Measuring the Internet’s Threat Level: A Global–Local Approach

Spyridon Kollias*, Vasileios Vlachos†, Alexandros Papanikolaou†, Periklis Chatzimisios‡, Christos Ilioudis‡, and Kostas Metaxiotis*

*Department of Informatics
University of Piraeus, Greece
Email: spyridon.kollias@gmail.com, kmetax@unipi.gr

†Department of Computer Science and Engineering
Technological Educational Institute of Thessaly, Larissa, Greece
Email: vsvlachos@teilar.gr, alxpapanikolaou@gmail.com

‡Department of Information Technology
Alexander Technological Educational Institute of Thessaloniki, Greece
Email: {peris, iliou}@it.teithe.gr

Abstract—The Internet is a highly distributed and complex system consisting of billion devices and has become the field of various kinds of conflicts during the last two decades. As a matter of fact, various actors utilise the Internet for illicit purposes, such as for performing Distributed Denial of Service Attacks (DDoS) and for spreading various types of aggressive malware. Despite the fact that numerous services provide information regarding the threat level of the Internet, they are mostly based on information acquired by their sensors or on offline statistical sampling of various security applications (antivirus software, intrusion detection systems etc.). This paper presents PROTOS (PROactive Threat Observatory System), an early warning system which is capable of estimating the threat level across the Internet, using both a global and a local approach. The proposed system is therefore able to determine whether a specific host is under an imminent threat, as well as to provide an estimation of the malicious activity across the Internet.

I. INTRODUCTION

The evolution of the Internet has given birth to novel services that utilise it and offer to individuals a better experience, in an attempt to improve the quality of their everyday lives. One of the current goals the scientific community is trying to achieve is the realisation of the so-called “Internet of Things” (IoT), where ideally all everyday physical objects, animals or people will be connected to the Internet and be able to uniquely identify themselves to other devices. They will further be expected to communicate among themselves and exchange data, thus taking active part in business, information and social processes.

Having a continuous connection to the Internet poses several security issues, since the attack surface increases alongside with the number of connected devices and, given the heterogeneity among such devices, one should therefore expect the simultaneous existence of multiple exploits. Recent real-world examples of “malicious” clothes irons [1], kettles [1] and fridges [2] demonstrate that such exploitation scenarios no longer belong to science fiction and should be taken into serious consideration. What is more, the wide range of personal electronic devices featuring internet connectivity, once compromised, can also become sources of valuable private information, apart from becoming members of a wider botnet. Given the continually-increasing availability of public WiFi hotspots (others having insufficient security mechanisms and others none at all) and the increased use of various Internet services (e.g. social networking, web surfing), the chances for an individual to fall victim of such attacks are significant. What is more, in areas featuring a large population of devices with Internet connectivity, their malicious exploitation may also have a significant impact on the local network’s normal operation (consumption of bandwidth, triggering of alarms and so on).

One way for dealing with such threats in a generic form, would be to evaluate the malicious activity of a network by examining the nodes’ firewall log files (wherever this is feasible) and send this information to a central processing server, in order to obtain a “global view” of the threat landscape. As soon as an increase in the global malicious activity is detected, the server will inform the member nodes to tighten their security settings, in order to protect themselves. This paper presents the architecture of one such scheme, as well as some results from an initial, small-scale experimental deployment.

The paper is organised as follows: Section II presents some related work. A high-level description of the system’s architecture is presented in Sec. III. Some initial results from the system’s experimental operation are presented in Sec. IV. Certain issues that have been identified and are expected to be dealt with in the future are presented in Sec. V and the paper concludes in Sec. VI.

II. RELATED WORK

A sufficient amount of sensors is required for systems like PROTOS for measuring the threat level with an acceptable
accuracy. Several frameworks for distributed detection have already been proposed, but none of them features a large-scale installation. One such example is the work in [3], where the authors propose algorithms for the early detection of the presence of Internet worms, by using a suitable Kalman filter on the monitored illegitimate traffic. Their results demonstrate that their algorithms are able to detect worms at the early stages of their life, while the infection rate is still quite low (1% - 2% of the vulnerable computers), as well as to give effective predictions of the number of vulnerable hosts. The architecture of a distributed intrusion detection system (DIDS) presented in [4] combines distributed monitoring of individual hosts with centralised data analysis, in order to be able to monitor heterogeneous systems. Each host is assigned a user ID (comprising, among others, a host ID) to facilitate monitoring, although more work is required on connecting instances of the same user in a networked environment, should the user leave the monitored domain and then comes back in with a different user ID. The system proposed in [5] operates by analysing network traffic characteristics and tries to detect patterns that denote the presence of a worm (e.g. highly repetitive packet content) and automatically generates content signatures. When tested on a small network, the scheme featured a low percentage of false positives. Similarly, the authors in [6] collect ICMP Unreachable messages from selected network routers and analyse them to identify patterns indicating malicious scanning activity and patterns that can identify a propagating worm. The proposed system is tested in a simulated environment, so as to assess its performance. Some variants of PROTOS tailored for different topologies are also in operation. They mainly follow either peer-to-peer or other decentralised topologies [7], [8]. Well-known security vendors provide such worm detection services to their users, with Symantec’s DeepSight [9] being perhaps the most famous system. Similar to that but focused on network hardware, Cisco has developed IronPort [10], which takes into consideration numerous parameters, in order to opine if a node of a network is secure or not. Both systems operate under commercial license. More specifically, DeepSight has a pricing plan which cannot be ignored and IronPort demands the presence of Cisco network hardware. However, these two systems cannot be adopted from individuals, small or medium companies. Nowadays, even large companies are reluctant to invest on such systems. Finally, DShield [11] is a well known system with more than 500,000 IP addresses measuring for current threat level.

III. ARCHITECTURE

A. High-Level Overview

The system PROTOS consists of different software and hardware layers. An overview of the system’s architecture is presented in Fig. 1. The most important and critical part of the whole system is the PROTOS Sensor, which is vital for obtaining an accurate measurement of the global threat level. The more the sensors, the better the accuracy will be. Although there are no any significant challenges from a software point of view, the whole system demands for a satisfactory amount of individual sensors. It can be installed to a wide range of computers, ranging from an average PC to a mainframe server. The sensors that are installed on systems with public IP addresses provide more accurate information about the “global” threat level; systems that are behind a NAT can provide significant information for the internal network ecosystem. This kind of intelligence can be utilised from administrators to realise any inside threat.

Another critical system is the PROTOS Server, which is responsible for collecting and aggregating the intelligence received by its sensors and the corporate internal servers. PROTOS Server must feature high availability to receive the information provided by its collateral systems on a 24/7 basis, without any interruptions. Apart from the reception system, the server’s hardware must be powerful and optimised to run small, yet intensive, tasks in little time.

Additionally, a sync subsystem between corporate servers with PROTOS Server instance and the main PROTOS Server instance must be installed, in order to have almost real-time synchronisation regarding the collected information from internal corporate hosts.

Last but not least, two supervisory subsystems will be implemented: A cross-platform desktop application, as well as a web application, in which all the aggregated intelligence will be depicted in an intuitive GUI.

B. Measuring the Malicious Activity

The typical operation of a PROTOS sensor is as follows: It checks the firewall log file every 30 seconds and calculates the number of the intercepted attacks in the form of dropped/denied packets. By using Equations (1) and (2) it estimates the rate of the locally-intercepted malicious activity and the epidemic rate, respectively. In these equations, \( t \) is the ordinal number of a fixed time interval, \( n \) is the client identifier, \( h^n \) is the number of security incidents received by node \( n \) in the time interval \( t \). The “time window” used in a number of \( t \) time intervals is \( k, k \in (0, t - 1) \).

\[
p^n_t = \frac{h^n - \sum_{k=1}^{\infty} h^n_{t-k}}{k} \quad (1)
\]

\[
q^n_t = \frac{p^n_t - \sum_{k=1}^{\infty} p^n_{t-k}}{k} \quad (2)
\]

Thereafter, the sensor transmits this information to the server, which computes the global malicious activity, based on Equation 3.

\[
p_{avg} = \frac{\sum_{t=1}^{n} p^n_t}{n} \quad (3)
\]

Should the calculated estimate of the global malicious activity exceed a predefined upper threshold, the server instructs the sensors to increase their security level by applying a set of predefined countermeasures. Similarly, if the global malicious activity drops under the lower threshold, the sensors loosen their security settings and resume their normal operation.
IV. EXPERIMENTAL OPERATION

The system, in its current form, is operational and the basic functions have been implemented. The service modules are working on a 24/7 basis without creating any critical issues. The PROTOS client has been installed in a small number of workstations and some initial data has been gathered. PROTOS is available for both 32-bit and 64-bit of Microsoft Windows OS, as well as for Linux and Mac OS X. There is work in progress on developing a secure update mechanism for the respective client. The system’s scalability has also been assessed in a laboratory environment, by using simulated data.

The PROTOS system was initially put into operation on 4 April 2013 and currently has more than 230 unique clients connected to it. Of course, not all of them are concurrently in operation; an initial statistical analysis showed that a few decades of sensors are usually transmitting data to the server at any given instance. The sensors’ scope is currently limited to the Greek cyberspace, as they have been deployed in three major Greek cities (Athens, Patras and Larissa). It is expected that the geographical coverage will increase soon, as several users have already opted for participating.

As far as the system’s performance is concerned, the CPU load is mainly observed for the various database-related (MySQL) tasks. The database server is responsible for:

- Inserting the received data whenever they arrive from the sensors. Hence, the more the sensors, the higher the load. At the same time, the table columns containing each record’s timestamp are indexed.
- Processing the aggregated intelligence of the last 30 seconds, for each user observing the live plot, either from the web site or the local client (the so-called “Universal Client”).
- Processing intelligence on demand (currently under development).
- Calculating the aggregate intelligence by running a scheduled task every 30 seconds.

Hence, within the aforementioned context, the observed peak CPU load of the database server daemon was 45%. Given that the server of this experimental operation is a Virtual Machine (VM) on quite old hardware, we are confident that running it on suitable, high-performance hardware it should be able to support an order of 100K sensors.

The system modules of PROTOS have shown that they are not inducing any significant overhead to the overall performance of the clients. PROTOS Sensor will be capable of running on systems with low-end hardware specifications, varying from netbooks to cheap laptops. The client has also been successfully deployed on a Raspberry Pi host (bearing an ARM CPU), running Ubuntu Linux as an indicative example of a non-x86 architecture. A number of available platforms are been currently evaluated, but the fact that several popular Linux distributions already support the ARM architecture significantly simplifies the implementation on ARM-equipped sensors. As has already been mentioned, PROTOS supports a variety of additional operating systems as well (e.g. Mac OS X, Linux), although it is currently dependent on their native firewall. A full evaluation of the prototype system has been planned for the near future, in terms of scalability and overhead of both the server and the client. It will also be investigated whether individual and corporate users are willing to use PROTOS with a software firewall other than the operating system’s native firewall.

Figure 2 demonstrates the intercepted activity over a 3-hour-long period on 3 February 2014. In particular, the time series depicts the number of blocked packets, as they have been recorded in 30-second-long intervals. In a local network there may be certain devices (e.g. broadcast packets from printers) or applications (e.g. file syncing) that tend to send broadcast packets. Since such packets get blocked by the hosts’ firewalls, any sensors installed on them will report some “malicious activity”, represented by the short periodic peaks. Using this information, the server calculated both the malicious activity and the epidemic rate for the given period of time, which are exhibited in Fig. 3. It is worth clarifying that, due to the order the calculations are performed, an observed peak in the number
of blocked packets within the time interval \( t \) will appear in the malicious activity graph at \( t+1 \) and in the epidemic rate graph at \( t+2 \).

V. Future Work

The functionality of PROTOS depends on the analysis of firewall log files, a task that its sensors perform for each host they are installed on. Nevertheless, there are cases where certain devices do not offer any sort of firewall functionality (e.g. smartphones and more “primitive” resource-constrained devices), as well as cases where access to the firewall log file is only possible by obtaining administrative access to the device, without having explicit functions for it (e.g. broadband modem/routers for home or office use). Therefore, one of the future tasks will involve the development of a firewall application for popular smartphone operating systems (e.g. Android, iOS), able to run transparently in the background whenever Internet access is enabled, so that its log file can be exploited by a suitable PROTOS sensor application. In addition, efficient and secure ways for gaining access to firewall log files produced by e.g. home broadband modem/routers should be investigated, where one of the greatest challenges is the diversity in both the functionality and characteristics of said devices.

Another issue worth investigating is the way information and control messages are communicated between the server and its sensors, in order to ensure maximum compatibility with different communication protocols, especially those for resource-constrained devices. For instance, if XML or SOAP messages are to be used, they will have to be carefully crafted, so as to ensure compatibility with the more resource-constrained versions of the standards, such as the Constrained Application Protocol – CoAP (a lightweight version of SOAP over CoAP was recently proposed in [12]). Although it may not always be possible for resource-constrained devices to offer PROTOS-sensor-like functionality, they could still benefit from the system’s warning messages. In turn, the applicability of suitable mechanisms for ensuring both the integrity and the authenticity of the transmitted data will be investigated, such as digital signatures and hash functions.

As has already been mentioned, the PROTOS system requires a server, responsible for communicating with its sensors. Since a world-wide installation of a single server does not seem a plausible task, having multiple such servers, each one responsible for a given “reign” is a possible solution (similar to the way multiple Kerberos systems can be configured to cooperate among them [13]). In turn, this raises issues of how the borders of these “reigns” will be defined, how communication among different “reigns” will be performed, what kind of information will it contain and so on.

Most of the past research has put significant efforts into developing large-scale Intrusion Detection Systems (IDS) and their successors, Intrusion Prevention Systems (IPS). The importance of detection and prevention is definitely necessary, however, as the number of the interconnected devices rises, the development of global services that monitor the threat level across the Internet is equally important. Most of the IDS/IPS system aim at protecting small- to medium-sized networks by acquiring and analysing large amounts of data of the hosts they supervise, in order to detect malicious activity. The idea of the PROTOS is based on the fundamentals of crowdsourcing intelligence which has been employed for solving various difficult problems. The first versions of the PROTOS system utilise well-known and widely-accepted epidemiological models which have been proved effective against biological as well as computer viruses, over the past years. The introduction of statistical forecasting models is currently under evaluation in order to obtain more accurate predictions of imminent threats. Theoretical research and empirical findings have proved that the available reaction timeframe against ultra-virulent malware and other threats cannot be achieved using the existing methods.

In order to improve the effectiveness of the system, work is in progress on developing a forecasting subsystem whose task will be to predict imminent epidemics and threats, rather than reacting only when a threat has been characterised as being a possible epidemic. However, in order for such a forecasting system to be effective, it needs to be trained with quite a large set of traffic data. Some indicative statistical models that are suitable for this purpose are the AutoRegressive Integrated Moving Average model (ARIMA) [14] for predicting malicious activity rate, General AutoRegressive Conditional Heteroskedasticity model (GARCH) [14] for predicting volatility of crowdsourcing intelligence which has been employed for solving various difficult problems. The first versions of the PROTOS system utilise well-known and widely-accepted epidemiological models which have been proved effective against biological as well as computer viruses, over the past years. The introduction of statistical forecasting models is currently under evaluation in order to obtain more accurate predictions of imminent threats. Theoretical research and empirical findings have proved that the available reaction timeframe against ultra-virulent malware and other threats cannot be achieved using the existing methods.

In order to improve the effectiveness of the system, work is in progress on developing a forecasting subsystem whose task will be to predict imminent epidemics and threats, rather than reacting only when a threat has been characterised as being a possible epidemic. However, in order for such a forecasting system to be effective, it needs to be trained with quite a large set of traffic data. Some indicative statistical models that are suitable for this purpose are the AutoRegressive Integrated Moving Average model (ARIMA) [14] for predicting malicious activity rate, General AutoRegressive Conditional Heteroskedasticity model (GARCH) [14] for predicting volatility of crowdsourcing intelligence which has been employed for solving various difficult problems. The first versions of the PROTOS system utilise well-known and widely-accepted epidemiological models which have been proved effective against biological as well as computer viruses, over the past years. The introduction of statistical forecasting models is currently under evaluation in order to obtain more accurate predictions of imminent threats. Theoretical research and empirical findings have proved that the available reaction timeframe against ultra-virulent malware and other threats cannot be achieved using the existing methods.

The scientific community is progressing at a fast pace towards the realisation of the Internet of Things (IoT), where everyday objects will bear electronic communication devices and will take actively part in everyday processes. At the same time, malevolent hackers devise highly-sophisticated ways of exploiting such devices for illicit purposes, the effects of which usually include both a significant world-wide impact and a small margin for reaction. The good quality of the provided Internet services is also affected by the degree to which malicious activity is successfully detected and contained, since any kind of problematic behaviour in an IoT world will directly impact our everyday lives.

A proactive system able to deal with such kinds of threats was presented in this paper. A central server analyses data regarding malicious activity submitted to it by sensors installed on multiple hosts and it then calculates the threat level, both at a local and global level. The system is currently in experimental operation and the obtained results are rather encouraging. Future work will deal with several open issues that have to be resolved in order for the system to be able to support a wider range of heterogeneous devices, as well as with the investigation of suitable forecasting methods, in an attempt to strengthen the system’s effectiveness.

REFERENCES

Fig. 2. Number of blocked packets in 30-second-long intervals on a given date.

Fig. 3. Calculated malicious activity and epidemic rate on a given date.


