Firewall leak testing

David Matousek of Matousec Transparent Security and Paul Whitehead of Comodo prepared, especially for hakin9 readers, personal firewalls leak – test. Here are the resultus.

What is a firewall?

Broadly speaking, a computer firewall is a software program that prevents unauthorized access to or from a private network. Firewalls are tools that can be used to enhance the security of computers connected to a network, such as a LAN or the Internet. They are an integral part of a comprehensive security framework.

Personal Firewalls are intended to isolate your computer from the Internet by inspecting each individual *packet* of data as it arrives at either side of the firewall – inbound to or outbound from your computer – to determine whether it should be allowed to pass or be blocked.

Firewalls have the ability to further enhance security by enabling granular control over what types of system functions and processes have access to networking resources. These firewalls can use various types of signatures and host conditions to allow or deny traffic. Although they sound complex, firewalls are relatively easy to install, setup and operate.

Why does a user need a firewall?

When your network is connected to a public network, it is potentially exposed to a number of threats including, hackers, spyware and Trojan horse programs. The increasing ubiquity of 'always on' broadband internet connections means users need to be increasingly vigilant of security issues, as network traffic coming into the computer can cause damage to files and programs even when the user is away from the computer and the computer is idle. In a system that is not protected with any security measures, malicious code such as viruses can infect systems and cause damage that may be difficult to repair. The loss of financial records, e-mail, customer files, can be devastating to a business or to an individual.

Unfortunately, many of these malicious programs employ very advanced techniques to conceal their activities in an attempt to bypass the standard protection mechanism provided by most personal firewalls. These techniques are commonly known as *leak* techniques.

What is a firewall leak-test?

Leak tests are small, non-destructive, programs designed by security experts that deliberately attempt to bypass a firewall's outgoing security measures. The rationale behind them is painfully simple: *If this test can get past your computer's security defenses, then so can a hacker.* Explicitly designed to help identify a firewall's security flaws, leak tests provide the invaluable function of informing the user whether or not their firewall is providing adequate protection. The tests pose no real threat to the security of a computer as they are harmless simulations of the attack techniques typically used by spyware and Trojan horse programs. There are many leak-testing programs available – each one designed to exploit a particular flaw and each using a particular attack technique to break a firewall's standard protection mechanisms.

Techniques employed by leak testing software

Substitution: This technique tries to present itself as a trusted application. There are a few different possibilities how to achive this. For example the application can try to rename itself to a commonly known, safe application name such as iexplore.exe. As a result, firewalls that do not verify application signatures or verify too late fail to detect such attempts.
Trojans that use this technique: W32.Welchia.Worm, The Beast *Leak Tests that emulate this technique*: LeakTest, Coat, Runner

Launching (parent substitution)

With this technique, a program launches a trusted program by modifying its startup parameters such as command line parameters, to access the Internet. This type of penetration bypasses the firewalls that do not apply parent process checking before granting the internet access.
Trojans that use this technique: *W32.Vivael@MM*
Leak Tests that emulate this technique: TooLeaky, FireHole, WallBreaker, Ghost, Jumper, Surfer, CPIL, CPILSuite1, CPILSuite2, CPILSuite3

DLL injection

Being one of the most commonly used techniques by Trojans, this method tries to load a DLL file into the process space of a trusted application. When a DLL is loaded into a trusted process, it acts as the part of that process and consequently gains the same access rights from the firewall as the trusted process itself. Firewalls that do not have an application component monitoring feature fail to detect such attacks.
Trojans that use this technique: The Beast, Proxy-Thunker, W32/Bobax.worm.a
Leak Tests that emulate this technique: pcAudit, pcAudit2, FireHole, Jumper, CPILSuite3, AWFT

Process injection

This technique is the most advanced and difficult to detect penetration case that many personal firewalls still fail to detect although it is used by Trojans in the wild. The attacker program injects its code into process space of a trusted application and becomes a part of it. No DLL or similar component is loaded.
Trojans that use this technique: Flux trojan
Leak Tests that emulate this technique: Thermite, CopyCat, CPIL, DNStest, AWFT

Default rules

Certain personal firewalls try to allow full access internet access rights to vital specific traffic such as DHCP, DNS and netbios. Doing so blindly may cause malicious programs to exploit these rules to access the Internet.
Trojans that use this technique: Unknown
Leak Tests that emulate this technique: YALTA

Race conditions

While filtering the Internet access requests per application, personal firewalls need the process identifier (pid) of a process to perform its internal calculations. Attacker programs may try to exploit this fact by changing their process identifiers before personal firewalls detect them. A robust personal firewall should detect such attempts and behave accordingly.
Trojans that use this technique: Unknown
Leak Tests that emulate this technique: Ghost

Own protocol driver

All network traffic in Windows operating systems are generated by TCP/IP protocol driver and its services. But some Trojans can make use of their own protocol drivers to bypass the packet filtering mechanism provided by personal firewalls.
Trojans that use this technique: Unknown
Leak Tests that emulate this technique: –

Recursive requests

Some system services provide interfaces to applications for common networking operations such as DNS, Netbios etc. Since using these interfaces is a legitimate behavior, a Trojan can exploit such opportunities to connect to the Internet.
Trojans that use this technique: Unknown
Leak Tests that emulate this technique: DNStester, BITStester

Windows messages

Windows operating system provides inter process communication mechanism through window handles. By specially creating a window message, a Trojan can manipulate an application's behavior to connect to the Internet.
Trojans that use this technique: Unknown
Leak Tests that emulate this technique: Breakout

OLE automation, DDE

Windows operating system also provides inter process communication mechanism through COM interfaces. By using a COM interface hosted by a server application, a Trojan can hijack the application to connect to the Internet. Another similar mechanism for inter process communication is Direct Data Exchange (DDE).
Trojans that use this technique: Unknown
Leak Tests that emulate this technique: PCFlank, OSfwbypass, Breakout2, Surfer, ZAbypass

Unhooking

Personal firewalls commonly use so called hooks to implement their protection mechanisms. There exist two major types of hooks – kernel mode hooks and user mode hooks. If the self-protection mechanisms are not implemented well by the firewall it may be possible to unhook its hooks. As a result, some or all protection mechanisms of the firewall are disabled.
Trojans that use this technique: Unknown
Leak Tests that emulate this technique: FPR

Testing

hakin9 asked Matousec – Transparent security to perform leak testing for popular personal firewall products. Each firewall was tested twice against 26 of the most powerful leak tests available – once with its default, out-of-the-box settings, and once with its highest security settings. Each firewall was then awarded an overall score derived from its pass/fail result against each test. The higher the score, the better the firewall performed against the range of leak tests. For every passed test on the highest security settings the firewall gained 100 points, for every passed tests on the default security settings the firewall gained 125 points.

The results of our tests are displayed in the table below. Some tests implement more than one leak test technique.

Appendix – description of each leak test used in the hakin9 tests

Atelier Web Firewall Tester 3.2 (AWFT)
Author: José Pascoa
Website: *http://www.atelierweb.com/awft/*
Category: Process Injection, Parent Substitution, DLL Injection

Atelier Web Firewall Tester contains 6 very effective leak tests each of which is used to calculate a grade over 10, for the personal firewall tested.

Test 1: Attempts to load a copy of the default browser and patch it in memory before it executes.

Test 2: Attempts to create a thread on a loaded copy of the default browser.

Test 3: Attempts to create a thread on Windows Explorer

Test 4: Attempts to load a copy of the default browser from within a thread in Windows Explorer and patch it in memory before execution. This attack regularly beats most personal firewalls which require authorization for an application to load another application.

Test 5: Performs a heuristic search for proxies and other software authorized to access the Internet on port 80. Then it loads a copy of this software and patches it in memory before execution from within a thread on Windows Explorer. This is a very difficult challenge for most personal firewalls!

Test 6: Performs a heuristic search for proxies and other software authorized to access the Internet on port 80 then requests the user to select one of them. It then creates a thread on the select process.

Unlike other leak tests, AWFT is not free. We would like to thank its author, José Pascoa, who provided us a free licence for our tests.

Tabela 1. *Firewalls Comparison*

TEST / PRODUCT	BlackICE PC Protection 3.6.cpv	CA Personal Firewall 2007 3.0.0.196	Comodo Personal Firewall 2.3.6.81	Jetico Personal Firewall 2.0.0.16 beta	Kaspersky Internet Security 6.0.0.303	McAfee Internet Security Suite 2006 8.0	Norton Personal Firewall 2006 9.1.0.33	Outpost Firewall PRO 4.0 (971.584.079)	Sunbelt Kerio Personal Firewall 4.3.268	Windows Firewall XP SP2	Zone-Alarm PRO 6.5.737.000
AWFT (?/10)	10*	-	10*	10*	3*/7+	1*	3*/6+	10*	5*	-	10*
BITStester	-	-	*	*	-	-	+	*	-	-	
Breakout	-	-	*	-	-	-	-	*	-	-	*
Breakout2	-	-	*	*		-	+	*	-	-	
Coat	*	*	-	*	+	*	*	*	+	-	*
CopyCat	-	-	*	*	+	-	-	*	*	-	*
CPIL	-	-	*	*	+	-	-	*	-	-	*
CPILSuite (?/3)	-	-	3*	3*	2+	-	-	3*	1+	-	1*
DNStest	*	-	*	*	+	-	-	*	*	-	*
DNStester	-	-	*	*	-	-	-	*	-	-	*
FireHole	*	-	*	*	+	*	+	*	*	-	*
FPR (?/38)	23*	4*	35*/3+	36*	3*/28+	7*/1+	6*/15+	12*/3+	6*/15+	-	33*
Ghost	*	-	*	*	+	-	+	*	+	-	*
Jumper	*		*	*	+	*	-	*	-	-	*
LeakTest	*	*	*	*	+	*	*	*	+	-	*
OSfwbypass	-	-	*	*	-	-	-	*	-	-	-
pcAudit	*	-	*	-	+	*	+	*	*	-	*
pcAudit2	-	-	*	*	+	-	-	*	*	-	*
PCFlank	-	-	*	*	-	-	-	*	-	-	-
Runner	*	*	*	*	+	+	+	*	+	-	*
Surfer	*	-	*	*	-	-	+	*	+	-	*
Thermite	-	-	*		+	-	-	*	*	-	*
TooLeaky	*	-	*	*	+	-	+	*	+	-	*
Wallbreaker (?/4)	1*	-	1*/3+	4*	4+	2*	1+	4*	4+	-	4*
YALTA	*	*	*	*	+	*	*	*	+	-	*
ZAbypass	*	-	*	*	+	*	+	*	-	-	*
TOTAL SCORE	5750	1000	9350	9125	6350	2325	4600	6675	4825	0	8250

* means the firewall passed the test on its default settings
+ means the firewall passed the test on its highest security settings, not on its default settings
- means the firewall did not pass the test

BITStester
Author: Tim Fish
Category: Recursive Requests

Since XP there have been Background Intelligent Transfer Service (BITS) installed in the Windows OS by default. Using a tool called BITSadmin from the Microsoft Windows XP Service Pack 2 Support Tools it is possible to control this service and order it to connect to a specific URL and download a file from the Internet. BITStester is a batch script that performs necessary steps to download a file.

Breakout
Author: Volker Birk
Website: *http://www.dingens.org/*
Category: Windows Messages

Breakout uses Windows Messages to control the Internet browser. It has two implementations, one for Internet Explorer and one for Mozilla or Firefox browsers. Using messages it is able to redirect the browser to the given location.

Breakout2
Author: Volker Birk
Website: *http://www.dingens.org/*
Category: OLE Automation

Breakout creates HTML page on the local disk that points to the Internet server. Then, it enables Windows Active Desktop and set that HTML page to be the desktop wallpaper. As a result, Windows Explorer connects to the given URL.

Coat
Author: Matousec – Transparent security
Website: *http://www.matousec.com/*
Category: Substitution

The Coat rewrites its own memory and tries to establish an Internet connection. It rewrites its image base, image name, command line, Windows title etc. and it also changes the information of the main module in the module list. All these data reside in the address space of its process. All the data are changed to match the image of the default browser. Then, it tries to establish the Internet connection.

Firewalls that are not able to handle this trick suffer from a big design bug because they trust ring 3 data of malicious processes. They do not have their internal list of running programs and obtain this information when it is needed. This gives malicious processes enough time to modify these data before they execute privileged actions. Such firewalls (as well as many other programs – e.g. Process Explorer from Sysinternals) then see the malicious process as something else – e.g. the default browser – and allows the execution of privileged actions without any questions.

CopyCat
Author: *bugsbunny@e-mail.ru*
Website: *http://syssafety.com/*
Category: Process Injection

CopyCat uses Windows API SetThreadContext to take control over the thread of the trusted process. This technique was invisible to personal firewalls for a long time and even today many firewalls are not able to handle it.

CPIL
Author: Comodo
Website: *http://personalfirewall.comodo.com/cpiltest.html*
Category: DLL Injection

CPIL test locates the executable file called explorer.exe and patch its memory loading its own DLL. Then, it tries to use the default browser to transfer the data from your computer to the Internet server.

CPIL Test Suite
Author: Comodo
Website: *http://personalfirewall.comodo.com/cpiltest.html*
Category: Process Injection

The CPIL suite contains three separate tests especially developed by Comodo engineers to test a firewall's protection against parent injection leak attacks. Each of the three tests involves the user typing some random text into a text box which CPIL will attempt to transmit to the Comodo servers.

Test 1: Attempts to disable firewall hooks by directly accessing the physical memory and then modifies explorer.exe to bypass the firewall by running iexplore.exe with a command line address.

Test 2: Attempts to inject cpil2.dll into explorer.exe by using Windows accessibility API and then tries to bypass the firewall by running iexplore.exe with a command line address.

Test 3: Attempts to inject cpil3.dll into explorer.exe by using Windows accessibility API and then tries to bypass the firewall by running iexplore.exe and modifying iexplore.exe with DDE communication.

DNStest
Author: Jarkko Turkulainen
Website: *http://www.klake.org/~jt/dnshell/*
Category: Process injection

DNStest attempts to launch and then infect svchost.exe that is usually a trusted application that can connect to the Internet because the default Windows DNS client service resides in svchost.exe.

DNStester
Author: Jarkko Turkulainen
Website: *http://www.klake.org/~jt/dnshell/*
Category: Recursive Request

DNStester uses Windows DNS API functions to make a recursive DNS query to the Internet server. DNS packets can be used to transfer extra data and this is why they should be controlled by firewalls as any other packets.

FireHole
Author: Robin Keir
Website: *http://keir.net/firehole.html*
Category: Launcher, DLL Injection

FireHole attempts to launch the default browser and then it uses Windows API *SetWindowsHookEx* to inject its own DLL into the browser's process. From inside of the browser it then establish the Internet connection.

Fake Protection Revealer (FPR)

Author: Matousec – Transparent security
Website: *http://www.matousec.com/*
Category: Unhooking

The Fake Protection Revealer is implemented to reveal fake anti-leak protection. For this purpose we define the fake protection as the protection which is implemented only to pass leaktests instead of fixing the real causation. FPR is implemented to reveal fake protection which is based on ring 3 hooks.

Firewalls that are not able to handle leaktests run by FPR are cheating on leaktests! This means not only that they do not protect their users properly but they try to cover their impotency and generaly do offer a fake sense of security to their users. You can recognize the fake protection revealed by FPR easily. If you have a leaktest that was not able to bypass the tested firewall and you run it using FPR, then the tested firewall implements fake ring 3 protection if the leaktests succeed. Succeeding or failing leaktests run by FPR that are able to bypass the tested firewall without FPR means nothing at all!

FPR is implemented to be used with other leaktests. This means you have to obtain another software to be able to test your firewall against FPR. FPR loads the given leaktest in its memory, unhooks all ring 3 hooks and then executes the code of the given leaktest.

Ghost

Author: Guillaume Kaddouch
Website: *http://www.firewallleaktester.com/*
Category: Parent Substitution, Race Conditions

Ghost tries to confuse firewalls by shuting down its own process and restarting itself. The reason for this is to change its Process Identifier (PID) such that the firewall is not able to identify its new process correctly. Then, it sends the information via the default browser to the Internet server.

Jumper

Author: Guillaume Kaddouch
Website: *http://www.firewallleaktester.com/*
Category: DLL Injection, Launcher

Jumper attemps to infect Windows Explorer with its own DLL. At first, it tries to modify the regitry value *Appl-*

nit_DLLs and then it terminates Windows Explorer. When the Windows Explorer is run again it loads DLLs specified in *AppInit_DLLs* to its process. Jumper's DLL running from the Windows Explorer process launch Internet Explorer and controls its behaviour to connect to the Internet server.

LeakTest

Author: Steve Gibson (Gibson Research Corporation)
Website: *http://grc.com/lt/leaktest.htm*
Category: Substitution

LeakTest is the oldest leak test program implemented to bypass stone-age firewalls that rely only on the name of the executable module when identifying applications.

OSfwbypass-demo (OSfwbypass)

Author: Debasis Mohanty (a.k.a. Tr0y)
Website: *http://www.hackingspirits.com/*
Category: OLE Automation

Using OLE automation OSfwbypass tries to load HTML page with Javascript into Internet Explorer. Javascript simply redirects Internet Explorer to the Internet server.

pcAudit

Author: Internet Security Alliance
Website: *http://www.pcinternetpatrol.com/pcaudit/*
Category: DLL Injection

pcAudit implements typical DLL injection technique. It tries to load library into trusted process to be able to establish the Internet connection without any alerts from the firewall.

pcAudit 6.3 (pcAudit2)

Author: Internet Security Alliance
Website: *http://www.pcinternetpatrol.com/pcaudit/*
Category: DLL Injection

Like *pcAudit*, its newer version called *pcAudit2* attempts to load its own DLL to other processes to bypass the protection of firewalls from the trusted process.

PCFlank

Author: PCFlank
Website: *http://www.pcflank.com/*
Category: OLE Automation

PCFlank attempts to control running instance of Internet Explorer using OLE automation to transfer information to the Internet server.

Runner

Author: Matousec – Transparent security
Website: *http://www.matousec.com/*
Category: Substitution

The Runner finds the default browser's executable and renames it. Then it copies itself to the file of the original default browser's executable. It runs this copy, renames it, copies the original executable of the default browser back and then it tries to establish an Internet connection.

Firewalls that are not able to handle this trick either do not verify the integrity of the default browser, or their verification occurs when the privileged action is executed instead of the moment of the fake executable execution.

Surfer

Author: Jarkko Turkulainen
Website: –
Category: DDE, Launcher

Surfer creates hidden desktop and runs Internet Explorer on it, then it uses Direct Data Exchange (DDE) to control its behaviour and transfer data to the Internet server.

Thermite

Author: Oliver Lavery
Website: –
Category: Process Injection

Thermite attempts to find running instance of Internet Explorer, inject tiny infection code and create a remote thread in it. From the Internet Explorer process it then tries to establish socket connections and transfer information to the Internet server.

TooLeaky

Author: Bob Sundling
Website: *http://tooleaky.zensoft.com/*
Category: Parent Substitution

TooLeaky attempts to launch hidden instance of Internet Explorer with the URL in the command line parameter. Personal data may be transfered in the URL to the Internet server.

WallBreaker

Author: Guillaume Kaddouch
Website: *http://www.firewallleaktester.com/*
Category: Parent Substitution
The WallBreaker tests contain 4 separate tests.

Tests 1, 3, 4: Wallbreaker *test 1, 3* and *4* attempt to load a copy of the default browser by using various techniques which require DDE (COM communication).

Test 2: Attempts to load iexplore.exe itself.

YALTA

Author: Soft4ever
Website: *http://www.soft4ever.com/security_test/En/*
Category: Default Rules, Own Protocol Driver

YALTA attempts to send UDP packet to a specific IP address and port. Some firewalls may not control connections to ports of specific services like DNS and trust connections that use these ports.

ZAbypass

Author: Debasis Mohanty (a.k.a. Tr0y)
Website: *http://www.hackingspirits.com/*
Category: DDE

ZAbypass was implemented to bypass old versions of ZoneAlarm PRO but it works against many other firewalls today. It uses *Direct Data Exchange* (DDE) to communicate with Internet Explorer and transfer data between its process and the Internet server. ●