into their organisation. When it comes to adware, the Emerging Internet Threats Survey, states that adware and the use of file-sharing tools in office hours are devious and offensive threats that frequently evade both firewalls and anti-virus defences [6]. In effect, ad-

/spyware creates problems, not only to user privacy, but also to corporate IT-systems and networks.

In this paper, we investigate what kind of privacy-invasive software that come bundled with five popular file-sharing tools. We also look into the Internet traffic that is being generated by these hidden programs. A discussion concerning the occurrence of ad-/spyware and its effects on privacy and security is undertaken. In the end, we present conclusions and findings.

2. Privacy-Invasive Programs and Their Implications

One of the major carriers of ad-/spyware programs are P2P file-sharing tools [16] [22]. P2P refers to a technology which enables two or more peers to collaborate in a network of equals [12] [18]. This may be done by using information and communication systems that are not depending on central coordination. Usually, P2P applications include file sharing, grid computing, web services, groupware, and instant messaging [12] [18]. In reality, there is little doubt that P2P networks furnish in spreading ad-/spyware [16]. Besides legal difficulties in controlling the content of P2P networks, another contributing factor is that the user is forced to accept a license agreement in order to use the software, but the contract terms are often formulated in such a way that they are hard for the user to interpret and understand. The effect is that most users do not really know what they have agreed to, and thus really cannot argue their right to privacy.

The occurrence of ad-/spyware programs in file-sharing tools pose a real and growing threat to Internet usage in many aspects, and to other interested parties than only to end users. Some examples argued on this topic are [6] [16] [22]:

- **Consumption of computing capacity**: Ad-/spyware is often designed to be secretly loaded at system start-up, and to run partly hidden in the background. Due to that it is not unusual for users to have many different instances of ad-/spyware running covertly simultaneously, the cumulative effect on the system's processing capacity can be dramatic. Another threat is the occurrence of distributed computing clients, bundled with file-sharing tools, that can sell the users' hard drive space, CPU cycles, and bandwidth to third parties.

- **Consumption of bandwidth**: Just as the cumulative effect of ad-/spyware running in the background can have serious consequences on system performance, the continual data traffic with gathering of new pop-ups and banner ads, and delivery of user information can have an imperative and costly effect on corporate bandwidth.

- **Legal liabilities**: With the new directives[1] concerning the use of file-sharing tools in companies, it is the company rather than a single user who is legally liable for, for instance, the breach of copyright (e.g., if employees share music files with other peers) and the spreading of sensitive information (e.g., if spyware programs transmit corporate intelligence).

- **Security issues**: Ad-/spyware covertly transmits user information back to the advertisement server, implying that since this is done in a covert manner, there is no way to be certain of exactly what information is being transmitted. Even though adware, in its purest form, is a threat to privacy rather than security, some adware applications have begun to act like Trojan horses allowing installation of further software, which may include malware. Security experts use the term "Trojan horse" for software that carries programs, which mask some hidden malicious functionality, but many web users and privacy experts use it to describe any program that piggybacks another. It is claimed that most of the latter are P2P file-sharing software that emerged as ad-supported alternatives in the wake of Napster's decline. In effect, if a computer has been breached by a Trojan horse, it typically cannot be trusted. Also, there is a type of spyware that has nothing to do with adware, the purpose here is to spy on the user and transmit keystrokes, passwords, card numbers, e-mail addresses or anything else of value to the software owner/author. In reflect, most security experts would agree that the existence of ad-/spyware is incompatible with the concept of a secure system.

- **Privacy issues**: The fact that ad-/spyware operates with gathering and transmitting user information secretly in the background, and/or displays ads and commercial offers that the user did not by him-/herself chose to view, makes it highly privacy-invasive.

Most ad-/spyware applications are typically bundled as hidden components of freeware or shareware programs that can be downloaded from the Internet [22]. Usually, ad-/spyware programs run secretly in the background of the users' computers. The reason for this concealing of processes is commonly argued as that it would hardly be acceptable if, e.g., free file-sharing software kept stopping to ask the user if he or she was ready to fetch a new banner or a pop-up window. Therefore, the client/server routine of ad-/spyware is executed in the background. In practice, there would be nothing wrong with ad-/spyware running in the background provided that the users know that it is happening, what data is being transmitted, and that they have agreed to the process as part of the conditions for obtaining the freeware. However, most users are unaware of that they have software on their computers that tracks and reports on their

Internet usage. Even though this may be included in license agreements, users generally have difficulties to understand them [22].

Adware is a category of software that displays commercial messages supported by advertising revenues [20]. The idea is that if a software developer can get revenue from advertisers, the owner can afford to make the software available for free. The developer is paid, and the user gets free, quality software. Usually, the developer provides two versions of the software, one for which the user has to pay a fee in order to receive, and one version that is freeware supported by advertising. In effect, the user can choose between the free software with the slight inconvenience of either pop-up ads or banners, or to pay for software free of advertising. So, users pay to use the software either with their money or with their time. This was the case until marketers noted three separate trends that pushed the development of adware into a different direction. Standard banner ads on the Internet were not delivering as well as expected (1% click-through was considered good) [22]. Targeted Internet advertising performs much better [21]. While office hours are dead-time for traditional advertising (radio, TV, etc.), many analyses showed a surprisingly high degree of personal Internet usage during office hours [21].

The conclusion was that targeted Internet advertising was a whole new opportunity for the marketing of products and services. All that was required was a method for monitoring users' behaviour. Once the adware was monitoring users' Internet usage and sending user details back to the advertiser, banners more suited to the users' preferences and personality was sent to the users in return. The addition of monitoring functionality turned adware into ad-/spyware, and the means to target advertising to interested parties accelerated. In reality, the data collected by ad-/spyware is often sent back to the marketing company, resulting in display of specific advertisements, pop-up ads, and installing toolbars showed when users visit specific web sites.

Spyware is usually designed with the same commercial intent as adware [20]. However, while most adware displays advertisements and commercial offers, spyware is designed with the intent to collect and transmit information about users. The general method is to distribute the users' Internet browsing history [22]. The idea behind this is that if you know what sites someone visits, you begin to get an idea of what that person wants, and may be persuaded to buy [21]. Given the fact that more than 350 million users have downloaded KaZaa and supposedly also installed it on their computers [4], this enables for customised and personalised marketing campaigns to millions and millions of end users. Moreover, information-gathering processes have been implicated in the rising occurrence of unsolicited commercial e-mail messages (so called spam) on the Internet [6].

Besides the monitoring of Internet usage, there is an even greater danger, namely when spyware is set to collect additional and more sensitive personal information such as passwords, account details, private documents, e-mail addresses, credit card numbers, etc.

3. Experiment Design

Problem Domain

Programs designed with the purpose of locating and defeating ad-/spyware components are available throughout the Internet. Even so, these programs are not very refined. For instance, there is usually no linking between the identified ad-/spyware processes inside the computers and the corresponding servers outside, on the Internet. Also, there is no anti-ad-/spyware program that analyses what data content is being transmitted to other third parties on the Internet. So, even when using existing software, it is difficult do keep track of what is going on inside the computer, and what nodes outside it that obtain user-oriented information. As a consequence, Internet browsing records and/or credit card numbers could easily be distributed without the user's consent or knowledge.

In this light, the overall research problem for this paper was to explore the nature and occurrence of privacy-invasive software included in file-sharing tools used over P2P networks. On an experiment level, the research problem was divided into the following subquestions:

- What ad-/spyware programs can be found in file-sharing tools?
- What is the content and format of network data generated as a result of ad-/spyware programs involved in Internet communication?
- What is the extent of network traffic generated by such programs?

Even though there may be numerous components bundled with the installation of file-sharing tools, it is primarily the programs engaged in Internet communication that are of interest to us. There are two reasons for this. First, without this delimitation, the experiment data would be too comprehensive to grasp. Second, for ad-/spyware programs to leak personal information, they must be involved in communication over the Internet. This is of course particularly interesting from a privacy perspective.

Throughout this paper, we use the word ad-/spyware as a synonym for both adware and spyware. In general, both adware and spyware are namely considered to be privacy-invasive software. Also, since they typically are closely intervened with each other, and more or less perform similar actions it is problematic to separate adware from spyware [22].

Instrumentation and Execution

The experiment sample consists of the five most downloaded file-sharing tools [4]. The tools are, in order, the standard, freeware versions of KaZaa, iMesh, Morpheus, LimeWire and BearShare. Also, to be sure that the experiment results were derived from the installed file-sharing tools, we set up a reference computer, which was identical to the other work stations, i.e., the same configuration, but with no file-sharing tool installed. The experiment was executed in January 2004 as one consecutive session that lasted three days. This time range was chosen, because we wanted to avoid getting excessive data quantities, but at the same time be able to capture reliable results.

The experiment was carried out in a lab environment on PC work stations equally connected to the Internet through a NAT gateway. We used OpenBSD's packet filter to deny any inbound network requests, which allowed us to protect the work stations from external threats. The packet filter also helped in reducing the network traffic and in doing so, resulting in less data to analyse. By not downloading or sharing any content in the file-sharing tools we further reduced the amount of network data generated. All incoming and outgoing network traffic of the local computer's network interface were dumped into a file using Winpcap.

Hardware were equivalent for all work stations, which also contained byte-identical installations of both the operating system Microsoft Windows 2000 and program applications[2]. In order to reflect work stations in use, they were all set to browse the Internet according to a predefined schedule containing the 100 most visited web sites in the world [1]. This was done through an automatic surf program. Also, ten identical searches (e.g., "lord of the ring", "star wars", and "britney") were carried out in each of the file-sharing tools, but no files were downloaded. In the end of the experiment, several anti-ad-/spyware programs[3] were used to locate any known ad-/spyware programs previously installed.

Binding network communication to programs is a key feature in the experiment. For allowing continuous monitoring and logging of processes and their use of sockets, we developed a program in C++, which was based on Openport. We chose not to use any Win32 firewalls claiming to support outbound filtering on application level for two reasons. First, they fail in allowing real outbound filtering per application, and there are a number of programs capable of penetrating these fake protections [14] [17]. Second, we have no detailed knowledge in the internal workings of such firewalls and therefore cannot foresee what to expect from them. Finally, it should be emphasised that there exist ways for a malicious program to send network data undetected by the monitoring application, due to the architecture of Windows.

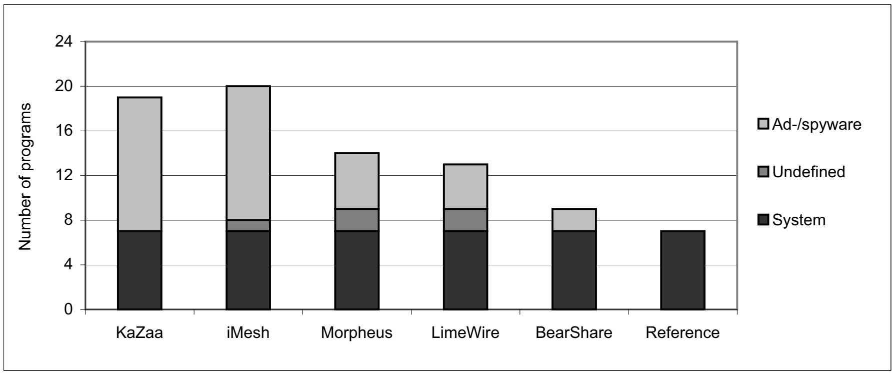

Figure 1. Identified programs in the experiment sample.

Data Analysis

After having performed the experiment, we compiled the data results and set to identify all programs that were bundled with each file-sharing tool. This data was provided by our own process-to-network mapping program in cooperation with the selected anti-ad-/spyware programs. We then isolated the operating system related programs found on the reference work station, since they were considered harmless. Next, we reduced all benign programs handling file-exchange tasks. Remaining were a set of programs that were not related to either the operating system or file-exchange tasks. Further, by using the results from the anti-ad-/spyware tools, we divided the set of programs into two subsets, namely known ad-/spyware programs and unknown programs. The nature of these unknown programs was analysed based on their corresponding network traffic. Also, in some cases we needed additional information and thus turned to Internet resources. Based on this analysis, the remaining ad-/spyware programs were located. In the final step, we divided the retrieved set of ad-/spyware programs into two subsets, namely those involved in Internet communication and those that were not. This analysis was founded on the data from our process-to-network mapping program. In effect, the results from the program analysis lead to a classification of programs as either ad-/spyware programs, system programs or unknown programs.

All data analysis was done in a Unix environment. The data was analysed and filtered using standard Unix programs such as sed, awk, sort, uniq and grep. Much of the analysis was automated using shell scripts and where this could not be done small programs in C were created. To analyse and filter network data, the program Ethereal was used.

In addition, we wanted to see if the corresponding servers were known ad-/spyware servers. Therefore, an effort to map the server names that were involved in Internet communication with a blacklist specifying known ad-/spyware servers [10] was also undertaken.

4. Experiment Results and Analysis

Ad-/Spyware Programs in File-Sharing Tools

According to the results, several programs were located for each file-sharing tool (see Figure 1.). Of these programs, we identified 12 ad-/spyware programs for iMesh and KaZaa respectively. Interestingly, these two file-sharing tools were among the two most popular ones [4]. The rates for the other file-sharing tools were five for Morpheus, four for LimeWire and two for BearShare. Also, iMesh, Morpheus and LimeWire contained programs that we were unable to define. However, these programs were all involved in Internet communication.

We discovered that all of the file-sharing tools contained ad-/spyware programs that communicated with the Internet. KaZaa and iMesh included a relatively high amount of such programs. Even so, the anti-ad-/spyware tools defined several other ad-/spyware programs also installed on the computers. Although this was the case, these programs did not communicate with servers on the Internet during the experiment session.

In Table 1., a detailed list of the retrieved ad-/spyware components can be found. As can be seen, the ad-/spyware components were divided into "Adware" respectively "Spyware" based on their actions. Also, we included a category entitled "Download" because some of the ad-/spyware programs included functionality that allowed further software and/or updates to be downloaded and installed on the computers. In addition, programs involved in Internet communication are specified in the category called "Internet". In the column entitled "Host", the five file-sharing tools utilised as carriers of ad-/spyware are listed[4]. In the cases where the empirical results could confirm the recognised view shared by anti-ad-/spyware tools and Internet resources, the x-markers in the table are declared with bolded capital letters.

One reason to why we could not confirm that every ad-/spyware program was involved in Internet communication was that so called Browser Helper Objects (BHO) were installed in Internet Explorer. Malicious BHOs infiltrate the web browser with the intent to access all data generated by Internet Explorer in order to spy on the user and transmit user behaviour to third parties [20]. Such BHOs typically gain the same privileges as its host (i.e., Internet Explorer), which endorse them to penetrate personal firewalls. This means that any possible ad-/spyware traffic distributed via BHOs is highly problematic to detect since it may very well be ordinary browser traffic. In Table 1., we also included two programs, New.Net and FavoriteMan, even though they were not

Table 1. Identified ad-/spyware programs.

Name	*Host*	*Adware*	*Spyware*	*Download*	*Internet*
BroadcastPC	M	x	x	x	**X**
KeenValue	K	x	x	**X**	**X**
Morpehus	M	**X**	x	**X**	**X**
BargainBuddy	I, K	x	x	x	
TopMoxie	L, M	x	x	x	
Cydoor	I, K	x	x		**X**
Gator	I, K	**X**	x		**X**
SaveNow	B	**X**	**X**		**X**
BonziBuddy	L	x	x		
Web3000	I	x	x		
ShopAtHomeSelect	I		**X**	**X**	**X**
WebHancer	K		x	x	
BrilliantDigital	K	x		**X**	**X**
MoneyMaker	L, M	**X**		**X**	**X**
Claria	I, K	x			**X**
iMesh	I	x			**X**
WeatherCast	B	x			**X**
CasinoOnNet	L	x			
MyBar	I, K, M	x			
New.Net	I			**X**	**X**
FavoriteMan	I			x	

classified as neither adware nor spyware. However, they allowed for installation of further software, which may be malicious.

The Extent of Network Traffic

The results showed that a significant amount of network traffic was generated, although there was no exchange of files between the file-sharing tools and other peers on the Internet (see Figure 2.). In that light, the amount of network traffic generated in this experiment can be seen as a minimum rate to be expected when running file-sharing tools. Notably, installing Morpheus and LimeWire resulted in a relatively high traffic quote, both when it came to incoming as well as outgoing traffic. On the contrary, iMesh, who also had the largest quantity of bundled programs, represented the least amount of network traffic.

In Figure 2., we included compilations of network traffic for both the installation process and the runtime part per file-sharing tool. In the cases of Morpheus, LimeWire and BearShare, a considerable amount of network activity was generated after the installation. For KaZaa, a significant quantity of network traffic was caused during the installation. In comparison, iMesh

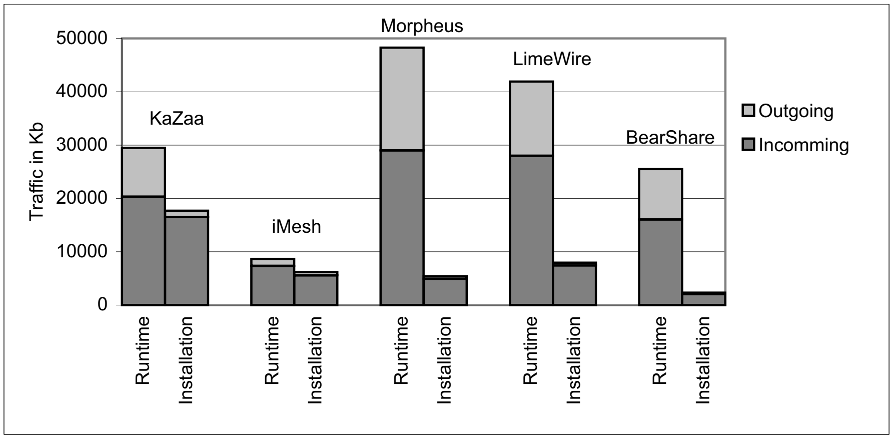

Figure 2. Network data traffic.

produced a notably limited size of network traffic, both during and after installation.

Furthermore, the results suggested a diversity in Internet communication. This is shown in that programs in the file-sharing tools communicated with several different servers on the Internet. Although Morpehus did not contain a particularly great number of bundled programs, it generated notably much network traffic. In reflection, Morpheus communicated with the largest amount of Internet servers, whereas the rates for the other file-sharing tools were in a relatively low accordance with each other. In addition, the results substantiated that most of the invoked servers had domain names. Overall, each of the file-sharing tools contained programs that communicated with known ad-/spyware servers from the specified blacklist [10].

The Contents of Network Traffic

The outgoing network data was in many cases problematic to analyse and understand. In most cases the data was not readable, meaning that it was either encrypted or in a format not graspable. This is also an explanation to why we could confirm only two spyware programs (see Table 1). Although most traffic data was not in clear text, we were able to extract and interpret some of the contents. We discovered that sensitive data such as information about the user (e.g., user name), geographical details (e.g., zip code, region and country) and Internet browsing history records were sent from identified ad-/spyware components to several servers on the Internet. Also, there were other types of information that were transmitted, for example, machine ID, details about program versions, operating system, etc.

According to the results, one spyware program (ShopAtHomeSelect) was found in the iMesh file-sharing tool. In the experiment, that program transmitted traffic measurement reports and Internet browsing history records to invoked servers on the Internet. Also, in BearShare, one spyware program (SaveNow) transmitted data such as Internet history scores and user-specific information.

The experiment results also reveal one of the methods for ad-/spyware programs to transmit user and/or work station data. In the BearShare tool, the information that was fed into the file-sharing software by the user was redistributed within the tool to one or numerous ad-/spyware programs (SaveNow and WeatherCast) that transmitted the information to servers called upon. This method makes it difficult to map various program components to the actual file-sharing activity. Also, it undermines the ability to control what software objects are useful and legitimate in relation to the redundant or privacy-invasive programs that clog down the computers, systems and networks.

The analysis of the contents of the incoming network traffic was more problematic to conduct than in the case of outgoing traffic. Foremost, because the data quantity was both comprehensive and widespread. Since our focus was on privacy-invasive software, the outgoing traffic content was the most interesting so the efforts were mainly put into that. This, in combination, with vast quantities of incoming network data made it difficult to confirm adware recognised by the anti-ad-/spyware tools and Internet resources. Also, the same discussion concerning the occurrence of BHOs would apply for the unconfirmed adware. However, in the retrieved incoming data, a few interesting results were found.

The retrieved adware programs performed activities such as displaying commercial ads, causing browser banners and pop-ups. In particular, Morpheus and LimeWire proved to contain adware programs that generated much incoming data traffic. In LimeWire, results showed that lists of Internet sites and new programs were retrieved from the Internet by the adware MoneyMaker. In Morpehus, the P2P program itself downloaded and displayed ads and banners.

5. Discussion

With the occurrence of ad-/spyware technology in file-sharing tools, the monitoring of Internet usage has become a common feature. Today, most ad-/spyware programs gather and transmit data such as Internet browsing history records to third parties. That type of information can be correlated to a user and thus employed for marketing purposes.

The experiment has shown that all of the investigated file-sharing tools contained ad-/spyware programs. The ad-/spyware programs that operated inside the computers had an open connection to several Internet servers during the entire experimental session. We know that content-sensitive information was sent, but we may only guess the full extent of information harvesting, because most packets were not sent in clear text. Even though we saw no example of highly sensitive personal information, such as passwords and key strokes, were transmitted by the ad/spyware programs in the experiment, we cannot be sure that these activities were not happening. Spyware may collect and transmit genuinely sensitive information about users such as, e.g., account details, private documents, e-mail addresses, and credit card numbers. The information is secretly sent back to numerous servers owned by companies that make a profit on these activities. Although it is problematic to elaborate on the business ethics of these companies, the occurrence of ad-/spyware programs are reasons enough to question this behaviour. In addition, ad-/spyware programs are responsible for all kinds of unwanted actions. Besides invasion of privacy, they can make the system unstable, degrade system performance, create scores of copies of itself to make removal difficult, and act as security holes in the system.

The actions performed by ad-/spyware programs are approaching the operations of a virus. Since users install them on voluntary basis, the distribution part is taken care of by the file-sharing tools. This makes ad-/spyware programs function like a slowly moving virus without the distribution mechanisms usually otherwise included. The general method for a virus is to infect as many nodes as possible on the network in the shortest amount of time, so it can cause as much damage as conceivable before it gets caught by the anti-virus companies. Ad-/spyware, on the other hand, may operate in the background in such a relatively low speed that it is difficult to detect. Therefore, the consequences may be just as dire as with a regular virus. In addition, the purpose of ad-/spyware may not be to destroy or delete data on the work stations, but to gather and transmit veritably sensitive user information. An additional complicating factor is that anti-virus companies do not usually define ad-/spyware as virus, since it is not designed to cause destruction. Overall, the nature of ad-/spyware substantiates the notion that malicious actions launched on computers and networks get more and more available, diversified and intelligent, rendering in that security is extensively problematic to uphold.

Ad-/spyware enables for the spreading of e-mail addresses that may result in the receiving of spam. Due to the construction of ad-/spyware, it may collect information that concerns other parties than only the work station user. For example, information such as telephone numbers and e-mail addresses to business contacts and friends stored on the desktop can be gathered and distributed by ad-/spyware. In the context that ad-/spyware usually is designed with the purpose of conveying commercial information to as many users as possible, not only the local user may be exposed to negative consequences of ad-/spyware. In other words, the business contacts and friends may be the subjects of ad-/spyware effects such as, e.g., receiving unsolicited commercial e-mail messages. This means that even though my computer may be secure, a breached computer owned by a network neighbour can cause me harm. So, the security of a neighbour very much becomes my own concern.

Besides security issues, ad-/spyware creates intrusion to privacy. An inconvenience commonly argued is that ad-/spyware programs display commercial messages based on the retrieval of personal information fetched without the explicit consent of the users. Even though the offers of these advertising campaigns may be in the interest of some users, there is a fine line between what users in general regard as useful information and what is an intrusion to personal privacy. One thought is that, the more personalised the offers get, the more likely users are to regard them as privacy invaders. If so, what happens when users are presented with advertisements in such an extent that they hardly are able to distinguish the possibly serious offers from all the offers. If users ignore marketing messages, there is evidently a great risk for the success of customer-based e-commerce.

A second privacy concern is the spreading of content that the ad-/spyware distributor did not intend for. One example of this would be a malicious actor that gained control of ad-/spyware servers, and broadcasted offensive unsolicited messages (e.g., adult material, political messages or smearing campaigns, etc.) to a great number of users. Although users may consider regular commercial ads to be harmless, most people react negatively upon frequently receiving repulsive pictures and texts. This suffices for that the ad-/spyware providers need to take their own security with great seriousness. If they lose control of their servers, the damage may be devastating. This could be even more devastating if the ad-/spyware program updates on the company servers were replaced with malicious software. In effect, real and destructive malware (e.g., viruses, Trojans, etc.) could be spread to vast groups of ad-/spyware hosts.

6. Conclusions

The experiment has shown that all of the investigated file-sharing tools contained ad-/spyware programs. The ad-/spyware programs operating inside the computers had an open connection where the information was secretly sent back to numerous servers owned by companies that make a profit on these activities. Measurements suggested that the carriers of ad-/spyware, file-sharing tools, generated a significant amount of network traffic, even when not exchanging files. The presence of ad-/spyware programs and the network traffic that they generate contribute in over consumption of system and network capacity.

Ad-/spyware is acting like a slowly moving virus, installed on a voluntary basis, with hidden properties problematic to detect and remove. The payload of ad-/spyware may not be to destroy or delete data on the work stations, but to gather and transmit veritably sensitive user information. The distribution part is taken care of by the file-sharing tools with an additional complicating factor; anti-virus companies do not usually define ad-/spyware as virus, since it is not designed to cause destruction.

The nature of ad-/spyware may lead to that not only host users are affected. Ad-/spyware may gather and distribute the details of business contacts and friends resulting in negative consequences to other parties than the infected desktop owner. This means that even though my computer may be secure, a breached computer owned by a network neighbour can cause me harm. So, the security of a neighbour very much becomes my own concern.

Furthermore, the occurrence of ad-/spyware can render in that privacy-invasive messages may be distributed and displayed to large amounts of users. Exposure to messages not chosen by the user, or collection and transmission of user information are two key privacy concerns. In this way, users right to control what, how and when information about themselves is communicated to other parties is almost non-existing. In conclusion, the nature of ad-/spyware programs ignore users' right to be let alone. The increasing presence of hidden and bundled ad-/spyware programs in combination with the abscence of proper anti-ad/spyware tools are therefore not beneficial for the development of a secure and stable use of the Internet.

Notes

1. Examples on legal directives are the "Directive on Privacy and Electronic Communications'" [5] of the European Union, and the "Spyware Control and Privacy Protection Act" [2] of the Senate of California, U.S.
2. These configuration properties were enabled through a self-developed disc cloning system based on standard FreeBSD components.
3. For a detailed list of the programs used, see http://www.ipd.bth.se/aja/PISiFST_Ref.pdf.
4. K is for KaZaa, I for iMesh, M for Morpheus, L for LimeWire and B is for BearShare.

References

[1] Alexa Web Search., http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none, 2004-04-27.

[2] California Senate Assembly Bill 1386, United States of America, 2003., http://info.sen.ca.gov/pub/bill/asm/ab_1351-1400/ab_1386_bill_20030904_chaptered.html, 2004-04-27.

[3] M. Caloyannides, "Privacy vs. Information Technology", in *IEEE Security & Privacy*, Vol. 1, No. 1, pp. 100-103, 2003.

[4] C|Net Download.com., http://www.download.com/, 2004-04-27.

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic

communications sector (Directive on Privacy and Electronic Communications), 2002., http://europa.eu.int/comm/internal_market/privacy/law_en.htm, 2004-04-27.

[6] Emerging Internet Threats Survey 2003, commissioned by Websense International Ltd., February, 2003., http://www.websense.com/company/news/research/Emerging_Threats_2003_EMEA-de.pdf, 2004-04-27.

[7] S. Fischer-Hübner, “Privacy in the Global Information Society”, in *IT-Security and Privacy - Design and Use of Privacy-Enhancing Security Mechanisms*, Lecture Notes in Computer Science LNCS 1958, Springer-Verlag, Berlin Germany, 2000.

[8] S. Garfinkel, *“Database Nation: The Death of Privacy in the 21st Century”*, O’Reilly & Associates Inc., Sebastopol CA, 2001.

[9] E. Grenier, “Computers and Privacy: A Proposal for Self-Regulation”, in *Proceedings of the First ACM Symposium on Problems in the Optimization of Data Communications Systems*, ACM Press, New York NY, 1969.

[10] Gorilla Design Studio: The Hosts Files., http://www.accs-net.com/hosts/, 2004-04-27.

[11] M. McCardle, “How Spyware Fits into Defence in Depth”, *SANS Reading Room*, SANS Institute, 2003., http://www.sans.org/rr/papers/index.php?id=905, 2004-04-27.

[12] A. Oram, *“Peer-To-Peer: Harnessing the Benefits of a Disruptive Technology”*, O’Reilly & Associates Inc., Sebastopol CA, 2001.

[13] T. Otsuka and A. Onozawa, “Personal Information Market: Toward a Secure and Efficient Trade of Privacy”, in *Proceedings of the First International Conference on Human Society and the Internet*, Lecture Notes in Computer Science LNCS 2105, Springer-Verlag, Berlin Germany, 2001.

[14] Outbound., http://www.hackbusters.net/ob.html, 2004-04-27.

[15] L. Palen and P. Dourish, “Unpacking Privacy for a Networked World”, in *Proceedings of the ACM Conference on Human Factors in Computing Systems*, ACM Press, New York NY, 2003.

[16] B. Robertsson, “Five Major Categories of Spyware”, in *Consumer WebWatch*, October 21, USA, 2002., http://www.consumerwebwatch.org/news/articles/spyware_categories.htm, 2004-04-27.

[17] Robin Keir’s FireHole., http://keir.net/firehole.html, 2004-04-27.

[18] D. Schoder and K. Fischbach, “Peer-to-Peer (P2P) Computing”, in *Proceedings of the 36th IEEE Hawaii International Conference on System Sciences*, IEEE Computer Society Press, Los Alamitos CA, 2003.

[19] C. Shapiro and H. Varian, *“Information Rules: New Rules for the New Economy”*, HBS Press, Boston MA, 1999.

[20] E. Skoudis, *“Malware - Fighting Malicious Code”*, Prentice Hall PTR, Upper Saddle River NJ, 2004.

[21] J. Sterne and A. Priore, *“E-Mail Marketing - Using E-Mail to Reach Your Target Audience and Build Customer Relationships”*, John Wiley & Sons Inc., New York NY, 2000.

[22] K. Townsend, “Spyware, Adware, and Peer-to-Peer Networks: The Hidden Threat to Corporate Security” (technical white paper), PestPatrol, 2003., http://www.pestpatrol.com/Whitepapers/CorporateSecurity0403.asp, 2004-04-27.

[23] S.D. Warren and L.D. Brandeis, “The Right to Privacy”, in *Harvard Law Review*, No. 5, pp. 193-220, 1890-91.