Operational Programme
"*Competitiveness*"

R&D Cooperations with Organizations of non-European Countries

Γ' ΚΟΙΝΟΤΙΚΟ ΠΛΑΙΣΙΟ ΣΤΗΡΙΞΗΣ
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ

ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ

ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ   ΥΠΟΥΡΓΕΙΟ ΑΝΑΠΤΥΞΗΣ

EAR: Early warning system for automatic detection of Internet-based Cyberattacks

(G.S.R.T. code: ΗΠΑ-022)

D5.1: "Commercial Viability Study"

Abstract: This document briefly describes the problem of cyber attacks and examines the possibilities for commercial exploitation of the tool for early warning system developed in this project

Contractual Date of Delivery	12/01/2006
Actual Date of Delivery	04/01/2006
Delivery Security Class	Public
Editors	Manolis Petsagourakis Giorgos Petsalakis Antonis Papagrigoriou
Contributors	FORTHnet

The EAR consortium consists of:

FORTH	Coordinator	Greece
GA Tech	Principal Contractor	USA
FORTHnet	Principal Contractor	Greece

Contents

1. Introduction

In recent years, there is an increasing number of large-scale attacks, such as severe worms and DDoS attacks, threatening organizations' systems and networks. Especially, fast spreading attacks present a serious challenge to todays attack defense systems. Speed, frequency, and damage potential of these attacks call for automated response systems. Research in automated defense systems for Internet-wide attacks is focused on large-scale monitoring infrastructures, such as network telescopes and honeynets; intrusion detection approaches, such as memory tainting, network anomaly detection; automated defense strategies, such as signature generation distribution; and identification and analysis of future threats, such as obfuscation methods and novel spreading techniques.

EAR, Early Warning System for Internet-Based Cyber Attacks, is a step towards achieving a more complete approach to networks and systems security. It consists an early warning system for the automatic detection of Internet–based cyber–attacks, at early stages. The system can efficiently detect intrusion attempts made by already known worms, at the beginning of their spread. Additionally, it can recognize new kinds of attacks, generate signature for these attacks and alert network administrators on these potential threats.

This document consists a commercial viability study for EAR. It is separated in five sections. In the first section, statistics concerning the cyber threats are presented. Then follows a section that summarizes the most frequently used security tools discusses the drawbacks of these tools. Following, there is an overall presentation of the EAR' s tool structure and a section regarding the future exploitation of this tool in the network security application market. Finally, there is a brief section that summarizes the main conclusions derived from this study.

2. Internet Security Issues

2.1 State of the art on cyber attacks

a. Statistics on Cyber attacks

An attack may be defined as any malicious activity crossing the network that has been detected by an intrusion detection system or a firewall[1]. These attacks are usually an attempt to exploit a vulnerability in software or hardware. Generally there are three kinds of attacks: those that tend to propagate autonomously (worms), those that are launched manually and attacks that are intended to gather information.

The statistics and data presented in this section are gathered using various defense devices, such as intrusions detection systems, intrusion protection systems, firewalls, proxies, filters and anti-virus programs.

a. Attack activity per day

Between July 1st and December 31st, 2004, the average attack rate for a median organization was 13.6 attacks per day (figure 1). In the previous six-month period (that is 1st of January to 30th of July, 2004) the average attack rate was 10.6 attacks per day.

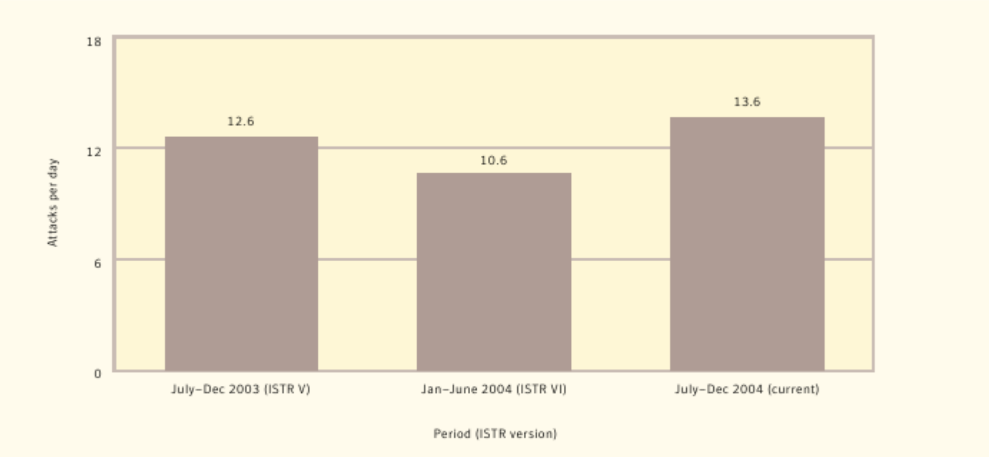

Figure 1 Attack activity per day

b. Attack activity by type

From July 1st to December 31st, 2004, 47% of detected attacks were classified as probes. Scanning for back doors services on high – level ports (that is ports higher than 1023) continues to contribute to the probe total.

Worm attack activity accounted for the 12% of the attack activity. The low rate of worm activity can be explained by the fact that no traditional worms

[1] Symantec definition

were discovered to be propagating during this time. In fact, the popularity of bot networks and semi-autonomous exploitation tools is making the distinction between worms attacks and non-worms attacks more difficult. What is more, the increasing of web application attacks and client-side exploitation, particularly through browser attacks and malformed files, such as images, are proving problematic for traditional intrusion detection systems.

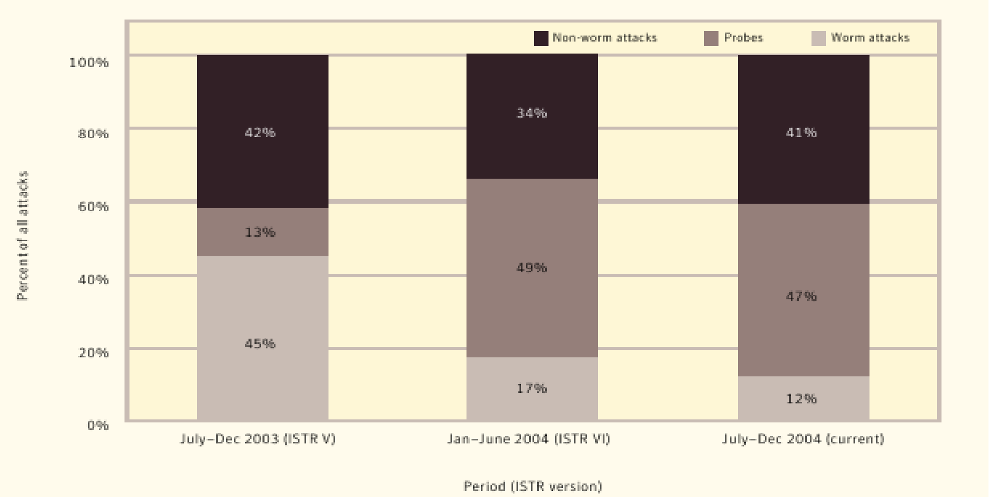

Figure 2: Attack activity by type

c. Bot networks

Bot networks are groups of compromised computers on which attackers have installed software that listens for and responds to commands, allowing them to remote control over the computers.

Between July 1st and December 31st, 2004, observed bot network computers actively scanning declined from a peak of over 30000 per day in late July, to 5000 per day by the end of the year.

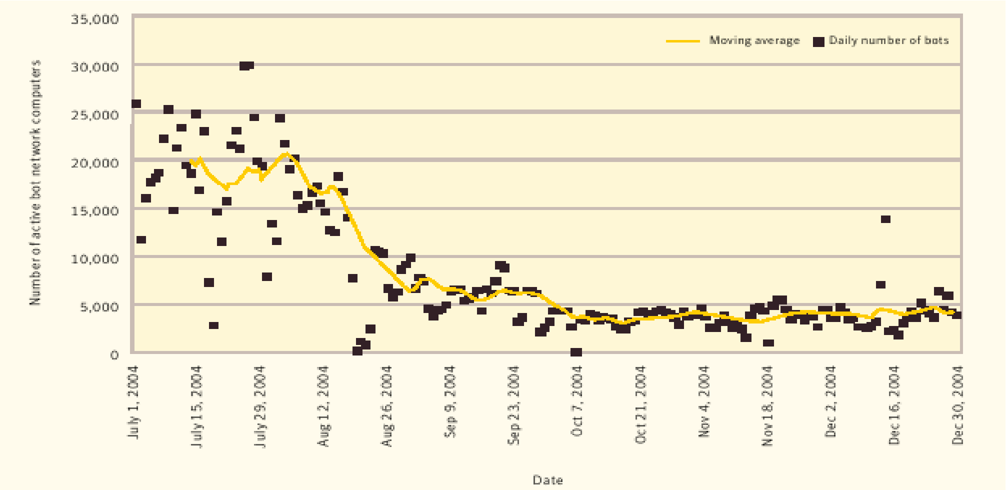

Figure 3: Bot networks attacks

d. Denial of Service attacks (DoS)

The term denial of service is a generic description and simple defines an event that blocks or slows legitimate access to a service provided by a computer. This type of attack relies on overwhelming an Internet service with connection attempts without completing the connection negotiation.

As figure 4 illustrates, the DoS attacks have a steadily increasing course. In fact, there is a trend for the attackers to using spoofed addresses in order to attack someone. Detecting against spoofed-source DoS attacks is a difficult task.

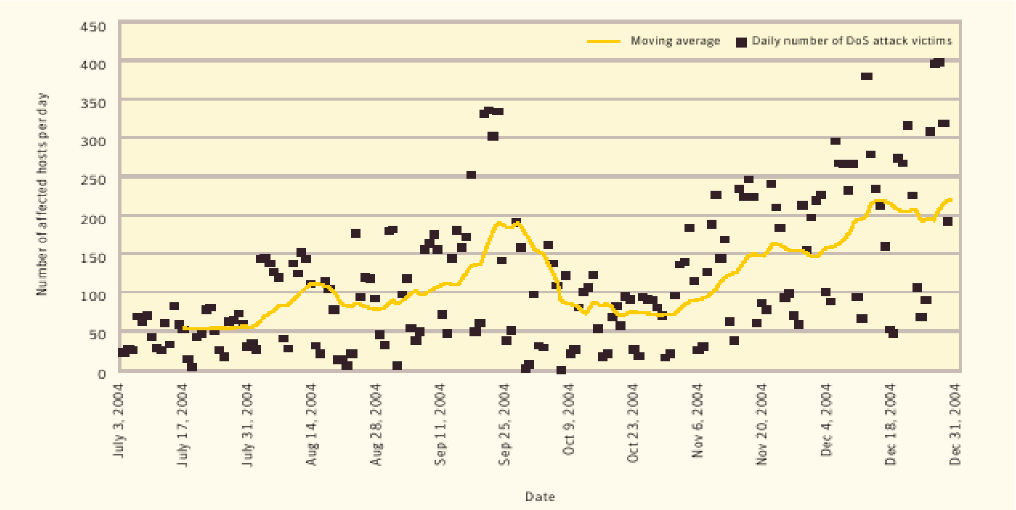

Figure 4: DoS attacks

e. Econom ic cost due to attacks

As of last year, the estimated minimum cost of the impact of high-tech crime on companies based in the U.K. with more than 1,000 employees was £2.45 billion (US$4.61 billion). The results of the yearly survey were announced on the first day of the e-Crimes Congress in London[2].

In the survey of 200 large and medium-size companies, 89 percent said that they had experienced some form of high-tech crime in 2004; of those, 90 percent suffered from unauthorized access to, or penetration of, their company systems, while 89 percent suffered theft of information or data, . Security breaches occurred from outside and, more often, from within a company's system.

Furthermore, 97 percent of all respondents said they had experienced virus attacks in the year, costing £70.8 million, while financial fraud cost 9 percent of respondents £68.2 million[3].

[2] April 2005, National Hi-Tech Crime Unit, London

[3] http://www.infoworld.com/article/05/04/05/HNcybercrime_1.html

f*. Targeted attack activity by industry*

Between July 1st and December 31st, 2004, the financial services industry was the most frequently targeted industry. In fact there is an increase concerning attacks against financial services.

The high tech industry was the second most frequently targeted industry. However, the attractiveness of those organizations to targeted attackers is waning, due to the advanced security systems they use.

Figure 5, illustrates the most frequently types of industries attacked.

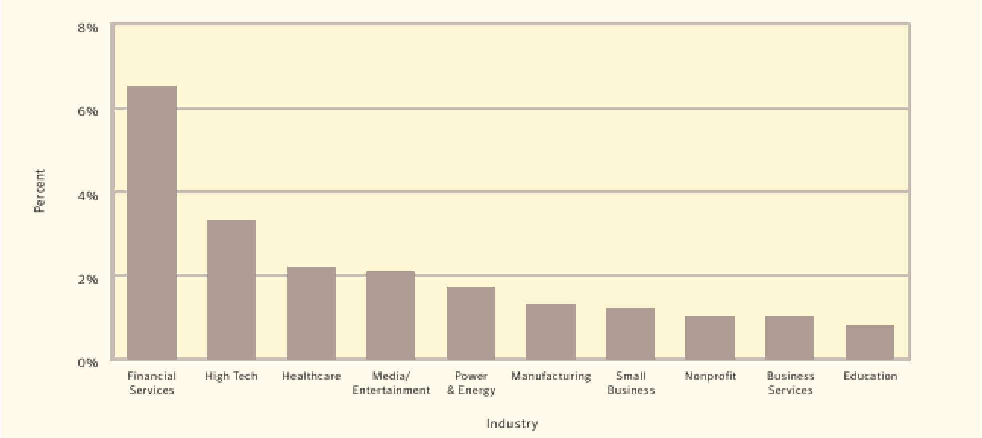

Figure 5: Attacks on industry

g. Attacks on ISP com panies

As the Worldwide ISP Security Report (Arbor Networks Survey, September 2005) mentions, over the 75% of the ISP organizations all over the world, perceive DDoS and worm – intrusion attacks (Figure 6). It is worth noting that the most obvious concern with the worms was not whether the worm itself actually deployed a DoS payload, but with the network congestion and the denial of service they caused.

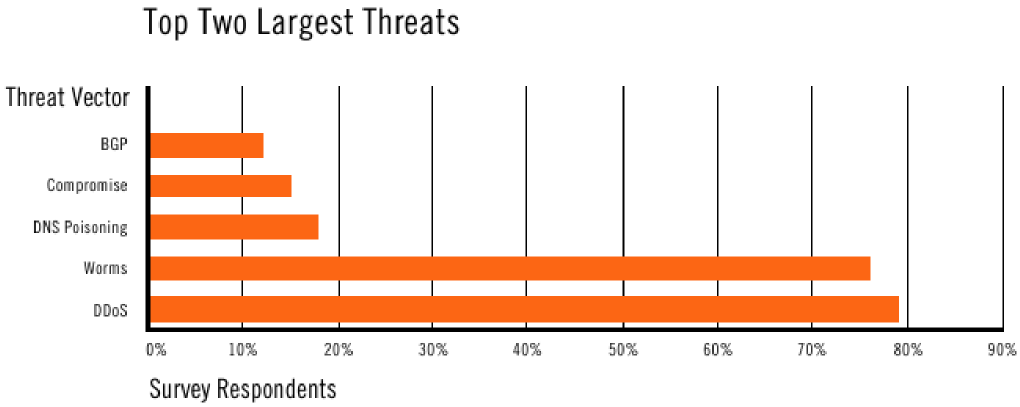

Figure 6: Type of attacks against ISPs

Surprisingly, given the prevalence of these types of attack in recent years, only 29 percent of ISPs offered services to counter and trace DDOS and worm intrusion in an automated way at the ISP level. The majority only discovered such events when a customer contacted them for help or by using commercial flow-based tools (Figure 7).

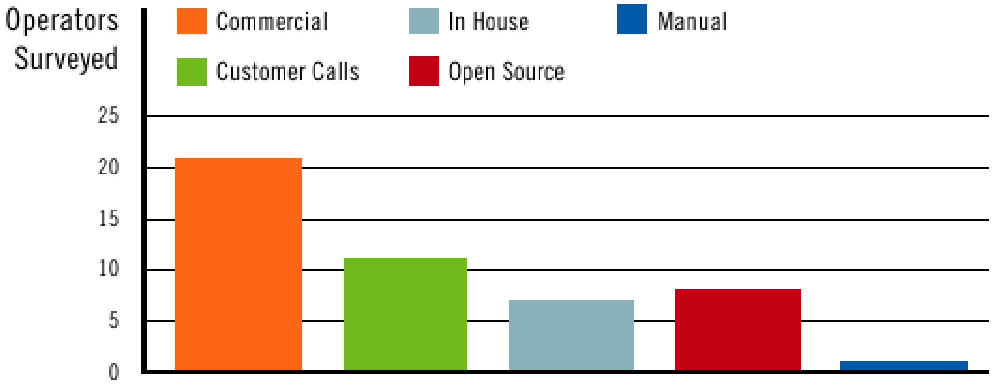

Figure 7: Tools used by ISPs

The conclusion derived from these last two figures, is that the tools used by the ISPs against cyber attacks (mostly Access Lists) are not sufficient enough and that network administrators do need superior detection tools, in order to tackle with all kind of cyber threats.

The overall conclusion derived from the presented statistics is that cyber attacks keep posing a serious threat for organization networks. Besides the well-known threats, attackers have started to invent new ways to attack corporate networks, such as bots and polymorphic virus. What is more, these attacks seem to target various kinds of organizations, trying to cause both network malfunction and economical damage to their victims.

Internet related organizations on the other hand, are facing these new challenges in protecting their network traffic and keeping their productivity at high levels by investing a grate ratio of their budget in research for the development of more efficient detection and traceback tools and infrastructures that will enable network administrators to correspond to the containment of cyber threats and the cleanup of infected costs.

b. Existing defense mechanisms

This section summarizes the security mechanisms that are most commonly used by organizations today, in order to encounter with the various cyber attacks.

I. Network Intrusion Detection Systems (NIDS)

The goal of a Network Intrusions Detection System is to alert the network administrator each time an intruder tries to penetrate to the network. A signature-based NIDS defines penetration via malicious signatures: if an on-going activity matches a signature an alert is raised. Such systems are widely deployed because they are simple to use and provide concrete information about the events that have occurred.

II. Firewalls

A firewall is a software application or a device that filters the information coming through the Internet connection into an organization's network. If an incoming packet is flagged by the filters, it is not allowed through.

Some common methods used by firewalls to control traffic flowing in and out of one's network are packet filtering, proxy service and stateful inspection. Firewalls are not able to recognize attacks or intrusion attempts. They just filter incoming and outgoing network traffic.

III. Traffic Monitoring Systems

Traffic monitoring systems intend to monitor and detect problems with traffic in an organizations network. Monitoring tools are separated in two major categories: active monitoring and passive monitoring tools.

Active monitoring is based on sending probe packets from a sender towards a receiver. Based on the behavior and response to packet probes, the sender is able to infer several performance characteristics of the network.

In passive monitoring systems, there are networks sensors used that capture all packets that pass through the monitored network. Based on the headers and payloads of the captured packets, passive monitors are able to produce a wealth of information including high-level performance metrics, as well as detection of attacks.

IV. Honeypots

Honeypots are computer systems that do not provide any regular production service. Instead, they are intentionally vulnerable and at the same time closely monitored systems, that wait to be compromised by the attackers. Once hit honeypots, can be used to analyze the attack. Therefore, honeypots can be though of as decoy computers: under normal conditions, a honeypot would not receive nor generate any traffic. But, if incoming or outgoing traffic is detected, it means that it is being compromised by an attacker.

c. Security gap of the existing defense mechanisms

Although currently existing security tools offer a very high level of protection, there is still a lot of research ongoing in the field of networks security. The most frequently used tools are anti-virus systems, intrusion detection and prevention systems, firewalls and other traffic monitoring tools for active or passive monitoring. The main drawback of the most of these tools ,that leads to a security gap, is the fact that they react efficiently only in cases of attacks that are already known. When challenged with new type of intrusions, they are not of very much help. What is more, in many of the mention security approaches, human intervention is necessary for issuing the potential attack.

Anti-virus systems, for example, can protect users against known virus, but are usually helpless when confronted with a new type of virus. As a result, despite the fact that almost every Internet user has a different anti-virus installed on their system, they are still vulnerable to newly emerging virus. This fact becomes even more threatening when considering that for the last two years the number of new virus has consecutively grown an average of 40percent per year[4].

The situation is similar for the Intrusion Detection Systems (IDS), as well. Although existing IDS' are able to generate an alert when detecting a known intrusion attempt, they are of little help when a new type of intrusion is introduced. What is more, recent studies show that the number and frequency of intrusions also increase[5] and the time required to cause harm decreases. So it becomes increasingly important to identify intrusions earlier and respond to them quickly. In extreme cases, time frames should be much below than those where human intervention is feasible.

EAR is a new approach introduced for Internet security. Based on the passive monitoring of the underlying network, it can identify strings that belongs to worms, send an alert to network administrators and, in case of a worm that appears for the first time, it can produce a signature for it.

[4] F-secure, “Data Security Summary, January to June 2005”

[5] http://all.net/journal/ntb/ids.html

3. Description of EAR

a. EAR' s structure

The EAR system operates as a network tap and monitor traffic directed from and to a set of local area networks. It inspects the contents of the monitored traffic and detects worms by identifying common substrings. The result of worm detection is the automatic generation of a signature that can be used to block the worm.

The main objectives of the system is to detect previously unknown Internet worms, at the begin of their spread, and also detect them without false positives and without human intervention.

EAR is composed of three major modules:

- Monitor: it implements the main algorithm for the worm detection and the generation of the signature for it,
- Logic: it processes further the alerts issued by the monitor,
- Graphical user interface: provided for the management of the system by administrators. It allows various configurations of the system and provides a list of issued alerts.

An overall view of the EAR' s components, as well as, the way these components communicate with each other, is illustrated in the figure below.

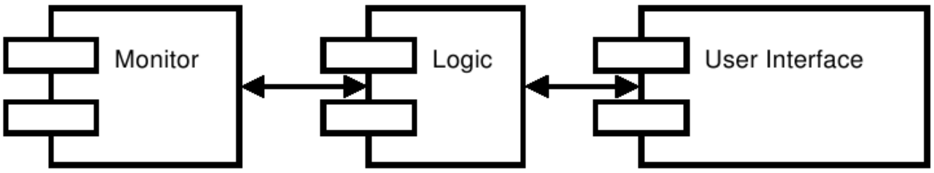

Figure 8: EAR overall structure

This section illustrates the main idea behind EAR' s work: the incoming traffic is monitored and new worms can be detected. Assuming an infected packet is arrived to one's network. This packet will be tapped to a node running EAR. There it will be recognized as a possible threat and an alert will be sent to the network administrator. Additionally, EAR generates automatic signatures for the detected worms.

b. *Installation of EAR*

The figure below illustrates where the EAR system is located in an organization's network.

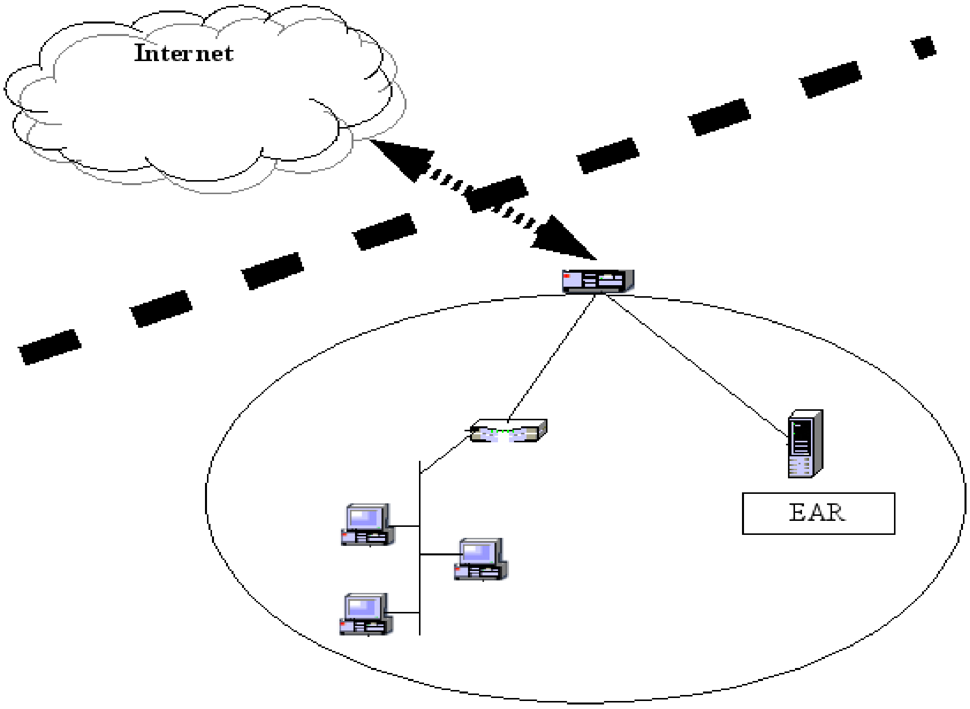

Figure 9: Topology for EAR

EAR is not connected in-line to one's network. It operates as a network tap, processing all traffic visible to its network interface, without introducing any traffic to the network.

c. *How EAR works*

All Internet traffic is tapped to a node which has the EAR system installed on.

Inside the EAR the following processes take place:

1. Firstly the traffic is processed by a flow sampling and load balancing module that picks an appropriate portion of the flows and distributes them to nodes running pre-processing filters.

2. The output of the filters are provided to the main module (which is responsible for detecting possible attacks).

3. If there is an attack detected, the generated signature about it is sent to various other mechanisms, such as: the notification mechanism for notifying the administrators, a containment mechanism and an alert verification mechanism.

d. Key features of EAR

System's evaluation in a experimental network consisting of almost 150 hosts has shown that the process followed by EAR, aiming at the detection of new threats, is very effective. Most of the detections were done with practically zero false positives and with a detection delay that suggests a 7-14% infection. The detection was sensitive to worms generating collectively at least one attack every 500ms. Furthermore, EAR provides mechanisms that can lead to a further reduction of false positives.

Results has shown that EAR is able of detecting almost all known worms, including stealth worms, and even more it can detect previously unknown worms. Protection against future types of worms, such as polymorphic worms, is also provided.

Finally, it is worth mentioning that human intervention in the process of identifying a new worm is needless. Human interaction with the system is limited in the primary configuration of system's parameters. However, every time a new worm is detected an automatic signature for it, is generated by the system.

Summarizing, the main key features of EAR are:

1. Worm detection with reduced false positives
2. Fast detection of intrusion attempts
3. Detection of previously unknown Internet worms
4. No need for human intervention, in the process of detecting and recognizing a worm.
5. The generation of automatic signatures for the detected worms.

4. Market Analysis

4.1 EAR contribution on Internet security

According to the statistics provided by one of the largest firms in network security area[6] , the current shift towards client-side attacks will result in the use of worms as an initial propagation mechanism for attacks targeting specific vulnerabilities in client-side software. As viruses and worms are excellent ways for client-side attacks to propagate initially it is expected that worms propagating in this way will become more common. This could mean that traditional security mechanisms and procedures will become less effective at protecting networks as a whole. Administrators and end users alike will have to execute extra vigilance to ensure that these new infection vectors are adequately secured.

In times like this, the need for an early warning system that can provide administrators enough time to take urgent action ahead of worm propagation, is more than necessary. Research in automated defense systems for Internet-wide attacks is currently focused on: 1) large-scale monitoring infrastructures, such as network telescopes and honeynets; 2) intrusion detection approaches, such as memory tainting, network anomaly detection; 3) automated defense strategies, such as signature generation distribution; and 4) identification and analysis of future threats, such as obfuscation methods and novel spreading techniques.

EAR 's contribution in the overall network security can be focused in the early detection of potential threats. EAR 's ability to detect previously unknown threats and automatically produce signatures for them, can be of great importance to network administrators. They will be able to tackle with the rising threats in time, before they become a major problem or create widespread damage.

What is more, as attacks are becoming more and more complex, EAR 's results can be useful in understanding attacker's sophistication and methods. These results may also contribute to the development of new more powerful network defense mechanisms. A step towards this direction, is the ability of EAR to detect stealth and polymorphic worms. Detecting such threats will provide valuable feedback on the design and the operation of those types of worms, and will help administrators and researchers understand their complex structure.

[6] Symantec Corp. http://www.symantec.com

4.2 Internet Security Market Analysis

Statistics presented in section 2, clearly indicate that cyber attacks are still a major threat for organizations using the Internet. The overall number of attacks per day keeps increasing and the types of attacks vary: viruses, worms, bots and DoS are the most frequently detected attacks. According to F-Secure reports, viruses is a “done deal” for the Internet. Despite the incredible number of viruses spread every day, the existing security systems seems to correspond well with them. However, as stated in previous sections, things look more difficult in the cases of intrusion attempts and DDoS attacks. New threats are continually emerging and traditional security tools cannot efficiently face them.

Statistics in section 2 also indicate that security attacks are not only targeting technology industries. In fact, the financial industry seems to be in great danger as the attacks against such industries are becoming very often. ISP companies and generally high technology industries also face increased danger from cyber attacks.

Taking into account the above metrics, it is clear that early warning systems like EAR will consume a serious ratio of organization's budget in the future. The cost for installing EAR in one's network can be estimated by adding the costs of the required software and hardware: The EAR system is developed and deployed on Linux operation system running on x86 machines. It is under the GPL agreement and it will be available both in a binary format (standalone application) and as source code, as well. This makes EAR system extend able , as it will be possible for anyone interested to perform any customizations necessary, in order to cover their security needs more efficiently. What is more, EAR can become part of other more generic security systems, developed by third parties, and in that way contribute in Internet security. For the proper operation of the system, a preferably dedicated host with a CPU approximately at 2.6 GHz and 1GB RAM is needed. Additionally, a sensor for monitoring traffic is also need. This hardware requirements keeps the cost of EAR in relatively low levels.

In fact, it is estimated, that installing multiple EAR nodes across FORTHnet' s network, will cost much less than current commercial security tools used. This fact makes EAR a very competitive product in the network security market, since it provides high quality of service (very encouraging results on attacks attempts) with relatively low cost.

4.3 Exploitation opportunities for EAR

a. Integration in FORTHnet' s Network Security Services

FORTHnet S.A, as one of the leading ISP companies in Greece, is greatly interested in the use of new security tools that will gradually contribute to the improvement of the Internet services provided to their customers. FORTHnet' s interest, is focused both on the protection of its backbone network against potential intruders and the development of new security services for their customers, in order to provide a smooth functioning at their network and a safer Internet use.

The possibility for exploitation of a security mechanism, such as EAR, that automatically and trustful detects attacks at early stages of their spread, seems very attractive for FORTHnet. Such a pioneer security mechanism, can easily be integrated in FORTHnet' s network services, and in collaboration with the existing/traditional security tools used, strengthen the backbone network and make it more difficult for intruders to force.

Considering the results of its evaluation, EAR can be used by FORTHnet for achieving the following targets:

1. protection of FORTHnet' s network infrastructure.
2. development of a new security service, that will be provided to FORTHnet' s customers and will contribute to the protection of their systems against potential cyber threats.

EAR' s usage for the protection of FORTHnet' s infrastructure, is applied in the installation of several EAR-nodes across its network, that will monitor all network traffic and, as soon as an attack is detected will instantly alert system administrators. Such monitoring hosts, can be deployed all over FORTHnet' s backbone network (Figure 10) in properly selected spots, such as the entry-points of the Internet traffic in data-centers, or next to backbone routers. Such possible point for EAR installation are mentioned in Table 1. It is worth pointing out, that the profit gained from such a security infrastructure is not limited inside FORTHnet but, on the contrary, it is extended to the overall Internet community. The acquired results, published through FORTHnet' s portal can contribute to the reduction of an attack' s scope, especially in the case of newly emerging threats (e.g. polymorphic worms).

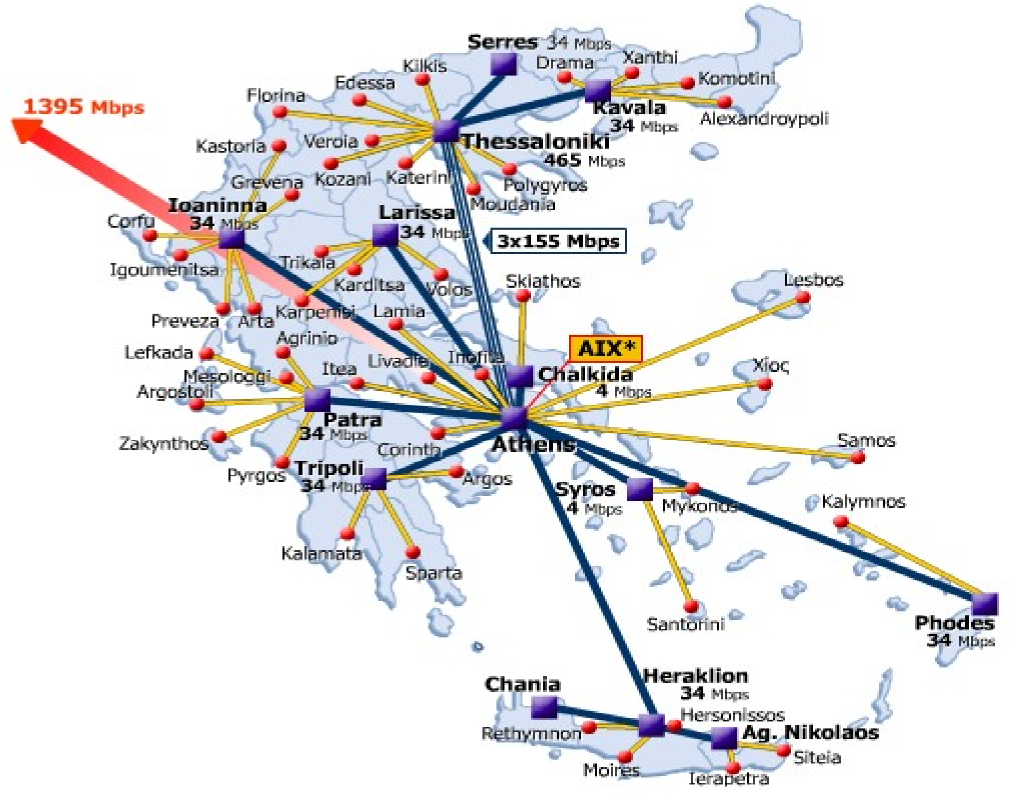

Figure 10: FORTHnet 's network

Site	Description
Athens	Interchange point with UUnet
Athens	Interchange point with Seabone
Athens	Interchange point with Greek ISPs (AIX)
Athens	DataCenter (Kalithea)
Athens	DataCenter (Hilton)
Ag. Stefanos	DataCenter
Thessalonikh	Backbone link with Athens
Heraklion	Backbone link with Athens

Table 1: Possible sites for EAR installation in FORTHnet' s Network

The cost of such an undertaking is not prohibitive. On the contrary, it is affordable and maybe even more economical than currently used solutions. Taking into account that the EAR system can be installed on a Linux server running a CPU at approximately 2.6 GHZ, with 1 GB RAM, it can be easily concluded that the cost for the deployment of such nodes across FORTHnet' s network, will be of order of certain thousand euros. With some off-hand calculations, the estimated cost will not exceed the 1500 euros. Considering both the amount of money spent by companies on traditional security mechanisms (e.g. antivirus systems and firewalls) and the money that will be saved due to the early detection of attacks, this cost becomes even more acceptable.

The low cost for EAR installation can become even more clear through a comparison with another widely used security mechanism, a firewall. In this example we refer to the CISCO PIX 525 firewall[7]. Even though EAR and CISCO PIX 525 do provide some similar functionality (e.g. detection of known worms and virus), they are still not directly comparable with each other, due to the different functionality each one provides: a firewall might be able to perform more actions, like applying access lists (ACLs) based on IP subnet. The EAR system on the other hand, is able to detect and produce a signature for a new emerging worm. Despite these differences, a cost comparison is still possible. So, for the needs of a specific project, FORTHnet has purchased and installed the CISCO PIX 525 firewall. The total cost for the purchase was about 11.500 euros and was installed only in one instance. The person months spent for the installation and the configuration of the firewall, which consists a quite painful and time consuming process, is not included. So, given that the estimated cost for the installation of a single EAR node is about 1500 euros, it is easily concluded that with the amount of money spent for the installation of one CISCO firewall, the installation of 8 EAR nodes would be possible. Obviously, eight (8) EAR-nodes can monitor a larger portion of a network than a single firewall.

The EAR system can very easily become a component of the on - line security service provided to FORTHnet' s Internet users, at low cost for them. FORTHnet, through the on-line “My Security” service, which includes existing security tools that covers many aspects of Internet security (anti-spams, anti-virus, etc), is currently providing to their subscribers as much safety in their Internet transactions and navigation as possible and a way to protect against various kinds of cyber threats. EAR seems to fit excellent in such a bundle of security services. Although, the direct economical benefit from an infrastructure like this may not be very high, there is a significant indirect profit for the company. It provides added value to the existing services, like dial-up, ADSL etc, it increases the public confidence in FORTHnet, it grows company's prestige and finally leads to the improvement of sales of company' s products and services.

It is worth pointing out that EAR' s technical specifications alone, make it a competitive software product, very attractive to Internet users. Its potential installation on customer' s systems, will be approved beneficial for them, especially for corporate customers. It will allow them to easily filter their Internet traffic and respond immediately in case of an alert regarding an outsider' s attempt to compromise their system. In this way, their Internet safety feeling will be increased and they will navigate even more fearlessly through the Internet.

[7]. http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2118/

The promising safety potentialities it provides, combined with the low installation cost (there is no cost for the acquisition of a user license, since EAR is under the GPL license), along with the fact that is constitutes a pioneer software product, safely lead to the conclusion that it can easily and shortly be established in the Internet security products market. What is more, EAR' s promotion by FORTHnet can be direct and at low cost. There are various ways it can be achieved. Firstly, the presence of the product in an Internet portal with hundreds of visitors every day, constitutes a major promotion of the product and the technology it represents. Another alternative for the promotion is by sending an informative e-mail to all FORTHnet' s subscribers or even the incorporation of an informative booklet in the accounts sent to them by standard mail. In this relatively simple ways, EAR' s existence can be propagated in the Internet community. Taking into account the piece of market it possesses, combined with the confidence that FORTHnet offers to the consumers, the results of a potential promotion of EAR system through FORTHnet' s marketing mechanisms, are expected to be ensured.

b. Target group for EAR.

Besides EAR' s exploitation by FORTHnet and its customers, many other can also benefit from its capabilities. An EAR – based system, seems to be helpful for all the organizations and enterprises that own a large scale network. An example of such enterprises are the financial industries (banking sector). Their primary interest in the network security and the electronic transactions, can very easily be combined with the spread of use of EAR: the installation of the EAR system on selected nodes across a bank's network, may be proved very useful for the safety of their transactions. Potential intrusion attempts, will be detected directly and will be immediately confronted. Thus, the danger of a wide scale damage is considerably reduced. It is worth pointing out that the potential cost of such a damage is very likely to be multiple than the cost of installing EAR in their network.

Another sector that may benefit from using EAR, is the telecommunications area. All telecommunication services providers would like their services to be of a quality, as higher as possible. For these organizations, a high quality of services is translated in the increase of their customers hence in the increase of their profits. The EAR system can considerably contribute in the achievement of high quality services. As in the case of FORTHnet mentioned earlier, it can be used by the telecommunication enterprises for the monitoring of their network and the protection of their network infrastructures against various kinds of cyber attacks. The prevention of their network infrastructure that is achieved in this way, leads to the offer of better quality services to their customers. Therefore, in this case, the installation of EAR is more an investment for these organizations.

Finally, the EAR system can be used by various research organizations and universities. In fact, due to the low cost of its installation, it seems ideal for these organizations, since, apart the security, it will also provide them with data that will eventually lead them to precious conclusions concerning the overall Internet security. What is more, the fact that EAR is under the GPL license, gives them the opportunity to widely use it and even modify it properly, in order to extend its capabilities so as to be able to detect even more cyber threats than those it can currently detect.

An important issue for the usage of EAR by the organizations and enterprises mentioned above, is its initial installation and parameterization, so as it better corresponds to the various requirements of each organization. The EAR system can be provided either as source code or as a standalone application (binary format). In the later case, the existence of a support service for potential users, might be necessary. For example, for the proper operation of EAR in a banking environment, the necessary steps are : a) its installation in the bank's network, b) system' s initial parameterization, so as to react to certain type of attacks and c) the education of the personnel that will interact with the system and accept the messages it generates. The organization that will lead the EAR' s promotion campaign (FORTH, FORTHnet or other), should be able to provide this kind of support. A first estimate for the promotion of the EAR product, is that it requires low human and financial resources, however, it will eventually become of great profit for the organization responsible for the promotion.

4.4 Intellectual property and copyrights.

The primary license in use by the EAR Project, the GNU GPL, relies on the basic framework of copyright to provide for enforcement of its freedoms. Nearly all of the sample code, documentation, header files, and reference material available about the EAR system is subject to some form of copyright: developers maintain their copyright in the developed source code, but license that code under the GPL for the use by others.

The following table lists all the constituent components of the EAR system, their ownership details and proposed licensing policy:

Module	*Developer*	*Proposed License*
EAR	FORTH	GPL
STRIDE	FORTH	GPL

5. Summary

The state of the art in the network security area declares that there is a imperious need for superior detection and traceback security mechanisms in order to enable infected host containment and cleanup. The sooner an attack is detected and confronted with, the lower the potential damage it may cause. Attackers tend to invent new ways in order to attack corporate networks and cause the bigger damage possible. Traditional security mechanisms seem to be insufficient in cases of emerging cyber threats.

The EAR system is a step towards achieving a more effective and complete approach to networks security. It constitutes an early warning mechanism that aims to provide systems administrators a valuable tool in their demand for better security. Based on passive monitoring of the underlying network it can identify strings that belongs to worms, send an alert to network administrators and, in case of a worm that appears for the first time, it can produce a signature for it. What is more, evaluation metrics shows that EAR system is very reliable and trustworthy, as the false positives rate is very low, practically zero.

These unique features of EAR makes it a viable solution and its introduction in the market is predicted to be smooth. There are significant exploitation opportunities for such a system. The business cases studied in this document clearly show that EAR may contribute not just to the security of a single organization's network infrastructure but to the overall Internet security, as well.

References

[1]. Symantec, Symantec Internet Security Threat Report, Volume VIII, March 2005

[2]. Arbor NetWorks, WorldWide ISP Security Report, September 2005

[3]. F-secure, “Data Security Summary, January to June 2005”, September 2005

[4]. Symantec Corp., http://www.symantec.com/index.htm

[5]. F-Secure, http://www.f-secure.com

[6]. e-Crimes Congress April 2005, National Hi-Tech Crime Unit, London

[7]. http://www.infoworld.com/article/05/04/05/HNcybercrime_1.html

[8]. http://all.net/journal/ntb/ids.html

[9]. http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/ps2118/

[10]. www.forthnet.gr

[11]. www.uunet.net

[12]. www.seabone.net