Astalavista Group Security Newsletter
Issue 17 - 30 May 2005
http://www.astalavista.com/
security@astalavista.net

[01] Introduction

Dear readers,

Welcome to the 17th issue of the Astalavista Security Newsletter!

In this issue of our newsletter you'll read **part 2 of our DNS Security article**, learn more about **Bluetooth hacking and security** and most importantly **how to protect yourself** or your friends; you will also go through an invaluable and comprehensive set of free resources, and read an interview with **Roman Polesek**, an editor for the hard cover security magazine **Hakin9.org.**

A mobile networks and devices security oriented section will soon be made available at the **Astalavista.com** site, so stay tuned! We believe the time has come that we pay serious attention to raising the awareness on current GSM standards and future technologies.

Due to the increased interest in our resources, we have also divided the Astalavista Recommends Section into **Recommended Tools** and **Recommended Papers**.

Meanwhile, **Astalavista.com** has been featured as **PC Magazine's Top Security Sites**:

http://www.pcmag.com/article2/0,1759,1782522,00.asp

Keep spreading the word about **Astalavista.com** and keep your feedback coming!

Astalavista Security Newsletter is constantly mirrored at:

http://www.packetstormsecurity.org/groups/astalavista/
http://www.securitydocs.com/astalavista_newsletter/

If you want to know more about Astalavista.com, visit the following URL:

http://www.astalavista.com/index.php?page=55

Previous issues of Astalavista Security Newsletter can be found at:

http://www.astalavista.com/index.php?section=newsletter

Yours truly,

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net

[02] **Security News**

The Security World is a complex one. Every day a new vulnerability is found, new tools are released, new measures are made up and implemented etc. In such a sophisticated Scene we have decided to provide you with the most striking and up-to-date Security News during the month, a centralized section that contains our personal comments on the issues discussed. **Your comments and suggestions about this section are welcome at** security@astalavista.net

---

[**DASHBOARD LEAVES MACS VULNERABLE**]

Dashboard, a new feature in Apple's latest operating system, OS X Tiger, could expose users to attack and theft of personal information. Dashboard allows users to keep "widgets", small programs that access the Internet for information, on their desktops. Anyone can make a widget using Javascript and HTML. Most widgets install themselves automatically, and cannot be deleted by the user once installed. Stephen Meyers, one of the first to publicize the danger of Dashboard, has developed Zaptastic, a widget that opens the Safari browser and directs users to a webpage promoting an online payment system. A more malicious version opens the webpage every time Dashboard is booted up. Users can manually delete widgets through the /Library/Widgets folder.

More information can be found at:

http://www.wired.com/news/mac/0,2125,67484,00.html

Astalavista's comments :

Apple's widgets are indeed very handy and the concept is great, but to put it in another way - a self-installing, hard to remove, Unix carrying commands(not only!) and a convenience-based feature concept might indeed come handy for malware authors targeting Apple customers, but are they doing it anyway?!

What is a malware author looking for these days? Obviously to infect as many PCs as possible, and to maintain a relevant number of victims, and it's getting even more competitive with malware removing other malware to take a larger share of the high-speed Internet access industry turned into an underground market. Given the obvious Microsoft domination of the market, the Apple OS vulnerabilities and exploits are more of a way of proving that "everything can be hacked". What's to consider in the upcoming future might be the economic or business espionage nature of the content on an Apple PC and the psychological fact that a great number of users still believe malware authors are busy targeting Windows and have a great feeling of "false security", while again keeping a great deal of information in interest of malicious attackers or business competitors.

And in case Apple doesn't provide a fix to the eventual abuse of this bug, end users are already finding ways to fix it as I came to various solutions reading various forum discussions. As far as their widgets are concerned, the widgets security model can be found at:

http://developer.apple.com/documentation/AppleApplications/Conceptual/Dashboard_Tutorial/Security/chapter_10_section_1.html

Also, check out the Dashboard Programming Guide if you're interested in developing widgets on your own :

http://developer.apple.com/documentation/AppleApplications/Conceptual/Dashboard_Tutorial/Dashboard_Tutorial.pdf

More resources on **Apple security**, or associated tools can be found at :

http://www.nsa.gov/notices/notic00004.cfm?Address=/snac/os/applemac/osx_client_final_v_1_1.pdf
http://members.lycos.co.uk/hardapple/
http://www.astalavista.com/?section=dir&cmd=file&id=4393
http://www.astalavista.com/index.php?section=dir&cmd=file&id=3821

[**RESEARCHERS REVEAL HOLES IN GRID**]

New research into security weaknesses in a popular secure remote access technology highlights the vulnerability of large-scale computing environments such as grids and supercomputing clusters to a potentially crippling form of attack.

The SSH (Secure Shell) technology is used by security administrators and other technical users to connect to remote machines via a secure, encrypted tunnel.

The system is used widely in university and research networks, and security researchers at the Massachusetts Institute of Technology last week published a paper showing how a simple worm could grab SSH user credentials from one machine and move rapidly among any number of connected systems, causing what's known as a "cascade failure."

More information can be found at :

http://www.eweek.com/article2/0,1759,1815795,00.asp

Astalavista's comments :

SSH became the logical alternative to plain-text authentication and since its introduction, it pretty much became a standard approach for ensuring that authentication details are not transmitted in clear text on pretty much every network out there, not just grid networks, although their content might be of a particular interest to high-profile attacks.

I especially enjoyed the practicality of using known_hosts to locate targets, but on the other hand if we were to develop a virtual roadmap for any network, beside the common network tools, we could also go for tools like GoogleSweep, while on the other hand, an educated script kiddie (anyone?) or a person having a degree of common sense would never delete scan logs or fingerprinting ones, a practice that represents a huge problem mainly because the fingerprinting issue on a mass scale is often neglected, but port knocking as a concept might still represent an opportunity for prevention.

Looking fur further "gold mines" like the ones mentioned in the article, consider that a large number of ISPs still allow zone transfers thereby exposing their infrastructure and outlining their customers' base.

The publication can be found at :

http://nms.csail.mit.edu/projects/ssh/sshworm.pdf

[**CISCO DEVICE TO UNITE SECURITY FUNCTIONS**]

Cisco Systems plans to announce a product that will combine into one box numerous security functions previously available only as separate products.

The new device, called the Adaptive Security Appliance 5500, will be unveiled Tuesday by CEO John Chambers during his keynote address at the Networld+Interop trade show in Las Vegas. The new product purportedly puts up to 18 different security and network management functions into a single device. These functions include detection of intruders, prevention of denial-of-service attacks, protection from spyware and adware, and network traffic micro-inspection, which can help detect when employees are burning up too much bandwidth by using software such as Kazaa.

More information can be found at :

http://news.com.com/Cisco+device+to+unite+security+functions/2100-7347_3-5693331.html

Astalavista's comments :

Cisco Systems was the fastest growing company during the boom of the Internet and the introduction of the network concept for doing business itself, whereas, from a business point of view, it hasn't been operating in the way it used to back then and it is all due to the fact that companies aren't often renovating their entire infrastructure these days. So what should the company do? Of course diversify, but where? Given Cisco's brand reputation and image positioning as THE company empowering the Internet Generation, the Security sector is indeed an obvious choice.

For quite some time now, there's been a shift in the trends towards all-in-one security Appliances mainly because of convenience reasons, CSOs and CIOs are exposed to a growing number of new or emerging threats targeting their organizations and even though product/service evaluation takes place, it's more convenient to get an all-in-one security appliance from an established and trusted brand.

My opinion is that in spire of the obvious convenience benefits, a company's security Strategies in terms of services should be justified in many more ways beside the trendy product extensions they have recently implemented through acquisitions and trust. Symantec doesn't specialize in spyware (although the company, of course, already has anti-spyware products in place). WebRoot for instance do, while they know pretty much nothing on the global.

At the bottom line, the product is just awesome, but don't let your entire organization's fortune rely on the integrity of single appliance. No matter how convenient or market-outspoken the product is, try to research or sense who's who in certain sectors and who you can really trust.

More info about the appliance can be found at :

http://www.cisco.com/en/US/products/ps6120/

[**L.AA COUNTRY JAIL TAGS INMATES WITH RFID**]

The next fashion accessory for some inmates at the Los Angeles County jail will be a radio frequency identification bracelet.

The country's largest jail system has launched a pilot project with Alanco Technologies to track inmates using the technology, also known as RFID.

The first phase will involve setting up an RFID system in the 1,800-inmate east facility of the Pitchess Detention Center in Castaic, Calif., by fall 2005. If it succeeds, and funding can be obtained, the county will spread the system throughout its prison facilities.

More information can be found at :

http://news.com.com/L.A.+County+jail+tags+inmates+with+RFID/2100-7337_3-5710561.html

Astalavista's comments :

What's with using RFID on a mass scale? Passports, supply-chains and inventories management, Gillete's razor blades, now jails, you name it, RFID seems to be the answer everyone's been waiting for decades.

It's flexible, it's cheap, but it's so insecure that it makes me open up a mobile-marketing department and just "warintercept" all my customers' behaviour or interests. As always, there's too much buzz on devices like these but whenever a jail decides to implement RFID, it makes me think on the possibilities to know exactly where's everyone at a particular moment, and what if someone suddenly disappears at least from the sensors or has a completely different location from the actual one? Do some research and you'll see that both theoretically and practically it's possible.

RFID is indeed the future, but let's secure it or highlight the posed threats before we dive ourselves into it!

Some more info on the topic can be found at :

http://www.forbes.com/home/commerce/2004/07/29/cx_ah_0729rfid.html
http://www.rsasecurity.com/rsalabs/node.asp?id=2115
http://lasecwww.epfl.ch/~gavoine/rfid/
http://www.astalavista.com/?section=dir&cmd=file&id=4466

[**RESEARCH : SPYWARE INDUSTRY WORTH BILLIONS**]

According to the State of Spyware Report issued by security company Webroot, the number of computers infected with spyware remains high but is declining. Webroot found spyware on 87% of business computers and 88% of private computers, with an average of 28 spywar programs on each. David Moll, chief executive of Webroot, said that growing consumer awareness and legal action may be slowing spyware, but have yet to translate into a strong decline. According to the report, spyware generates $2

billion in revenue annually.

More information can be found at :

http://news.com.com/Research+Spyware+industry+worth+billions/2100-1029_3-5693730.html

Astalavista's comments :

The following report (get it directly instead of the leads based link on WebRoot's site below) conducted by the well - known anti-spyware solutions company WebRoot is perhaps the most recent study on spyware highlighting that spyware is indeed a growing problem for both home and enterprise users. At the bottom line, users are not just getting aware of spyware, they're getting pissed off at the "vendors" that distribute it and they actually started realizing that what used to be free downloads of music, software and movies is now downloads bundled with spyware, adware, trojans, you name it – they hate it. "Vendors" are continuing operations untouched by the globalization of the Net, trying to get hold of as many intermediaries as possible.

When it comes to fighting spyware in the corporate environment, in my opinion it's productivity instead of privacy exposure that matters most, naturally depending on the spyware. Implementing "secure by default" , "security through obscurity" , namely mitigating to a less targeted browser for the time being, integrity checking and restoration of default setups, content monitoring and filtering of potential "intermediaries" are among the best approaches that I usually recommend.

Get the 8.6 MB report at :

http://www.astalavista.com/media/files/webroot_state_of_spyware_report.zip

Not surprisingly, **CoolWebSearch Spyware** is listed as the leading spyware, and in case you're interested you can check its chronicles at :

http://cwshredder.net/cwshredder/cwschronicles.html

[**WOMAN HELD OVER INDUSTRIAL ESPIONAGE**]

French police have arrested a Chinese woman on charges of "intrusion in an automatic data system" and "abuse of confidence" for allegedly stealing car designs during her internship at Valeo. Police say a search of her home office found six computers and several high capacity hard drives with confidential information. The woman came under suspicion after an executive frequently noticed her walking around the office with her portable computer. The woman holds degrees in mathematics, applied physics, and fluid mechanics and can speak German, Spanish, English, French and some Arabic. She has worked as an intern for Valeo since February 2005.

More information is available at :

http://www.news.com.au/story/0,10117,15162906-31037,00.html

Astalavista's comments :

Playing a "catch up" or not interested in "reinventing the wheel", Asian countries have a long history of industrial espionage cases targeting information societies or developed economies. Although no further details are available as to who was about to take advantage of the information, in my opinion recruiting such a highly educated person might only be done through extortion or based on a nationality level. Besides, it's not a

"woman held over industrial espionage" but an "intern" held. Putting the problem in this way clearly highlights the issues to be considered – insiders are on the rise, interns are not to be trusted, and an organization actively operating in today's information society simple cannot ignore the problem, while it should strive to keep its workforce as empowered as possible if it's seeking productivity and innovation.

More resources on **insiders** can be found at :

http://www.astalavista.com/data/insider01.pdf
http://www.astalavista.com/data/280_camera_ready_paper.pdf
http://www.astalavista.com/data/insiderthreatsystemdynamics.pdf
http://www.astalavista.com/data/bankfin040820.pdf
http://www.astalavista.com/data/csipresentation.pdf

[**MASTERCARD SHUTS DOWN 1,400 PHISHING SITES**]

MasterCard International Inc. said Tuesday that it has shut down nearly 1,400 phishing Sites and more than 750 sites suspected of selling illegal credit-card information since launching an ID-theft-prevention program in June. The program also has led to the discovery and protection of more than 35,000 MasterCard account numbers that were in jeopardy of being compromised.

More information can be found at :

http://www.informationweek.com/story/showArticle.jhtml?articleID=163100641

Astalavista's comments :

Shutting down "sites", coming across 1,400 infected home users, or making actual Investigations - who's behind these frauds? From my point of view this story highlights how phishing shouldn't be fought in the long-run, namely shutting down pages when the phishing trends are reaching an automation level and the obvious coordination with spammers and malware authors. Use these as honeypots, get to know who's who, follow the financial leads and in case you really care about your customers, set up a web site that goes in-depth into anti-fraud and anti-phishing best practices. Besides, try to establish trusted security communication with them over the Web. Anyway, it's a great PR achievement, at least MasterCard are aware and catching up. These days a financial institution that doesn't address these issues will face loss in customers' confidence and the upcoming fututre legislations might hold banks liable for processing such transactions; although this shouldn't be done, there has to be a reasonable incentive for them to act on protecting and educating their customers.

[**GOOGLE DNS GLITCH SPARKS HACKING FEARS**]

A Domain Name System (DNS) glitch left many surfers unable to reach Google for a short time on Saturday (7 May). The SNAFU also left Google services such as Gmail and AdSense unavailable for around 15 minutes between 2345 and 0000 (BST) on Saturday night. "It was not a hacking or a security issue," Google spokesman David Krane told AP.

More information can be found at :

http://www.theregister.co.uk/2005/05/09/google_dns_glitch/

Astalavista's comments :

It finally happened – Google.com disappeared, OMG, I cannot even remember Yahoo's mail login URL like this! ☺ Although a great deal of our interviews and comments question Google on all fronts, we're not Anti-Google orieated, of course not! We're just privacy conscious because of its usability and U.S based headquaters. We like diversification but we hate dependence. The story will hopefully act as a wake up call for a lot of people out there, either express your privacy concerns by contacting Google or look for alternatives, but are there any? In future issues of the ***Astalavista Security Newsletter*** *we'll review possible alternatives to Google, as there're some to consider!*

[**CISCO CONFIRMS ARREST IN THEFT OF ITS CODE**]

Cisco Systems issued a statement Monday confirming that police in Sweden have arrested a suspect in connection with the theft of its networking equipment source code last year. A spokesman for the FBI, which began working on the theft last May, said the case is ongoing and declined to offer details.

The stolen code was a portion of Cisco's Internetworking Operating System version 12.3. The incident has been a matter of concern because malicious hackers might find flaws in the code that could be exploited to impair the functioning of Cisco's routers, which handle a significant portion of traffic on the Internet. At the time of the incident, however, Cisco said that the availability of its code did not pose an increased security risk.

More information can be found at :

http://www.theregister.co.uk/2005/05/10/cisco_hack_investigation/
http://informationweek.com/story/showArticle.jhtml?articleID=163101155#

Astalavista's comments :

That's indeed a high-profile break-in given the worldwide adoption and popularity of the IOS, and although Cisco would naturally deny that the availability of its code to malicious attacks might result in security vulnerabilities, I'd rather go through the code instead of trying to restore it. On the other hand, I really, really enjoy the 16 old hacker whiz kid media stories and the usual place where all the leads usually end up – a university's network. Does anyone remember the Kuji hacker? My point is that behind every scam/hack or whatever there's always the mastermind and the puppers/wannabes who usually do the dirty job and get caught. Besides, once something like this has been online, even worse in the hands of the dark side - someone out there still has a copy of it.

On the other hand this might indeed have something to do with the SSH Worm MIT's researchers mentioned given the systems concerned.

http://nms.csail.mit.edu/projects/ssh/sshworm.pdf

http://www.wasc.noaa.gov/wrso/security_guide/hacking.htm

[**HACKER HUNTERS**]

In an unmarked building in downtown Washington, Brian K. Nagel and 15 other

Secret Service agents manned a high-tech command center, poised for the largest-ever roundup of a cybercrime gang. A huge map of the U.S., spread across 12 digital screens, gave them a view of their prey, from Arizona to New Jersey. It was Tuesday, Oct. 26, 2004, and Operation Firewall was about to be unleashed. The target: the **ShadowCrew**, a gang whose members were schooled in identity theft, bank account pillage, and the fencing of ill-gotten wares on the Web, police say.

More information can be found at :

http://www.businessweek.com/magazine/content/05_22/b3935001_mz001.htm

Astalavista's comments :

Do you think the security vendors or security researchers are overhyping the threats when it comes to online scam, identity theft and phishing? Think twice, there's indeed an Underground out there, where individuals are actually trained in identity theft and Financial scams. What's to note about this case is the global reach of the gang and its actual transformation into online Ebay for identities etc.

The ShadowCrew gang bust is perhaps the most recent one of such a well- organized Web mob and the extremely well written BusinessWeek article will turn you into a participant of the actual bust.

*How did the actual **ShadowCrew.com** looked like before the bust can be seen at :*

http://web.archive.org/web/20041128051935/http://www.shadowcrew.com/

*The **U.S Secret Service's** "defacement" of **ShadowCrew.com** can also be found at :*

http://web.archive.org/web/20041128051935/http://www.shadowcrew.com/

[03] **Astalavista Recommends**

This section is unique with its idea and the information included within. Its purpose is to provide you with direct links to various white papers and tools covering many aspects of **Information Security**. These **security tools** and **security documents** are defined as a **"must see"** for everyone interested in deepening his/her knowledge in the security field. The section will keep on growing with every new issue. **Your comments and suggestions about the section are welcome at security@astalavista.net**

" **OPEN HIDS – WINDOWS HOST INTRUSION DETECTION SYSTEM** "

Open hids is a free, near-real time host intrusion detection system. The agent supports windows clients and servers, with other operating systems planned

http://www.astalavista.com/?section=dir&act=dnd&id=4133

" **TRIPP – A TOOL FOR REWRITING OUTGOING IP PACKERS** "

TRIPP is a utility to rewrite outgoing IP packets

http://www.astalavista.com/?section=dir&act=dnd&id=4128

" **FORENSIC ACQUISITION UTILITIES** "

This is a collection of utilities and libraries intended for forensic or forensic-related investigative use in a modern Microsoft Windows environment

http://www.astalavista.com/?section=dir&act=dnd&id=4119

" **HTML MANGLIZER** "

A tool that automatically checks for HTML parsing flaws

http://www.astalavista.com/?section=dir&act=dnd&id=4112

" **AIRJACK – WIRELESS MAN-IN-THE-MIDDLE DRIVER**"

AirJack is a device driver (or suit of device drivers) for 802.11(a/b/g) raw frame injection and reception.

http://www.astalavista.com/?section=dir&act=dnd&id=4138

" **HACKME BANK** "

Hacme Bank™ is designed to teach application developers, programmers, architects and security professionals how to create secure software. Hacme Bank simulates a "real-world" online banking application, which was built with a number of known and common vulnerabilities such as SQL injection and cross-site scripting.

http://www.astalavista.com/?section=dir&act=dnd&id=4205

" **PROXYPOT**"

The proxypot project aims to intercept spam messages as they are being sent, record the sender's identity, and provide evidence that can be used to get the spammers kicked off the Internet and thrown in jail.

http://www.astalavista.com/?section=dir&act=dnd&id=4097

" **BINTEXT V3.0** "

A small, very fast and powerful text extractor that will be of particular interest to programmers. It can extract text from any kind of file and includes the ability to find plain ASCII text, Unicode (double byte ANSI) text and Resource strings, providing useful information for each item in the optional "advanced" view mode. Its comprehensive filtering helps prevent unwanted text being listed.

http://www.astalavista.com/?section=dir&act=dnd&id=4089

" **WKNOCK**"

WKnock is a GPL tool that allows you to hide your Access Point against

opportunistic attackers (wardrivers, etc).

http://www.astalavista.com/?section=dir&act=dnd&id=4073

" **GALLETA V1.0** "

Galleta, the Spanish word meaning "cookie", was developed to examine
the contents of the cookie files. Galleta will parse the information in a cookie
file and output the results in a field delimited manner so that it may be imported
into your favorite spreadsheet program.

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4066

[04] **Astalavista Recommended Papers**

" **VIRUSES AND WORMS** "

An in-depth presentation about viruses, worms, defenses, why attacks continue etc

http://www.astalavista.com/?section=dir&act=dnd&id=4064

" **OIS GUIDELINES FOR SECURITY VULNERABILITY REPORTING AND RESPONSE** "

OIS's guidelines and recommendations for reporsting and responding to
software vulnerabilities

http://www.astalavista.com/?section=dir&act=dnd&id=4069

" **BETTER ANONYMOUS COMMUNICATIONS** "

This (215 pages) thesis contributes to the field of anonymous communications
over widely deployed communication networks

http://www.astalavista.com/?section=dir&act=dnd&id=4110

" **A CRYPTOGRAPHIC COMPENDIUM** "

This site contains a brief outline of the various types of cipher systems that have
been used historically, and tries to relate them to each other while avoiding
a lot of mathematics

http://www.astalavista.com/?section=dir&act=dnd&id=4106

" **GSM INTERCEPTION** "

Gives a brif overview(graphs included) of the GSM protocol and the
associated security risks

http://www.astalavista.com/?section=dir&act=dnd&id=4148

" **DESIGN AND IMPLEMENTATION OF A P3P-ENABLED SEARCH ENGINE** "

This paper introduces our prototype P3P-enabled Privacy Bird Search engine

http://www.astalavista.com/?section=dir&act=dnd&id=4124

" **INTERNET FILTERING IN CHINA IN 2004-2005 : A COUNTRY STUDY** "

The following report gives an in-depth overview of issues related to China's censorship such as : Sensitive/Controversial topics for media coverage Internet infrastructure and access Proxy testing results E-mail filtering Blog filtering Google cache testing Filtering search engines etc

http://www.astalavista.com/?section=dir&act=dnd&id=4202

" **REVERSE ENGINEERING AND PROGRAM UNDERSTANDING** "

Relatively comprehensive overview of reverse engineering and various programming concepts

http://www.astalavista.com/?section=dir&act=dnd&id=4195

" **PHISHING – BEHIND THE SCENES OF PHISHING ATTACKS** "

This paper focuses on real world incidents that the Honeynet Project has observed in the wild, but does not cover all possible phishing methods or techniques

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4185

" **BOTNET TRACKING** "

In this paper we show that preventive mechanisms can be as effective with much less effort : We present an approach to (distributed) DoS attack prevention that is based on the observation that coordinated automated activity by many hosts need a mechanism to remotely control them

http://www.astalavista.com/?section=dir&act=dnd&id=4162

[05] **Astalavista.net Advanced Member Portal v2.0 – Become part of the community today!**

Become part of the **community** today. **Join us!**

Wonder why? Check out :

The Top 10 Reasons Why You Should Join Astalavista.net

http://www.astalavista.net/v2/?cmd=tour&page=top10

and our **30%** discount this month

http://www.astalavista.net/v2/?cmd=sub

What is Astalavista.net all about?

Astalavista.net is a global and highly respected security community, offering

an enormous database of **very well-sorted and categorized Information Security resources - files, tools, white papers, e-books.** At your disposal are also thousands of **working proxies**, **wargames servers**, where you can try your skills and discuss the alternatives with the rest of the members. Most important, the daily updates of the portal turn it into a valuable and up-to-date resource for all of your computer and network security needs.

Among the many other features of the portal are :

- Over **5.5 GByte** of Security Related data, **daily updates** and always responding links.
- Access to thousands of anonymous proxies from all over the world, daily updates
- **Security Forums Community** where thousands of individuals are ready to share their knowledge and answer your questions; replies are always received no matter of the question asked.
- Several **WarGames servers** waiting to be hacked; information between those interested in this activity is shared through the forums or via personal messages; a growing archive of white papers containing info on previous hacks of these servers is available as well.

[06] Site of the month

---

http://project.cyberpunk.ru/

The **Cyberpunk Project** is an online, not-for-profit organization whose purpose is to promote, support, research, study, and create **cyberpunk** subculture.

[07] Tool of the month

Game Maker

Game Maker is a program that allows you to make exciting computer games, without the need to write a single line of code. Making games with Game Maker is a lot of fun. Using easy to learn drag-and-drop actions, you can create professional looking games within very little time. You can make games with backgrounds, animated graphics, music and sound effects, and even 3d games! And when you've become more experienced, there is a built-in programming language, which gives you the full flexibility of creating games with Game Maker.

http://www.astalavista.com/?section=dir&act=dnd&id=4257

[08] Paper of the month

Rocket science or social science? Involving women in the creation of computing

Women are not going into computing as a career in the same numbers that men do, but WHY? Great report!

http://www.astalavista.com/index.php?section=dir&act=dnd&id=4283

[09] **Geeky photo of the month – 'Enigma and Endemian'**

Every month we receive great submissions to our Geeky Photos gallery. In this issue we've decided to start featuring the best ones in terms of uniqueness and IT spirit.

'Enigma and Endemian' can be found at :

http://www.astalavista.com/images/gallery/enigma_endemian.jpg

[10] **Free Security Consultation**

Have you ever had a Security related question but you weren't sure where to direct it to? This is what the "Free Security Consultation" section was created for. Due to the high number of Security-related e-mails we keep getting on a daily basis, we have decided to initiate a service, free of charge. Whenever you have a Security related question, you are advised to direct it to us, and within 48 hours you will receive a qualified response from one of our security experts. The questions we consider most interesting and useful will be published at the section. Neither your e-mail, nor your name will be disclosed.

Direct all of your security questions to security@astalavista.net

Thanks a lot for your interest in this free security service, we are doing our best to respond as soon as possible and to provide you with an accurate answer to your questions.

Question : Hi folks, I might say that I'm pretty new to the security world, but I have extensive programming experience, and I'm interested in pursuing a career in the security industry, any suggestions would be greatly appreciated?

Answer : I'm sure you're aware of the fact that from a security point of view it's efficiency that matters, but from a security point of view it's the CIA of information that's most important, namely Confidentiality, Integrity and Availability of information. Programmers trying to get into the security industry usually start with gaining security knowledge or at least changing their mode of thinking to a certain extent depending on the position they seek. As **web application vulnerabilities** are on the rise, possible **code auditing** or **secure programming** initiatives might be something to consider. Most of all, know who's who and where to apply for a certain position. **Vulnerabilities research** is and hasl always been a trendy sector to pay attention to. Check out the following :

Information Security Career Roadmap :

http://www.infosec.co.uk/files/White_Paper_2002_intenseschool_career_roadmap.pdf

and the **InfoSec Career Hacking - Sell Your Skillz, Not Your Soul** book at :

http://www.bookpool.com/ss?qs=InfoSec+Career+Hacking+-+Sell+Your+Skillz%2C+Not+Your+Soul&x=25&y=14

As far as job opportunities are concerned, **SecurityFocus**.com is perhaps the most visited and active job placement service around these days.

http://securityfocus.com/jobs/opportunities

http://ukjobs.ostg.com/ - Europe mainly

Question : Hi folks, I've been an active P2P user for the past several years, and I must say I've witnessed the rise and fall of these when it comes to viruses, trojans and spyware, and even though the music industry thinks I'm a criminal, I'm not as I believe that if they cannot find a way to take advantage of P2P as concept of distributing information – it's not my fault. Getting back to my question now – as a U.K citizen I'm getting very concerned on getting busted for living in a digital age, any comments on how not to get busted?

Answer : Western European, even Eastern European countries are getting pretty tough on what they believe is privacy and copyrights infringement, and even though it is to a certain extent, they're successfully catching up on how to monitor, detect and actually prosecute the most active violators even users of P2P networks. **Lorrie Cranor** has written a very interesting document entitled "**Analysis of Security Vulnerabilities in the Movie Production and Distribution Process"** with the idea to highlight the vulnerabilities in the distribution process itself, you can find the paper at :

http://lorrie.cranor.org/pubs/drm03-tr.pdf

Make sure you know the laws in your country, and their actual enforcement, although the **Grokster case** might indeed have a global impact although the U.K is a well-known enforcer of P2P legislations.

Find more about the **Grokster case** at EFF's site :

http://www.eff.org/IP/P2P/MGM_v_Grokster/

Or in case you're interested in what the industry thinks is going on when it comes to piracy, go through the **"The Recording Industry 2005 Commercial Piracy Report"** at :

http://www.astalavista.com/?section=dir&act=dnd&id=4495

As far as **anonymous P2P** networks are concerned, check out the following site :

http://www.anonymous-p2p.org/

Recently, we have also come across a very well written report on the eventual commercialisation of P2P networks, take a look at it at :

http://www.dcia.info/P2PRE.pdf

Hope this was sufficient enough to provide you with even more insight on the topic!

Question : Hello Asta guys!! Cheers for the good work on your web site, among the most resourceful and up-to-date security ones these days. I've been reading quite a lot on passwords security recently and the introduction of biometrics as an alternative to passwords. My question is would I have to carry smartcards, usb authentication ticks or best of all use my voice to access my email because I'm not very comfortable with an idea like this?

Answer : Password insecurities are indeed getting more and more reasonable attention as an insecure authentication method, but they continue and will continue to be the standard or the first step of authentication we're all so used to. It's all because of the fact that everyone is looking and experimenting with alternative, more secure, yet cost-effective and flexible ways to authentication ourselves. Passwords will eventually turn into one of the many authentication factors, beside something we have, our smart card, or something we are – our voice, or retina, in the next couple of years. Meanwhile, make sure that you don't authenticate yourself in plain-text, that your PC's integrity is untouched by keyloggers, that you don't use the same passwords on different services and consider encrypting or adding more security layers to protect what's most valuable to you.

You can find more on passwords at :

http://www.windowsecurity.com/articles/Passwords-Attacks-Solutions.html

A passwords strength meter is accessible at :

http://www.securitystats.com/tools/password.php

"**Authentication and Session Management on the Web**"

http://www.astalavista.com/?section=dir&act=dnd&id=4455

"**Biometrics - A look at facial recognition**"

http://www.astalavista.com/data/db396.pdf

[11] Astalavista Security Toolbox DVD v2.0 - what's inside?

Astalavista's Security Toolbox DVD v2.0 is considered **the largest and most comprehensive Information Security archive available offline**. As always, we are committed to providing you with a suitable resource for all your security and hacking interests - in an interactive way!

The content of the **Security Toolbox DVD** has been carefully selected, so that you will only browse through quality information and tools. No matter whether you are a computer enthusiast, a computer geek, a newbie looking for information on "how to hack", or an IT Security professional looking for quality and up to date information for offline use or just for

convenience, we are sure that you will be satisfied, even delighted by the DVD!

More information about the DVD is available at:

http://www.astalavista.com/index.php?page=3

[12] Enterprise Security Issues

In today's world of high speed communications, of companies completely relying on the Internet for conducting business and increasing profitability, we have decided that there should be a special section for corporate security, where advanced and highly interesting topics will be discussed in order to provide that audience with what they are looking for - knowledge!

- DNS Security and the introduction of DNSSEC Part 2 -

In this brief article, Part 2 of our introduction to DNSSEC, we will review DNSSEC, its implications for the global community, its most distinguished Benefits. We will discuss some threats and usability issues and we will provide further info and resources on DNS Security and BIND.

What is DNSSSEC?

DNSSEC is the logical alternative to the outdate and prone to DNS fundamental Internet protocol – the DNS (Domain Name System). **DNSSEC** stands for DNS Security Extensions as its primarily function is to act as an extension to the existing DNS protocol, to verify origins of data and its integrity with the idea to prevent the many DNS associated threats we covered in our previous issue. **DNSSEC** takes care of verifying that all data must be authenticated through the use **Public Key Cryptography** and digital certificates before it can be trusted. It takes care of authentication by using cryptographically trusted digital signatures when signing DNS RRSets. Basically, **DNSSEC** seeks to provide authentication and integrity of this public data, which is so vital to the proper functionality of the Internet.

Why do we need DNSSEC and what are its benefits?

The distribution nature of DNS information on a worldwide basis can be considered an untrusted approach namely because of the time it takes to distribute it and because of the fact that not all the participants can be verified as trusted at the time of the request. In our previous issue we discussed the most important threats posed by DNS, and as we've seen recently, malware authors and malicious attackers are starting to realize the fact that due to software vulnerabilities, misconfigured or breached servers, they can take advantage and pretty much exploit the biggest vulnerability I see here – the end user who like me and everyone else cannot type IP numbers to visit a web site. Besides, the UDP based DNS service unlike the TCP where a certain degree of verification is possible, can easily receive spoofed information.

Although a bit outdated, this **Domain Health Survey** clearly highlights the fact that a

great number of actual participants in DNS information exchanges are spoofed :

http://www.menandmice.com/9000/9211_dns_spoofing.html

Are there any threats posed to DNSSEC?

Of course there're, while I believe the biggest threat if we can say it's a threat, is the lack of adoption of **DNSSEC** resulting in the growing exploitation of DNS in principle. **DNSSEC** does not provide confidentiality of the data, and naturally a breached server eventually results in a weak link in the whole chain, besides DoS or DdoS attacks, software vulnerabilities, the increased server load are some of the issues to consider. **A Threat Analysis of the Domain Name System** on the other hand can be found at :

http://www.rfc-archive.org/getrfc.php?rfc=3833

How to implement DNSSEC or how to at least secure Bind?

Check out the following documents :

DNSSEC in the .nl zone mini HOWTO - http://www.xtdnet.nl/paul/dnssec/
DNSSEC HOWTO : A tutorial in Disguise - http://www.ripe.net/disi/dnssec_howto/
DNSSEC Deployment Roadmap - http://www.dnssec-deployment.org/Roadmap%20rel%201.pdf

As far as securing BIND is concerned, "**Securing an Internet Name Server**" is a must read :

http://www.linuxsecurity.com/resource_files/server_security/securing_an_internet_name_server.pdf

Also the Internet Systems Consortium maintains a list of known BIND vulnerabilities at :

http://www.isc.org/index.pl?/sw/bind/bind-security.php

What to consider?

- Harden the OS and the machine itself
- Diversify by deploying servers with different ISPs
- Try to make sure server banners and fingerprinting techniques are out of the question
- Make sure ACLs and access controls are in place
- Don't reveal too much information, zone transfers should also be out of the question
- Consider realizing that DNS can indeed be very handy when fighting malware and spam
- Naturally apply the latest patches or IP stack updates to protect against associated threats
- Monitor your logs!!

Further reading on the topic can be found at :

http://www.sans.org/rr/whitepapers/dns/991.php
http://www.cs.jhu.edu/~ateniese/papers/dnssec.pdf
http://www.bleedingsnort.com/blackhole-dns/
http://isc.sans.org/presentations/dnspoisoning.php
http://www.astalavista.com/data/dnssec.pdf

[13] Home Users' Security Issues

Due to the high number of e-mails we keep getting from novice users, we have decided that it would be a very good idea to provide them with their very special section, discussing various aspects of Information Security in an easily understandable way, while, on the other hand, improve their current level of knowledge.

- **Mobile Phones' Bluetooth Attacks and how to Protect yourself -**

This article will provide with a brief introduction to the growing threat posed by Bluetooth-enabled devices, mobile malware and how to protect yourself. In future issues of the **Astalavista Security Newsletter** we'll go in-depth into mobile viruses and some future trends.

What is Bluetooth?

Bluetooth wireless communications quickly emerged as THE standard for short-range communication between countless number of digital devices without the need to use cables or any connectors. We caught ourselves using Bluetooth at home, at work, on the road and the content of our smart devices, being a notebook, PDA, or mobile phone could now be quickly and conveniently distributed among many others, primarily because of the mass adoption of the protocol as a "must have" by leading consumer electronics, and even car manufacturers. The protocol quickly gained worldwide acceptance and as you can image, they're currently more vulnerable Bluetooth enabled or Symbian OS based devices in the world than personal computers!

Is Bluetooth vulnerable to hacking attacks?

Although Bluetooth was tough to be developed with built-in security controls, its worldwide acceptance and the wireless nature of the protocol, combined with application and device based vulnerabilities resulted in a great level of attacks and vulnerabilities discovered during the last year – and yes, Bluetooth-enabled devices are vulnerable to hacking attacks, snooping or privacy violation attempts. What else motivates the research and actual exploitation of Bluetooth or mobile devices? Mobile phones cloning, communications and mobile multimedia interception, the perfect device tracking which could even be used on a mass-scale citizens identification and localization. Besides, we all store all of our contacts and in the upcoming future I picture the same scenario whenever I receive malware because someone in possession of my email in their Address Book got infected, namely we would be targeted by mobile malware and other hacking attempts on the basis of identifying our device and the overall lack of awareness that Bluetooth is under attack in the same way Wardriving is still relevant. And in case you're not aware Bluetooth-enabled devices can be attacked over a mile away with the help of the **Bluetooth Rifle** introduced at DEFCON 2004 :

http://www.tomsnetworking.com/Sections-article106-page1.php

How to protect myself and where can I find more resources on the topic?

- Be aware, know about the threats themselves, and no matter how uncomfortable you felt when you first found out that your wireless connection traffic might be intercepted, consider that it's your mobile device or Bluetooth enabled one that targeted this time

- Don't turn something ON when you don't use it, namely Bluetooth

- Make sure your device is in "undiscoverable" mode

- Consider that attacks might be "broadcasting" connection attempts

- Use encryption when communicating with Bluetooth devices

- Whenever pairing use a longer than the average 4 digits PIN, it's as easy to guess as your 4 characters password is

A great resource on **Bluetooth attacks** can be found at :

http://www.thebunker.net/security/bluetooth.htm

A summary **of Bluetooth Security Tools** can be found at :

http://www.astalavista.com//data/tools.pdf

also :

http://www.astalavista.com/data/redfang.2.5.tar.gz
http://www.astalavista.com/data/btscanner1.0.tar.gz
http://www.astalavista.com/data/blooover.jar - auditor
http://www.astalavista.com/data/bluehoc2.0src.tar.gz
http://www.astalavista.com/data/btexplorer0.3.2.rar
http://www.astalavista.com/data/tbear.tar.gz

As well as the following documents/sites on the topic :

http://www.symbian.com/phones/ - Symbian OS based phones
http://trifinite.org/
http://www.astalavista.com/data/107.pdf
http://www.astalavista.com/data/thesis0101.pdf
http://www.astalavista.com/data/preliminarystudy.pdf
http://www.astalavista.com/data/atstake_war_nibbling.pdf

[14] Meet the Security Scene

In this section you are going to meet famous people, security experts and all personalities who in some way contribute to the growth of the community. We hope that you will enjoy these interviews and that you will learn a great deal of useful information through this section. In this issue we have interviewed Roman Polesek, editor of **Hakin9's** security magazine.

Your comments are welcome at security@astalavista.net

Interview with Roman Polesek, http://www.hakin9.org/

Astalavista : Hi Roman, would you please introduce yourself, share some info about your background in the security industry, and tell us what is

Hakin9 all about?

Roman : My name is Roman Polesek, I am an editor-in-chief of the 'hakin9 - practical protection' magazine since Summer of 2004 [**http://hakin9.org/en**]. I'm 27 years old if it does matter. This might be a bit surprising for folks who know our magazine well, but I'm more a journalist/editor (and that is my education) than a CS/security master. Of course, I worked as a sysadmin for some time, use mainly Unices and code in several languages, but in the IT industry world I'm rather a self made man. I suppose I have no right to call myself "a hacker" in the proper [**http://www.catb.org/~esr/jargon/html/H/hacker.html**] meaning of the word. In short, 'hakin9' -- subtitled as "Hard Core IT Security Magazine" – aims to be a perfect source of strictly technical, IT security related quality information. We noticed that both the market and the community lack comprehensive, in-depth works on this topic. Decision was pretty simple: "Let's do it and let's do it good – we cannot fail". At the moment, with total circulation of nearly 50 thousand copies, we have 7 language versions. The magazine is available worldwide, by subscription or in distribution. However, it's important to remember that we are not encouraging anyone to commit any criminal acts. Beside disclaimers published in every issue of the mag, we emphasize on the legal matters wherever possible. We do not want to make a magazine for the so-called script-kiddies and assume that our readers are professionals and require some portion of knowledge to fully utilize magazine's content. On the other hand, as we all know, "The information wants to be free". There's no reason to avoid any particular subjects. Every article that precisely describes an attack technique includes a section that is to help defending from the threat we present. 'hakin9' is not only a magazine. The free cover CD is attached to every hardcopy. The disc includes a live Linux distribution called 'hakin9.live' [also available for download from **http://www.haking.pl/en/index.php?page=hakin9_live**] along with plenty of useful documentation [RFCs, FYIs, HOWTOs] and a really huge amount of computer/network security applications. We also prepare our own tutorials that allow readers to exercise the techniques described in articles [only in their very own networks!]. Since the next issue of 'hakin9', the CD will also contain full versions of commercial applications for Windows. Athough we rarely use Microsoft Windows, we consider it useful and some of the readers requested such software. One of the articles from each issue is available for free, just to make sure anyone that buys 'hakin9' won't regret the purchase. See our website if you're interested in trying 'hakin9' articles.

Astalavista : What do you think are the critical success factors for a security oriented hard cover magazine?

Roman : I am convinced that the crucial matter is honesty. Our target readers are highly educated, extremely intelligent people and would easily recognize any marketing lies. We just do not say things that aren't true. Everyone can see what we publish and how we do it. The other important thing is diversity. It's obvious that creating a magazine that fits everybody is impossible. There will always be a guy that is not satisfied with, say, the cover story or the layout or anything else. This is nothing unusual, but should be expressed loud and clear. That's why we cover different topics -- from e.g. attacks on Bluetooth stack, through data recovery in Linux or anti-cracking techniques for Windows programmers to methods of compromising EM emissions. Last but not least, the mother of all successes is making people aware of magazines' existence. Nobody would buy 'hakin9' unless they know we are available. But the main thing is that magazines like ours will never be mass publications, they have their niche that needs to be cultivated.

The general rule -- for all press publishers, not only us -- is "Respect your readers and they will respect you". Selling many copies of one issue, using lies and misleading information, is not difficult. What's difficult is to make sure that users will consider you a professional who just makes a good magazine, not a travelling agent.

Astalavista : What is the current situation on Poland's IT and Security scene, and do you think it's developing in the right direction from your point of view, beside Poland's obvious anti-software patents policy?

Roman : Yes, "Thank you Poland" and all. It's always nice to know that someone in the world has positive connotations with your country. But I cannot give you any general overview of the Polish scene. It's just too diverse and I work with IT specialists from all over the world, so I do not concentrate on Poland particularly. After all, most of the important things happen in the USA. Really, the main problem in Poland is software piracy. I'm not talking about P2P networks specifically, I'm talking about the consciousness of Polish people. They are just not aware of the fact that using cracked apps is a crime, a pure theft. I suppose this problem is present in all countries. And poverty does not justify such a procedure at all, we have plenty of free substitutes for even the most popular software. The Polish scene (I mean community by that, of course) is not very different from any other country. We do have a very strong group of open source ideologists (some might call them the followers of Richard Stallman :)), we do have some anti-patent people (I'd recommend http://7thguard.net for those who understand Polish). But we do not have any spectacular successes with any real inventions or discoveries (mind that for now I'm talking about the community, not the corporations). I'd only mention two phenomena your readers might have heard of. One is the LSD, [Last Stage of Delirium] an independent research group known for pointing out bugs in Microsoft RPC some years ago. The other well known is Michal "lcamtuf" Zalewski [http://lcamtuf.coredump.cx], an author of a powerful passive network scanner called "p0f" and a set of very useful debugging/binary analysis called "fenris". The reason for this unimpressive situation is the fact that Poland was cut off from the capitalist world for nearly 50 years [and ENIAC was introduced in 1947], so we were isolated from real computing during that time. We just have to make these 50 years in the next few years. On the other hand, IT specialists from Poland -- say, programmers -- are considered very ingenious and good workers. For offshore corporations they are really attractive.

Astalavista : During 2004/2005 we've seen record breaking *reported* vulnerabilities. What do you think is the primary reason, increasing Internet population, programmers' deepening their security knowledge, companies in a hurry to integrate more features with a trade-off in security or perhaps something else?

Roman : All of them. The increasing number of Internet users does not directly influence the number of vulns found, though. The new Internauts are mainly people who have never used computers and networks before. Of course the other thing is that Internet "aggregates" huge amounts of data, which was publicly unavailable before. There are more and more programmers and IT security specialists. Their population is constantly growing, be it because of the money they can earn or just the popularity of Computer Sciences. To be honest, most of them are at most average at their job,

but for example people from India an China have great potential.
But you are right. Marketing and pressure for higher sales make companies work in a great hurry, they just don't care about average Joe Sixpack. And Joe Sixpack would hardly ever notice any security vulnerabilities, not mentioning they would probably never report such flaws. Finding bugs in software has also become some kind of a fashion these days. It's an intellectual challenge, similar to solving riddles. No wonder that along with the increasing number of people able to understand, say, the C code, the number of vulns reported increases.
There is one more thing I'd like to mention. I suppose that the scale of reported vulns would appear far greater if proprietary software creators informed about all flaws found in their products. It's not in their interest of course.

Astalavista : Thought or at least positioned to be secure, MAC's and Firefox browsers have started putting a lot of efforts to patch the numerous vulnerabilities that keep on getting reported. Is it the design of the software itself or the successful mass patching and early response procedures that matters most in these cases?

Roman : I have great respect for Apple products, though the only Mac I use is a very old Performa :), just for experiments with BSD distributions. I consider Macs secure in general. I also use Mozilla Firefox daily.
I'd bet on the latter case, but like I said I'm no programming guru. The developers try to act fast and release patches as soon as possible, so at least average users can feel secure. The fact that there are plenty of developers makes it only better. Bugs in the code are not a nemesis themselves, you cannot avoid bugs in more complex applications. The only solution that makes sense for me is to conduct constant audits and release patches frequently.
Look at the Microsoft Internet Explorer [I am aware this example is a bit trivial]. I have a feeling that this company's ways of dealing with flaws is just childish, reminds me of covering your own eyes and hoping it will make yourself invisible to other kids on the playground.
I'm not criticizing Microsoft at all -- it's just that the company with so many great specialists has problems with securing their code, and their software is the most popular solution in the world, no doubt.
Apple is competing with Windows in general and Firefox tries to bite a part of the browser market. Looking at their financial and market share results makes me sure that the way the patches are done by these enterprises are the only right solution. Repeating that your product is secure and just better does not make it secure and better.

Astalavista : In may, a DNS glitch at Google forwarded its traffic to www.google.com.net (GoSearchGo.com) for 15 minutes. What are your comments about this event when it comes to security and mass DNS hijacking attempts on a large scale? Do you also picture a P3P enabled Google used on a large scale in the near future and do you fear that Google might be the next data aggregator (they are to a certain extent) breached into?

Roman : The real point is -- DJB mentioned that in an interview for the next issue of 'hakin9' -- that some of the protocols we use, especially SMTP and DNS, are outdated. To be precise, they were outdated at the moment they were being created. It's nobody's fault. We have a saying in Poland

that "Nobody is a prophet in his own country". Even Bill Gates didn't notice the potential of the Internet. I would say Google has really nothing to do with any DNS forgery. The protocol is flawful. What's worse, we can live without the problematic SMTP. Without DNS, which is a core of the Internet. For example, I just cannot imagine my mother using IP addresses to surf the WWW. I'm not afraid of threats to Google security. They have technology, they have money, they have ideas. I might say that it's Google, which will start and force security improvements in domain resolving mechanism. Daniel J. Bernstein claims that the first thing we should do is to implement some method of authentication in DNS protocol. Be it PKI, be it anything else -- we have to do it so that we would have some time to introduce a really secure DNS replacement. As for the hijacking itself, I consider it one of the most primitive kinds of abusing IT infrastructure. It's just like taking over somebody's house. It's as bad as deleting someone's data for sports or DDoS attacks used for fun and/or profit.

Astalavista : Anonymous P2P networks have been getting a lot of popularity recently namely because of RIAA's lawsuits on a mass scale. How thin do you think is the line between using P2P networks to circumvent censorship in Orwellian parts of the world, and the distribution of copyrighted materials?

Roman : 'hakin9' team likes P2P networks, the more anonymous, the better. We use them for distributing our free articles and our CD. It makes me laugh when **AAs send e-mails with legal threats based on the American legal system to Polish or Swedish citizens. Sometimes they're like an old blind man in the fog. Instead of adopting P2P for selling their video or music, they make the community angry. Digressions aside. I don't feel that P2P networks will help anyone make their transfers safe [security through obscurity, right?] and that they will help to fight censorship in countries like North Korea or even China. On the other side, I can imagine modifying XMPP [Jabber] protocol to transfer SSL-secured data -- it may be already done, I had no time to investigate it further. Unauthorized distribution of copyrighted content, however, will always be a problem. There's no way to prevent such behaviour. Recent events show us that writing a P2P client is a piece of cake, even a clever 9 years old boy can do this. I would rather make it easier for people to buy electronic copyrighted materials without the need to download it illegally. Regarding that according to some statistics even 30 per cent of total internet transfers are generated by P2P networks, I'm rather afraid that some stupid people downloading pr0n or Britney Spears MP3s could easily kill the Net some day. To sum up, each technology has its profits and costs. Obvious :). The profit of P2P is the ease of distributing any content. The cost is the people using it in an illegal manner. I can see no reason for prohibiting these network just because some people prefer bad quality motion pictures to going to the movies. Should we prohibit usage of knives only because of the fact that someone tabbed the kitchen knife in someone s stomach?

Astalavista : In conclusion, I wanted to ask you what is your opinion of the Astalavista.com's web site, in particular, our security newsletter?

Roman : I'm very impressed with the amount of data available for Astalavista's visitors. I'm not a member though, so I cannot really make a detailed

review. To be honest, I had some problems with recognizing which of your websites are free and which ones are not. But I have managed to do it and use it almost daily :). As for the newsletter, it's one of the most informative and professional ones I have ever seen. Since having read Issue 16, I couldn't stop myself from reading the archives. I am a subscriber and strongly advise everybody to do the same. As a person professionally dealing with IT security, I mean it – this is not an advertisement for Astalavista. This is the truth.

Astalavista : Thanks for your time Roman!

[15] IT/Security Sites Review

The idea of this section is to provide you with reviews of various highly interesting and useful security or general IT related web sites. Before we recommend a site, we make sure that it provides its visitors with quality and a unique content.

-
Irongeek.com
-
http://www.irongeek.com/

Quite a few video tutorials on various security topics, a small site with great potential

-
Electronics-lab.com
-
http://www.electronics-lab.com/

Useful circuits, diagrams, electronics articles, you name it!

-
Googlesightseeing.com
-
http://www.googlesightseeing.com/

Take a look at the best and weirdest spots in the world via Google Maps
-
Top100.cyberpunk.co.uk
-
http://top100.cyberpunk.co.uk/

A great top list of techno culture and cyberpunk related sites
-
Gsm-security.net
-
http://www.gsm-security.net/

Comprehensive site on GSM security, protocols, devices, etc.

[16] Final Words

Dear readers,

Thank you for going through our Issue 17, enjoy yourselves, stay secure and most of all– be aware!

Watch out for more quality stuff at Astalavista.com, meanwhile, keep your feedback coming!

Expect the new **Astalavista.com** web site in the upcoming weeks,
it will simply impress you.

Editor - Dancho Danchev
dancho@astalavista.net

Proofreader - Yordanka Ilieva
danny@astalavista.net