

HAKING

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

TOR PROJECT



DUQU: THE PRECURSOR

STUXNET ATTACK – DETECTION

ANONYMIZING

YOUR ONLINE PRESENCE WITH TOR

Vol.6 No.12
Issue 12/2011(48) ISSN: 1733-7186

PLUS

**TOOL TIME: WIRESHARK:
THE SECRETS OF THE SHARK
(IL)LEGAL: CYBER INSURANCE – A RISKY BUSINESS**



It's here! Penetration testing for Students



**Click here
To enter the
early bird list**

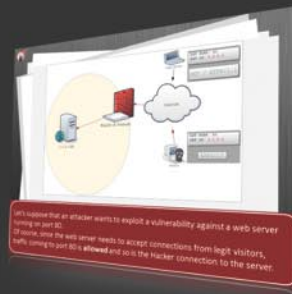


80% of beginners remain beginners or give up completely

We know the pain of being a beginner. You either don't have the foundational skills or you don't have a clear path to follow. Don't give up. There is a better way. Our course will teach you basics of networks and web apps.

It's not just about 1337 instructors

Expert teachers hardly remember what took them to the expert status. It's a fact. There is no way to effectively teach beginners other than help them building strong foundations and showing them the correct path.



You can do it

If you keep studying without a clear learning path you are probably wasting time. Secret is path and perseverance. Better a single step in the correct direction than 10 random steps. Our course will save you months of struggling and frustrations.

You gotta see this.

www.elearnsecurity.com



Still hacking virtual machines?



Coliseum Lab is here!

The most epic web app hacking lab
you have ever seen

CLICK HERE

14 educational challenges
in a multi-platform
environment.

Epic!

www.coliseumlab.com



HAKIN9 team

Editor in Chief: Grzegorz Tabaka
grzegorz.tabaka@hakin9.org

Managing Editor: Marta Jabłońska
marta.jablonska@hakin9.org

Editorial Advisory Board: Rebecca Wynn, Jesus Rivero, Leonardo Neves Bernardo, Narainder Chadwani, Andreas Veniris, Juan Manuel Altamirano Argudo, Julian Evans, Aby Rao

DTP: Ireneusz Pogroszewski
Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

Proofreaders: Bob Folden, Nick Malecky

Top Betatesters: Francisco J. Gómez, Jeffrey Smith; Sanjay Bhalerao

Special Thanks to the Beta testers and Proofreaders who helped us with this issue. Without their assistance there would not be a Hakin9 magazine.


Senior Consultant/Publisher: Paweł Marciniaak

CEO: Ewa Dudzic
ewa.dudzic@software.com.pl

Production Director: Andrzej Kuca
andrzej.kuca@hakin9.org

Publisher: Software Press Sp. z o.o. SK
02-682 Warszawa, ul. Bokszerska 1
Phone: 1 917 338 3631
www.hakin9.org/en

Whilst every effort has been made to ensure the high quality of the magazine, the editors make no warranty, express or implied, concerning the results of content usage.
All trade marks presented in the magazine were used only for informative purposes.

All rights to trade marks presented in the magazine are reserved by the companies which own them.
To create graphs and diagrams we used smartdraw.com program by  SmartDraw

Mathematical formulas created by Design Science MathType™

DISCLAIMER!

The techniques described in our articles may only be used in private, local networks. The editors hold no responsibility for misuse of the presented techniques or consequent data loss.

Dear Readers,

We decided to dedicate this issue to Duqu and TOR. Duqu was discovered by the Laboratory of Cryptography and System Security (CrySyS) at Budapest University of Technology and Economics identified a worm on October 14th 2011 and named the threat Duqu [dyü-kyü] because it creates files with the name prefix “:~DQ”. More information you will find in articles devoted to Duqu. First one is written by Rebecca Wynn – “Duqu: The Precursor Stuxnet Attack”. You will learn what is W32.Duqu, how is it different from Stuxnet, using the Duqu Detector Toolkit. Second article “Duquv5” by Narainder Chandwani is very informative and will help you to understand what Duqu is.

As I mentioned at the beginning we also focus on TOR in this issue. Jesus Rivero provided us with an article “Anonymizing your online presence with TOR”. Before getting into the technical details of Tor, it is important to note that Tor is comprised of two parts. The first part is the Tor network, which is described by Dingledine, Mathewson and Syverson as a “distributed overlay network designed to anonymize TCP-based applications like web browsing, secure shell and instant messaging”. This means that this first component of Tor provides a network of virtual tunnels sitting on top the internet, so the now the intermediate hops between End-to-End communications, are Tor routers. To learn more go to page 22 and read the article.

Cyber insurance is an area that an increasing number of insurance companies around the world are looking at. In part, this is a function of their ongoing search for new products to offer, in the same mode as the ever-increasing proliferation of car insurance options. But what, exactly, is cyber insurance? You will find out reading (IL)LEGAL column by Drake.

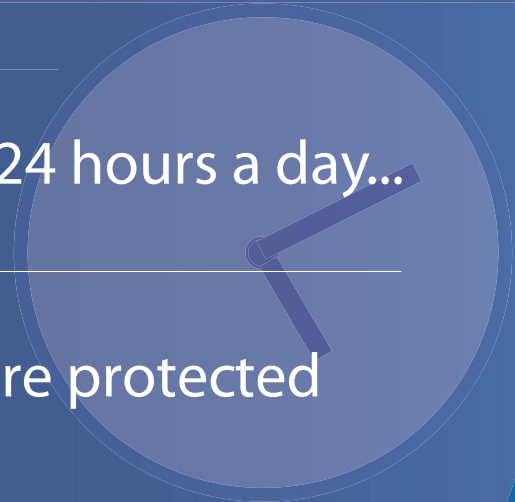
Later in the issue article about securing your personal information written by Andreas Veniris and “Secure OpenLDAP Infrastructure” by Leonardo Neves Bernardo.

The last article is about iOS – “Information on iOS devices”. We also recommend TOOL TIME column and an interview with Kevin Beaver – an independent information security consultant, expert witness, author, and professional speaker with over 22 years of experience in IT – the last 16 years of which I’ve dedicated to information security.

We wish you good reading!
Marta & Hakin9 Team

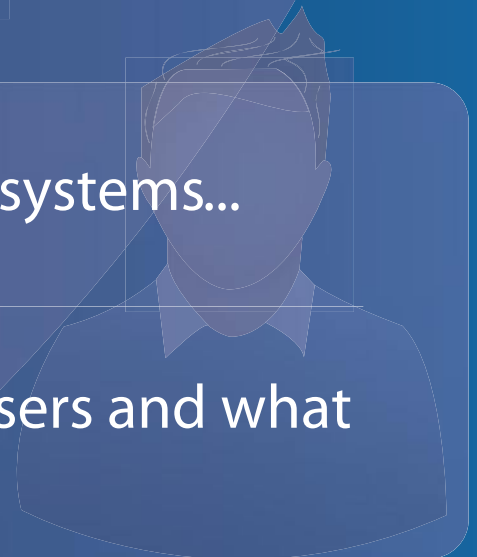
Be reactive...

- Your systems are being attacked 24 hours a day...
- You understand the threats and are protected against them...



Be proactive...

- My users' behaviour threatens our systems...
- I understand what motivates my users and what threats are coming my way...



ID Theft Protect provides information on threats from a user perspective.

IN BRIEF

08 Latest News From IT Security World

By Armando Romeo, eLearnSecurity and ID Theft Protect

BASICS

10 Duqu: The Precursor Stuxnet Attack

By Rebecca Wynn

Duqu is essentially the precursor to a future Stuxnet-like attack. The threat was written by the same authors, or those that have access to the Stuxnet source code, and the recovered samples have been created after the last-discovered version of Stuxnet. Duqu's purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, in order to more easily conduct a future attack against another third party. The attackers are looking for information such as design documents that could help them mount a future attack on various industries, including industrial control system facilities. This article summarizes the white papers by Symantec and the CrySyS Duqu Detector Toolkit. (References: Symantec Security Response, W32.Duqu: The precursor to the next Stuxnet Version 1.3, November 1, 2011; CrySyS Duqu Detection Toolkit version 1.02)

16 Duquv5

By Narainder Chandwani

The landscape of malware has drastically changed in the last few years. It has hardly been a year that the security community identified Stuxnet, which some believe was the most menacing malware in history and now we have Duqu making the news. The Laboratory of Cryptography and System Security (CrySyS) at Budapest University of Technology and Economics identified a worm on October 14th 2011 and named the threat Duqu [dyü-kyü] because it creates files with the name prefix “~DQ”. Duqu carries build dates of February 2008 and its drivers go back to August 2007. From this it would appear to seem that its creators have worked on the code for at least 4 years. The driver was most likely created specifically for Duqu by the group responsible for the attacks. It is also believed that the Duqu team had access to the Stuxnet code or both pieces of malware were authored by the same team. Duqu is far more sophisticated than Stuxnet and corrects a number of the mistakes that were observed in Stuxnet. Duqu unlike stuxnet is not self replicating.

18 How safe is our personal information?

By Andreas Veniris

The actual incident that this article is based on was 100% real but for privacy reasons all referred user names are

not the real ones and they have been chosen randomly. According to the same reason all images have been obscured. The existence of the Internet, among other things, saves us from many tedious tasks as well as speeding up many real life obligations, such as: account payments, bank account monitoring and checking, purchasing almost all goods (from books to bookstores ...!) from online stores, avoiding going at the post-office for our mail and many others that could easily fill up all the pages of this magazine! We can do all these amazing feats, calmly and nicely from the sofa of our home. It is much better than running on roads in the cold or heat, in crowds etc. Isn't it? The problem is that these pros have (always) some cons! In this article we will play the role of a bad guy.

DEFENSE

22 Anonymizing your online presence with TOR

By Jesus Rivero

End to End communications over the internet are comprised of a number of intermediate systems, or hops, that help the request from a client machine (e.g. your computer) to reach a server machine (e.g. a web server). In general, these intermediate machines know exactly the whole route taken from the origin to the destination making it easy to record or reconstruct that information at any given time. Even if you encrypt the data payload portion of the IP packets sent by your computer, the IP headers can reveal a lot of your identity to interested parties, such as timing information, origin of the packet, destination, interests and behavior, among other things. Whatever your source for privacy concern is, be it legislation like the USA-PATRIOT Act, visits to internet-unfriendly countries, commercial research or if you are just paranoid, like me, and you want to avoid attackers knowing about your behavior while surfing on the internet, then TOR can help you.

30 Secure OpenLDAP Infrastructure

By Leonardo Neves Bernardo

This article will discuss how to install OpenLDAP and increase security level using TLS to implement confidentiality and ACLs to implement access control. At the end, we'll see how to improve availability using syncrepl method of replication. You will learn how to use install OpenLDAP, secure OpenLDAP with TLS and ACL and configure OpenLDAP replication using syncrepl. The Lightweight Directory Access Protocol, or LDAP, is a standard technology for network directories. LDAP is both a network protocol and a standard architecture based on X.500 to store information related to computer networks.



Coliseum

Virtual labs
100% practical hands on
training
by eLearnSecurity

FIND OUT
14 educational challenges

- ✓ Real world scenarios
- ✓ No set-up time
- ✓ Play on MS SQL Server
- ✓ Got stuck? We support!

www.coliseumlab.com

X.500 is a series of computer networking standards developed by ITU-T. In the X.500 directory architecture, the client queries and receives responses from one or more servers in the server directory service. To control the communication between clients and information, ITU-T created a protocol named DAP (Directory Access Protocol). DAP is a heavyweight that runs over a full OSI stack and consequently, like almost all OSI protocol, was not popular.

36 Information on iOS devices

By Juan Manuel Altamirano Argudo

Lately mobile devices have become a great source of information about us, it is our personal assistant and it knows every one of our secrets, if it falls into the hands of a bad person, we could suffer big damage. You will learn how to access to iOS filesystem, apps installation via SSH, explore and get information on iOS devices.

TOOL TIME

44 Wireshark: The Secrets of the Shark

By Mervyn Heng

This column was inspired by the international screening of the Tintin movie by Steven Spielberg and Peter Jackson. Just like Tintin, Wireshark is an international icon too. It is primarily harnessed for network troubleshooting and packet analysis but did you know that there are other applications of this powerful tool?

(IL)LEGAL

46 Risky Business

By Drake

Cyber insurance is an area that an increasing number of insurance companies around the world are looking at. In part, this is a function of their ongoing search for new products to offer, in the same mode as the ever-increasing proliferation of car insurance options. But what, exactly, is cyber insurance? This is big business; one recent UK government report estimated the annual cost of cyber crime to the UK economy alone as something in the order of L27billion (USD 43billion).

INTERVIEW

48 Interview with Kevin Beaver

By Hakin9 Team

Kevin Beaver is an information security consultant, author, expert witness and professional speaker with Atlanta-based Principle Logic, LLC. With over 22 years of experience in the industry, Kevin specializes in performing independent security assessments revolving around minimizing business risks. He has authored/co-authored 10 books on information security including one of the best-selling information security books Hacking For Dummies (Wiley). In addition, he's the creator of the Security On Wheels information security audio books and blog providing security learning for IT professionals on the go.

ANDROID 4.0 – SECURITY HOLES IDENTIFIED IN ICE CREAM SANDWICH

Android 4.0 has been found to have several security flaws. On-Device Encryption opens a variable which can make the encryption on one Android device stronger than the encryption on the next one. Email Copy and Paste could lead to data loss as it appears possible to take email content or data from file attachments and open it in third-party apps. Facial Recognition Unlock allows you to unlock the device with your face but it appears that a picture of you is all that is needed to activate the facial recognition and access the Android device. Android Beam has a flaw that allows a hacker to packet sniff non-encrypted data in transit. Finally Capture Screen Shots allows for someone else to screen grab sensitive data, which can be stored and shared with others.

Source: ID Theft Protect

BACKDOOR CAPHAW ACTIVEX TROJAN ATTACKS FACEBOOK NETWORK

Cyber criminals have targeted Facebook to get information of the users and to insert malicious files into the website. Hackers used social engineering techniques to allow users to install a particularly nasty backdoor Trojan in their computer systems. Once the user is urged to download a new version of *Video Embed ActiveX Object* to play the video file it offers setup.exe file which is a Caphaw Trojan.

The Caphaw Trojan bypasses firewalls, installs an FTP client and a proxy server and a keylogger on the affected target systems. Caphaw has a remote desktop capability which uses the VNC open source project. The keylogging, FTP and remote desktop functionality are a major threat vector.

Source: ID Theft Protect

GOOGLE CHROME 15.0.874.121 UPDATE FIXES HIGH-RISK VULNERABILITIES

Google has launched Chrome 15.0.874.121 version that updates the Java Script engine and fixes high risk vulnerability. It uses a native sandbox that prevents Hackers from executing malicious code. Mozilla security engineer Christian Holler has discovered this vulnerability and was paid US\$1,000 through the Chromium Vulnerability Rewards Programs for reporting it. The new Google Chrome for Windows, Mac and Linux also addresses a non-security issue that causes SVG elements loaded within iframes to ignore specified dimensions. This is known as a regression bug which was introduced by recent code modifications. Other fixes included changes to the default NAT traversal

policy, the download folder display, the login process, the V8 JavaScript engine and the GPU blacklist.

Source: ID Theft Protect

HACKERS POSTING PORN ON FACEBOOK IN MAJOR ATTACK ON SOCIAL NETWORK

Facebook has been under attack from violent images and porn on several users' profile pages. It appears to be one of the most prolific breaches of Facebook security since it was first launched. Users have been tricked into pasting malicious code (possible clickjacking or XSS?) into their browsers which enable hackers to gain access to profiles and post images that are visible to users' friends. An example is *spiderooooo.co.cc* which takes you to a fake Facebook page which if your browser has JavaScript enabled will load up the real Facebook login page in a pop-up window. This malicious script will capture your login details.

Source: ID Theft Protect

MICROSOFT TO STREAMLINE WINDOWS 8 PATCH PROCESS

Microsoft aims to streamline the update and provide smart messaging as part of it's new Windows 8 release next year (2012). Redmond aims to reduce the number of restarts to updates – hopefully removing the need for changes to 'code in use' having to reboot the OS. Windows restarts are disruptive to user experience especially if you are working on something important. Apart from smart updating, Windows 8 will also no longer show on-the-desktop notifications (those annoying pop-ups on the taskbar).

When one or more updates require a restart, Windows 8 will alert users in a message on the Windows log-in screen which will persist for three days. If a user does not action a restart within the three day timeline, Windows 8 will do it either at the end of a grace period or if critical apps are open, the next time a user logs in.

Source: ID Theft Protect

STEAM BREACH

Another video game company fell victim to cyber-attacks – Steam. Steam is an online gaming platform for computers which allows users to purchase, download and play videos games onto any computer. It also provides forums, chat features and player profiles for its community. End users first noticed an issue when the forums were defaced toward the beginning of November. Steam confirmed the issues the following day; they announced their forums had been comprised and were investigating the possibility of a deeper breach.

They soon found evidence of a much deeper breach and announced, *We learned that intruders obtained access to a Steam database in addition to the forums. This database contained information including user names, hashed and salted passwords, game purchases, email addresses, billing addresses and encrypted credit card information. We do not have evidence that encrypted credit card numbers or personally identifying information were taken by the intruders, or that the protection on credit card numbers or passwords was cracked. We are still investigating.*

Source: Schuyler Dorsey – ELS

TDSS SPREADING DNS CHANGER

TDSS is a rootkit designed to be extremely stealthy and infected 4.52 million machines just in the first three weeks of this year. The latest version functions as a backdoor to push other malware to the system. Its latest antics appear to be pushing the trojan, DNS Changer. After DNS Changer is installed, it changes the DNS settings of the device and points it to rogue DNS servers controlled by the attackers. They use these DNS servers to direct victims to infected and/or malicious sites instead of legitimate ones.

Some of the attackers were recently prosecuted after having used the DNS Changer to net \$14 million. They used the rogue DNS servers to redirect victims to websites with paid advertisements. DNS Changer has the ability to infect Windows and Apple OSX machines as well as routers. The TDSS rootkit itself can infect x86 and x64 systems, infect master boot records and communicates over the Kad network.

Source: Schuyler Dorsey – ELS

MS11-083

Microsoft has posted a new security bulletin and corresponding update for a vulnerability in all versions of Windows Vista, Windows 7, Windows Server 2008 and Windows Server 2008 R2. Attackers could have complete remote code execution by sending a continuous flow of specially crafted UDP packets to completely closed ports. The update changes how the TCP/IP stack handles continuous UDP traffic in memory to address the security threat. The update is categorized as critical so all systems with automatic updates enabled will download and install the update.

Many independent security researchers are already setting up honey pots to test and evaluate how attackers may be exploiting this vulnerability. Some researchers speculate it could lead to another mass spread like that of Conficker.

Source: Schuyler Dorsey – ELS

DROIDLIVE

Another new malware has invaded the Android scene, DroidLive. ANC University research team uncovered the new sms Trojan which acts as a device administration application. It disguises itself as a Google library can receive commands directly from a remote server. Once installed, the app has the capability and permissions to read/send sms, make phones and access personal data on the phone. Xuxian Jiang of the research team explains, *Though this requires user consent, if such consent is given, DroidLive can obtain privileges closer to those granted only to the device's firmware.*

There are currently several apps infected with the malware but none are present in the official Droid marketplace; users need to use extra precaution when installing apps from third party marketplaces. Jiang advises that all users should exercise common sense when using these marketplaces; check reviews, ratings, developer information, permissions of app and watch for suspicious behavior.

Source: Schuyler Dorsey – ELS

MALWARE INFECTS NZ AMBULATORY SYSTEM

A massive malware infection has attacked the New Zealand ambulance system. The malware disabled the network used by the St. John ambulance service. Dispatch uses the network to transmit mobile data to terminals in the ambulances. After the network was hindered, dispatch had to manually call the mobile phones of the ambulance crews. Al Goudge said *Anti-virus software protected the systems but as a result of the virus it impacted on some of the systems services, mainly those related to paging and radio.*

The infection was fixed within hours and they believe the ambulance network was not a direct target of the virus. The St. John ambulance network covers 90% of New Zealand but they did not release information as to whether or not the attack affected response times. Malware attacks can have a devastating impact on the healthcare industry as not long does it put protected health information at risk but it could also decrease the level and efficiency of care received by patients.

Source: Schuyler Dorsey – ELS

Duqu:

The Precursor Stuxnet Attack – Detection Toolkit

On October 14, 2011, Symantec Security Response was alerted to a sample by the Laboratory of Cryptography and System Security (CrySyS) at Budapest University of Technology and Economics. The threat appeared very similar to the Stuxnet worm from June of 2010. CrySyS named the threat Duqu [dyü-kyü] because it creates files with the file name prefix “~DQ”.

What you will learn...

- What is W32.Duqu
- How is it different from Stuxnet
- Using the Duqu Detector Toolkit

What you should know...

- Basic MS Visual Studio 2005 or 2008
- Basic MS C++
- Basic Shell Code

The research lab provided their detailed initial report to Symantec and they confirmed W32.Duqu is a threat nearly identical to Stuxnet, but with a completely different purpose.

Quick Comparison of Stuxnet and Duqu

Duqu is essentially the precursor to a future Stuxnet-like attack. The threat was written by the same authors, or those that have access to the Stuxnet source code, and the recovered samples have been created after the last-discovered version of Stuxnet. Duqu's purpose is to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers, amongst others not in the industrial sector, in order to more easily conduct a future attack against another third party. The attackers are looking for information such as design documents that could help them mount a future attack on various industries, including industrial control system facilities. This article summarizes the white papers by Symantec and the CrySyS Duqu Detector Toolkit. (References: Symantec Security Response, W32.Duqu: The precursor to the next Stuxnet Version 1.3, November 1, 2011; CrySyS Duqu Detection Toolkit version 1.02).

Duqu – Symantec Analysis:

Duqu does not contain any code related to industrial control systems and is primarily a *remote access Trojan* (RAT) – a malware program that gives an intruder

administrative control over a target computer.. The threat does not self-replicate.

The threat has been highly targeted toward a limited number of organizations for their specific assets. However, it's possible that other attacks are being conducted against other organizations in a similar manner with currently undetected variants. According to Symantec, Duqu infections have been confirmed in

Feature	Stuxnet	Duqu
Modular malware	✓	✓
Kernel driver based rootkit	✓	✓ very similar
Valid digital signature on driver	Realtek, JMicron	XXXXX
Injection based on A/V list	✓	✓ seems based on Stux.
Imports based on checksum	✓	✓ different alg.
3 Config files, all encrypted, etc.	✓	✓ almost the same
Keylogger module	?	✓
PLC functionality	✓	✗ (different goal)
Infection through local shares	✓	No proof, but seems so
Exploits	✓	?
0-day exploits	✓	?
DLL injection to system processes	✓	✓
DLL with modules as resources	✓ (many)	✓ (one)
RPC communication	✓	✓
RPC control in LAN	✓	?
RPC Based C&C	✓	?
Port 80/443, TLS based C&C	?	✓
Special "magic" keys, e.g. 790522, AE	✓	✓ lots of similar
Virtual file based access to modules	✓	✓
Usage of LZO lib	?	✓ multiple
Visual C++ payload	✓	✓
UPX compressed payload,	✓	✓
Careful error handling	✓	✓
Deactivation timer	✓	✓
Initial Delay	? Some	✓ 15 mins
Configurable starting in safe mode/dbg	✓	✓ (exactly same mech.)

Figure 1. Quick Comparison of Stuxnet and Duqu

six organizations in eight countries. The confirmed six organizations include:

- Organization A – France, Netherlands, Switzerland, Ukraine
- Organization B – India
- Organization C – Iran
- Organization D – Iran
- Organization E – Sudan
- Organization F – Vietnam

Note

Some organizations are only traceable back to an *Internet Service Provider* (ISP) and thus, all six may not be distinct organizations. Other security vendors have reported infections in:

- Austria
- Hungary
- Indonesia
- United Kingdom
- Iran (Infections different from those observed by Symantec.)

Duqu Geographical Map

In one case, the attackers used a specifically targeted email with a Microsoft Word document. The Word document contained a currently undisclosed Zero-day kernel exploit that was able to install Duqu. It is unknown whether the attackers used the same methodology and the same Zero-day in other cases. (Note: A *zero day* attack occurs on or before the first or *zeroth* day of developer awareness, meaning the developer has not had any opportunity to distribute a security fix to users.)

The attackers used Duqu to install another infostealer that can record keystrokes and collect other system information. The attackers were searching for information assets that could be used in a future attack. In one case, the attackers did not appear to successfully exfiltrate (extract, withdrawal) any sensitive data, but details are not available on all cases.



Figure 2. Duqu Geographical Map

Two variants were initially recovered by Symantec and, in reviewing their archive of submissions, the first recording of an attack occurred in early August. However, based on file-compilation times, attacks using these variants may have been conducted as early as November 2010. Additional variants were created as recently as October 17, 2011 and new payload modules downloaded October 18, 2011. Thus, at the time of discovery, the attackers were still active.

Duqu consists of a driver file, a *dynamic-link library* (DLL) that contains many embedded files, and a configuration file. These files must be installed by another executable – the installer. The installer registers the driver file as a service so it starts at system initialization. The driver then injects the main DLL into services.exe. From here, the main DLL begins extracting other components and these components are injected into other processes. (Note: A dynamic-link library (DLL) is an executable file that acts as a shared library of functions.)

This process injection hides Duqu’s activities and may allow certain behaviors to bypass some security products.

One of the variant’s driver files was signed with a valid digital certificate that expires on August 2, 2012. The digital certificate belongs to a company headquartered in Taipei, Taiwan and was revoked on October 14, 2011. The private keys used to generate the certificate were stolen from the company. Having a legitimate certificate allows Duqu to bypass default restrictions on unknown drivers and common security policies.

Duqu uses *Hypertext Transfer Protocol* (HTTP) and *Hypertext Transfer Protocol Secure* (HTTPS) to communicate to a command and control (C&C) server at 206.183.111.97, which is hosted in India and 77.241.93.160 hosted in Belgium. Both of these *Internet Protocol* (IP) addresses are inactive. To date these are the only C&C server IPs encountered and are reliable indicators of Duqu activity on a network. Duqu also has proxy-aware routines, but these do not appear to be used by default.

Through the C&C server, the attackers were able to download additional executables, including an infostealer that can perform actions such as enumerating the network, recording keystrokes, and gathering system information. The information is logged to a lightly encrypted and compressed local file, and then must be exfiltrated out. In addition to this infostealer, three more DLLs that queried for additional basic system information were pushed out by the C&C server on October 18, 2011.

The threat uses a custom C&C protocol, primarily downloading or uploading what appear to be *.jpg* files. However, in addition to transferring dummy *.jpg* files, additional encrypted data is appended to the *.jpg* file for exfiltration, and likewise received. The use of the *.jpg* files

is simply to obfuscate network transmissions. The threat does not self-replicate, but based on forensic analysis of compromised computers, the threat was instructed, likely using the C&C server, to replicate through network shares to additional computers on the network.

Duqu Spreading Across Network

A non-default configuration file was created for those infections, instructing the threat to not use the external C&C server, but instead use a peer-to-peer C&C model. In these cases, the newly compromised computer is instructed to communicate with the infecting computer, which proxies all the C&C traffic back to the external C&C server. Using a peer-to-peer C&C model allows the threat to access computers that may not be connected directly to the external Internet and also avoid the detection of potentially suspicious external traffic from multiple computers.

The peer-to-peer SMB protocol is not configured by default for use, but has been seen configured for use in cases where a computer cannot reach the external C&C server. The attackers set a byte in the configuration file to one, and instead of an IP address, provide a string representing a remote resource (e.g. `\\RemoteServer\`). Typically, the remote resource would be a peer-infected computer. The peer-to-peer command and control protocol uses IPC (*Inter Process Communication*) over SMB (Server Message Block), also known as Named Pipes. In particular, a newly infected computer will typically be configured to connect back to the infecting computer through `\\[INFECTING COMPUTER]\IPC$` using a predefined named pipe. The peer computer (which was previously the infecting computer) then proxies the C&C traffic to the external C&C server.

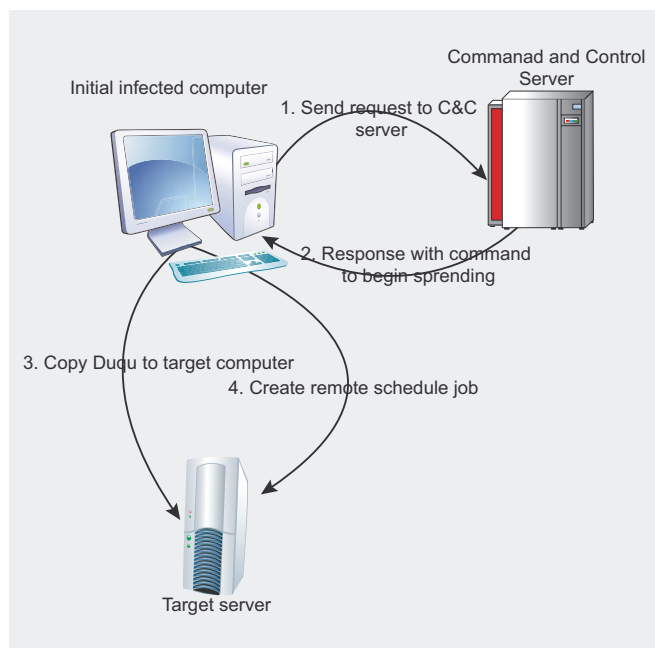


Figure 3. Duqu Spreading Acrossed Network

Duqu Peer-to-Peer C&C

The peer-to-peer command and control protocol is the same the original HTTP protocol used, except without the HTTP transaction headers and no .jpg files are transferred.

This is a very clever technique for spreading through a network. Most secure networks are configured to have a *secure* zone, where internal servers are located. This zone is heavily monitored and controlled. Outside this zone is a less well-protected network: the general corporate network. As Duqu spreads through the network, moving from less secure to more secure areas, it is able to always retain a connection back to the C&C server. It effectively builds a private bridge between compromised computers, leading back to the C&C server. A second aspect of this technique is that it is discreet. Only one compromised computer in the network will connect directly to the C&C server, thus reducing the amount of suspicious traffic.

Finally, the threat is configured to run for 30 days by default. After 30 days, the threat will automatically remove itself from the system. However, Duqu has downloaded additional components that can extend the number of days. Thus, if the attackers are discovered and they lose the ability to control compromised computers (for example, if the C&C servers are shutdown), the infections will eventually automatically remove themselves, preventing possible discovery.

Duqu shares a great deal of code with Stuxnet; however, the payload is completely different. Instead of a payload designed to sabotage an industrial control system, it has been replaced with general remote access capabilities. The creators of Duqu had access to the source code of Stuxnet, not just the Stuxnet binaries. The attackers intend to use this capability to gather intelligence from a private entity that may aid future attacks on a third party.

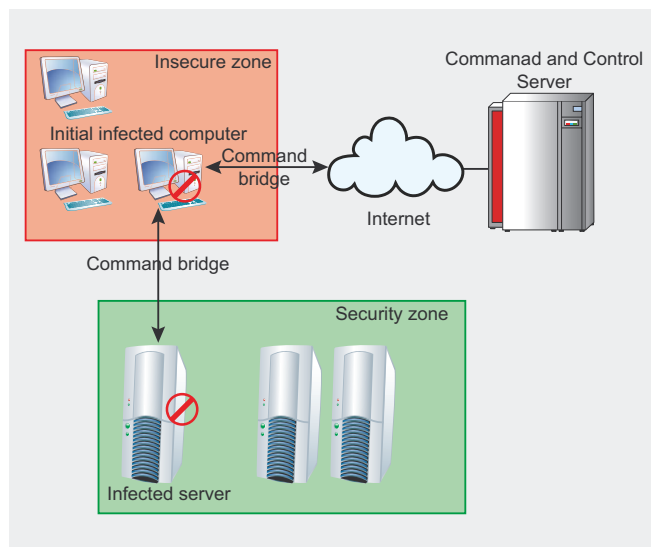


Figure 4. Duqu Peer-to-Peer C&C

While suspected, no similar precursor files have been recovered that date prior to the Stuxnet attacks.

CrySys Duqu Detection Toolkit

This detector toolkit combines simple detection techniques to find Duqu infections on a computer or in a whole network. The toolkit contains signature and heuristics based methods and it is able to find traces of infections where components of the malware are already removed from the system.

The intention behind the tools is to find different types of anomalies (e.g., suspicious files) and known indicators of the presence of Duqu on the analyzed computer. As other anomaly detection tools, it is possible that it generates false positives. Therefore, professional personnel are needed to elaborate the resulting log files of the tool and decide about further steps.

This toolkit contains very simple, easy-to-analyze program source code, thus it may also be used in special environments, e.g. in critical infrastructures, after inspection of the source code (to check that there is no backdoor or malicious code inside) and recompiling.

How to Use

The toolkit contains 4 different executable components:

- FindDuquSys.exe
- CalcPNFEntropy.exe
- FindDuquTmp.exe
- FindPNFnoINF.exe

All of these programs can be executed directly from command line.

The programs accept a single optional parameter `<filename>`, which stands for the specification of the log file where the program should save its results. If the optional parameter is not specified, the program saves log information into `duqudetector_log.txt` of the working directory. During the execution of the program log information is also written to the console.

For convenience, the toolkit includes a batch file, `FindDuqu.bat`, which executes all 4 tools with the same log file parameter.

How to build from scratch

Basically, there are 4 main source files for the executables, respectively:

- `findduqusys.cpp`
- `calcpnfentropy.cpp`
- `findduqutmp.cpp`
- `findpnfnoinf.cpp`

Furthermore, each of these source files use common functions and constants that are contained by `common.cpp`

and `common.h` files. Executables are compiled by MS Visual Studio 2008 with default settings. Before compiling please make sure that one of the main source files, `common.cpp` and the `common.h` header file comprise a Visual C++ project. Note that current executables are built on a 32-bit system.

Duqu Detector Toolkit v1.02

Details and Analysis

The toolkit detects suspicious files that can be indicators for the presence of Duqu.

The toolkit may also detect new, modified versions of the Duqu threat. As stated earlier, Duqu deactivates after a time limit and removes itself from the computer, but some temporary files could still indicate that the computer was affected by a former Duqu infection; the toolkit might identify these cases, too.

Working Method

FindDuquSys.exe

The tool tries to find the loader executable component, the `.sys` kernel driver file of Duqu. It uses binary signature matching on all driver files in the `system32\drivers` directory. The signature components were selected in a way that possibly modified versions of Duqu might be detected as well. It is not impossible; however, that the tool can detect these signatures in legitimate files, so if any string is detected, it is just an indication for the need of detailed manual analysis of the particular file. Care should be taken that running the program might need elevated privileges to successfully test all `.sys` file.

CalcPNFEntropy.exe

The `CalcPNFEntropy` tool tries to find suspicious `.PNF` files in the windows installation.

Both Duqu and Stuxnet put components in encrypted form into the `%WINDIR%\inf` directory with a `.PNF` extension.

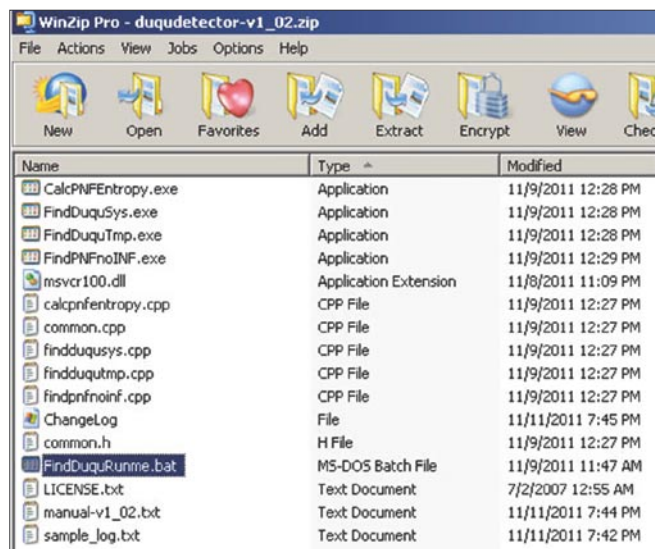


Figure 5. Duqu Detector v1.02

Encrypted and compressed files generally have a distinct characteristic: their entropy calculated over the binary file is larger than those of other standard binary files. The detection tool calculates entropy of all files in `%WINDIR%\inf`. If any suspicious file is found where the entropy is above the threshold of 0.6, it indicates it in the log files. For real-life Duqu samples this entropy is around 0.9 according to the tool developers' experience.

FindDuquTmp.exe

Remember, the Duqu malware got its name after the usage of temporary files beginning with `~DQ`. In fact, multiple types of temporary files are used in Duqu; the tool tries to find all related temporary files, namely:

- The existence of `~DN1.tmp` shows that the keylogger/infostealer component might be installed on the computer. The tool checks files in the `%TEMP%` directory, i.e., only in the temporary directory of the current user.
- `~DQ*` files might be related to the keylogger/infostealer log files. Some parts of the files are checked against Duqu's magic and if found, indicated in the log files.
- `~DF*` (generally with five hexadecimal digits) are files created by some unknown part of Duqu and contain compressed files stolen from the computer. The tool checks those files if they begin with a modified bzip magic, which shows that the file is likely related to Duqu. If such files are found, this fact is indicated in the log file.

FindPNFnoINF.exe

The PNF files installed by Duqu have no corresponding `.inf` files. Therefore, PNF files with missing `.inf` files are also suspicious. The tool checks all `.PNF` files in `%WINDIR%\inf`, and indicates if some file does not have a related file with `.inf` extension. Sometimes, it is normal to have such files; improper uninstalling drivers can cause such cases, so professionals should check the results as this can easily be a false positive.

Use on a Large Network

You should consider running the tool on every login to the domain in your network and collect log files to a central directory. Then, you can analyze the results for the whole network.

Evaluation of results

The toolkit was created in such a way that if a real and active Duqu infection is found, then running all the tools will result in clear indications. However, a single suspicious result may just be a false positive. In any case, professional experience is needed to carefully analyze these results and findings.

If you should find files related to Duqu do NOT delete all the files and do NOT panic. In Duqu infections, forensics is very important, so instead of deleting files, start a careful process to save forensics material (memory dump, whole disc copy). You might need additional steps, like lock-down of the infected portion of the network, etc. It is always best to follow your corporate Incident Response Plan and consult professionals.

The analysis can be done remotely if someone gathers the log file and all corresponding (seemingly suspicious) files on the computer, and transfers those to professionals.

Liability

The toolkit is provided *as is*, and no guarantee or warranty is given for the results or side effects that it may produce. The use of the toolkit is at the sole risk and liability of the user.

License

This toolkit is released under GPLv3 license. The binary files can be freely used in commercial and non-commercial environments.

Contact

Laboratory of Cryptography and System Security
CrySys – <http://www.crysys.hu/>
Budapest University of Technology and Economics
Department of Telecommunications
1117 Magyar Tudósok Krt. 2.
Budapest, Hungary

Conclusion

In this article, we reviewed the existence of a malware found in the wild that shows striking similarities to Stuxnet, including its modular structure, injection mechanisms, and a driver that is digitally signed with a compromised key. It was named *Duqu* as its key logger creates temporary files with names starting with `~DQ...` The technical analysis by Symantec was summarized as well as the CrySys Duqu Detection Toolkit v1.02.

According to Symantec and CrySys the following traces may indicate an infection of Duqu:

- Unexpected connections to 206.183.111.97 or 77.241.93.160.
- The existence of the following registry entry:
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\“CFID”`
- Unknown drivers in `%System%\Drivers\`.
- A services registry subkey with the following attributes:
 - *ImagePath* matching the unknown driver found in `%System%\Drivers`
 - “Start” = “1”

Additional References

- DailyTech – Nasty Duqu Worm Exploits Same Microsoft Office Bug as *Stuxnet.html*
- Duqu Attack's Installer Discovered – F-Secure Weblog News from the Lab.html
- Duqu Questions and Answers – F-Secure Weblog News from the Lab.html
- F-Secure finds rare digitally signed malware InSecurity Complex – CNET News.html
- Microsoft Security Advisory (2639658) Vulnerability in TrueType Font Parsing Could Allow Elevation of Privilege.html
- Same authors created Duqu, Stuxnet malware – Technology & science – Security – msnbc.com.html
- Technology News Malware Microsoft Issues Fix to Keep Duqu at Bay.html
- Threat Description *BackdoorW32-Duqu.html*

- "Type" = "1"
- FILTER has unknown hex data for a value
- DisplayName, Description, and keyname all match
- Drivers signed by unknown publishers that expire on August 2, 2012.
 - Recent .pnf files in %Windir%\INF:
 - Are either under 10K or ~200K in size
 - Do not have a corresponding *.INF file
 - Have no ASCII strings inside
- Unexpected scheduled tasks or job files. (These can be seen by unexpected modification time to the Tasks • folder.)
- An Event Log entry matching the following attributes:
 - An EventID of 0xC0002719 or 3221235481
 - Event type: 1 (Error)
 - Event source: DCOM
- May have the following description:
- DCOM was unable to communicate with the computer (computer name) using any of the configured protocols

Business Best Business practices and your corporate Incident Response Plan should be followed once an infection has been identified.

Non-professionals – those who are not highly trained in malware detection and removal should not try to *clean* systems with the infection.

REBECCA WYNN

Dr. Rebecca Wynn, DHL, MBA, CISSP, CRISC, LPT, CIWSA, MCTS 2005, GSEC, CCSK, NSA/CNSS NSTISSI 4011-4016 is a Lead/Principal Security Engineer with NCI Information Systems, Inc. She has been on the Editorial Advisory Board for Hakin9 Practical Protection IT Security Magazine since 2008 and is a regular contributor for Hakin9, PenTest, and Enterprise IT Security magazines.

[GEEKED AT BIRTH]



You can talk the talk.
Can you walk the walk?
Here's a chance to prove it.

[IT'S IN YOUR PULSE]

LEARN:

Advancing Computer Science
Artificial Life Programming
Digital Media
Digital Video
Enterprise Software Development
Game Art and Animation
Game Design
Game Programming
Human-Computer Interaction
Network Engineering

Network Security
Open Source Technologies
Robotics and Embedded Systems
Serious Games and Simulation
Strategic Technology Development
Technology Forensics
Technology Product Design
Technology Studies
Virtual Modeling and Design
Web and Social Media Technologies

www.uat.edu > 877.UAT.GEEK

Duquv5

The landscape of malware has drastically changed in the last few years. Hardly a year has passed since the security community identified Stuxnet, which many believe to be the most menacing malware in history and now we have Duqu making the news.

What you will learn...

- Traces of Stuxnet executable have been found in Duqu.
- Duqu has an installer which has not been found. There is a driver, DLL, configuration file.
- Duqu is configured to run for 36 days and in that period it downloads other components which run for days.

What you should know...

- Duqu is being used for reconnaissance purpose to capture key strokes, network information and send back information to the people who planted the bug.
 - Duqu is not a self replicating worm.
 - Duqu has a driver signed by a stolen certificate of Taiwan based C-Media
-

The Laboratory of *Cryptography and System Security* (CrySyS) at Budapest University of Technology and Economics identified a worm on October 14th 2011 and named the threat Duqu [dyü-kyü] because it creates files with the name prefix ~DQ.

Duqu carries build dates of February 2008 and its drivers go back to August 2007. From this it would appear that its creators have worked on the code for at least 4 years. The driver was most likely created specifically for Duqu by the group responsible for the attacks. It is also believed that the Duqu team had access to the Stuxnet code or the same team authored both pieces of malware. Duqu is far more sophisticated than Stuxnet and corrects a number of the mistakes that were observed in Stuxnet. Duqu unlike stuxnet is not self-replicating.

Although CrySys first detected the Duqu worm in October 2011, traces of it can be dated back to April of 2011. This corresponds to when Iran detected a virus and called it *Stars*. Researchers in Iran only found a key logger along with a photo of the NGC 6745 galaxy.

Many organizations have fallen victim to Duqu. The names of the organizations have not been revealed but it is believed that corporations in Austria, Iran, Sudan and America have been its victims. Further, each instance of Duqu identified has been a variant. Each of the dozen Duqu binary's are part of a multifunctional framework that is able to work with any number of

any modules. Duqu is thus highly customizable and designed to evade easy detection. Duqu attacks also appear to have been custom-created with the malicious files compiled immediately prior to the malware being utilized against a target. While, relatively minor, the differences between two of the Duqu attacks contain unique files tailor-made for each operation. The names of registry keys and files used are differ, often with unnecessary code removed from each version. Every attack to date has had its own command-and-control [C&C] server, with the C&C location embedded in the configuration of the malware. Location of the C&C server changes with every attack iteration. In the past few weeks, C&C servers have been identified at various places including Mumbai and Belgium and have been promptly taken down.

Vulnerability & Exploit

Duqu's purpose is to gather intelligence data and assets from target entities. It looks for information such as design documents that could help mount a future attack on various industries. It utilizes a 0-day Microsoft Window's kernel vulnerability. Microsoft has confirmed that that the Duqu campaign exploits a vulnerability in the Windows kernel-mode driver *W32k.sys*, and the TrueType font parsing engine to escalate rights on the compromised PC sufficient enough to install the malware. The font exploited is called Dexter Regular and has been created by Showtime Inc. This appears

to be in reference to the television series Dexter on the Showtime cable channel.

All attacks have involved a social engineering aspect in them as well. An individual at a victim's organization receives an email with a Microsoft Word document attachment. Upon opening up the attachment, the exploit payload is initiated on the victim's PC. The exploit also does not become active until there is no keyboard or mouse activity for ten minutes. The exploit consists of 3 components: a driver, DLL library and a configuration file. Different instances of Duqu found have had different drivers included along with the main DLL file. Typically the exploit process loads the driver initially which then injects the primary DLL into services.exe. The DLL in turn then references the configuration file to obtain the customized exploit information.

Remediation

While Microsoft has yet to patch the exploit, it has urged customers to disable the font parser to protect themselves. Microsoft pushed out an emergency workaround on the November 3rd, 2011 that disables access to the `T2EMBED.DLL`, the dynamic link library that allows applications to display TrueType fonts. In addition to this, CrySys has also developed a toolkit to detect Duqu infections on a computer or on the whole network.

It was observed that the driver `igdkmd16b.sys` has a new encryption key with every install, which means that detection of known PNF files (main DLL) are rendered useless. Furthermore, the DLL itself is encoded differently in every single attack. Existing detection methods from the majority of anti-virus vendors are able to successfully detect Duqu drivers, but the main DLL component often goes undetected due to these stealth measures. Some methods to guard against Duqu are:

- Install the hotfix released from Microsoft
- Run the toolkit from CrySys to detect Duqu infected computers/networks.
- Beware of malicious Microsoft Word documents from strangers or unexpected sources.
- Monitor your network traffic for files that bear the ~DQ files extension.

NARAINDER CHANDWANI

Narainder has over five years of experience in information technology. Based out of Foundstone's New York office Narainder has participated in a wide range of projects that include web application penetration testing, code reviews, thick client testing, web services testing, internal and external network penetration testing, smart phone application testing, social engineering, virtualization environment review and developing policies for our clients. Narainder has industry standard certificates like CISSP and CEH and has Masters in Computer Science from Polytechnic University, Brooklyn.

Join

hakin9 team!



If you would like to help our team in creating hakin9 magazine you can join our authors or betatesters today!

All you need to do, is to send an email to:

editors@hakin9.org

and give us a brief description of your field of interest.

We look forward to hearing from you!

How Safe Is Our Personal Information?

The existence of the Internet, among other things, saves us from many tedious tasks as well as speeding up many real life obligations, such as: account payments, bank account monitoring and checking, purchasing almost all goods (from books to bookstores ...!) from online stores, avoiding going at the post-office for our mail and many others that could easily fill up all the pages of this magazine!

What you will learn...

- How bad people can use the information that already exists on the net to gain access to:
 - your email accounts,
 - your financial information such as credit cards, PayPal accounts etc,
 - your internet hosting accounts (if you have any),
 - your personal web sites,
 - your personal life in general!
- How you can protect yourself from such bad situations by following some very simple (but, believe us) very important security rules.

What you should know...

- Nothing more than Google and some... cunning thoughts.

We can do all these amazing feats, calmly and nicely from the sofa of our home. It is much better than running on roads in the cold or heat, in crowds etc. Isn't it? The

problem is that these pros have (always) some cons!

In this article we will play the role of a bad guy. We will show how easy is for us to spy on someone (even stranger) and to collect, with a minimum of effort, almost all of his/her personal information. In an era, where the security of personal data starts to concern even public parties, we will show how easily is for a bad guy to gain access to personal data of another person, such as occupation info, photos, names, family records, personal preferences (hidden and not ;-)), credit card account numbers, etc.

In addition, we will present how we can easily steal the *identity* of our victim in order to appear on the internet as him or her (see *impersonation* – <http://is.gd/f3ha>)! Does this remind you something like 007? We assure you that everything presented here is true; it

The actual incident that this article is based on was 100% real but for privacy reasons all referred user names are not the real ones and they have been chosen randomly. According to the same reason all images have been obscured.

can happen to anyone and we will prove it. But of course, in the end we will give you the necessary *arsenal* and tips to not fall or to be very difficult to fall into such an unpleasant situation.

So, let us begin with Google! One evening we have an appetite for *searching*. We get to Google and start searching for directories that contain the file *classifieds.cgi*. We enter something like the following in the Google box:

```
intitle: „Index of” classifieds.cgi
```

What we get as a result is a fairly long list of sites. We start studying it one by one. After some searching we find a site that allows directory listing. This is not necessarily a security hole but it is a bad security practice. You will never know when a forgetful administrator will leave, in a dark corner of a directory, a file full of username and passwords or emails (Figure 1)!

What have here? We have a list of usernames and passwords with their email. Ok, by using this information we can only impersonate a user of the current site. But, this is not enough. We want to try

our theory which is this: *many users use the same password for their favorite sites (forums etc.) and their email account too!* This is because it is difficult for a human to remember many and especially complex passwords. Ok, to not remember is reasonable.

What is not reasonable (and dangerous too) is to use the same password to enter your email account and to enter your favorite forum!

Let's try our theory: We check the file *default.users*, for all users with a yahoo email and we start trying every single of them to enter to his/her email using as password the one displayed in this file. Incidentally, the third user to the series is *vulnerable* to our theory (Figure 2). To be specific, we found that an approximately 50% of users fall into this *trap*.

Figure 2 shows the email of Mrs. Mary (okay, we only testify to her first name). From what we can see in *MyFolders*, Mrs. Mary has everything neat and tidy: Personal messages in a folder, work in another, the forums she is registered to in another etc. Consider the number of emails that Mrs. Mary retains on yahoo. It is 13969! It is a matter of time, from now on, to find all of her personal data. We can start by focusing on the following search rule:

Search for emails that welcome the victim as a new member in a forum. In such emails you will usually find that user credentials are presented. One such email is displayed at Figure 3.

So, let's enter to this forum as Mary. By doing this we can find even more information about her. We can also respond to other members by impersonating Mrs. Mary. In short, we can impersonate Mrs. Mary in order to make a love confession to a friend of her, to reject a friendship and generally to mess up her forum life. In addition, we find a very interesting group of information titled *View Profile*. This is the personal details of Mrs. Mary along with her photo! In the same location, we found her CV along with phone numbers, addresses and names of friends and relatives (Figure 4).

According to this type of forum and the data we get, we can create a profile of Mrs. Mary. We can use the dark-net to sell her personal data and preferences to promote-products companies! The same can be done for her relatives. Since we knew her whole family, why not to exploit it?

While we are talking about spam and spammers, we should not omit to mention this: the joy of the spammer is to *dive* into a sea of real emails. Once again, aiming for profit, we can extract and sell a short list of about 100 emails

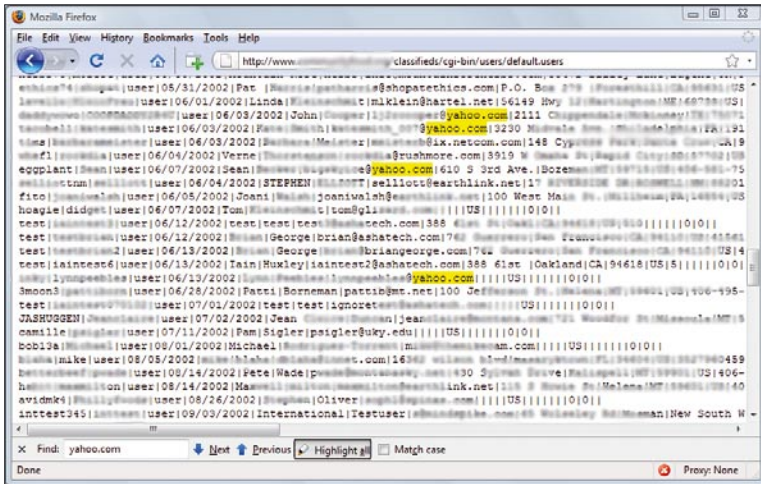


Figure 1. When admin is forgetful, users are the victims!

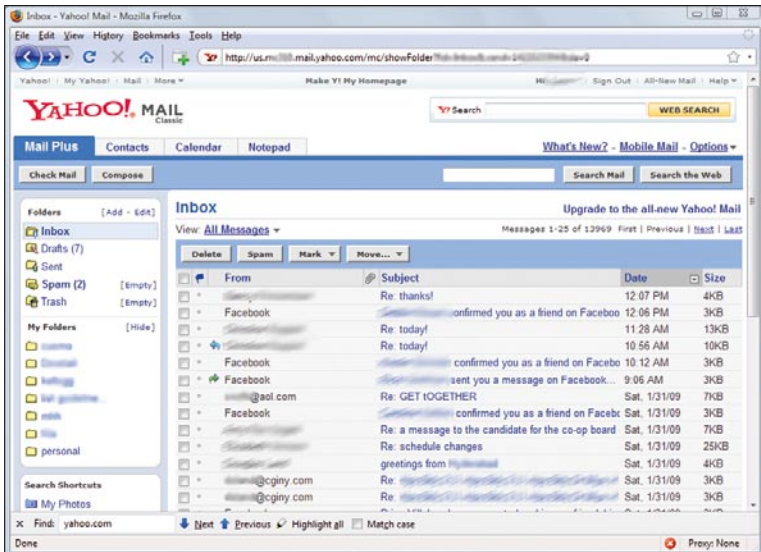


Figure 2. Our victim Mrs. Mary and ... her email!

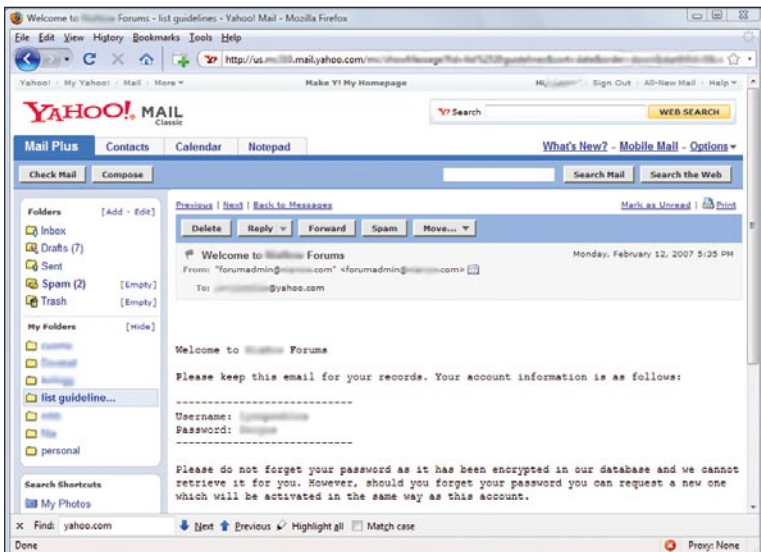


Figure 3. Username and Password to login to a forum!

(real names included!) that we found in the account of the indeed very popular Mrs. Mary (Figure 5).

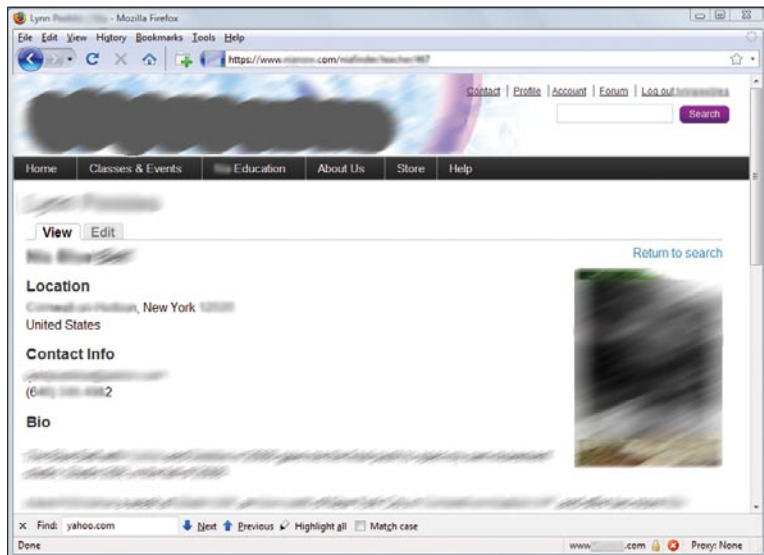


Figure 4. The personal data of our „victim“!

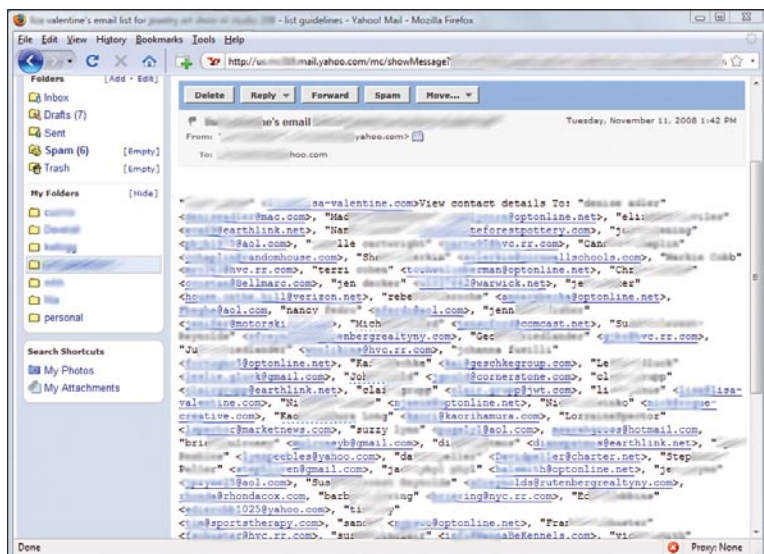


Figure 5. A „gift“ to the spammers!

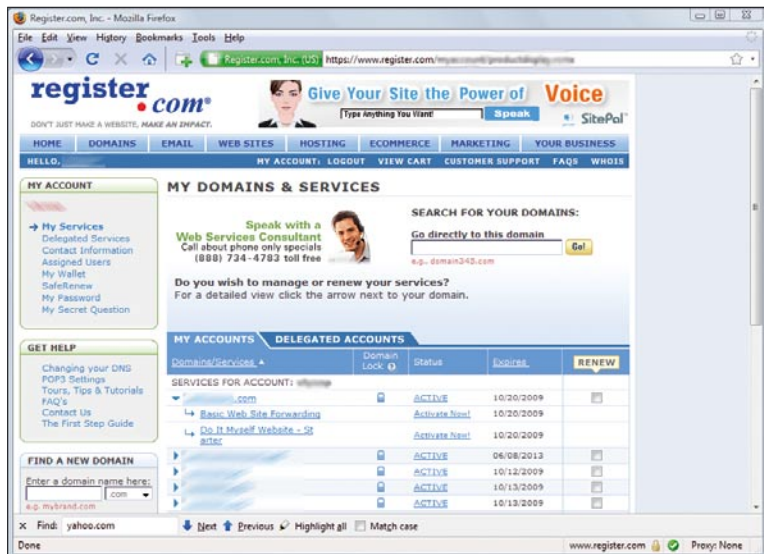


Figure 6. Domain names and the corresponding DNS Servers

In another email of Mrs. Mary, we find something equally interesting: usernames and passwords for a couple of domains. Does Ms. Mary own some domain on the Internet? Yes! To be honest, we easily got access to her domain manager (Figure 6).

If we are really bad, we can change the password of every domain she owns in order to lock her out and then redirect the DNS servers to deface the site (at the least) or to increase the traffic of another site! But ... just a minute! There is something more serious here: a *My Wallet* option. Getting there we have the credit card information of Mrs. Mary. Ok, this is not the full number but we have all of her data (area, phone, city etc.) that is very useful information (Figure 7). As you can see the connection, is a secure one (ssl).

And now we come to the most evil part of our search. In yahoo-mail there is a very useful button that is called *Search*. By pressing it, we can find a string that appears in one or more emails. We can search for any word we like. We have chosen the word *PayPal*. For those who do not *remember* PayPal is a service on the internet that connects to your bank account or your credit card with which you can make purchases by giving only a PayPal user code.

To be honest, we must say that we found many emails referring a PayPal account, but no password information was available. Actually we don't need it! What we can do is go to PayPal and choose the functionality *I forgot my password* (Figure 8)

Immediately PayPal will send, to Mary's email address, a new password assuming that Mrs. Mary is the only one that has access to her email. What a wrong assumption! Now, we can buy goods with Mrs. Mary's credit card. Fair enough, don't you think?!

We can do many more things but let's stop here. We *played* enough with Ms. Mary. Let's try another yahoo mail that we found in our earlier list. Maybe our luck is still *good* (Figure 9).

Hello Mr. Alan! We are ready to uncover your secrets! History repeats itself.

Conclusions and Ways of Protection

We presented a very simple method that a bad guy can violate the privacy (and also the personal life) of another person by getting access to his/her personal information simply because some administrator was stupid enough to let a data file with sensitive info reside in a directory accessible from the web. You may

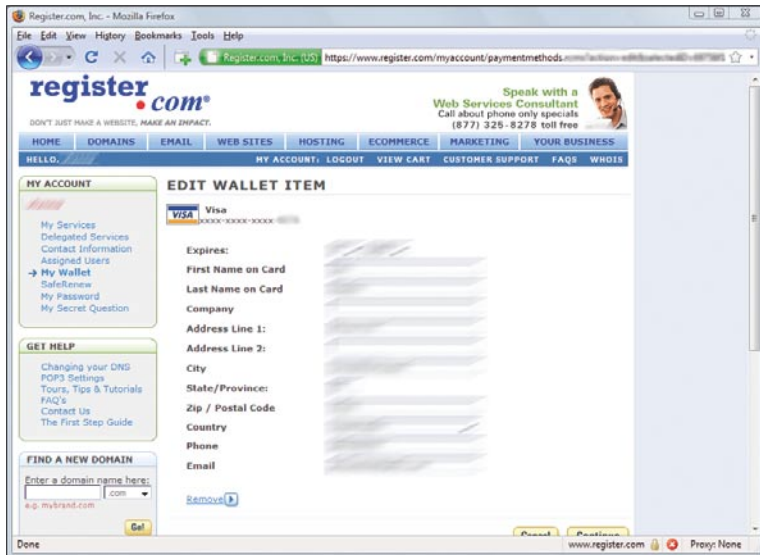


Figure 7. And the credit card info

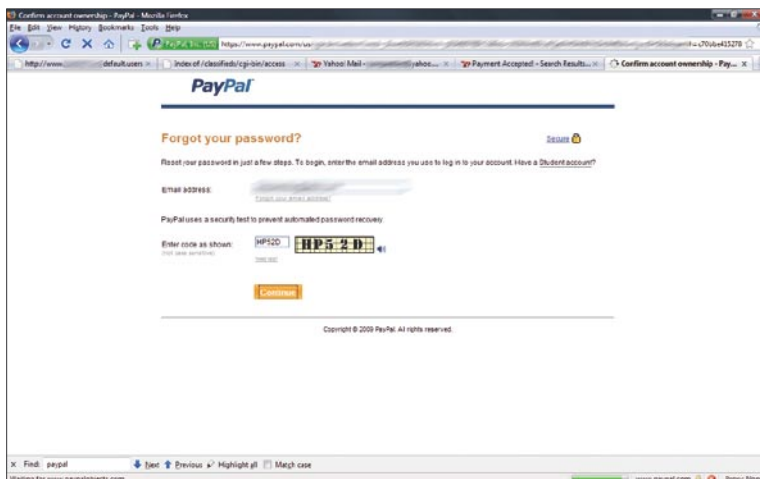


Figure 8. Tricking the PayPal ...

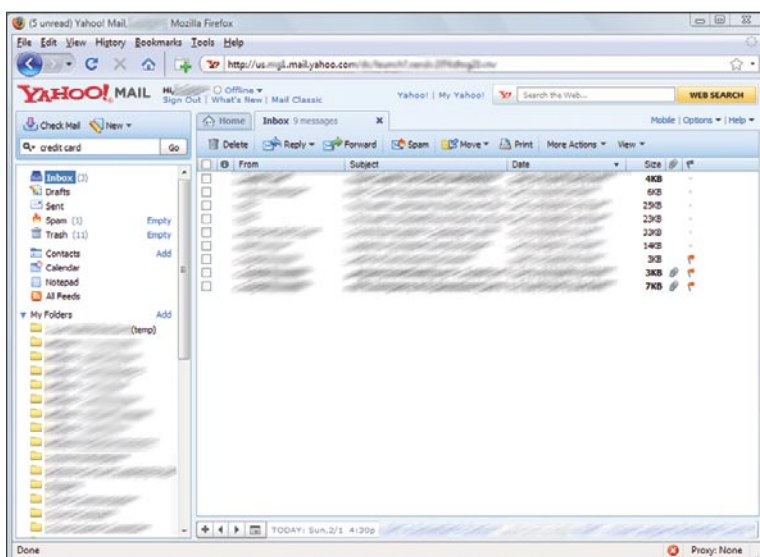


Figure 9. Hello Alan ...!

ask *Well well!* All my private life is on the hands of any stupid admin?. The answer is: Unfortunately yes, if you do not follow some basic safety rules. If you choose to have the same password on your favorite

forum as the one that you have to access your bank account, then do not blame SSL if you suddenly see a 2000 euro bill for your new journey to Seychelles!

So please pay a full attention to a few small but golden rules to avoid unpleasant surprises.

Rule 1

Do not be *ashamed* to use multiple passwords! If you have difficulties remembering them, use a Password Manager (there are many free that you can download from the net). Personally, I prefer KeePass (you can download it from <http://keepass.info/>). It is a free standalone application that can be run on the user's box. It uses strong encryption (AES, Twofish) and can function well on both Linux and Windows. In addition, it has many handy features, such as web form auto fill, strong random password generator etc.

Rule 2

Use at least two emails: One for the public sites (forums etc.) and one for your personal and financial account sites.

Rule 3

Choose a strong password. Strong passwords are those that are longer than 15 characters (ok, and smaller than 100!) and contain lowercase, uppercase, numbers and special characters such as `!@#$%^&*()_+=='`.

Rule 4

Always delete your emails that contain username and passwords from any web service to which you registered. Remember to really delete them. We mean, delete them from your inbox (or any subfolder) and from any trash-can that they may be placed after the deletion.

Rule 5

When you finish with your financial web tasks always logout from the corresponding site and clear the cache (delete history) of your web browser.

Finally, never forget the general rule in computer security (and not only):

The chain is as strong as its weakest link.

Safe Surfing!!

ANDREAS VENIRIS

Anonymizing

your online presence with TOR2

End to End communications over the internet are comprised of a number of intermediate systems, or hops, that help the request from a client machine (e.g. your computer) to reach a server machine (e.g. a web server).

What you will learn...

- A bit of networking (TCP, UDP and HTTP), but not much.
- How does a Proxy work.

What you should know...

- What is Tor and it works.
- How to configure and use Tor.
- About projects built around Tor.

In general, these intermediate machines know exactly the whole route taken from the origin to the destination making it easy to record or reconstruct that information at any given time. Even if you encrypt the data payload portion of the IP packets sent by your computer, the IP headers can reveal a lot of your identity to interested parties, such as timing information, origin of the packet, destination, interests and behavior, among other things.

Whatever your source for privacy concern is, be it legislation like the USA-PATRIOT Act [0], visits to internet-unfriendly countries, commercial research or if you are just paranoid, like me, and you want to avoid attackers knowing about your behavior while surfing on the internet, then TOR can help you. The Tor project aims to provide:

- Perfect Forward Secrecy: Compromised nodes would not be able to decrypt old traffic once keys expire.
- Multiplexing TCP circuits: Many TCP streams may share already (newly) created circuits (more on circuits later). This means that as the amount of Tor users goes up, the less likely traffic analysis will work, by hiding users among users.
- Congestion control: Tor nodes use End-to-End ACKs to control bottlenecks at the frontier of the network.
- Directory services: Some Tor trusted nodes provide a directory service to let Tor clients know about the state of existing routers in the network.

- End-to-End integrity check: Tor verifies data integrity at the edges of the network, to make sure the data wasn't modified.

What exactly is Tor

The Onion Router, Tor for short, is described as a *circuit-based low-latency anonymous communication service*. Is a project first presented by Dingledine, Mathewson and Syverson in a paper called *Tor: The Second-Generation Onion Router* in the USENIX Security Symposium in 2004. According to the overview page on the Tor Project website [2], it was initially intended for, and supported by, the U.S Naval Research Laboratory, before the Tor Project, Inc. was established. A number of NGOs (like Human Rights Watch), private companies (Google, Internews Europe), individuals and others donate or have donated to the project.

The term Onion Router comes from the first implementation of this technology and refers to the fact that to get the original message (after entering the network) it is necessary to strip several layers of encryption, much like peeling the layers of an onion.

Before getting into the technical details of Tor, it is important to note that Tor is comprised of two parts. The first part is the Tor network, which is described by Dingledine, Mathewson and Syverson as a *distributed overlay network designed to anonymize TCP-based applications like web browsing, secure shell and instant messaging*. This means that this first component of Tor

provides a network of virtual tunnels sitting on top the internet, so the now the intermediate hops between End-to-End communications, are Tor routers. The second part of Tor is the client part. This client is an Open Source application that implements a SOCKS [3] proxy that is able to interact with Tor routers to make your requests arrive at the intended destination through paths created between the routers.

How does Tor actually work?

Tor client provides a SOCKS interface (also called OP for Onion Proxy) for TCP-based applications like IM clients and browsers. The idea is that the Tor client selects a Tor router (also known as OR for Onion Router) from the Tor network (see Figure 1) to create a path or circuit between your machine and the destination, by hop at a time. The client, then negotiates public keys with this selected OR, and with subsequent hops, to incrementally encrypt the data with each OR's keys (see Figure 2).

Tor circuits are created one hop at a time and are identified by a circuit ID (circID). The OP selects an OR from the directory information it got from Tor's directory service and ask it to create a new circuit with half of its key and circID_A. This OR, let's call it OR_A, responds with an acknowledgment that the circuit with ID circID_A was created, along with OR_A public key for that circuit.

If the OP wants to extend circID_A with another hop, then it will send OR_A an Extend command, which OR_A will receive and will choose another OR_B and create a circuit circID_B between them. OR_B will send its keys to OR_A, which in turn, will relay to OP, so the message can be encrypted using K_A and K_B, in that order. OP will never know about circID_B, that is just between OR_A and OR_B, but OP will get K_B sent by OR_B, through OR_A.

Once the data is encrypted using each of the OR's keys, it is sent in order through the created circuit, in subsequent hops through every selected OR. Every OR in the circuit peels one layer of encryption (and thus the Onion pronoun) with its own private key before forwarding the request to the next OR in the circuit. The process is repeated until the last OR (or Exit Node) in the circuit is reached and then, the original data (and not the original IP headers) is then forwarded to the destination.

By this method, it is not possible for the destination, where this request was sent from, as they'll only see the Exit Node as the origin of the information. Moreover, the ORs in the circuit only know the existence of the previous router in the circuit (or the origin, if it is the first router) and the next router in the circuit (or the destination of the data, if it was the Exit Node).

This approach to privacy makes it highly difficult for an attacker to know the whole route a request took to

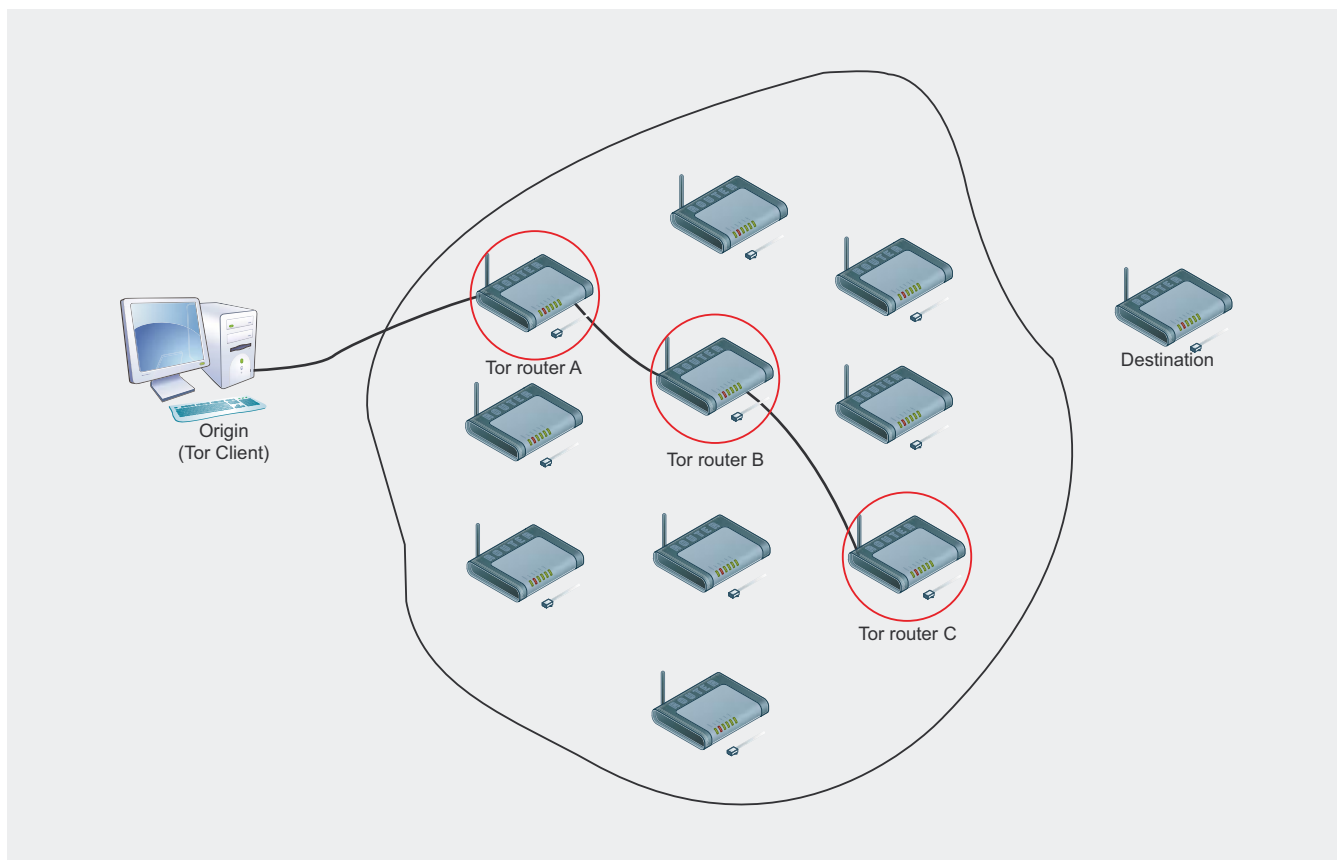


Figure 1. Tor Network with data flow in a circuit between Client -> Tor router A -> Tor router B -> Tor router C -> Destination

reach a destination. Tor makes it even more difficult for attackers, as the circuits initially created by the OP change in time (new circuits are created periodically).

Every OR is connected to the others, and to the OP using TLS encryption with short-term keys. This guarantees perfect forward secrecy [5] and makes it impossible for attackers to intercept the data with Man-in-the-Middle attacks. The communication unit between OP/OR and OR/OR is the *cell*. These are fixed-size (512 bytes) packets that include Tor specific headers and a payload. Cells can be of two types, *control cells* or *relay cells*. *Control cells* carry Tor commands and are interpreted by the destination OR. They are used to create, extend or destroy circuits and other network tasks. *Relay cells* carry End-to-End data (e.g. OP requests or keys from extending ORs). If you want to know more about the cells and their types, we encourage you to read the paper on Tor [1].

Tor sounds great. How can I use it?

Until this point, we have covered Tor from a design and internals point-of-view. So let's start getting our hands dirty.

One of Tor's design goals was for it to be simple, as in simple to install, configure and use. The first thing we are going to need, is to download a release from the Tor project download page [4]. Tor runs on a variety of platform, including but not limited to Linux, Windows, MacOS X, Android, *BSD Unix, etc. As you'll see later on, the Tor project also provides bundles, LiveCD/USBs and other projects to help you get started quickly with Tor.

Our aim here is to get Tor running in your machine, so we will be focusing mainly on that but we will talk about other of the Tor projects [6] in a bit.

To get Tor running in your machine, you will need first to install it. If you are using Linux/*BSD, you can get you favorite distro's package manager to install it for you. You can find Tor in most Linux distros, like Gentoo Linux, Debian, Ubuntu, RedHat, etc.

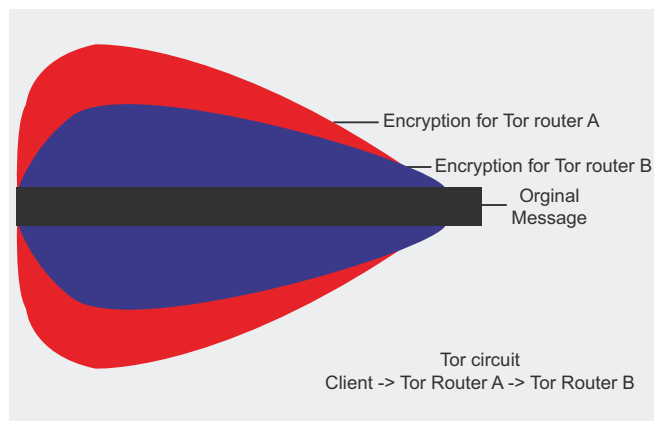


Figure 2. Topology of a Tor message in a circuit of Client – Tor router A – Tor router B

If you are using Windows, you can download the Tor Expert Bundle (just includes Tor) from the downloads page [4] and use the installer provided there. For MacOS X users, there are some bundles with everything you need to get Tor configure and running in no time.

For installs from source code, you'll need to follow the all familiar `./configure`, `make`, `make install` steps. Please refer to the README found in Tor's source code for more information about configure options and steps.

Once you have Tor installed, we need to get it running. As you may recall, Tor is composed of two parts, Tor network and Tor client. The software you installed corresponds to the Tor client (OP), which is a SOCKS proxy that will be used by your applications to forward requests through the Tor network. This OP bind to the port 9050 (default SOCKS port) in your machine to listen for connections coming from your SOCKS aware applications.

In Linux and Unix-based systems, you will generally find a Tor initscript (see Listing 1) that you can start to make Tor listen on the specified port. In other systems such as Windows or MacOS X, depending on the bundle you install, you'll find different tools and panels (like Vidalia, a graphical Tor controller) to help you get Tor running.

Once Tor is running and listening in port 9050 in your machine, you need to *Torify* your applications. In other words, you need to make your applications aware of Tor's existence by setting them to go through Tor. If your application support SOCKS, then configure it to use a SOCKS proxy pointing to `localhost:9050`. For example, Mozilla Firefox can be configured to use a SOCKS proxy to connect to the internet. You can configure this by following the steps in Figure 3.

To test if your OP and application are getting along and that you are indeed connected to the Tor network, you can browse to <http://check.torproject.org> and it will tell you if you are, or not, connected to the Tor network correctly. If you are connected and everything is running smoothly, then you will see a green message saying *Congratulations. Your browser is configured to use Tor.* If you are not, you'll see a red message saying *Sorry. You are not using Tor.*

If you get the red message, then re-check your application configuration and make sure Tor is running (you can verify this with commands like `netstat`, to see if Tor is up and listening in port 9050), and that your

Listing 1. Starting tor with an initscript in Linux

```
kafka ~ # /etc/init.d/tor start
```


application is setup to go through a SOCKS proxy located at `localhost:9050`. On the other hand, if you get the green message, congratulations are in order because you are browsing using the Tor network.

Further tweaking Tor configuration

You can find Tor's configuration file in `/etc/tor/torrc`. There, you'll find some variables you can manipulate to better suit your needs. Listing 2 shows the `torrc.sample` file that comes with Tor's source code.

From this file, we can point to some of the variables you might find interesting:

- `SocksPort` and `SocksListenAddress`: Address and port where Tor will bind to listen for connections. Defaults are 9050 and localhost, respectively.
- `SocksPolicy`: With this variable you can specify networks from where to accept or reject (or both) connections from. For instance, if you want to provide a proxy for your local network 192.168.0.0/16, then you can add two lines like these: `SocksPolicy accept 192.168.0.0/16` and `SocksPolicy reject *`. This means you are going to be accepting connections from your network, but rejecting everything else. (Note: If you want to do this, you may have to change the `SocksListenAddress` to use an IP within the 192.168.0.0/16 network).

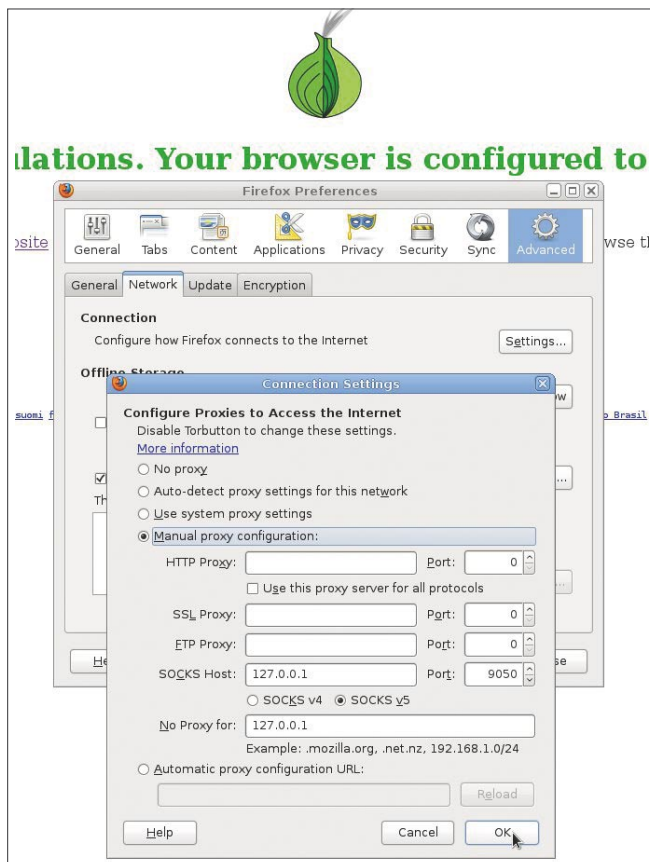


Figure 3. Firefox proxy configuration. You can access this dialog by `Edit -> Preferences -> Advanced -> Network -> Settings...`

- `Log`: Specifies the level and facility that will collect Tor's log messages.
- `DataDirectory`: Location for data concerning the connections to the Tor network. For examples, this location is used to store negotiated keys with the ORs of a circuit.

Other Tor goodies

As we mentioned before, Tor comes in different flavors for different platforms. It also hosts some other Tor related projects that can help you enhance your Tor overall experience.

Here are some of the other Tor goodies, in no particular order:

- `TorButton`: Firefox plugin to make it really easy to turn Tor On/Off by 1-clicks. Without `TorButton`, you can use Firefox with Tor (Figure 3), but that means everytime you need to switch between enabling/disabling Tor, you need to go to the Network Configuration panel in Firefox to enable/disable the SOCKS connections. With `TorButton`, is possible to let this tedious task in the past. `TorButton` can also do many other things [7].
- `Vidalia`: Qt-based front-end for Tor. It provides a control panel for Tor, status indication (whether you are connected to the Tor network, or not), Tor settings manager, and other goodies like access to the message log or a bandwidth meter [8].
- `Arm`: The Anonymizing Relay Monitor, is a Cli, or command-line interface for Tor. It gives you information about used bandwidth, memory usage, relaying information, Tor configuration file editor with validation [9].
- `Tails`: The Amnesiac and Incognito Live System, is a Linux distribution based on Debian GNU/Linux that is completely ready and pre-configured for your security [10].
- `Orbot`: Tor port for the Android OS. You may have to install a proxy-capable browser in your smartphone before using Tor. You can use Firefox Mobile with the Proxy Mobile add-on, that will allow you to set Firefox Mobiles' proxy settings [11].

There are some other projects you might like. We encourage you to visit the Tor Projects page [6].

Tor pitfalls and other considerations

As noted at the bottom of the Projects page [6], Tor does not solve all privacy/anonymity related problems. Tor goal are concerned with securely transporting your data, to anonymize certain information regarding your requests, such as origin and destination addresses.

For example, Tor, by itself, won't prevent destination websites from obtaining information leaked by your

Listing 2a. torrc.sample. Tor Configuration file

```

## Configuration file for a typical Tor user
## Last updated 16 July 2009 for Tor 0.2.2.1-alpha.
## (May or may not work for much older or much newer
      versions of Tor.)
##
## Lines that begin with "## " try to explain what's
      going on. Lines
## that begin with just "#" are disabled commands: you
      can enable them
## by removing the "#" symbol.
##
## See 'man tor', or https://www.torproject.org/tor-
      manual.html,
## for more options you can use in this file.
##
## Tor will look for this file in various places based
      on your platform:
## https://wiki.torproject.org/noreply/TheOnionRouter/
      TorFAQ#torrc

## Default username and group the server will run as
User tor

PIDFile /var/run/tor/tor.pid

## Replace this with "SocksPort 0" if you plan to run
      Tor only as a
## relay, and not make any local application
      connections yourself.
SocksPort 9050 # what port to open for local
      application connections
SocksListenAddress 127.0.0.1 # accept connections only
      from localhost
#SocksListenAddress 192.168.0.1:9100 # listen on this
      IP:port also

## Entry policies to allow/deny SOCKS requests based
      on IP address.
## First entry that matches wins. If no SocksPolicy is
      set, we accept
## all (and only) requests from SocksListenAddress.
#SocksPolicy accept 192.168.0.0/16
#SocksPolicy reject *

## Logs go to stdout at level "notice" unless
      redirected by something
## else, like one of the below lines. You can have as
      many Log lines as
## you want.
##
## We advise using "notice" in most cases, since
      anything more verbose
## may provide sensitive information to an attacker
      who obtains the logs.
##
## Send all messages of level 'notice' or higher to
      /var/lib/log/tor/notices.log
#Log notice file /var/lib/log/tor/notices.log
## Send every possible message to /var/lib/log/tor/
      debug.log
#Log debug file /var/lib/log/tor/debug.log
## Use the system log instead of Tor's logfiles
#Log notice syslog
## To send all messages to stderr:
#Log debug stderr

## Uncomment this to start the process in the
      background... or use
## --runasdaemon 1 on the command line. This is
      ignored on Windows;
## see the FAQ entry if you want Tor to run as an NT
      service.
#RunAsDaemon 1

## The directory for keeping all the keys/etc. By
      default, we store
## things in $HOME/.tor on Unix, and in Application
      Data\tor on Windows.
#DataDirectory /var/lib/lib/tor
DataDirectory /var/lib/tor/data

## The port on which Tor will listen for local
      connections from Tor
## controller applications, as documented in control-
      spec.txt.
#ControlPort 9051
## If you enable the controlport, be sure to enable
      one of these
## authentication methods, to prevent attackers from
      accessing it.
#HashedControlPassword 16:872860B76453A77D60CA2BB8C1A7
      042072093276A3D701AD684053EC4C
#CookieAuthentication 1

##### This section is just for location-
      hidden services ###
## Once you have configured a hidden service, you can
      look at the
## contents of the file "../hidden_service/hostname"
      for the address
## to tell people.
##

```

Listing 2b. torrc.sample. Tor Configuration file

```

## HiddenServicePort x y:z says to redirect requests
        on port x to the
## address y:z.

#HiddenServiceDir /var/lib/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir /var/lib/lib/tor/other_hidden_
        service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22

##### This section is just for relays
#####

#
## See https://www.torproject.org/docs/tor-doc-relay
        for details.

## Required: what port to advertise for incoming Tor
        connections.
#ORPort 9001
## If you want to listen on a port other than the one
        advertised
## in ORPort (e.g. to advertise 443 but bind to 9090),
        uncomment the
## line below too. You'll need to do ipchains or other
        port forwarding
## yourself to make this work.
#ORListenAddress 0.0.0.0:9090

## A handle for your relay, so people don't have to
        refer to it by key.
#Nickname ididnteditheconfig

## and Tor will guess.
#Address noname.example.com

## Define these to limit how much relayed traffic you
        will allow. Your
## own traffic is still unthrottled. Note that
        RelayBandwidthRate must
## be at least 20 KB.
#RelayBandwidthRate 100 KB # Throttle traffic to
        100KB/s (800Kbps)
#RelayBandwidthBurst 200 KB # But allow bursts up to
        200KB/s (1600Kbps)

## Use these to restrict the maximum traffic per day,
        week, or month.
## Note that this threshold applies to sent _and_ to
        received bytes,
## not to their sum: Setting "4 GB" may allow up to 8
        GB
## total before hibernating.
##
## Set a maximum of 4 gigabytes each way per period.
#AccountingMax 4 GB
## Each period starts daily at midnight (AccountingMax
        is per day)
#AccountingStart day 00:00
## Each period starts on the 3rd of the month at 15:00
        (AccountingMax
## is per month)
#AccountingStart month 3 15:00

## Contact info to be published in the directory, so
        we can contact you
## if your relay is misconfigured or something else
        goes wrong. Google
## indexes this, so spammers might also collect it.
#ContactInfo Random Person <nobody AT example dot com>
## You might also include your PGP or GPG fingerprint
        if you have one:
#ContactInfo 1234D/FFFFFFFF Random Person <nobody AT
        example dot com>

## Uncomment this to mirror directory information for
        others. Please do
## if you have enough bandwidth.
#DirPort 9030 # what port to advertise for directory
        connections
## If you want to listen on a port other than the one
        advertised
## in DirPort (e.g. to advertise 80 but bind to 9091),
        uncomment the line
## below too. You'll need to do ipchains or other port
        forwarding yourself
## to make this work.
#DirListenAddress 0.0.0.0:9091
## Uncomment to return an arbitrary blob of html on
        your DirPort. Now you
## can explain what Tor is if anybody wonders why your
        IP address is
## contacting them. See contrib/tor-exit-notice.html
        in Tor's source
## distribution for a sample.
#DirPortFrontPage /etc/tor/tor-exit-notice.html

## Uncomment this if you run more than one Tor relay,
        and add the identity
## key fingerprint of each Tor relay you control, even
        if they're on
## different networks. You declare it here so Tor

```

Listing 2c. torrc.sample. Tor Configuration file

```

        clients can avoid
## using more than one of your relays in a single
        circuit. See
## https://wiki.torproject.org/noreply/
        TheOnionRouter/
        TorFAQ#MultipleServers
#MyFamily $keyid,$keyid,...

## A comma-separated list of exit policies. They're
        considered first

## the default exit policy, end this with either a
        reject *.* or an
## accept *.*. Otherwise, you're _augmenting_
        (prepending to) the
## default exit policy. Leave commented to just use
        the default, which is
## described in the man page or at
## https://www.torproject.org/documentation.html
##
## Look at https://www.torproject.org/faq-abuse.html
        #TypicalAbuses
## for issues you might encounter if you use the
        default exit policy.
##
## If certain IPs and ports are blocked externally,
        e.g. by your firewall,
## you should update your exit policy to reflect this
        -- otherwise Tor
## users will be told that those destinations are
        down.
##
#ExitPolicy accept *:6660-6667,reject *.* # allow
        irc ports but no more
#ExitPolicy accept *:119 # accept nntp as well as
        default exit policy
#ExitPolicy reject *.* # no exits allowed
#
## Bridge relays (or "bridges") are Tor relays that
        aren't listed in the
## main directory. Since there is no complete public
        list of them, even if an
## ISP is filtering connections to all the known Tor
        relays, they probably
## won't be able to block all the bridges. Also,
        websites won't treat you
## differently because they won't know you're
        running Tor. If you can
## be a real relay, please do; but if not, be a
        bridge!
#BridgeRelay 1
#ExitPolicy reject *.*

```

browser, like the OS you are running or the browser and version you are using. That information is encoded in the requests sent by the browser and it would require an HTTP aware service to modify your HTTP requests before forwarding them to the Tor network. TorButton might help, but be aware that TorButton only works with Mozilla Firefox (and Google Chrome in the future) and won't work with other browsers. That is why you will often see Tor being used in conjunction with other proxy solutions like Polipo or Privoxy. These web proxys are special HTTP proxies that understand HTTP well enough and that might help you with HTTP headers modifications and ad-blocking features.

Another thing you have to know is that by having Tor installed, configured and running, it won't magically *Torify* all your applications. You have to manually (or using other tools) make your applications to send requests through Tor, by configuring the application-specific options (e.g. setting SOCKS proxy to localhost:9050 in the relevant option in your application). Tor provides a configuration option (when you are configuring the source code) `--transparent-proxy`, that can help you configure Tor for all applications transparently, but this requires root access and configuring your advanced firewall (e.g. iptables) to redirect requests to the Tor proxy. You can read more about this feature in the Tor Trac [12].

Please, keep in mind that Tor is for TCP-based applications. It won't *catch* some leakage you might have with other protocols. For example, Tor admits to only support Mozilla Firefox because other browsers are proven to leak information such as DNS resolves or direct FTP connections.

Another thing worth being mentioned, is that if you send unencrypted information through the Tor network, although while transiting the Tor network it will remain encrypted, at the exit node the information will be unencrypted again. Anybody listening for packets going out from the exit node, will be able to see the data sent (not the original sender information, though). So, if you want End-to-End encryption, you should encrypt your information before handing it to Tor.

How to contribute

If you fall in love with Tor, you can help the project by donating, becoming a developer, running your own Tor relay (OR), or all of those.

To donate, you can visit the *Make a Donation* [13] page and you could use different payment methods to help the project. You can also donate hardware, various services or becoming an sponsor.

To help with Tor development, you can visit the *Get Involved* page [14] and see what kind of task you can contribute to. There are many tasks, translation and

References

- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA-PATRIOT Act). http://en.wikipedia.org/wiki/USA_PATRIOT_Act [0]
- Roger Dingledine, Nick Mathewson and Paul Syverson. "Tor: The Second-Generation Onion router". 13th USENIX Security Symposium. August 2004. [1]
- Tor Project Homepage. <http://www.torproject.org> [2]
- SOCKS Proxy. <http://en.wikipedia.org/wiki/SOCKS> [3]
- Tor Project Downloads page. <https://www.torproject.org/download/download-easy.html.en> [4]
- Perfect Forward Secrecy. http://en.wikipedia.org/wiki/Perfect_forward_secrecy [5]
- Tor-related Projects page. <https://www.torproject.org/projects/projects.html.en> [6]
- TorButton page. <https://www.torproject.org/torbutton/index.html.en> [7]
- Vidalia, (Tor GUI) page. <https://www.torproject.org/projects/vidalia.html.en> [8]
- Arm (Anonymizing Relay Monitor) page. <https://www.torproject.org/projects/arm.html.en> [9]
- Tails (The Amnesic Incognito Live System) page. <https://tails.boum.org/> [10]
- Orbot (Tor port for Android OS) page. <https://guardianproject.info/apps/orbot/> [11]
- Transparent Proxy (Tor feature) howto. <https://trac.torproject.org/projects/tor/wiki/doc/TransparentProxy> [12]
- Make a Donation page. <https://www.torproject.org/donate/donate.html.en> [13]
- Get Involved page. <https://www.torproject.org/getinvolved/volunteer.html.en> [14]

documentation and tasks for developers in the various projects associated with Tor.

Other helpful way to help Tor would be to run your own OR. The software you already installed (the Tor client) is capable of running a fully compliant Tor relay. To configure it, you can modify the relevant bits in the torrc configuration file, or if you have Vidalia installed, then you can use it to easily set the relay running. You can tweak more configuration options to limit the bandwidth used for the Tor network and other Exit policies to limit what kind of services could be reached through your newly set relay.

JESUS RIVERO

Jesus Rivero, a.k.a Neurogeek, is a Computer Scientist programming for the past 10 years from embedded systems to web applications. Currently, he develops software for the financial world and is a Gentoo GNU/Linux developer.
jesus.riveroa@gmail.com
neurogeek@gentoo.org
Website/blog: <http://dev.gentoo.org/~neurogeek>



HAKIN9

Join our
**Exclusive and Pro club
and get:**

- HAKIN9 HAKIN9 HAKIN9** Hakin9 one year subscription
- HAKIN9** Full page advertisement in Hakin9 every month!
- HAKIN9** Information about your company send to over 100,000 Hakin9 readers!

More information at
en@hakin9.org

Background text includes: "In his business experience, Bryden says his involvement has always been as a major shareholder and top executive, but in a company based on the vision of other people who he believed knew what they were doing, and whose dream had commercial value." "Not much work gets done on the weekends, with summer trips back to Cape Breton to visit family and winters skiing at Mount Tremblant. A lot of tennis, swimming and fishing is sandwiched in between." "Bryden says that right now retirement isn't on the horizon." "I'm probably old enough, I just haven't got smart enough yet," jokes Bryden. "He says in the case of WorldHeart, there's probably another five years to go when it's a commercial drive that's required at the top. At that point, he says experienced running a major medical science company might be more appropriate to lead WorldHeart." "I certainly wish that point would be surprised if at that time there wasn't something else to do," says Bryden.

Secure OpenLDAP Infrastructure

This article will discuss about how to install OpenLDAP and increase security level using TLS to implement confidentiality and ACLs to implement access control. At the end, we'll see about how to improve availability using syncrepl method of replication.

What you will learn...

- how to use install OpenLDAP
- how to secure OpenLDAP with TLS and ACL
- how to configure OpenLDAP replication using syncrepl

What you should know...

- basic understanding of LDAP protocol
- basics of Linux shell.

The Lightweight Directory Access Protocol, or LDAP, is a standard technology for network directories. LDAP is both a network protocol and a standard architecture based on X.500 to store information related to computer networks. X.500 is a series of computer networking standards developed by ITU-T. In the X.500 directory architecture, the client queries and receives responses from one or more servers in the server directory service. To control the communication between clients and information, ITU-T created a protocol named DAP (*Directory Access Protocol*). DAP is a heavyweight that runs over a full OSI stack and consequently, like almost all OSI protocol, was not popular.

University of Michigan, in 90's developed LDAP, supported by the National Science Foundation. Since then, *Internet Engineering Task Force* (IETF) published more than two hundred RFCs and drafts related to LDAP. LDAP implements basics DAP operations like Bind, Read, List, Search, Compare, Add, Delete and Modify DN. Different from DAP, LDAP runs over TCP/IP.

We described a little about the protocol, standards, history and operations of LDAP. Now we need discuss a little about common information stored inside LDAP services. First of all, a directory is like a database, and information in a directory is generally read much more often than it is written. Indeed, the best information to store in LDAP is almost static data, like

users information. In general, if you need to change data frequently, it's probably better to use a relational database rather a directory service. If information is truly static, such as port numbers (from `/etc/services`), then it is likely better to use another way to distribute this type of information rather than use LDAP and incur network communication overhead every time. LDAP is good for handling small and simple units of data and bad to handle complex data.

Another characteristics of LDAP and directory services is its support for high volumes of data, reduced response time, and the ability to replicate information to other systems. LDAP servers, on the other hand lacks most database operations and has poor performance when updating data.

Why I need an LDAP server?

The major benefit around the use of LDAP is to simplify administrative tasks. With LDAP it is possible to manage several services and configurations from a single point, favoring auditing and security in general. When user information and configuration data from critical services are migrated to an LDAP store and you assure that the LDAP store is the only source for this type kind of information, you have a standardized environment.

Let's see an example about inputing user information in LDAP. When you do this, if you need to block a user, the changes are respected for all computers

automatically. If you don't use LDAP, it's more difficult to assure that this user is blocked in every server of your environment. As always there is a bad side in centralized information, because you create a single point of failure, where an intruder can get access to the entire network. In this article we will cover a little about how to create an LDAP server with a minimal level of security.

Some necessities like how to distribute user information and configurations in a secure way are eliminated automatically. And with LDAP it's possible to monitor some critical files of servers, like `/etc/passwd` and `/etc/shadow`, with a host/file integrity checker.

The best way to start is inputting user and group information into LDAP. With this, it's possible to use LDAP for Linux and Unix authentication, proxy authentication, etc. After that, you can increase the functionality, inputting other types of information like sudo authorization, SSH public keys, email information, printer information, file server information, and so on.

Why OpenLDAP?

There are a lot of commercial and non-commercial software related to LDAP services. Even though each LDAP server has its advantages and disadvantages, OpenLDAP is the most compliant LDAP server.

The LDAP protocol was born inside University of Michigan, and the team related to the LDAP project maintained LDAP software to prove that LDAP was useful. LDAP code was maintained as free software and when the LDAP team joined Netscape, the original code evolved into OpenLDAP.

The current release of OpenLDAP has been proven to scale to hundreds of millions of objects in data volumes in excess of a terabyte, with performance in excess of 22,000 queries per second at sub-millisecond latencies. Compliance continued as the major goal of the project, and when new features are published in RFCs or even in drafts, OpenLDAP project includes the feature in the software. OpenLDAP supports modules, and is easier to extend the functionalities without changes in the core code.

Other good features of OpenLDAP are that, it supports all you need to use LDAP securely, such as TLS, ACLs and policy. OpenLDAP supports other modern features like dynamic configuration, Idif schemas, multimaster replication, and so on.

Planning the infrastructure

When you are planning a new service, in particular a very important service related to authentication, it's very important to be concerned about security. Availability is one security concern that is necessary to start in the planning step.

First of all, it's necessary to use two or more servers for your directory server. In this way, your directory

server can be available even in the event of disaster in another one servers.

For this, we need replication between the servers. The current way to configure replication with OpenLDAP uses LDAP sync replication, or `syncrepl`.

There are at least two methods to ensure clients have high availability. The first is using a load balancer and the second is when clients are configured with multiple servers.

The second method is recommended, in particular when we use TLS, because it's possible to assure end-to-end confidentiality. Since our goal is to create a secure environment, we will use the second method.

To have a high availability LDAP service, it's necessary to monitor all services and the replication process as well.

In this article, we will explain how to create LDAP infrastructure using two servers. It will be named `ldapserver1` and `ldapserver2`, inside the `localdomain` domain.

Installing OpenLDAP

Let's install OpenLDAP with TLS support, a feature necessary to improve the level of security. The following procedures are about the compilation of OpenLDAP, using this method we cover more operating systems with the same procedure. If you prefer, you can install OpenLDAP via the other method.

First, download the latest source release 4 of Berkeley DB from Oracle site (www.oracle.com/technetwork/database/berkeleydb) and last version of OpenLDAP source from the OpenLDAP site (www.openldap.org).

Compiling and installing Berkeley DB:

```
# tar -zxvf db-4.8.30.NC.tar.gz
# cd db-4.8.30.NC/build_unix/
# ../dist/configure && make && make install
```

OpenLDAP needs to find Berkeley DB before compilation:

```
# export CFLAGS="-I/usr/local/BerkeleyDB.4.8/include"
# export CPPFLAGS="-I/usr/local/BerkeleyDB.4.8/include"
# export LDFLAGS="-L/usr/local/BerkeleyDB.4.8/lib"
# export LD_LIBRARY_PATH="/usr/local/BerkeleyDB.4.8/lib"
```

Compiling and installing OpenLDAP:

```
# tar -zxvf openldap-2.4.26.tgz
# cd openldap-2.4.26
# ./configure --with-tls
# make depend && make && make install
```

Do the above procedures on both servers.

Create a minimal directory

First of all, you need to create a password for the manager of directory. You create a hashed password with the command `slappasswd`. Use `slappasswd` with `-h {SSHA}` arguments to create a secure SHA hash:

```
# slappasswd -h {SSHA}
New password:
Re-enter new password:
{SSHA}l5+OQhtI4pNzAhFqc7myUaH23yw+qe8Y
#
```

This hash will be used to manage the directory. Like a root user on a UNIX system, use of the directory manager should be avoided. We will see how to configure admin users to manage the directory service further below in the article.

Create a `/etc/openldap/ldapserver1` directory to be used as a configuration directory of node `ldapserver1` and copy directory schema from `/usr/local/etc/openldap/schema` to it:

```
# mkdir -p /etc/openldap/ldapserver1
# cp -rp /usr/local/etc/openldap/schema /etc/openldap/
    ldapserver1
```

Create a directory for your base (Berkley DB):

```
# mkdir -p /var/lib/ldap/ldapserver1
```

Create a `/etc/openldap/slapd.conf` file with Listing 1 content.

Start the LDAP server with the command:

```
# /usr/local/libexec/slapd -f /etc/openldap/ldapserver1/
slapd.conf -h „ldap://ldapserver1.localdomain“
```

Now, we need to improve LDAP security using TLS, prior to continuing.

Create your own OpenSSL CA

To assure a minimal level of security, we will use TLS and assure that the entire communication between LDAP servers is encrypted, including replication communication. In this manner confidentiality will be assured. In our example, we will use certificates in server side only, but in really secure environment it's important to use certificates on the client side and ensure that servers don't accept communication from clients without certificates signed by a reliable CA.

If you have a private CA or prefer to use a commercial CA to sign your certificates, you can skip this part of the article. We will explain only the minimal steps to sign certificates using OpenSSL, because it is the most common software related to SSL key management,

however you can use GnuTLS or MozNSS, if you prefer. It's highly recommended to avoid self-signed certificates.

The CA, like the LDAP server needs to be protected more than other common servers. It's a good idea to maintain your CA outside of the LDAP servers and control access to the server with the CA. Make sure that OpenSSL is installed on your system, and locate the Perl script named `CA.pl`. In my system, `CA.pl` is located in the directory `/usr/lib/ssl/misc`. Run the script with `-newca` argument, and answer the questions with your own information:

```
# /usr/lib/ssl/misc/CA.pl -newca
```

Make sure that password is well protected. Directory `demoCA` will be created in your current directory. Move `demoCA` to another directory of your preference. I use `/etc/CA`:

```
# mv demoCA /etc/CA
```

Now, adjust the dir setting inside the `openssl.cnf` file (in my system, `/usr/lib/ssl/openssl.cnf`):

```
[ CA_default ]

dir                = /etc/CA                # Where
                everything is kept
```

Your CA is ready to sign TLS certificates for your LDAP servers.

Listing 1. Minimal `slapd.conf`

```
#slapd.conf file
include            /etc/openldap/ldapserver1/schema/
                    core.schema

pidfile            /usr/local/var/run/slapd-
                    ldapserver1.pid

argsfile           /usr/local/var/run/slapd-
                    ldapserver1.args

database           bdb

suffix             "dc=example,dc=com"

rootdn             "cn=admin,dc=example,dc=com"

rootpw            {SSHA}yourhashhere

directory          /var/lib/ldap/ldapserver1

index objectClass eq
```


Create certificates and sign them

For each server, you need to create a certificate request and sign it in your CA.

On the LDAP server, create a directory for your key and certificates:

```
# mkdir /etc/openldap/ldapserver1/certs

# Inside this directory, create a private key:
# openssl genrsa -out ldapserver1.key 1024
```

Create a request, with the command:

```
# openssl req -new -out ldapserver1.csr -key ldapserver1.key
```

Make sure that Common Name (eg., YOUR name) []: is filled with FQDN of the LDAP service, in my case ldapserver1.localdomain.

Copy/transfer ldapserver1.csr to the CA directory in CA server and sign the request:

Listing 2. Replica configuration

```
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100

syncrepl rid=000
provider=ldaps://ldapserver1.localdomain
bindmethod=simple
tls_reqcert=never
type=refreshAndPersist
retry="5 5 300 +"
searchbase="dc=example,dc=com"
attrs="*,+"
binddn="cn=replica,dc=example,dc=com"
credentials=secret

syncrepl rid=001
provider=ldaps://ldapserver2.localdomain
bindmethod=simple
tls_reqcert=never
type=refreshAndPersist
retry="5 5 300 +"
searchbase="dc=example,dc=com"
attrs="*,+"
binddn="cn=replica,dc=example,dc=com"
credentials=secret

mirrormode TRUE
```

```
# openssl can -out ldapserver1.pem -in ldapserver1.csr
```

ldapserver1.pem was created with ldapserver1 certificate. Copy the files to the /etc/openldap/ldapserver1/certs directory on ldapserver1 along with the public certificate from the CA, named cacert.pem.

Configuring OpenLDAP to use TLS explicitly

After you have obtained all files that you need, you need to configure slapd.conf to include TLS directives. Insert the following above the database line:

```
TLSCACertificateFile /etc/openldap/ldapserver1/certs/cacert.pem
TLSCertificateFile /etc/openldap/ldapserver1/certs/
                    ldapserver1.pem
TLSCertificateKeyFile /etc/openldap/ldapserver1/certs/
                    ldapserver1.key
TLSVerifyClient never
```

Now your directory server is ready to accept secured communication using the TLS protocol, however your LDAP server also accepts unsecured communications as well. There are three additional general configuration directives necessary to improve the security level of slapd:

```
disallow bind_anon
require bind
security simple_bind=128
```

With these three directives, access to the directory server will be granted only to authenticated users and only using the TLS channel. Configure ldapserver2 in the same manner.

It's possible to configure slapd to listen only on a secure port (636/TCP) changing the -h argument of slapd from ldap:// to ldaps://. The following example could be used to start ldapserver1:

```
# /usr/local/libexec/slapd -f /etc/openldap/ldapserver1/
slapd.conf -h „ldaps://ldapserver1.localdomain“
```

Restart both servers to apply the changes. Every client that needs to access the LDAP servers, needs only the public certificate of the CA, but it's possible to require client certificate. This configuration is not within the scope of this article and won't be covered.

Configure Replication

We have two standalone servers and now it's necessary to configure replication between them. To do this, we need a user for replication. It's possible to use the manager/administrator user, however it's recommended to create a specific replication user.

In our example, we will use `cn=replica`. Unfortunately, credentials for the replica user needs to stay in plain text in the `slapd.conf` file. Because of this, it's recommended to monitor all activities from the `cn=replica` user (cn is Common Name), including any activities from servers or systems outside of the LDAP cluster.

Create a new password for `cn=replica` user and insert the content of Listing 2 below into both server `slapd.conf` configuration files.

Restart both `slapd` daemons. With these configurations, LDAP servers will work in a read/write mode. All replication will be secured using encrypted communications.

Access control using ACL's

After basic configuration of LDAP servers, it's necessary to create access control lists (ACL's) to protect information from authenticated users. In the following example ACL's, we will create a container (Organizational Unit) of admin users named `ou=admins`. With `ou=admins`, it's possible to create and use different users and use them in place of the `cn=admin` user. `ou=admins` will also permit auditing of changes in the directory service.

One special attribute to protect is the `userPassword` attribute. `UserPassword` contains hashes of passwords, and if an intruder obtains this information, he can crack the hash and obtain the password. Because of this, this attribute should be accessible only by the user. Listing 3 shows the `userPassword` ACL.

All users can read the `userPassword` attribute, but it's necessary to protect writing to this attribute even from users. Write access is permitted via the users `cn=admin`, `cn=replica` and members of the `ou=admins`. The *All ACL* is showed in Listing 4 below.

Listing 3. `userPassword` ACL

```
access to dn.subtree="dc=example,dc=com" attrs=userPassword
  by dn.subtree="ou=admins,dc=example,dc=com" write
  by dn.exact="cn=admin,dc=example,dc=com" write
  by dn.exact="cn=replica,dc=example,dc=com" write
  by self write
  by anonymous auth
```

Listing 4. *All ACL*

```
access to dn.subtree="dc=example,dc=com"
  by dn.exact="cn=admin,dc=example,dc=com" write
  by dn.exact="cn=replica,dc=example,dc=com" write
  by dn.subtree="ou=admins,dc=example,dc=com" write
  by * read
```

Insert ACL directives inside database directive (above replica configurations).

Final steps and conclusions

After following the above instructions, you will have a directory service that is much more secure than a default configuration. Many others procedures weren't covered in this article, but could be implemented to improve security:

- Create user and group specific to `slapd` and start it using the `-u` and `-g` arguments instead of the root user and group
- Use `chroot`
- Configure audit level (`loglevel`)
- Protect the servers with firewall
- Use `selinux`
- Use `ppolicy` to control users from directory service

LDAP can be used by many applications to improve levels of security. When services and software rely on LDAP they are assured a greater level of security.

LEONARDO NEVES BERNARDO

Leonardo Neves Bernardo got started with Unix in 1996 when many considered this operating system more interesting than any other. For more than fifteen years he worked in several IT areas and now he is more focused within the IT security area. Leonardo is LPIC-3, LPIC-302 and LPIC-303 certified and holds a Bachelor's degree in Computer Science from Universidade Federal de Santa Catarina, Florianópolis, Santa Catarina Brazil as well as RHCT and ITILv3 Foundation certifications. Visit his LinkedIn profile at: <http://br.linkedin.com/in/leonardoneves>

Join Today Free!



Go Premium to support & enjoy the full potential!

New

Astalavista - The IT News and Security Community

- Forum Posts SHOW
- Downloads SHOW
- Events HIDE
- Official Blog SHOW
- News SHOW
- Jobs SHOW

Astalavista has taken another step into the future. **Stay Up-to-date**

With our relaunch we focus even more on the IT & Security world.

Our continuous news stream on the main page gives you all the information you need – 24/7. What do you think about that? Give us a shout on our Astalavista Blog, you find it by clicking on the first news item on our news stream.

Now
25% OFF!

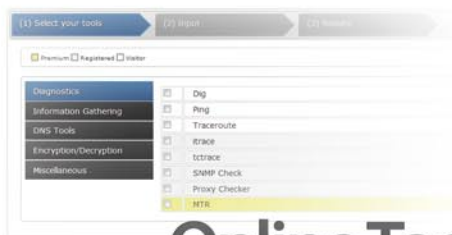
Join Today

Use coupon: **hakin9astadiscount**

www.astalavista.com

Go Premium!

IT News and Security Community



Online Tools

The new **Online Tools** overview page features nearly 50 tools covering typical IT needs, like Whois, Dig, Proxy List or Encryption.

The **Rainbow tables** section lets you hash your plain text in more than forty different types and crack your hashes. The **blacklist checker** runs your domain against the most important black lists and checks if your IP/Domains are flagged as spam.



Wargames

Wargames by its broad definition is a military drill under real life conditions. It is about testing strategies without the actual combat.

The **"World Gold Reserve"** is where most of the world's gold is stored. The combat in IT is virtual. Here the purpose of a wargame server is to allow you to practice hacker tricks without damaging anything or violating the law. The aim is to find gaps in security and to learn the necessary precautionary actions to prevent this.

Go Premium to support & enjoy the full potential!

Astalavista.com

No There is no fingerprint, but there is a secret code that gives you a sweet discount: hakin9astadiscount

Information On iOS Devices

Lately mobile devices have become a great source of information about us, it is our personal assistant and it knows every one of our secrets, if it falls into the hands of a bad person, we could suffer big damage.

What you will learn...

- Access to iOS filesystem
- Apps installation via SSH
- Explore and get information on iOS devices

What you should know...

- How to jailbreak an iOS device
- Basic knowledge about iOS

Access to iOS device and exploring for data can be quite simple, today there are many interesting applications for Macs and PCs that offer direct access to the information. Also, we have the ability to jailbreak, giving us a lot of completed work. We can access to the filesystem with SSH making this all the more simple.

In this article, I will talk about various ways to access the filesystem allowing us to *search, browse and obtain* information on iOS4. If you have previous versions of iOS, you maybe can't find some files or they can have a different structure. At the same time, previous versions could access information that iOS4 can not; for example, the passcode reset without resetting the device:

Access To The Filesystem

If you access via SSH to the iOS device, you will have full access to all directories and you can also install, modify



Figure 1. The ip device

and uninstall the applications that you want manually. For that all that *is necessary is to have a jailbroken device.*

Installing OpenSSH

Once we have a Jailbroken device, we install OpenSSH to enable SSH in our device:

- Open Cydia, go to Search and look for OpenSSH.
- Install the application and after that, reboot your device.
- You need your iOS device and your PC or Mac on the same Wifi network to get access via SSH
- You should get the device IP because you go to need it to setup the access from your machine, find the ip in

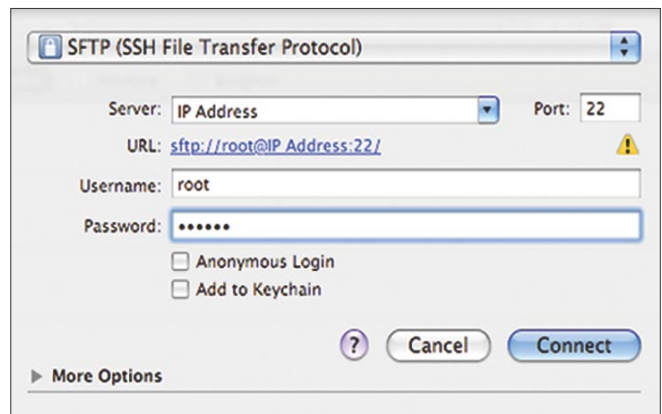


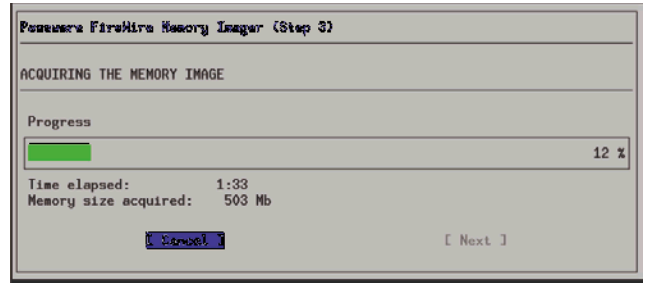
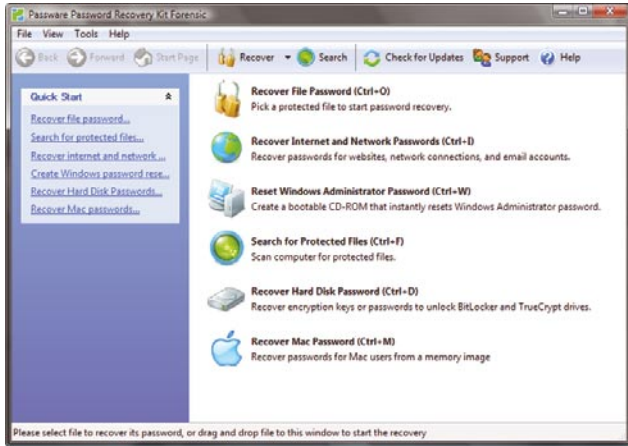
Figure 2. Screen after running CyberDuck and creating a new connection

Passware Password Recovery Kit Forensic 11.0

A Complete Password Recovery and E-Discovery Solution for Computer Forensics

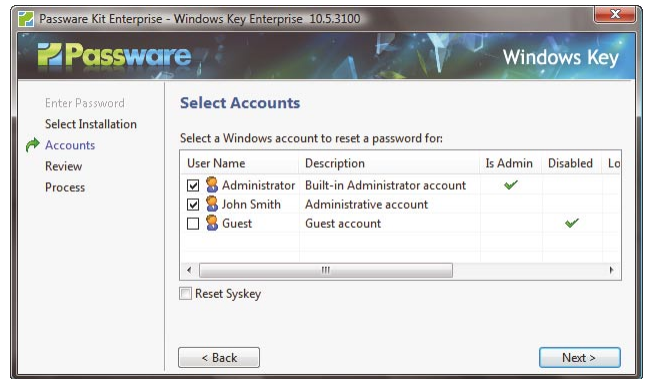
Now with Mac User Password Recovery!

Passware Kit Forensic includes over 30 password recovery tools, Encryption Analyzer Professional, Search Index Examiner, FireWire Memory Imager, and a Portable Version to provide immediate password recovery for any protected file detected on a PC or over the network while scanning. It recovers or resets passwords for more than 200 different types of files, as well as decrypts hard drives, PGP archives, and unlocks Windows 7 and Mac OS Lion Administrator accounts. Many types of passwords are recovered or reset instantly.



Key Features

- Scans computers and network for password-protected files
- Recovers passwords for **200+ file types** Updated
- Unlocks hard drives protected with **BitLocker** and **TrueCrypt**
- Retrieves electronic evidence in a matter of minutes from a Windows Desktop Search Database
- Includes a **Portable Version** that runs from a USB thumb drive and recovers passwords without installation on a target PC
- Acquires memory images over FireWire Updated
- Recovers Mac user login passwords from computer memory New!



Advanced Features

- Instant recovery for many password types
- Acceleration with distributed computing **(Distributed Password Recovery)**
- Multiple-core CPUs and nVidia GPUs acceleration
- **Tableau TACC** hardware acceleration
- 8 different password recovery attacks (and any combination of them) with an easy-to-use setup wizard
- Detailed reports with MD5 hash values



After losing my password to important encrypted documents, I thought it was the end of the world. Thanks for saving my work, Passware.

Conor LaHiff, LaHiff & Company.

5

editions for consumers, small business, professional, corporate, and forensic users.

Starting from **\$49!**

For additional information, please visit:
www.lostpassword.com/kit-forensic.htm

Passware Inc.
 800 West El Camino Real, Suite 180
 Mountain View CA 94040

Contacts
 Nataly Koukoushkina
media@lostpassword.com
 Phone: +1 (650) 472-3716 x 101



Preferences > Wi-fi, and here, touch the disclosure button that you can see in the wifi network that you are using, now you could see the ip device (Figure 1).

Finally, I will explain three ways to access different machines:

* MAC

To access from MacOS, we use *CyberDuck*, you can download this program from <http://cyberduck.ch>. Run CyberDuck and create a new connection, now you can see the next screen (Figure 2), fill the fields with this data:

- Protocol: SFTP (SSH File Transfer Protocol)
- Server: device IP
- Port: 22
- Username: root
- Password: dottie or alpine

When you have filled all the fields, please, click *Connect* button.

* Windows

To access from Windows, we use *WinSCP*, you can download this program from <http://winscp.net>.

Run WinSCP and you can see the next screen (Figure 3), fill the fields with this data:

- Host name: device IP
- Port: 22
- User: root
- Password: dottie or alpine
- Private key file: empty
- File Protocol: SCP
- Check: Allow SCP fallback

When you have filled all the fields, please, click *Connect* button.

* Linux

From the Terminal window run the command:

```
ssh root@(device ip)
```

Example: `ssh root@192.168.1.10`



Figure 3. Screen after running WinSCP

Confirm the connection and insert the root user password, this can be dottie or alpine.

After access with one of the three ways, you will see the folders library and media; then you can begin to explore.

Changing the Default root Password

The root password is always the same in iOS, if you have a jailbreak device, this can be a security problem for you, because everyone knows and everyone can have access to your device. The best thing you can do is change it.

To change your password, you must install Mobile Terminal, this is a terminal emulator. And you install this application via SSH:

- Download Mobile Terminal (You can find it easily using Google)
- Access to your iOS device via SSH
- Copy the downloaded file (mobileterminal*.deb) to the folder `/Media/Cydia/AutoInstall/`
- If you can't find this path, you must create them at Media folder
- Reboot your device

After the reboot you should have an installed Mobile Terminal, now you can proceed to changing the password:

- Open the application: Mobile Terminal.
- Run Mobile Terminal
- Write `su` to access like root
- Write the password: *alpine* (Figure 4)
- You are logged into the root, now write `passwd` to remove the password
- Terminal will request that you write the new password twice

After this, you have a new password and only with this do you avoid future problems.

Now you have an access to device's filesystem. It's time to explore for information.

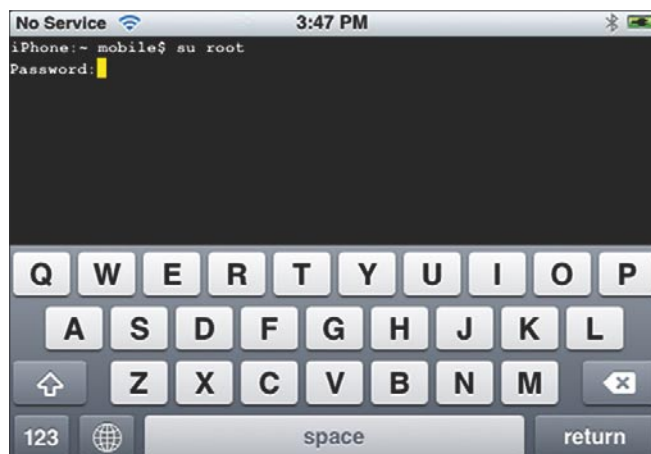


Figure 4. Writing the password

ROWID	address	date	text	flags
7	2	1414141801	Thank Thanks Thanks Thanks	3
8	3	1414144123	Awesome!	2
9	4	1414144159		4

Figure 5. The „message“ table contains information about SMS and MMS

iOS Information Source: What, Where And How

What kind of information you can find? There are different kinds of information on a mobile device, I will talk about three types:

- Pre-installed applications– Data: These applications are already installed on the device when you purchase it. A common user can not delete them from their device. These applications contain sms, mails, calendar events, email accounts, call history, contacts, photos, videos, browser information, GPS data, etc. ...
- Third-party apps– Data: This group would include all the information that is stored by any downloaded applications from the AppStore; IOS installed or other ways, for example, this would include data from Facebook, Skype, WhatsApp, Evernote, etc.....
- Device Preferences: This part would contain the general device information grouped (firmware, baseband, version, ...) as well as preferences for wifi, bluetooth, tethering, ...

Where you can find this information?

* LIBRARY FOLDER

Messages (SMS)

Source Type

SQLite Database

Where

/Library/SMS/sms.db

What

The database contains information about SMS and MMS from the device

How to

- If you want access to the information it is as simple as opening the database (sms.db) with the Terminal (sqlite3) or SQLite management application
- “message” table
- The “message” table contains information about SMS and MMS (Figure 5)
- In the fields from the table you will find information like the phone number (Address) that sends or receives the message (Text) with the date in Unix epoch (Date – \$date -r 2402932513) and an indication (Flags) with information about if the message was “sent” (3), “received” (2), “received mms” (4), “not sent” (33), “not sent” (35), “deleted message” (129) or “unknown – no address” (131)

- “msg_pieces” table
- “msg_pieces” table contains information about MMS
- In the fields you can find the text (Data) sent with the attachment file, with a name (Preview_id) and one type (Content_Type),
- The MMS attachment files are located in the path / Library/SMS/Parts/

Keyboard (keyboard cache)

Source Type

Plain Text

Where

/Library/Keyboard/dynamic-text.dat

What

This file is, more or less, like the key logger of the device, here you will find the used words by autocomplete, this is disabled with password, but you can use this file to rebuild deleted information by the user, and you can make a search with some key word to get something.

How to

- This file can be opened with most Text Editors, for example, Notepad in Windows or TextEdit in MacOS
- All the information is stored in words, oldest to newest and one after another

AddressBook (contact, information and images)

Source Type

SQLite database

Where

/Library/AddressBook/AddressBook.sqlite and Address BookImages.sqlite

What

Two databases, one with information about contacts and the other with the image for every contact

How to

- To access information is as simple as opening the database with a web browser or SQLite databases from the same terminal
- Open these files with Terminal (sqlite3) or some management SQLite application
- AddressBook.db
- The two more interesting are, ABMultiValue that contains phone and mail accounts of the contacts,

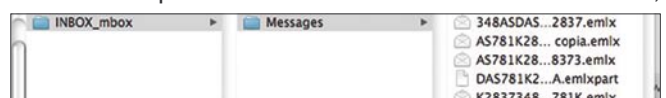


Figure 6. Each email file in .emlx format

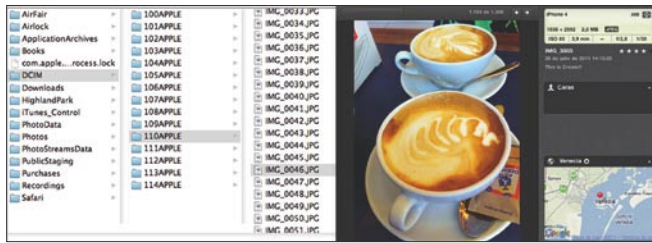


Figure 7. This shows a map with the ubication of the photo and more information in a popover

and ABPerson, that contains the first name, last name, company, etc...

- “Record ID”, from ABMultiValue, and “ROWID”, from ABPerson, are the same field, you can link the databases to get all the important information about one contact
- AddressBookImages.sqlite
- ABThumbnailImage table contains all data about the used images for the contacts

Mail (mail accounts and mails)

Source Type

Plain Text

Where

/Library/Mail/[MailType]-[MailAddress]/*

What

Inside the Mail folder you can find more folders, everyone of these represents one mail account, and inside them you will find each mail file in .emlx format (Figure 6).

How to

- The .Emlx can be viewed with any text editor and its content is quite readable
- You can find the attachment files of the mail in the same folder, these have the .emlxpart extension, and they are in base64

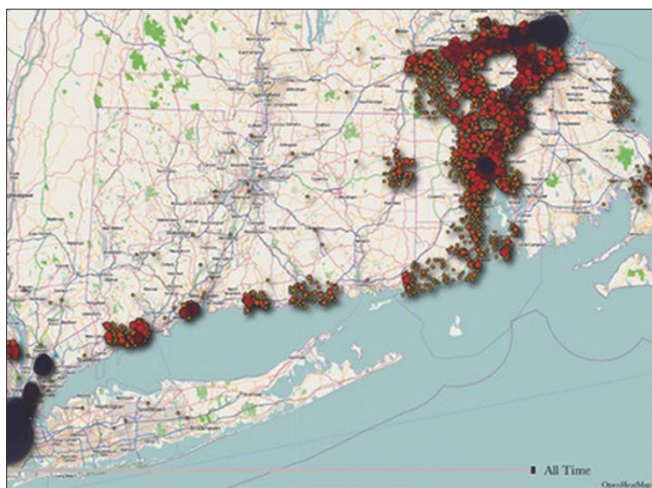


Figure 8. Demonstration of all info Location stored in your iOS device

* MEDIA FOLDER

Photos and Videos

Source Type

Image Format // Video Format

Where

/Media/DCIM/*

What

Photos and Videos with formats like png, jpeg, m4v, mov,...

How to

- To open the photos you can use any image viewer and Quicktime video. You should not have problems.
- You can open all the photos with an Image viewer or iPhoto in MacOS and videos can be opened with Quicktime
- Each one has information like the date, coordinates, etc... all this information can be seen with applications like iPhoto. This show a map with the ubication of the photo and more information in a popover (Figure 7)

* LOCATION DATA

Cell Tower Data

Source Type

Database and Plist Files

Where

/Library/Caches/locationid/

What

Inside you will find information about preferences and system configuration

How to

- Cell.plist: gives the latitude and longitude for the cell towers that the device was connected to
- h-cells.plist: contains more information about the cells, latitude, longitude, course (compass heading), etc...
- h-wifi.plist: gives a list for the Wifi access point that the device was connected to
- consolidated.db: contains GPS data, Wifi connection information, cell tower logs and locations, etc...

You can download the iPhone Tracker application to see a demostration of all info Location stored in your iOS device (Figure 8) [petewarden.github.com/iPhoneTracker](https://github.com/petewarden/iPhoneTracker).

* PREFERENCES

System Configuration

Source Type

Plist Files

WHAT IS A GOOD FUZZING TOOL?

Fuzz testing is the most efficient method for discovering both known and unknown vulnerabilities in software. It is based on sending anomalous (invalid or unexpected) data to the test target - the same method that is used by hackers and security researchers when they look for weaknesses to exploit. There are no false positives, if the anomalous data causes abnormal reaction such as a crash in the target software, then you have found a critical security flaw.

In this article, we will highlight the most important requirements in a fuzzing tool and also look at the most common mistakes people make with fuzzing.

PROPERTIES OF A GOOD FUZZING TOOL

There are abundance of fuzzing tools available. How to distinguish a good fuzzer, what are the qualities that a fuzzing tool should have?

Model-based test suites: Random fuzzing will certainly give you some results, but to really target the areas that are most at risk, the test cases need to be based on actual protocol models. This results in huge improvement in test coverage and reduction in test execution time.

Easy to use: Most fuzzers are built for security experts, but in QA you cannot expect that all testers understand what buffer overflows are. Fuzzing tool must come with all the security know-how built-in, so that testers only need the domain expertise from the target system to execute tests.

Automated: Creating fuzz test cases manually is a time-consuming and difficult task. A good fuzzer will create test cases automatically. Automation is also critical when integrating fuzzing into regression testing and bug reporting frameworks.

Test coverage: Better test coverage means more discovered vulnerabilities. Fuzzer coverage must be measurable in two aspects: specification coverage and anomaly coverage.

Scalable: Time is almost always an issue when it comes to testing. User must also have control on the fuzzing parameters such as test coverage. In QA you rarely have much time for testing, and therefore need to run tests fast. Sometimes you can use more time in testing, and can select other test completion criteria.

Documented test cases: When a bug is found, it needs to be documented for your internal developers or for vulnerability management towards third party developers. When there are billions of test cases, automated documentation is the only possible solution.

Remediation: All found issues must be reproduced in order to fix them. Network recording (PCAP) and automated reproduction packages help you in delivering the exact test setup to the developers so that they can start developing a fix to the found issues.

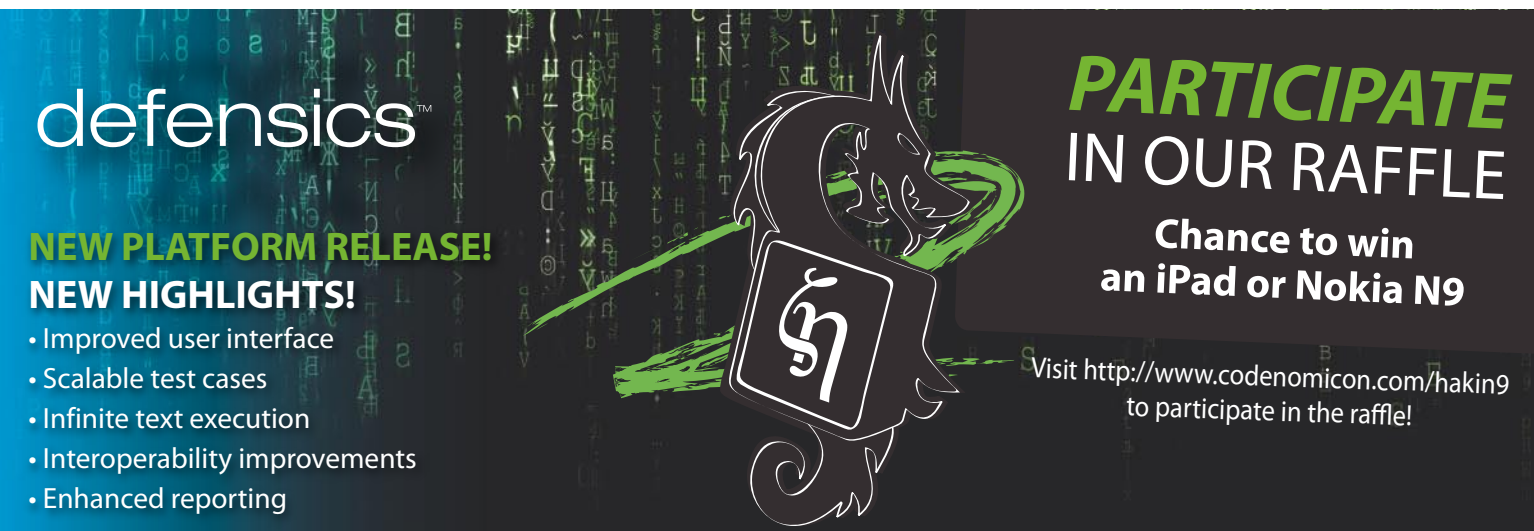
MOST COMMON MISTAKES IN FUZZING

Not maintaining proprietary test scripts: Proprietary tests scripts are not rewritten even though the communication interfaces change or the fuzzing platform becomes outdated and unsupported.

Ticking off the fuzzing check-box: If the requirement for testers is to do fuzzing, they almost always choose the quick and dirty solution. This is almost always random fuzzing. Test requirements should focus on coverage metrics to ensure that testing aims to find most flaws in software.

Using hardware test beds: Appliance based fuzzing tools become outdated really fast, and the speed requirements for the hardware increases each year. Software-based fuzzers are scalable in performance, and can easily travel with you where testing is needed, and are not locked to a physical test lab.

Unprepared for cloud: A fixed location for fuzz-testing makes it hard for people to collaborate and scale the tests. Be prepared for virtual setups, where you can easily copy the setup to your colleagues, or upload it to cloud setups.



defensics™

NEW PLATFORM RELEASE!

NEW HIGHLIGHTS!

- Improved user interface
- Scalable test cases
- Infinite text execution
- Interoperability improvements
- Enhanced reporting

PARTICIPATE IN OUR RAFFLE

Chance to win an iPad or Nokia N9

Visit <http://www.codenomicon.com/hakin9> to participate in the raffle!

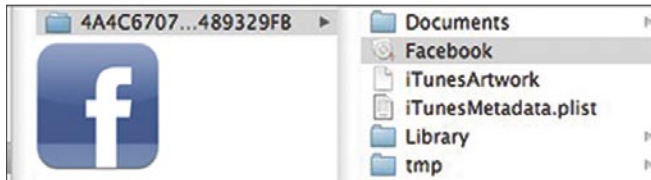


Figure 9. Send messages, update your state and upload photos or videos

Where

/Preferences/*.plist

What

Inside there is information about preferences and the system configuration.

How to

- All of them are .plist files, and these files can be open with some Text Editor
- Network.identification.plist, when the device is connect with one ip, that ip is stored here
- Wifi.plist, contains information about SSID

* SECURELY INFORMATION

Keychain Service

Source Type

Database

Where

/Keychains/keychain-2.db

What

- Apple provides a safer way for developers to not store sensitive information on plist or plain text files
- Keychain Service is an API that is used to store any application important information more securely.
- Inside database you will see five tables: cert, genp, inet, keys, sqlite_sequence and tversion.
- The “genp” table contains sensitive information and “inet” is where you can find all about mail account information
- On iOS3, if you remove the keychain-2.db and the file com.apple.springboard.plist on the device, you could bypass the passcode in the lock screen, in iOS4 this does not work.
- Let’s go to see how gain access to passwords using the “keychain_dumper” utility

How To

- First, download “keychain_dumper” (by Patrick Toomey) from <https://github.com/ptoommey3/Keychain-Dumper>.

- Take a look at the README.md file to install the utility
- Install LDID (Link Identity Editor) from Cydia on your device
- Upload “keychain_dumper” to “/private/var/” via SSH
- Dump all entitlements from your target’s keychain using:

```
./keychain_dumper -e > /var/tmp/entitlements.xml
```

- Sign the obtained entitlements into keychain_dumper using:

```
ldid -S/var/tmp/entitlements.xml keychain_dumper
```

- To complete, dump the contents

```
./keychain_dumper
```

Here is an example for the dump contents:

```
Service: DropBox
Account: littlebigcode@gmail.com
Entitlement Group: CF2F7822A.*
Label: Generic
Field: data
Keychain Data: mypassword1234
```

* THIRD-PARTY APPLICATIONS

Third-party applications are apps download from the AppStore, all these applications are stored in the same path `/private/var/mobile/Applications`.

Inside the Applications folder, you will see many folders with an alphanumeric name (Application Identifier); everyone is an application.

And to finish let’s go to check an example with the Facebook app

Facebook

It’s one of most famous apps. You can send messages to friends, update your state and upload photos or videos (Figure 9).

Where and What

- /Library/Preferences/com.facebook.Facebook.plist
 - User’s Facebook login (full name, email address, number id,..)
- Documents/friends.db
 - List of all the user’s Facebook friends and a link to their image profile
 - Tables: “name”, “address”, “phone number”, “e-mail address”, ...

JUAN MANUEL ALTAMIRANO ARGUDO

During the last 4 years, i have been working on projects related with iPhone and iPad (iOS). I have long experience with Objective-C/Cocoa applications and Apple technologies. I’m currently heavily involved in development and mobile usability and new technologies





Fix Windows Registry & Repair PC Errors!

- ✓ Improve PC stability and performance
- ✓ Prevent crashes and freezes
- ✓ Boost PC speed



DUBAI CLICK announced the release of PC FIX 2011 Registry Cleaner version 3.0.6, the next generation software for Windows registry maintenance. PC FIX 2011 Registry Cleaner 3.0.6, extends the capabilities of its predecessor, adds more functionality and enhances user experience with numerous improvements.

Below are 5 new features that the latest version includes:

Free Registry Scan: PC FIX Registry Cleaner 3.0.6 features the fully functional free Registry Scan that lets you see the health of your registry just by clicking a link in your desktop application.

"Set and Forget": Schedule registry scan, fix, backup and compact, and eliminate the routine in registry maintenance. Select the most convenient time and PC FIX 2011 Registry Cleaner will do the rest;

Email Notification: Get automatic notifications with complete reports about errors, fixes and the health of your registry;

Scanning Engine Enhancements: Further improved performance and advanced problem resolution.

SmartScan(tm): PC FIX 2011 Registry Cleaner features the new SmartScan(tm) technology for registry cleaning. It fixes system problems and improves the performance of Windows desktops. The product is intended for home and small business users, and is simple and safe to use by an ordinary desktop user.

"It's been only a little more than a year since the first version of PC FIX Cleaner was released," - said Hamad Al Samhisi, Managing Director at Dubai Click. "During this time, the software has become very popular among users from all over the world, earning sound industry reputation, confirmed by numerous awards and reviews. We are very excited about the market adoption of our product and looking forward to becoming the leading product in the registry management category with the introduction of PC FIX 2011 Registry Cleaner 3.0.6".

More information about PC FIX 2011 Registry Cleaner 3.0.6 is available at:
<http://www.pc-fix-cleaner.com> <<http://www.pc-fix-cleaner.com>>

Wireshark: The Secrets of the Shark

This column was inspired by the international screening of the Tintin movie by Steven Spielberg and Peter Jackson. Just like Tintin, Wireshark is an international icon too. It is primarily harnessed for network troubleshooting and packet analysis but did you know that there are other applications of this powerful tool?

Besides displaying information related to network traffic, there is a digital forensic useance to this tool.

Wireshark 1.2.7 was installed on a *Ubuntu 10.04 LTS* system. For example, I suspect a malicious file had been downloaded and I investigate this by combing through the packet capture.

I discover an archive *u.zip* that warrants further investigation. There must be an easier way to filter out such suspicious activities versus manually reviewing every single line. How about using the built-in filters within *Wireshark*?

The default filters do not support searching for *HTTP GET* traffic. An alternative would be engaging a PCAP-aware tool such as *ngrep* but that tool also requires the user to utilise certain search syntaxes.

I prefer a string search that does not require me to remember search syntaxes. *Tshark* is a non-GUI version of *Wireshark* that supports conversion of packet captures to text files.

```
commandrine@bridge:~$ tshark -r network.pcap -T text >
network.txt
```

By default, *Tshark* only extracts one line summaries of the packets from your packet capture. Specifying the switch *-Vx* will include packet details and *Hex/ASCII* information from original source. A word of caution, the text output from using the *-Vx* switch will result in a text file that is exponentially larger than the original *PCAP*.

After converting the packet capture to a text file, I can run string searches against the text file with a tool or method of my choice. My preferred tool is *Splunk* which quickly allows me to locate the same suspicious download using the search keywords *HTTP GET*. It also permits me to drill down and see details about that particular traffic.

Tshark can be exercised to directly capture network traffic information into text files.

```
commandrine@bridge:~$ sudo tshark -i <interface> -Vx -T
text > textcapture.txt
```

The limitation of this tool is that it does not support the *Follow TCP Stream* feature available in the *GUI* version. You still need to access the *GUI* to access the raw reassembled archive file's *Hexadecimal* values. This would be a nice feature to enhance *Tshark*.

MERVYN HENG

Mervyn Heng is into Ubuntu, Comic Universe characters, Pop culture and Art outside of Information Security. If you have any comments or queries, please contact him at commandrine@gmail.com.

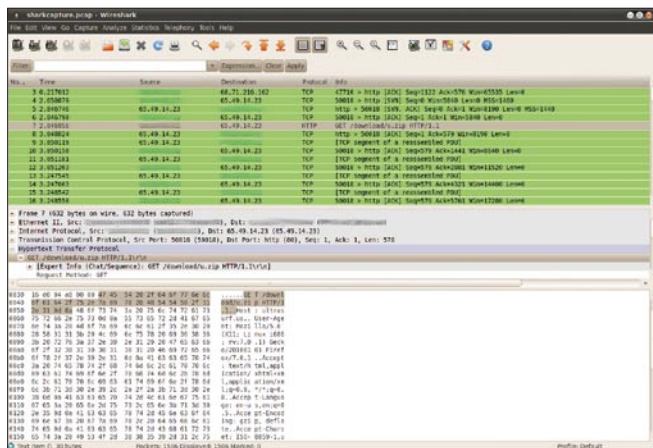


Figure 1. Wireshark GUI

2ND ANNUAL
CIO Saudi Arabia
 Forum

NOVEMBER 21ST 2011, RIYADH,
 KINGDOM OF SAUDI ARABIA

WWW.CIOSAUDI.COM



EMPOWERING CIOs TO THRIVE AND NO JUST SURVIVE

PLATINUM SPONSORS



GOLD SPONSOR



SILVER SPONSORS



BRONZE SPONSORS



MEDIA SPONSORS



ASSOCIATION PARTNERS



CO-ORGANISERS



For more information, contact:
 Ali Khalid Rana, Marketing Manager | Tel: +971 4455 7962 | alir@naseba.com

A TELECOM & IT SERIES SUMMIT BY **naseba** SUCCESS IS A CHOICE

Cyber Insurance

– A Risky Business

Cyber insurance is an area that an increasing number of insurance companies around the world are looking at. In part, this is a function of their ongoing search for new products to offer, in the same mode as the ever-increasing proliferation of car insurance options.

What you will learn...

- Cyber insurance, and the problems involved
- The costs associated with certification

What you should know...

- The purpose of international standard ISO27001
- The existence Of the business continuity standard BS25999

But what, exactly, is cyber insurance? This is big business; one recent UK government report estimated the annual cost of cyber crime to the UK economy alone as something in the order of £27billion (USD 43billion).

The theory is simple enough – insuring a business against losses from, for example, hacking, viruses, and identity theft. Many of these policies are aimed at small-to-medium enterprises. And this, in the detail, is where a number of problems lie. If you insure your car, you are expected to take sensible measures to protect it. For example, you, as a responsible individual, would drive sensibly, and within the relevant laws and regulations relating to road traffic. You wouldn't leave it unlocked when you park it. You may get a reduction in your insurance premium if your car is fitted with an alarm, or if you normally leave it in a locked garage overnight. If you were lucky enough to drive, say, a Lamborghini, a Bentley, or some other top-end vehicle, you may even fit it with a tracking device, to facilitate recovery if it's stolen.

But this simply illustrates one of the issues with cyber insurance for many organisations. By definition, their security is often poorer, since they just don't have the resources to devote to it. One of the first businesses known to have been *hacked out of existence* some years ago was a small ISP; I'll not name them to save embarrassment. Although very successful, with a rapidly growing customer base, and the recipient of

multiple awards, a business decision was made not to acquire anti-DDoS technology. Lo and behold, they were the victim of repeated DDoS attacks, completely negating their business model – if an ISP's availability is poor or non-existent, would you use it?

This example underlines a fundamental, and very difficult, question – how much do “cyber” losses cost? This is a question that the biggest, most sophisticated global organisations struggle with, let alone small ones. Of course, there are some guides to cost – the Ponemon Institute would be happy to supply you with those. But, as essentially a technical viewpoint, these types of figures are often difficult for business people to trust. I myself have sat in a meeting to discuss the cost of a potential loss event in a global organisation, where a multi-million dollar figure was mentioned. This was dismissed, out of hand, by senior management; however, recent examples, for example at Sony have indicated that the figure would, if anything, have been an underestimate.

Quality Security Staff are Expensive

Smaller organisations frequently do not have dedicated security personnel; where this role is filled, it is often by the IT manager. But as we know, the motivations of an IT manager and a security manager can be quite different. The first wants to keep system available and easy to use; the second wants to make them secure. In other words, difficult to use for everyone not explicitly

entitled. Of course, external specialist resource is available – but it is expensive. In the UK, a reasonably competent security contractor could cost upwards of £450 (USD720 or 525 Euros) per day. And what can one contractor achieve? Consultants, of course, will be more focussed, and usually with more resources and tools at their disposal, but consequently even more expensive. Vendors will offer all sorts of products to help you secure your enterprise – of course at a cost – but what's the use of, for example, a SIEM solution if you don't have the staff to monitor it. Or worse, if all it does is highlight the fact that there is yet more work that hasn't been done – poor firewall configuration, untamed users, poor privilege management, information leakage

The Problem of Moral Hazard

All of this points towards one of the key problems with insurance – moral hazard. This can be defined, in this instance, as a situation where an organisation with insurance acts differently from one that isn't insured. In other words, if insurance shelters the organisation from some of the risk, then they take less care over controls than they otherwise would. Such a course of action might seem even more attractive in the current difficult economic climate.

One solution to this problem that is being pushed by some insurers is that organisations can get a reduction in the cost of insurance if they have relevant certifications. Examples might be ISO27002, for information security, BS25999, for business continuity, and PCI-DSS for organisations which handle credit card data. However, there are a number of issues with this. Firstly, the process of getting certified is likely to be a lot more expensive than the cost of the insurance. Many small organisations will not have, for example, a robust information security policy. Writing a decent one, for a small organisation, will take a reasonably long time, perhaps a month or more. You need to gather information, get stakeholder buy-in, review it repeatedly, make sure it aligns with company culture, align existing procedures with it – probably at the very least a full man/month of effort. And would you want that policy written by a non-specialist IT manager, or an experienced specialist. The one you don't have, as a small organisation. But, without the policy and procedural framework, and the risk assessment that underpins it, an organisation has no hope of certification against any of the standards mentioned.

A second problem with certification is, to put it succinctly, what is being certified. In most cases, it is the management system, not the controls. In other words, you can have a great policy, great procedures, a brilliant set of (theoretical) technical controls – but that does not mean you will never suffer an incident. There are two ways of looking at this issue. Firstly, the organisations

that are generally willing to spend the most on securing themselves are often those with the most to protect. Put differently, they are the most attractive targets for attacks. Secondly, the certification is only ever a *snapshot* of the situation in an organisation – the controls may have been fine during an auditor's visit, but all turned off after he left.

So what is the answer? I think that there are a number. First of all, insurance companies, if they want to offer cyber insurance responsibly, need to deploy proper resource. Experts are deployed to risk assess potential clients in other areas, and to estimate real losses (loss adjusters, in insurance terminology). Perhaps we should see insurers acquiring similar resources for *cyber* risk. Secondly, there needs to be a clearer methodology for estimating the real costs of cyber incidents. At present, we can't reasonably say it's more than educated guesswork – there are not enough economists and accountants with information security knowledge for it to be otherwise. Lastly, there needs to be a more cost-effective way for smaller organisations (which make up the bulk of most countries' economies) to secure themselves; quality contractors and consultants are just in too short supply. Perhaps there is an argument for security as a managed service for smaller organisations? Unless or until all these conditions are met, cyber insurance just seems to be a risky business.

DRAKE

Drake has worked on information security and strategy with government agencies, the military, financial institutions and other blue chip organisations in Europe, the Middle East, and Africa since Boris Yeltsin was President.

Interview With Kevin Beaver

Kevin Beaver is an information security consultant, author, expert witness and professional speaker with Atlanta-based Principle Logic, LLC. With over 22 years of experience in the industry, Kevin specializes in performing independent security assessments revolving around minimizing business risks. He has authored/co-authored 10 books on information security including one of the best-selling information security books *Hacking For Dummies* (Wiley). In addition, he's the creator of the Security On Wheels information security audio books and blog providing security learning for IT professionals on the go.



Hakin9: Based on your extensive consulting experience, how has the security landscape changed in the last 10 years?

Kevin Beaver: It's interesting. We've become more aware of what we're up against but yet we continue to have many of the same problems. I think the greatest problems we're up against today are 1) users acting on impulse and not making well thought out choices, 2) management not providing the financial and political backing needed to truly manage information risks and 3) the increase in information systems complexity which makes it difficult to uncover the security risks that matter.

H9: With the latest attacks by hacker groups such as Anonymous and Lulzsec, what kind of Incident Response Management should be planned and practiced to mitigate risks posed by such groups?

KB: Surprisingly, many businesses don't even have an incident response plan. Certain businesses that do have plans haven't tested them or worked enough on them to get to where they need to be. You can't possibly respond to security incidents in a mature and professional manner if you haven't thought through what you're going to do when things go awry. Another impediment to businesses protecting themselves from these threats is the lackadaisical attitude that many managers have. They see criminal hackers as a mere nuisance and not a real threat to their businesses. They're wrong.

H9: Getting into the Information Security industry is not easy, why is that the case?

KB: I actually think it can be easy. If you get to know the basics of operating systems, software development and network protocols you've already got a leg up. Where many people fail in their careers is choosing to not learn about the business side of IT and letting their egos get in the way of rational thought. Becoming a good communicator on paper and in front of people is critical. Also, you have to focus on *why* information security matters to the business and not just proclaim the sky is falling because you've discovered some random vulnerability and not put any context around what it means in your environment. Approaching security this way will help you get the ear of management and gain some credibility with other people who can help you in your career.

H9: Many companies find it constantly challenging to manage and keep up with various laws and compliance requirements. What is your advice on this conundrum?

KB: Our problem today is that we overthink compliance. We lend too much credence to the bureaucrats in government agencies and industry bodies who think they know what's best for everyone's business. Then we end up becoming *compliant* with this or that regulation without actually addressing information security at the right level. I recommend stepping back and addressing information *risks*. This means understanding what's creating business



Foundstone Professional Services

A Division of McAfee

PROTECT | DETECT | RESPOND | REMEDIATE
The Foundstone Incident Response Team

877.91.FOUND (877.913.6863)

www.foundstone.com/ir

risks in your environment and fixing the security basics that are so often overlooked to help stop the bleeding. If you do these things well over time, compliance will come naturally.

H9: Which information security certification(s) in industry today do you hold to highest esteem?

KB: I don't hold any certifications in high regard. It's the person and the attitude behind the certification and the value they bring to their employers and clients that matters the most.

H9: The current approach by most organizations is of passive security management. Why is proactive security management so challenging?

KB: Because like most things in life: driving without a seatbelt, eating too much, smoking cigarettes and so on, it's easier to get motivated to do something about it once something bad happens. It's human nature to ignore the obvious and it's the very reason we're going to have a lot of job security moving forward.

H9: You have experience assessing the security posture of several companies, what are some of the security issues that are still being neglected?

KB: I see a handful of predictable security weaknesses in practically every assessment I do: missing patches, open network shares, weak passwords, no full disk encryption on laptops, zero controls on smartphones and Web applications that go untested. If you get your arms around these areas and keep things in check over time you'll be way ahead of the security curve.

H9: Several organizations still don't take security seriously, how would you go about convincing the management about information security?

KB: The formula I've found that works best is: 1) get involved with the business by attending meetings and understanding what the basic challenges are to your business, 2) build your credibility and become a person of value to the company and 3) show that management's investment of money and resources wasn't for nothing by keeping them in tune with how information security is working. In other words, be a likeable and trustworthy person that cares about the business's success.

H9: What motivates you to write a book?

KB: I knew early on that in order to compete with the big name-brand information security and accounting firms that I had to do something to establish my credibility.

H9: What book are you working on currently?

KB: I just finished an e-book titled *Implementation Strategies for Fulfilling and Maintaining IT Compliance* for Realtimepublishers.com. It doesn't sound all that

sexy but I feel that it's one of my better books. I've also started gathering ideas for the 4th edition of *Hacking For Dummies* whenever that may come about.

H9: How do you receive feedback from your audience about your books?

KB: I get quite a few emails from my readers who want to share their stories. Others approach me with their feedback at security shows and seminars where I'm presenting. I also like reading the reviews on Amazon and the various blogs and editorials sites that have featured my books.

H9: What's your opinion about Shady Rat?

KB: I didn't know it at the time but I worked on an incident response/breach analysis project that involved one of the organizations discussed in the report. In summary: fascinating.

H9: Lot of companies are coming up with various Governance Risk and Compliance (GRC) solutions, what has your experience been in the GRC domain?

KB: I think the GRC products and related technical controls are great. Implemented correctly, they can help take the pain out of information security – especially in more complex environments.

H9: What do you need to know after you get the CISSP certification to become a practical information security analyst?

KB: Focus on becoming a good communicator. That's half the battle. Learn all you can about computers, software, and networks and then continue learning. Take classes if you have to. Things change on a daily basis so it pays to keep up. And, of course, never forget that information security is about exercising common sense, being reasonable and balancing true risks and usability.

H9: What can be done to shutdown botnets? They seem to have their own protocols and resilience.

KB: Obviously, the best antidote is prevention. But the reality is that any given network is just one click away from compromise. It's tough. Once the infection is there, it's like cancer – it can be a tough uphill battle. There are some vendors such as Damballa and FireEye that can help. Just do something before it gets worse.

H9: What do you say to the system administrators who don't see the need for additional information security measures?

KB: I actually don't see this with system administrators. I work with a lot of really sharp admins who get security but their hands are often tied. It's executives who have their heads in the sand.

Taking On Mobile & Wireless **Security**

TAKEDOWNCON

LAS VEGAS | 2011

Training: Dec 2 - 5

Conference: Dec 6 - 7

Las Vegas, M Resort



www.takedowncon.com

Is your
MISSION-CRITICAL
security strong enough
to stop a
SKILLED ATTACKER?

Don't guess
Don't believe
Don't hope

KNOW!



An ACROS Penetration Test is **conducted exactly like a real attack by a skilled, motivated adversary** – only without the damage. We will find the weakest links in your security and use all our knowledge, skills and capabilities to try to achieve exactly what your security measures and policies are there to prevent. If it sounds difficult, we're interested.

Experience **the ultimate test of your security.**
(After all, the only alternative is to wait for an actual attack.)