Global Information Assurance Certification Paper

Open Source Firmware on a Commodity Broadband/Wireless Router: A Powerful Low Cost Solution for Network Monitoring, Management and Security.

Fred Dulles
GIAC Security Essentials (GSEC)
Practical Assignment
Version 1.4c, Option 1
12 December 2004

Abstract: The use of open source replacement firmware on a commodity broadband router and wireless access point (Linksys WRT54GS[1]) is described. The hardware and software basis for these devices is described, as is the utility inherent in the use of open source licensing. The capabilities offered by the Sveasoft firmware[2] (Alchemy 6.0rc3[3]) are described and compared to alternatives with emphasis on the networking security features. Possible uses are described and discussed, particularly in the creation of sophisticated, secure, broadband-attached, home networks with wireless access. Concluding remarks address the subject matter in the context of the development of modern technological trends and implications for the future.

[1] Linksys (a division of Cisco Inc.), "Linksys Wireless-G Broadband Router with Speedbooster", 2004 http://www.linksys.com/products/product.asp?grid=33&scid=35&prid=610

[2] Alchemy 6.0rc3 firmware, Sveasoft Inc., 2004 http://www.sveasoft.com/, this version of the software is not freely distributable, as will be discussed below.

[3] A newer version (rc4) of this firmware was released very close to the deadline for this report, and will not be addressed. See <http://www.linksysinfo.org/modules.php?name=News&file=article&sid=167>

Introduction: Recently, it was found that among active home users, broadband had overtaken modems as the most popular means of accessing the Internet.[4] It is also clear that home computers are particularly poorly protected from the longstanding plague of Internet based security threats, particularly broadband (predominantly cable or DSL) attached computers.[5] As a result, the need for effective tools to protect home networks where they come in contact with the Internet is greater than ever. This is not to discount the importance of 'defense in depth' network security[6] by neglecting other best practices for securing home computers, but the combination of Sveasoft software and Linksys hardware constitutes a remarkably powerful and inexpensive tool for monitoring and protecting a broadband-attached home network.[2,7]

The particular Sveasoft firmware discussed here is not the only alternative. Most obviously the firmware provided by the manufacturer Linksys was the basis of the Sveasoft product, and has incorporated innovations from it.[8] There are also other third party options, essentially because Linksys obtained its firmware from Broadcom and its subcontractor, who based their software on an embedded version of Linux, releasing the source code in accordance with the GNU Public License (GPL)[9] and therefore made it possible for others to extend that source code. These options are not necessarily needed for some home users, particularly since the default software offered by the manufacturer has been further developed to it's current version, 3.37.2.[10] The utility of the stock Linksys configuration has been noted in other GSEC reports.[11] There are also more cutting edge version with new capabilities that may appeal more to [particular users depending on a their needs and tolerance for lightly tested software and its bugs.

---

[4] Web Site Optimizations, LLC. November 2004 <http://websiteoptimizations.com/bw/0411/> citing data attributed to Nielsen/NetRatings

[5] Home Computer Security, CERT Coordination Center, Carnegie Mellon University, Pittsburgh, November 2004 < http://www.cert.org/homeusers/HomeComputerSecurity/>
This is by the way a very good resource for explain how and why to secure home computers.

[6] SANS Institute. Track 1 – SANS Security Essential and the CISSIP 10 Domains. Volume 1.2 . Defense In-Depth SANS Press, January, 2004.

[7] LinksysInfo.org, 2004 <http://www.linksysinfo.org/>

[8] "The Little Engine that Could", Robert X. Cringley, 27 May 2004 <http://www.pbs.org/cringely/pulpit/pulpit20040527.html>

[9] GNU Foundation, "GNU General Public License v. 2", Boston, MA 2 June1991 <http://www.gnu.org/copyleft/gpl.html>

[10] Linksys website: <http://www.linksys.com/download/firmware.asp?fwid=207>

[11] See e.g. Herman, Shane Hitchhiker's Guide to Securing the Mobile Worker SANS GSEC Practical Assignment, 4 October, 2004 <http://www.giac.org/practical/GSEC/Shane_Herman_GSEC.pdf>

Linksys WRT54GS

Hardware:
The hardware platform used is the Linksys model WRT54GS broadband router[1]. It is quite commonly available, for this report it was purchased new for $79 plus shipping from newegg.com. It comes with four switched 10/100baseT full duplex ports, a similar WLAN/uplink port and a wireless 802.11b/g[12] access point. The WRT54GS is the most capable member of a family or routers sold by Linksys in that it has 32 MB RAM and 8 MB flash RAM (Used to store the firmware image and configuration) and is driven by a 200MHz MIPS processor.[13] The memory installed is twice that in other members of its family. It also includes a wireless throughput enhancement technology developed by Broadcom, the supplier of the wireless chipset included which involves the use of packet bursting to improve throughput over standard 802.11g and seems to be the main selling point.[14]

Software Base
The base software used by Sveasoft is the Linux 2.4 kernel and a carefully tailored set of libraries and tools (relative to a common desktop Linux distribution such as RedHat) that fit in the space available. The kernel itself has been compiled with fewer modules than in a desktop distribution (8 in the running firmware as compared to 85 in the present author's fairly plain Debian[15] (testing) distribution.) Of course a great deal of space is saved because no graphical interface (other than web pages) is needed. One key to minimizing the size of the software is replacing the standard libc core library with uClibc[16], which is designed for use in embedded applications by replacing most of the standard glibc's functionality transparently. The author of uClibc claims that when

[12] Wikipedia, "802.11" <http://en.wikipedia.org/wiki/IEEE_802.11 - 802.11g>
[13]Depew, J "Autopsy: Linksys WRT54 Hardware Versions Under the Knife" LinksysInfo.org 17 May 2004 <http://www.linksysinfo.org/modules.php?name=Content&pa=showpage&pid=6>
[14] Judge , Peter "G Whizz - the 802.11g boosters" Techworld, 25 March 2004 <http://www.techworld.com/mobility/features/index.cfm?FeatureID=442>
[15]Debian, "Debian web page" December 2004 < http://www.debian.org/>
[16] Erik Andersen, "uClibc Frequently Asked Questions" <http://www.uclibc.org/FAQ.html>

compared on a similar basis, uClibc requires 570KB, where the standard Linux glibc needs 30 MB of space[16].

As mentioned above, the open source origins of the firmware lead Linksys to release its derived version in accordance with the GPL.[9] This in turn allowed James Ewing to start a company, Sveasoft, to enhance Linksys's firmware while making money by selling a subscription service for support and access to pre-release versions of the software.[8] A number of other open source tools were added to the Linksys software as well including small SSH client[17], WonderShaper[18] and support for more sophisticated firewalling.[19]

Licensing

The use of open source software has been a key reason for the present success of this project. Initially it (presumably) allowed Linksys access to a substantial ready-made base of software, development tools and documentation at no initial cost, meaning it could bring its product to market sooner and more cheaply than otherwise. The *quid pro quo* of using GPL licensed software means that they continue to make the source code for their product available and freely redistributable.[20] This in turn allowed the birth of a number of projects[21] that develop enhancements to the firmware including the subject of this report. Linksys has continued to improve its software at least partially by incorporating work from those projects, increasing the payoff for the company and its customers[8].

The business model of Sveasoft deserves some discussion. Sveasoft put in place a system that allows it to remain compliant with the GPL while also producing revenue to fund their development. Essentially, Sveasoft supports two versions of their software, release and pre-release. The release version is older and is completely open source. The original parts of the pre-release version are not open-source and may not be freely redistributed. Instead, access to the newer, enhanced (but potentially more buggy) pre-release is obtained by subscription which also provides greater support services for $20/year. Over time, the pre-release version matures and released as the new public version, open to all. Then a new pre-release development version is started. (Recently, Sveasoft has started to use the Apache Software License rather than the GPL[22], a change which affects nothing at the level of detail discussed here.) According to the Sveasoft site, they have approximately 8,000 subscribers (32,000 free

---

[17] Johnston, Matt, DropBear SSH web page, December 2004 <http://matt.ucc.asn.au/dropbear/dropbear.html>

[18] Hubert, Bert "The Wonder Shaper" 2002 <http://lartc.org/wondershaper/>

[19] L7 packet filter group, "Application Layer Packet Classifier for Linux" web page <http://l7-filter.sourceforge.net/>

[20] See [1] above and <http://www.linksys.com/support/gpl.asp>

[21] See e.g. Jans, Timothy "HyperWRT" web page 2004 <http://www.hyperdrive.be/hyperwrt/index.php?page=home-page>

[22] Sveasof Site Admin, "I am a Sveasoft subscriber, can I redistribute?" 2 November 2003 <http://www.sveasoft.com/modules/phpBB2/viewtopic.php?t=3868>

registrants) as of December 2004, which suggests revenues in the range of $170,000/year. There has been some criticism of this model, including claims that it violates the GPL or at least its spirit, but the Free Software Foundation does not agree:

> I see no problems with this model. If the software is licensed under the GPL, and you distribute the source code with the binaries (as opposed to making an offer for source code), you are under no obligation to supply future releases to anyone" Peter Brown ,GPL Compliance Manager, Free Software Foundation[23]

So, the Sveasoft model appears to be a good example of a productive open source project that also generates enough revenue to sustain itself now and going forward.

Capabilities

The capabilities of this system are extensive. What follows is an overview with emphasis being placed on those capabilities not found in the standard Linksys software and either are most directly related to security or otherwise of the greatest practical utility. It will not be possible to cover all the options in full depth, but this discussion is meant to serve as an introduction that can encourage further study elsewhere. The discussion below will be based around the organization of the web interface provided for managing the router.

The initial setup page provided Alchemy is quite similar to those provided by Linksys. It provides options for the interface for connecting to the ISP, e.g, DHCP, PPPoE or PPTP. The local time zone can be set as can basic DHCP parameters for the local network.

The next tab, DDNS, allows the router to work with a number of services in the Internet to provide a constant host and domain name for a dynamic address, as is often provided by broadband ISP. In effect, it makes it possible to connect to the home network from outside using a name the is more user friendly and constant than the potentially variable IP number dynamically handed out by the ISP. The Sveasoft package offers more options for the DDNS service provider. The following MAC address cloning tab allows the router to present the MAC address registered with the ISP. Here the Alchemy adds the ability to set the MAC address used by the wireless access point.

The subsequent tag allows the WRT54GS's routing function to be configure for use in networks more complicated than the prototypical home situation. It is

[23]Sveasoft site Admin, "What is the Free Software Foundation stance on Sveasoft", 17 June 2004 <http://www.sveasoft.com/modules/phpBB2/viewtopic.php?t=2823>

possible to hand configure static routes or rely on RIP2 based dynamic routes for networks which have more than one router. Sveasoft has added the ability to use OSPF, which fill the same function but more efficiently the RIP2[24]. Finally, the Sveasoft firmware adds the ability to configure VLANS and also to do link aggregation for ports 3 and 4. VLANs (Virtual LANs) are a large topic in and of themselves, but it is enough to say the they are a way to organize traffic by defining logical as opposed to physical LANs, for managerial ro security based reasons. They can be very useful, though they should not be relied on solely to provide security. The link aggregation for ports 3 and 4 allows those ports to act as a single link with twice the bandwidth.

The Wireless configuration options provide the ability to set the channel used (including channels legal only in Europe and/or Japan), whether wireless service is disabled, b mode only, g mode only or both, and set the SSID and allow or prevent SSID broadcast. The security sub-tab control whether WEP is used or its more secure successor WPA is used, with a choice of encryption and authentication options including RADIUS when a RADIUS authentication server is present on the network. MAC filtering provides the ability to define a list of MAC addresses the can act as either a black or white list for wireless access control.

The advanced settings tab allows a large number of parameters controlling the details of wireless transmission to be adjusted. Two setting of note are the transmit power parameter which can be used to increase the range of outgoing packets (but does nothing for reception). The other Afterburner setting (called packet burst in the Linksys stock software) is a method of increasing wireless bandwidth by packet bursting.

WDS (Wireless Distribution System) service configuration is available in the last wireless configuration tab, and is a Sveasoft addition. WDS is a way of networking wireless access points to each other over the air, rather than through a wired Ethernet backbone. As such, it is a form of mesh networking. In practice this can allow a community of wireless access points to network to each other and to the Internet even though only a small number of nodes have internet connections.

The Security tab offers two sub-tabs, Firewall and VPN. The Firewall tab enables the firewall (but not its configuration) and offers the option to block ping requests from the Internet. Note that without further configuration available under other tabs, the default is to block incoming connections. The VPN tab allows Virtual Private Network traffic to be passed by the router for the three most common VPN protocols, IPSec, PPTP and L2TP.

[24] Hall, Eric, Internet Core Protocols, The Definitive Guide Sebastopol, CA 2000, pp. 39

The Access Restrictions tab contains options for blocking access to the Internet from the inside of the network. This tab is heavily modified in the Sveasoft firmware as compared to Linksys'. (Linksys has a page missing here which provides an interface to an external commercial parental control service.) Up to ten rules may be configured, each of which blocks or allows Internet access to be blocked for a combinations of times and days, for particular MAC addresses or IPs, for particular ports, or URLs or even website keywords. Parental access control seems to be the main intended purpose.

The Applications & Gaming tab provides port range forwarding for seqences of ports in cases where there are services that need to be made available to the Internet. In the next tab, 'Port triggering' applications can temporarily casue ports to be opened in cases where the router detects outgoing access on certain other ports. This permits a kind of stateful access where a port generally closed can be temporarily opened when needed. The following tab allows a DMZ (DeMilitarized Zone) computer, designated by its IP, to be exposed to the Internet. This in effect forwards all ports to this computer, which may be insecure. The final sub tab, added by Sveasoft, adds QoS (Quality of Service) regulation. Bandwidth can be allocated based on the service type, the destination subnet, the sending MAC address or the physical router port. Priorities may be set to bulk, standard, express and premium. This prioritizing of traffic can make the sharing of bandwidth much more effective, and can effectively improve throughput[8].

The Administration tab controls a number of management related settings. These include the ability to turn on SNMP (Simple Network Management Protocol, which has itself been a security liability in the past), and external syslogd reporting. It also allows both telnet and (much more securely) ssh access to the router command line. This enabled less friendly but even more powerful and detailed configuration of the router. It is also possible to enable Internet access to the web management features, including setting the port and using https to encrypt the link. The server can also be set up to use DNSmasq which will act with the DHCP service as a sort of caching nameserver for local machines, forwarding non-local requests to the external DNS server. It is also possible to permanently assign IP to given local machines that are leased via DHCP rather than being statically assigned. NTP client services can be enabled and assigned to an external server as well.

There are sub-tabs for loading new firmware, and for resetting firmware to factory settings. It is also possible to backup setting to a file on a local client for subsequent reloading. The diagnostic tab in the Sveasoft OS gives somewhat limited access to the command line to perform, pings, traceroutes and other monitoring commands.

Extensibility and Possible Future Directions

The Sveasoft web site a users forums are a very useful resource for information on who to use the firmware. That being said, as is sometimes the case with complicated software, better documentation is needed. The web interface described above also could be reorganized to promote ease of use. It feels as though as features were added they have been placed in the web pages in a fairly unplanned manner and thus can be hard to find.

There are a number of impressive third party applications linked at the Sveasoft site that are not discussed here but deserve to be. These integrate well with the Sveasoft package and enhance its power, including MRTG, ntop, FirewallBuilder and WallWatcher[25]

Conclusion

The power and configurability of the WRT54GS combine with the Sveasoft firmware is impressive. It seems likely that the usability and power of follow on devices and firmwares will increase while their cost falls, riding the same technological trends current in all of information technology. This is a case where the open source model has worked very well. This is a good thing, both for information security where the threats are also growing more potent, but also in other applications, some of which may be truly disruptive, as Cringely predicts[8].

[25] Sveasoft, 2004, <http://www.sveasoft.com/component/option,com_weblinks/catid,70/Itemid,4/>