International Journal of Security and Its Applications
Vol. 3, No. 3, July, 2009

Security Services in the Greek School Network

Michael N. Kalochristianakis[1, 2], Michael Paraskevas[1], and Emmanouel A. Varvarigos[1, 2]
[1]*Research Academic Computer Technology Institute and*
[2]*University of Patras, Dept. of Computer Engineering & Informatics*
Rion Patras, 26500, Greece
manos@ceid.upatras.gr

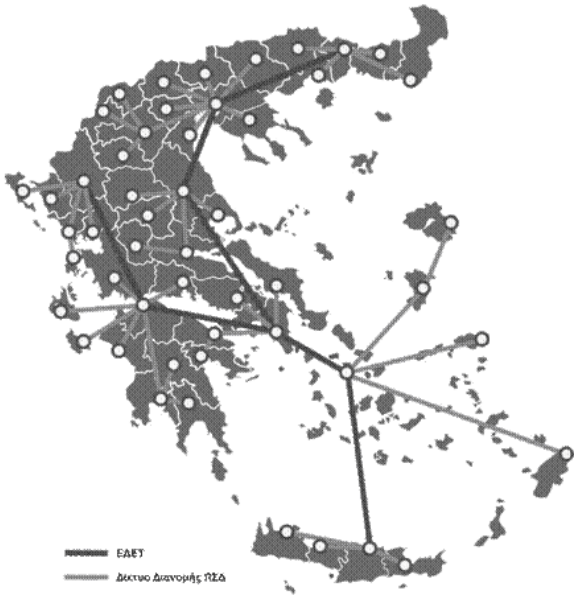
Abstract

The Greek School Network (GSN) is a closed educational network that offers advanced telematic and networking services to all primary/secondary education schools and educational administration offices in Greece. The primary objective of GSN is to provide a network infrastructure for the interconnection of school PC laboratories so that modern educational methods and pedagogical models can be used in the school community securely and effectively. GSN has scaled in size, reached maturity, and is currently delivering a wide range of network and telematic services to students and educators. Being the second largest communications network nationwide, GSN is exposed to all kinds of security threats and, due to its educational hypostasis, naive user behaviour. The current paper presents an evaluation of security management solutions for the enforcement of policies, practices, and user protection methodologies proven viable within the GSN environment, as indicated by statistics and metrics on the use of the related services. The paper reaches the conclusion that GSN security services constitute a sound framework that can successfully cover the needs of the school community.

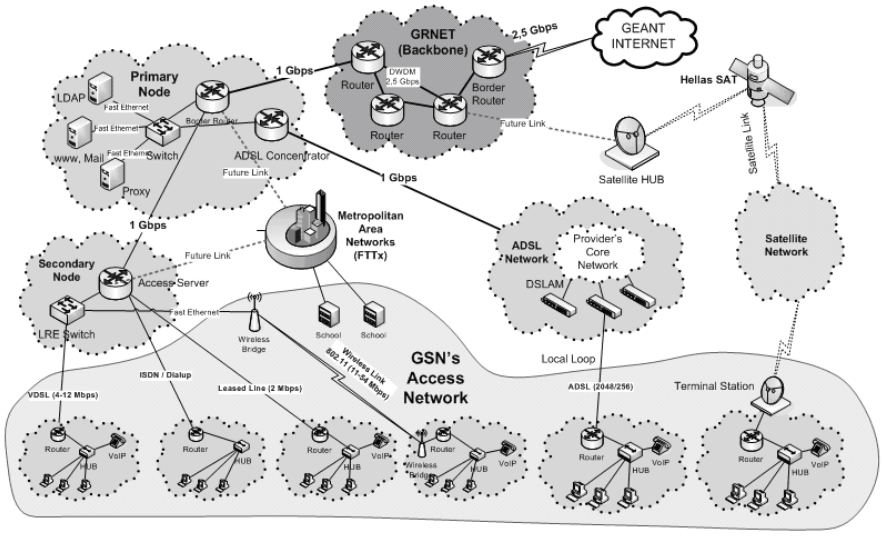
Keywords*: web filtering, anti-spam, anti-virus, educational network, K-12 network*

1. Introduction

The Greek school network (GSN) [1], founded in 1998, constitutes the educational intranet of the Ministry of Education and religious affairs [2]. GSN interlinks all Greek schools and educational administration offices, providing basic and advanced telematic services to students, teachers, and school administrator communities [3]. It has been designed and is maintained by a group of twelve research centers and universities [4], under the directions of the Ministry of Education and religious affairs, and the support of national and European Union (E.U.) funding. Currently, GSN offers a large number of diverse services to 14.142 schools and 2.748 administrative units, serving more than 65.000 teacher accounts [1]. Fig. 1 presents the architecture of the backbone and distribution network layers, while Table 1 summarizes the services offered. GSN plays a substantial role in fulfilling the social-political goals for the diffusion of Internet access and the promotion of modern educational models in the Greek society [5] and has received international best practice awards [6]. GSN must play a multidimensional role; it must continue improving the Internet service to its users, introducing technologically and educationally pioneering and innovative services, while ensuring secure, smooth and uninterrupted operation. To meet its operational goals, GSN is expected to build rigid security infrastructure based on cutting-edge technology and sound policies.



(a)



(b)

Figure 1. GSN architecture, (a) The GSN backbone and distribution networks and (b) The GSN access network

As a service provider of professional and managed services GSN has developed a full range of security services under high-availability requirements. Student protection against exposure to harmful or offensive internet content is of outmost importance for GSN. The adopted policies regarding student's safe access to the Internet and cyber-crime confrontation are enforced via integrated state of the art enterprise systems. Security enforcement is designed to be modular so as to follow international advancements, and adaptable so as to

meet changing legal requirements. Policy enforcement essentially expands to multiple layers, starting from policy application research and development, student sensitizing, press campaigns and educational material preparation and diffusion. GSN has defined the policies and terms of acceptable use for students and schools for safe use of the internet within the scope of pedagogical purposes [7]. GSN contributes to other known efforts in the security area, including the SaferInternet [8] and the Digital Awareness Response Team (DART) [9] projects. To this end, the Ministry of Education has institutionalized proper collective bodies [4] manned with expert scientists, responsible for mapping out policies and for the management of the content that is distributed via the GSN [10]. The services subject to the above policies are the web filtering service, the forums service, the mailing lists and the web hosting service. GSN is also contributing to research and development in techniques and methods for security policy enforcement. GSN has adopted and consolidated on technology and best practices utilized in educational networks internationally and has managed to achieve a satisfactory degree of reliability in its policy enforcement. In sensitive environments, such as pedagogical institutions, policies must not solely be confined within the scope of technical boundaries, but they must also expand to sensitize students in internet e-ethics and electronic society issues. This is a pedagogically sound and highly effective means of policy acceptance and student conformance. GSN reaches students through informative services that diffuse information about its services, and especially those that are related to security. Information is addressed to both students and parents and is delivered through numerous means including the GSN and the students' portals, conferences and educational actions. Last but not least, GSN contributes to the creation of high value, certified pedagogical material.

The rest of the paper discusses broad security policy and specific technical solutions adopted by GSN in order to ensure the required security and trust within the educational network. Section 2 presents an overview of the web filtering, anti-spam, anti-virus and cert services in GSN. Section 3 presents our conclusions and describes GSN future directions related to security.

2. GSN Security Policy

In order to protect assets and infrastructure, GSN employs distributed security schemes and policies, implemented at different network layers. Global policies are enforced on connections whose one end lies outside the GSN network. In this case black listing is employed on the backbone network layer to block out unwanted web traffic. Filtering is performed on clusters of cache-box machines. The rest of GSN services are protected using white listing. The distribution network layer is further protected by access control lists (ACLs) that allow free access to the ports of well known services, disallowing any other traffic. The trusted IP address space, as configured in network active elements, includes only GSN addresses. The GSN security policy is complemented by security oriented services for responses to incidents and services protecting the electronic mail service and the internet services. GSN also employs authentication, authorization and accounting protocols, PKI and key management technologies, secure routing protocols, intrusion detection and prevention.

2.1. Content control service

Protecting schools from abusive, offensive or illegal internet traffic is performed through the web filtering service, provided by GSN since 1999. The service is based on

transparently proxying all internet traffic using the Squid [11] server software and the SquidGuard [12] combined filter, redirector and access controller. As incoming traffic flows into GSN, it is directed through the proxy server where it is filtered before reaching GSN users. Transparent proxying is employed so that it is invisible to users who do not need to declare a proxy server in their browser's configuration and they do not even need to know that one exists. Evidently, the proxy server is the ideal point for both policy enforcement and web filtering [13].

The web filtering service implementation is deployed on a distributed system of 14 island servers located at the backbone network. The nodes are distributed according to traffic requirements at the 7 points where the GSN is interconnected with the national academic network [14], which is the national branch of GEANT [15]. Connection points can be identified in Fig. 1(a); the distribution of the cluster nodes across the seven cross points is 4, 3, 2, 2, and 1, proportionally to traffic volume handled. The cumulative traffic volume through the proxy typically reaches 166 GB/day and the rate of generated requests reaches 13.5 millions per minute. Web filtering rejects 2.56% of these requests that is, about 345 thousands per minute. Related statistical data are presented in Table 2. Tables 4 present the same data for the year 2005. In 2005, the cumulative traffic volume through the proxy typically reached 85 GB/day and the rate of generated requests reached 8.5 millions per minute. Web filtering rejected 1.67% of these requests, about 140 thousands per minute. The adoption of the open source solution for the web filtering service has been fully justified by the operational results obtained, availability, performance, and, of course, cost [16].

If a user attempts to access a banned web page, the web server response traffic will be rejected by the proxy, and users will instead be informed that the page they are trying to access has been rejected or filtered out. The implementation of the service offers layered parameterization such as content control rules applied to users or to user groups, access denial or access deterring, notification for entering insecure or non-trusted areas, time-scheduling policy enforcement, reporting, dummy robot blacklisting. According to the data presented in Table 2, the page filtering rate for 2006 was 2.56%, increased by a factor of 54% in relation to 2005, as presented in Table 4. For the same time period total traffic volume increase reached 95% and requests increased by 59%. The conclusion is that page filtering scales smoothly with the traffic volume.

Table 1. Services Offered by GSN

Service	**Information**
Internet access	
Dial-up service	
Internet safe use	www.sch.gr/safe
Secure access	
Protection and incident handling	www.sch.gr/cert
GSN Portal	www.sch.gr
Students portal	students.sch.gr
Open, educational software & content	opensoft.sch.gr
Web hosting and authoring tools	
E-mail, web mail, anti-spam, anti-virus protection	www.sch.gr/mail, www.sch.gr/webmail
Mailing lists	www.sch.gr/lists

Forums	www.sch.gr/forums
Asynchronous tele-education	www.sch.gr/e-learning
Synchronous tele-education	www.sch.gr/lms
Livecasts	www.sch.gr/rts
VoD	www.sch.gr/vod
e-Class	www.sch.gr/eclass
GSN magazine	e-emphasis.sch.gr
Electronic magazines	www.sch.gr/periodika
News channels	
GIS	www.sch.gr/gis
GSN statistics	www.sch.gr/statistics
Hostmaster - Domain name service	
E-cards	www.sch.gr/e-cards
Instant messaging	
Proxy and web filtering	
Safety aspects	www.sch.gr/safe
Directory service	
Remote systems management and monitoring	
Helpdesk and contact center	www.sch.gr/helpdesk

Table 2. Proxy Operational Statistics for 2006

Average data volume MB/Day (typical daily traffic)	**165,976**	**MB/day**
From the internet	165,976	MB/day
From the cache	-	MB/day (*)
Average number of Requests/Day	13,537	requests/minute
Total available space for caching or content delivery	980	GB
Percentage of rejected requests by the web filtering service	2.56	%
Messages/day accepted by GSN cachemaster	73	Month

Table 3. Filtered Pages Categorization for 2006

Page filter category	**Domains**	**urls**	**Regexp**	**Comments**
Aggressive	234	49	-	Aggressiveness
Drugs	494	982	-	Drugs
Gambling	1,146	35	-	Gambling
Porn	873,455	104,865	x	Pornography
Proxy	3,123	12	-	Proxy servers
Violence	23	13	-	Violence
Edudeny	1,593	107	-	GSN exception pages
Edupass	673	765	-	
Totals	880,741	106,828		

Table 4. Proxy Server Operational Statistics for 2005

Average data volume MB/Day (typical daily traffic)	**82.746**	**MB/day**
From the internet	82.746	MB/day
From the cache	-	MB/day (*)
Average number of Requests/Day	8.675	requests/minute
Total available space for caching or content delivery	980	GB
Percentage of rejected requests by the web filtering service	1.67	%
Messages/day accepted by GSN cachemaster	57	Month

Table 5. Filtered Pages Categorization for 2006

Page filter category	**Domains**	**urls**	**Regexp**	**Comments**
Aggressive	195	42	-	Aggressiveness
Drugs	330	477	-	Drugs
Gambling	932	33	-	Gambling
Porn	138535	32994	x	Pornography
Proxy	94	14	-	Proxy servers
Violence	21	14	-	Violence
Edudeny	801	44	-	GSN exception pages
Edupass	220	333		
Totals	141128	33951		

The decision on whether or not a page should be filtered out is made by the content control engine based on keyword blocking, black/white listing, and content labeling/rating techniques. Each technique has strong and weak points. GSN combines both techniques to create robust content control mechanisms. Keyword blocking is fast and easy to deploy, but it is ineffective for non-textual content, it is easy to bypass and there is always the possibility of non-abusive content being blocked. Pages may fall into categories such as aggressive, drugs, gambling, porn or violence. The keyword blocking is based on page, metadata and request parsing for offensive content. Table 3 summarizes the distribution of banned pages over the filtered categories. Black/white listing is an effective technique but its effectiveness is restricted within the range of the lists. Black list records include domains records, specific urls, or expressions. List maintenance and updating is administratively demanding, given the size and growth rate of abusive content. Content labeling and rating is effective since categorization is retrieved from international organizations and user associations or communities that maintain databases of abusive web destinations. GSN also maintains a database for the implementation of its own black and white listing in order to provide customized access control to content that is inconsistent with or in agreement with, respectively, the GSN terms of use. The definition of content with the use of content labelling and rating systems [17] is performed by attaching a set of tags to each webpage that specifies the type of information it contains. Organizations that provide such ratings for web sites include the Internet Content Rating Association (ICRA) [18], SafeSurf [19], and the Entertainment Software Rating Board (ESRB).

The small-scale side effect of the above large-scale automated filtering is the phenomenon of mis-categorization, which takes place when regular pages are categorized as offensive (overblocking), or when offensive pages are not blocked. Even if mis-categorization rates are low for GSN, as illustrated in Table 3, mis-categorization is resolved by manual corrections, usually following user reporting. As can be seen from Table 3, exceptions due to mis-categorization represented 0.82% of total URL access in 2006. A percentage of 0.10% of the pages that should have been filtered were not, while the corresponding percentage for pages that should not have been filtered but were is 0.72%, that is, 7.2 times higher. Domain mis-acceptance percentage is 0.18% and mis-denial percentage is 0.08%. Table 5 presents the same data for 2005; In 2005 exceptions due to mis-categorization represented 1.2% of total url access in 2005. 0.13% of the pages were mis-accepted, while the corresponding percentage for pages that should not have been filtered but were is 0.98%, that is, 7.5 times higher. Domain mis-acceptance percentage is 0.57% and mis-denial percentage is 0.15%. The former numbers are small considering the size and average user profile of the GSN network and they do not scale with respect to traffic or requests increase. Low mis-categorization is attributed to the sound operation of the content filtering and control system as well as to user gradual adaptation and conformance with content control directives and general guidelines.

2.2. Ant-span and anti-virus service

Spam has long been a major problem for GSN, as for other internet stakeholders. Spam is costly to the receiver[1] and not to the sender, unethical since it is unasked, and is recognized as harassment in many legal systems [20]. In E.U. the directive 2002/58/EC [21] defines the legal framework against spam. Spam started as unwanted incoming e-mail messages but the term currently applies to similar abuses in other types of media such as instant messaging, Usenet newsgroups, search engines, blogs, mobile phone messaging, internet forum and fax transmissions. It is a major threat to organizations such as GSN that offer most of the above services (Table 1), since it increases operational costs in terms of personnel, maintenance and infrastructure. If spam is not handled properly it may even put production services into peril. Despite the efforts of governments, industry [22] and academia [23] to diminish it, spam is increasingly intense. According to [24] 75-80% of total worldwide incoming mail traffic is abusive and can be traced to fewer that 600 spammers.

It is argued if the strategy for spam minimization should be focused on tools at the side of the end user, or at the server and administration side [25]. In sensitive environments involving school networks the problem must be handled in a multilateral manner, by combining rigid technological solutions, and preventive methods, such as promotion and user sensitizing. GSN enforces anti-spam protection policies on the server tier while publication services [26] are employed to disseminate spam protection

[1] For example, AOL reported reception of 1.8 million of spam messages from Cyber Promotions per day until a court injunction was issued. Assuming it takes the typical user only 10 seconds to identify and discard a message, that is still 5,000 hours of connect time per day spent discarding their spam, just on AOL. In contrast, the spammer probably has a T1 line that costs him about $100/day. Spam costs much in term of download time, man hours lost, organizational costs, etc.

related information to users. The volume and growth[2] of spam, the fact that it is often combined with malicious code, attacks, fraud and forgery (phishing or spoofing), make user as well as backend systems protection necessary in the form of a central GSN anti-spam policy. In addition to protection, GSN also makes sure that users are conscious about the essence of spam through press announcements and the GSN portal [1]. The material published or sent clarifies spam's business purpose and legal hypostasis. Students are kept knowledgeable of the fact that spam breaks the terms of use enforced by GSN as well as all internet service providers (ISPs), that it constitutes a form of harassment and that it results in substantial receiver side costs. GSN also publishes techniques, best practices and methods that protect users from spam.

The GSN anti-spam service is hosted on clustered servers in the GSN backbone interfacing with the GSN directory server to offer personalisation functionality. Effective spam recognition is performed by employing different identification methods such as real time black listing (RBL) and mail filtering. RBL listing is performed with the aid of the caching proxy software Squid [11] and the Squid Guard url redirector that integrates blacklisting support within Squid. Squid reduces bandwidth usage and improves response times while SquidGuard checks incoming mail against the custom GSN RBL database as well as against known RBL real-time databases, such as Spamhaus [26], DSBL [27], SpamCop [28], DNSBL [29]. The spam databases have been chosen for their general acceptance by the administration and anti-spam community and for their specialization in spam sources registration. These databases have also been mirrored in GSN servers; Spamhaus is a widely accepted real-time spam sources registry that is offered as a free service for anti-spam protection. DSBL includes sources verified to distribute messages freely that is, open relays and open proxies. The SpamCop list relies on spam sources reported to and verified by the SpamCop project. The size of the above lists is huge, as each one may include entries as many as one percent of the size of the internet space. Messages coming from sources designated by Spamhaus, DSBL SpamCop, are not accepted by GSN servers, while messages coming from sources in the Sorbs list for open relays and proxies are marked as spam messages.

The technical essence of spam is that abusive messages are indistinguishable from non-abusive ones as there is no way of accurate, real-time source verification, since the associated communication protocols do not support authentication and authorization procedures [30]. Even though sophisticated spam control techniques such as Bayesian networks [31][32] and collaborative filtering [33] reflect recent research achievements, cutting edge spam employs image-based communication and turn the battle to the image processing of mail [34]. Spam exhibits strong resilience to defense techniques and outstanding adaptability [35]. GSN filters out mail spam using a customized solution that employs cutting edge anti spam technology. The solution is based on Spam Assassin 3.17 [36] and supports various filtering mechanisms such as header and text analysis, Bayesian filtering, domain name service (DNS) block-lists and collaborative filtering databases. Statistics regarding the anti-spam service are presented in Table 6. Each incoming mail message is given a score, calculated through trained neurone

[2] In 1978 the first spam was sent to 600 addresses [18], in 1994 the first large scale spam was sent to 6000 newsgroups, reaching millions of people. In February 2007 spam is measured to 90 billion messages per day

network technology; the score represents the probability that it is spam. This number is utilized by custom mail routing code. If the score is high the mail is marked as spam and is routed to the GSN spam folder. Grades of messages that originated from the same source can also be combined in order to produce a score that characterises the sender and thus to automatically classify him in white or black lists, appropriately. Optimization of the grading threshold for spam as well as scores for individual filtering tests for spam is an interesting area for research and consolidation planned for the future of the GSN anti spam service. The filtering mechanism is also integrated with the GSN user directory service to offer personalization for each user mailbox, delivered through the GSN portal. To achieve user configurable anti spam protection, anti-spam engine configuration files are retrieved from the directory server instead of the file system. Personalization is exposed to users through the GSN portal, after logging in. Thus, users can activate or deactivate RBL anti spam; they may also decide to move the spam messages into the "spam" mail folder, or into the trash folder. Users can also choose the spam grading for spam characterization. Smaller grade thresholds result to less spam, but the likelihood of tagging useful mail as spam is then increased. Tests and measurements showed that a good value for that threshold is around 7, while values less than 5 result to loss of healthy mail. Users are presented with the option of automatically deleting highly graded mail. Besides filtering, users may personalize their black and white lists; they have the option to enable/disable them, to move matched content into trash or spam folders. Additionally they may choose the time interval before spam is deleted.

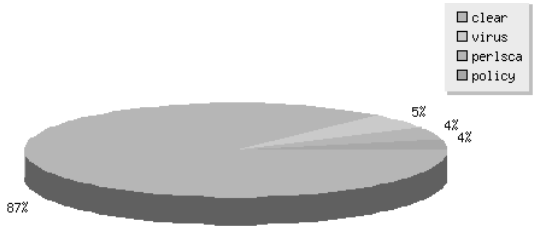
The electronic mail service is complemented with the message content control service. This is an additional step in the chain of electronic mail service protection, allowing the control of those message characteristics that can certify that a message is infected or malicious. The anti virus service is offered to all GSN users, namely to more than 150.000 mailboxes and user home directories [1]. The anti-virus service is based on mail scanner software installed on all GSN mail servers. The software used is the Sophos Mail Monitor Connect [37]; it interfaces with the core GSN mail engine and scans input streams for viruses and threats. The incoming traffic is filtered by RBL lists mirrored by GSN, as discussed in the previous paragraph, and it is then scanned for abusive code. All sources that transmit abusive content are categorized in the black list bl-mail-abuse.sch.gr maintained by GSN. Sophos scans for improper sequences of characters in concrete headings of messages (headers), extensions of attached files, text suspicious for phishing, viruses and malware. The control of files attached to the incoming or outgoing messages is performed by the anti-virus scanner. The program also prevents sending mail with attached files of type .vbs, .lnk, .scr, .wsh, .hta, .pif, .exe, .bat, .com, .cmd. In case a message is blocked by the software, the sender is informed appropriately about the incident, the rank of the possible threat and possible solutions. If the user account is responsible for sending large amounts of malicious traffic, the account can be set into quarantine state. Identification of such accounts is usually the result of log file analysis performed by the antivirus software. This procedure is capable of identifying accounts that exhibit extraordinary behaviour, such as periodically sending malicious software, sending too many messages or consuming too many resources of any kind. Unusual behaviour is registered, the corresponding user accounts are added in the GSN RBL list (bl-mail-abuse.sch.gr), the corresponding educational units are informed, and the GSN helpdesk is also notified. Accounts are

kept quarantined until problems are resolved. Mail messages sent by users during their quarantine time are returned to their mailbox explaining the reasons for the quarantine and providing useful pieces of information for GSN security.

Table 6. Spam Filtering Distribution

9/2004

Message state	# Messages	% of Total
Policy violation	78.042	3,83%
Perl scanner violation	83.899	4,11%
Virus infection	108.468	5,32%
Clear	1.769.597	86,74%



4/2005

Message state	# Messages	% of Total
Policy violation	13.884	1,00%
Perl scanner violation	15.956	1,15%
Virus infection	13.335	0,96%
Clear	1.344.354	96,89%

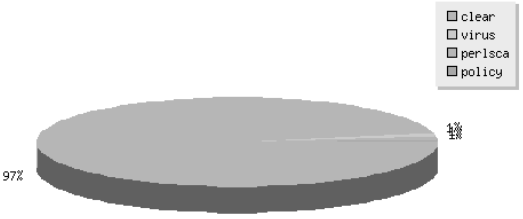


Table 5. Top ten of recent virus alerts hoaxes

Latest 10 virus alerts		Top 10 virus hoaxes	Top 10 viruses in May 2004	
1 Jun	W32/Rbot-V	Meninas da Playboy	1	W32/Sasser
28 May	W32/Agobot-XX	Hotmail hoax	2	W32/Netsky-P
28 May	W32/SdBot-BC	Spunkball	3	W32/Netsky-B
28 May	W32/Bagle-AA	Budweiser frogs screensaver	4	W32/Netsky-D
27 May	W32/Sdbot-BW	Bonsai kitten	5	W32/Netsky-Z
27 May	W32/Agobot-JF	Bill Gates fortune	6	W32/Netsky-Q
26 May	W32/Rbot-T	A virtual card for you	7	W32/Netsky-C
26 May	W32/Francette-K	WTC Survivor	8	W32/Sober-G
25 May	Troj/Adtoda-A	JDBGMGR	9	W32/Bagle-AA
25 May	Troj/StartPa-AE	Jamie Bulger	10	W32/Lovgate-V

2.3. Responding to incidents

GSN security-related incidents have scaled in number during the last years, following international tendencies. Compromised stations or misbehaving accounts may have negative impact on GSN operation and, therefore, the response must be immediate. Any organization that requires an accessible Internet presence 99.999 percent of the time probably has a high profile, one that can be damaged as much by a publicized security incident as by having its site unavailable. The requirements for availability and security within GSN are stringent. The GSN Computer Emergency Response Team (CERT) has been founded in order to create and maintain the security plan for GSN. CERT designs for security, monitors the smooth and sound operation of GSN, reacts to incidents according to their importance and informs users about security matters. It analyses network resources, produces periodic reports, cooperates with all the necessary GSN teams in order to be informed about problems or to resolve them and also consults for security. The team is manned with security engineers, expert on monitoring and incident identification, network attacks and prevention, penetration analysis and testing, and security consulting.

Effectively managing security issues is key to the success of school networks, such as GSN. Incidents must be reported, registered and dispatched efficiently, since GSN inevitably faces a large spectrum of security incidents. Designing and implementing for redundancy and failover, removing single points of failure, and effective testing are the critical upfront elements of high-availability secured systems. CERT maintains the security architecture for GSN; security service engineers need to design services or architectural elements that can tolerate failures of security devices (for example, firewalls, honey pots, honey nets and demilitarized zones) that would adversely affect availability. This may include elements such as hot standby firewalls, where a primary firewall is backed up by a second firewall. A third device can then monitor the primary device and divert traffic to the backup firewall upon detecting a failure in the first firewall. A more flexible architecture may include dynamic load balancing across two or more firewalls to maintain maximum throughput. If the configuration also includes a failover capability, fault detection causes the remaining functional firewall to assume the full traffic load. According to established practices for security management and organization, incidents and attacks must be dispatched, categorized according to scale, traffic direction, target area, method, timing and importance. Attempts to exploit security holes in operating systems, zero day vulnerabilities, denials of service, sniffing and identity theft, and all sorts of attacks are bound to happen daily unless preventive measures have been taken. Even then, the rate of compromises cannot be minimized to zero. The platform used for security management and event analysis has developed by CERT.

CERT communicates with GSN users who are kept up to date through the web site maintained by CERT (Fig. 3). Mailing lists that disseminate security information about incidents within GSN are also supported. The web site and the list both appeal to novice and experienced users. According to the information published, the most common incidents related to schools are, according to frequency, web pages defacements, compromised work stations (privilege escalation), massive spam generators, worms, port scanners and botnets. In an effort to prevent and effectively face problems

cooperatively with other administrative groups, GSN-CERT often proposes changes in procedures, practices, and GSN regulations, or recommends and produces solutions.

Figure 3. The GSN response service web page

3. Future work and conclusions

Future GSN plans include the consolidation of security related services. Refinements will include advanced monitoring of connections, such as reverse DNS checks for incoming connections, grey listing, maximum connection time checks and advanced log analysis, mail grading optimization, idle timeouts and mis-categorization optimization. Moreover, security policies have to be made more flexible, reliable, and configurable by being enforced at the network access layer. The technical solution will employ extended directory schemas and regular profiles for schools and administrative units. Each administrative unit connected via a GSN-managed router will belong to a default group with respect to the local loop technology. Thus, units can be isolated in terms of policing from school units. School units will also be categorized in groups. The regular profiles will be enriched with ACL definition attributes defining the policies to be enforced on connections. This solution is expected to be flexible enough to cover all diverse network configurations within the limits of the GSN network. GSN also plans to continue to provide information about security to students through is publication services. According to research conducted in 2006 on behalf of the Pan-Hellenic Consumer Organization [36], 21% of all the Internet users have been informed about security perils of internet through school.

The GSN security services offer a solid, high quality environment, as it is appropriate for a school network. Internet growth rates encumber content control. GSN combines cutting edge techniques such as keyword blocking, access listing, content rating and content labelling in order to achieve reliable traffic filtering, anti-spam and anti-virus protection. GSN plans for security and maintains internal operational and collaboration mechanisms for monitoring and planning through the CERT service. At the same time GSN offers highly personalized services and attempts to raise students' awareness about internet perils through dense information services.

References

[1] The Panhellenic school network site, http://www.sch.gr, 20 July 2008
[2] Ministry of Education and Religious Affairs, http://www.ypepth.gr, 20 July 2008
[3] C. Bouras, M. Paraskevas, “Educational Information Society in Greece: The Greek School Network”, IADIS International Conference, e-Society, Lisbon, 179-186, 2003
[4] The Panhellenic educational network information site, GSN implementation consortium, http://www.edunet.gr/ergo/foreis.php?ID=6, 30 November 2007
[5] N. Xypolitos, M. Paraskevas, E. Varvarigos “The Greek School Network: Structure, design principles and services offered”, Proc. Inl Joint Conference on E-business and Telecommunications (ICE-B 2006), Setubal, Portugal, pp. 283-288, Aug 2006
[6] "Information Society as a tool for regional development: exchange of best practices at European level", http://www.campaniasi.it/eng/program.htm). http://www.europa.eu.int/comm/employment_social/news/2004/jan/el2_1_en.pdf, http://www.sch.gr/sch-portlets/aboutSch/honors/GSN@Best_Practice_2004.pdf, http://www.sch.gr/sch-portlets/aboutSch/honors/GSN@Best_Practice_2003.pdf, 30 November 2007
[7] GSN safe usage principles, http://www.sch.gr/safe, 30 November 2007
[8] European network of e-safety awareness, www.saferinternet.org, 30 November 2007
[9] Digital awareness and response to threats, www.dart.gov.gr, 30 November 2007
[10] M. Avgoulea, C. Bouras, M. Paraskevas, G. Stathakopoulos, “Policies for content filtering in educational networks”, J.Telematics and Informatics, 20(1), 71–95, 2003
[11] Squid, http://www.squid-cache.org/, 30 November 2007
[12] SquidGuard url redirector, http://www.squidguard.org/, 30 November 2007
[13] G. Houtzager, C. Jacob, and C. Williamson, “An Evolutionary Approach to Optimal Web Proxy Cache Placement”, IEEE Congress on Evolutionary Computation, Vancouver, July 2006
[14] The Greek universities network, http://www.gunet.gr/, 30 November 2007
[15] The GEANT project, http://www.geant.net, 30 November 2007
[16] M. Kalochristianakis, M. Parakeyas, E. Varvarigos, N. Xypolitos, “The Greek school network , a paradigm of successful educational services maturing based on open source technology“, IEEE transactions on Education, Nov. 2007, vol. 50, issue 4, pp.321-330 (ISSN: 0018-9359)
[17] M. D. Lytras, N. Pouloudi, and A. Poulymenakou, “A framework for technology convergence in learning and working,” Educational Technology and Society, Journal of International Forum of Educational Technology & Society and IEEE Learning Technology Task Force, Vol. 5(2):99-106, 2002
[18] The Internet Content Rating Association, http://www.fosi.org/icra/, 30 November 2007
[19] The safesurf internet content rating system, http://www.safesurf.com, 30 November 2007
[20] ITU survey on anti spam legislation world wide, http://www.itu.int /osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf
[21] Directive 2002/58/EC of the European Parliament and the Council on the processing of personal data and the protection of privacy in the electronic communications sector, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&numdoc=32002L0058&model=guichett&lg=en, 30 November 2007
[22] B. Krishnamurthy. (2003) SHRED: Spam Harassment Reduction via Economic Disincentives. AT&T Labs Research. Available at: http://www.research.att.com/~bala/papers/shred-ietf56-talk.pdf, 30 November 2007
[23] Contact Network of Spam Authorities (CNSA), http://europa.eu/rapid /pressReleasesAction.do?reference=IP/05/146&format=HTML&aged=0&language=EN&guiLanguage=en, 30 November 2007
[24] Register of Known Spam Operations, http://www.spamhaus.org/ rokso/index.lasso, 30 November 2007
[25] The messaging anti-abuse working group, MAAWG Issues First Global Email Spam Report, http://www.maawg.org/news/maawg060308, 30 November 2007
[26] The spamhaus project, http://www.spamhaus.org/, 30 November 2007
[27] Distributed Sender Blackhole List, http://dsbl.org/main, 30 November 2007
[28] Spamcop reporting services, http://www.spamcop.net/, 30 November 2007
[29] SORBS spam and open-relay blocking system, http://www.de.sorbs.net/, 30 November 2007
[30] Electronic Mail Related RFC Documents, http://www.tac.nyc.ny.us/mail/rfc-index.html
[31] M. Sahami, S. Dumais, D. Heckerman, E. Horvitz (1998). A Bayesian approach to filtering junk e-mail. AAAI'98 Workshop on Learning for Text Categorization.
[32] I. Androutsopoulos, J. Koutsias, K. Chandrinos, G. Paliouras, and C. Spyropoulos, An Evaluation of Naive Bayesian Anti-Spam Filtering. Proc. of the Workshop on Machine Learning in the New Information Age,

11th European Conf. on Machine Learning, Barcelona. Available at: http://www.ics.forth.gr/~potamias/mlnia/paper_2.pdf, 2000.
[33] J. Kong, O. Boykin, B. Rezaei, N. Sarshar, V. Roychowdhury, Collaborative Spam Filtering Using E-Mail Networks ," IEEE Comp. Magazine, 9 (8), Aug. 2006, pp 67-73
[34] G. Hulten, A. Penta, G. Seshadrinathan, M. Mishra, Trends in Spam Products and Methods, Proc. 4th Conference on Email and Anti-Spam (CEAS), 2007.
[35] G. L. Wittel and S. F. Wu, On Attacking Statistical Spam Filters, Fourth Conference on Email and Anti-Spam, CEAS 2007
[36] The spam assassin open source spam filter, http://spamassassin.apache.org/, 20 July 2008.
[37] The Sophos anti-virus / anti-spam software for businesses, http://www.sophos.com/, 20 July 2008.
[38] Pan-Hellenic Consumer Organization, http://www.ekato.org/index_en.html, 20 July 2008.

Authors

Michael Kalochristianakis received a Diploma in Electrical Engineering and Computer Technology from the University of Patras and an MS degree in Computer Science from the University of Crete, in 2001 and 2003, respectively. From 2003 until 2005 he worked in the private sector in the IT and Networking areas. In 2005 he joined the Network Technologies Sector of the Research Academic Computer Technology Institute where he is working as an IT Engineer in the implementation of advanced network services.

Michael Paraskevas received an electrical engineering degree in 1989 from the University of Patras, Greece. In 1995 he received the PhD degree in digital signal processing area. He has also worked at a number of E.C. projects, mainly on designing networks, telematic services, speech synthesis and broadcasting applications. His current research interests are the digital signal processing techniques, designing and implementation of networks and services, especially for the education sector. He is the technical director of the Greek School Network and he is also a member of the Technical Chamber of Greece and the Audio Engineering Society.

Emmanouel (Manos) Varvarigos received a Diploma in Electrical and Computer Engineering from the National Technical University of Athens in 1988, and the M.S. and Ph.D. degrees in Electrical Engineering and Computer Science from the Massachusetts Institute of Technology in 1990 and 1992, respectively. He has held faculty positions at the University of California, Santa Barbara (1992-1999, as an Assistant and later an Associate Professor) and Delft University of Technology, the Netherlands (1998-2000, as an Associate Professor). In 2000 he became a Professor of Computer Engineering and Informatics at the University of Patras, Greece, where he heads the Communication Networks Lab. He is also the Director of the Network Technologies Sector (NTS) at the Research Academic Computer Technology Institute (RA-CTI), which through its involvement in pioneering research and development projects, has a major role in the development of network technologies and telematic services in Greece. Professor Varvarigos has served in the organizing and program committees of several international conferences, primarily in the networking area, and in national committees. He has also worked as a researcher at Bell Communications Research, and has consulted with several companies in the US and in Europe. His research activities are in the areas of protocols for optical networks, network protocols, switch design, network services, grid computing and ad hoc networks.