WASTE - komunikační program a sdílení souborů pro paranoiky

Vložil/a cm3l1k1 [1], 23 Červenec, 2006 - 00:23

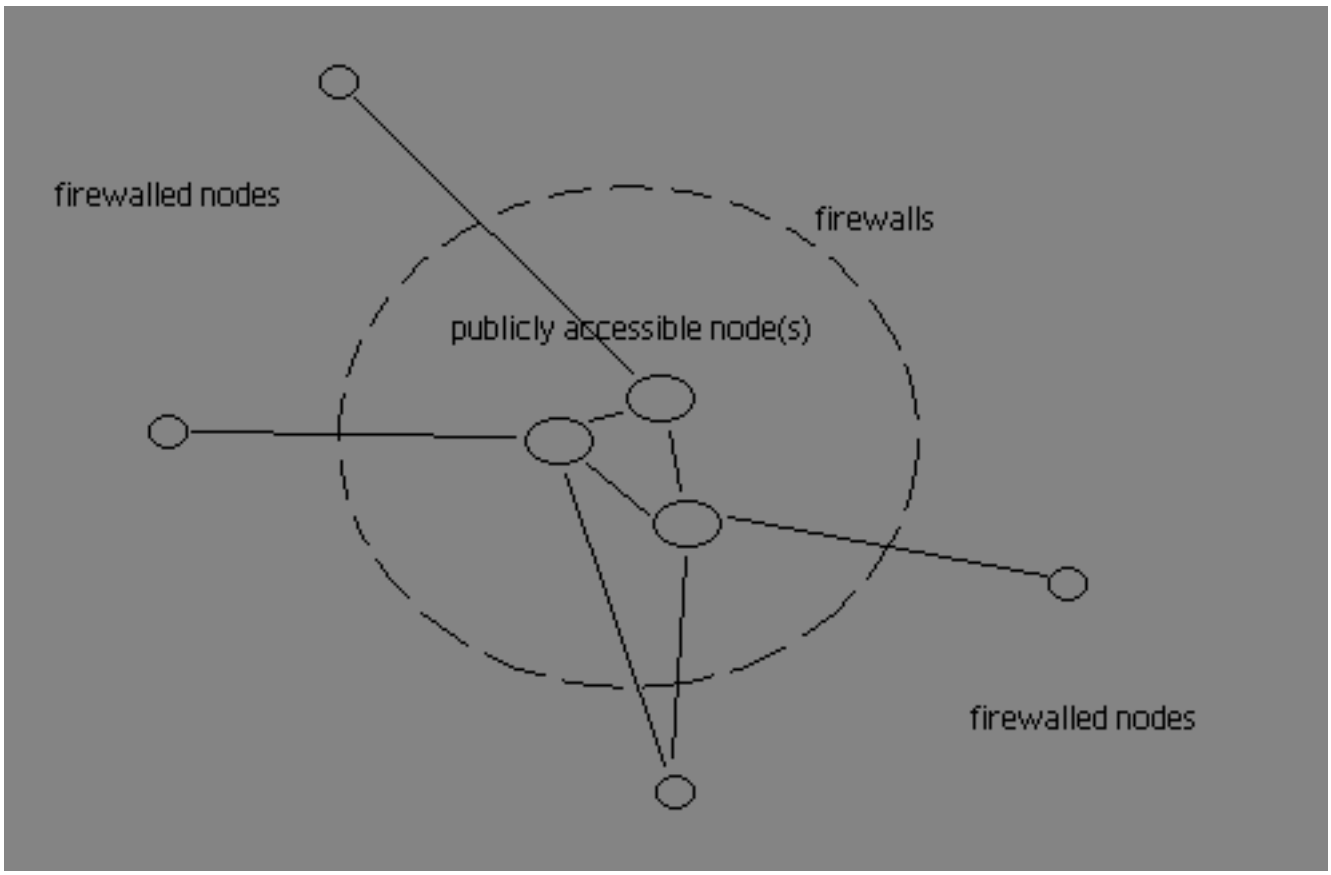
- Anonymita [2]
- Encryption [3]
- Recenze [4]
- Security [5]

V tomto článku bych vám rád představil program WASTE, který určitě stojí za pozornost a zatím jsem k němu na Internetu nenašel vhodnou alternativu.

O programu

WASTE je program se kterým dokážete šifrovaně komunikovat mezi účastníky, ve skupinách (jako IRC) a stahovat či uploadovat data. Všechny jeho funkce podrobněji rozeberu v průběhu článku.
První verzi programu napsal známý Justin Frankel z Nullsoftu, který je taktéž tvůrcem eDonkey apod. Musel však z webu stáhnout program i jeho zdrojové kódy. Avšak ten se už pak začal dále vyvýjet jinými programátory, kteří na něm dále pracovali.
WASTE je považován za nejbezpečnější P2P a nejbezpečnější protokol používaný v této síti. Šifruje data na linkové vrstvě a používá veřejné klíče k autentizaci, příčemž pro každé nové spojení (chat, stahování) je generován nový session key, který se díky RSA mezi dílčími stranami vygeneruje a obě strany se autentizují. Používá se šifrování Blowfish v PCBC módu (jeden z módů používaný u blokových šifer, varianta na CBC, používá se např. u protokolu Kerberos v4). Maximální délka klíče je 4096bit.

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn



Síť je "distribuovaná" a určená pro skupinku 10ti až 50ti důvěryhodných účastníků. Uzly dokážou vysílat broadcast a předávají si routovací tabulky, přičemž uživatelé za firewallem nebo s pomalým připojením k Internetu tuto volbu mohou vypnout a snížit tím traffic. Síť je vysoce anonymní, generuje se i náhodný šum v síti, abyste nepoznali kdo od vás stahuje, nebo od koho stahujete vy. Jediné podle čeho je možné vás identifikovat je váš nick (v opravené verzi může být i prázdný). Klienti i servery jsou napsány pro operační systém Windows, Mac OS X, FreeBSD a Linux. Smutnou zprávou ale je, že stabilně běží jen pod Windows a pár jedincům s drobnými chybami pod wine.

Šéfem projektu je sh4rd a projekt už celkem pěknou dobu stojí. Snad není všemu konec, protože napsal do fóra waste toto:

```
By: Eric - sh4rd
RE: Has the development halted? NO
2005-12-01 18:05
Any chance we can get you guys to develop for SourceForge?
I'd be more than happy to welcome you all and give some creative control.
I need devs!

Also, is the course included in that package?
I'd like to take a look at what's new and perhaps implement it here if no one minds
too much.
But since that's mostly just stealing it all and making nearly the same thing, my
first offer still  stands.
```

Co jsem četl dále, tak v březnu 2006 mu nabídli pomoc tři programátoři, takže budeme jen doufat. Byla by to velká škoda zabít tenhle projekt nemyslíte?
Dále tu máme skupinku lidí okolo sítě Nullnet. Co je to Nullnet? Je to WASTE síť, která je otevřena všem. Nevím jestli ještě pořád funguje, ale určitě byla aktivní ještě před rokem, kdy stačilo do fóra poslat svůj veřejný klíč. Mluvím o tom proto, že pár lidí z této sítě taky pěkně štvalo, že se vývoj tak táhne a proto udělali vlastní verzi programu s drobnými úpravami a opravami. Momentálně je verze 1.6 [build 421] (Win only)

```
Release Notes:
1.6.420
Changed about page in an act of freedom of expression. Never let it be
said I'm trying to take credit for SourceForge's accomplishments
Added encrypted PMs ("WASTE Stealth User Chat").
Usernames starting with . are no longer hidden from the rest of the
network.
You can now chat with a blank username, but you can't recieve replies,
except for encrypted PMs which work off key signatures instead.
1.6.421
Removed 'other names color' option added by SourceForge team. Their
code introduced that annoying "chat scroll" flickering chat window bug.
Added "Encrypted Chat user" option to menus to make encrypted PMs
more user friendly.
Added "Allow incoming encrypted user chats" to preferences.
Detail:
I copied the encryption thats used for the peer to peer connections
except it encrypts to the key of the user you want to talk to
and when they send replies, they are encrypting that to your key
its all in the m_chat.cpp and m_chat.hpp files
also some small changes in d_chat but the encryption code is in m_chat
C_MessageCryptChat and C_MessageCryptChatReply
thats the short version
its just a second layer of encryption
the network encryption protects the users inside the network from anyone outside the
network
and this chat encryption protects you further, even from the trusted users inside the
network
two people can have a completely secure conversation
bong@work
```

Ke stažení: http://www.wasteuser.com/soft/WASTE_NULLNET.rar [6]
-- executable, bez instalace, ENG (bez instalace je právě vhodný i pro wine)

Běh pod Wine

Wine není emulátor. Wine je překladová vrstva (a zavaděč programů) schopná umožnit běh aplikací z Windows na Linuxu nebo na jiném operačním systému kompatibilním s normou POSIX. Pokud si s ním chcete pohrát, tak si sežeňte aplikaci winesetuptk. Po spuštění si ošahá váš systém, naklikáte si co požadujete a ona poté vygeneruje konfigurační soubor pro váš wine. Pokud například máte někde namountovanou partišnu s windows, tak si můžete nechat zkopírovat rozhraní a různé ovladače do adresáře ~/.wine/drive_c/windows (např.) a odtud je wine bude používat v případě potřeby. Já jsem zatím zkoušel jen PSPad a WASTE, které beží v pořádku.

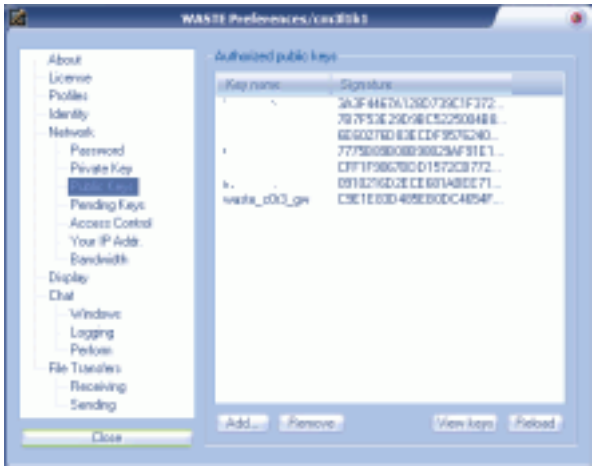
CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn



[7]

Používání

Se čtyřmi kamarády jsme se rozhodli WASTE otestovat. Nasadil jsem na jeden server přes VNC serverovou část WASTE a rozdali jsme si klíče. Aby jste tomu rozuměli, pro přístup do gatewaye je nutné mít její veřejný klíč u sebe a zároveň ona musí mít uložený váš klíč. Když se do sítě připojí další user jehož veřejný klíč nemáte, tak vám ho gateway automaticky distribuuje a vy si ho můžete uložit, protože pro pozdější přenosy s tímto klientem to bude nezbytné. Tento mechanizmus distribuce je sice pohodlný, ale odstraňování klíče ze sítě je už obtížnější, protože si ho musí odebrat všechny uzly.



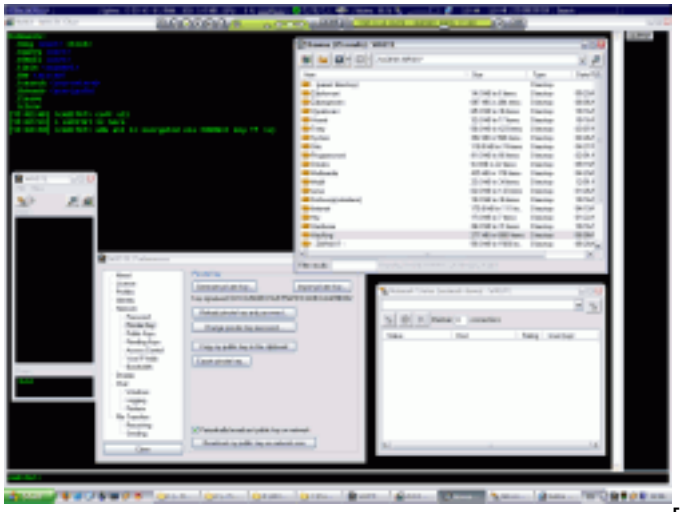
[8]

Při prvním spuštění budete generovat svoje klíče (2048bit je fajn), zvolíte typ připojení (když máte pomalý, tak se přes vás nebudou posílat routovací tabulky) a pak už jen zadáte passphrase a spustí se vám program. Na ovládání si člověk bude chvilku zvykat, ale není to nic nezvládnutelného (uživatelé gimpu budou ve svém živlu :)). Určitě vás zaujme, že skupinový chat je velmi podobný IRC. Nejsou zde sice módy (operator, voice apod.), ale můžete použít spoustu přikazů které již znáte (me, whois, msg, query, join, leave...). Dále funguje hajlajt u oken a při minimalizaci se okna schovají do traye.

Připojeným uživatelům můžete prohlížet složky, které nasdíleli a také jim cokoliv uploadovat (defaultně povoleno). Což se hodí v případě brany do sítě, kterou můžete takto používat jako např. dočasné překladiště dat. Rozhraní je velmi jednoduché na ovládání, ale chtěl bych upozornit, že pokud přidáte nějaké nové soubory do sdílené složky a ostatní je neuvidí, tak musíte refreshnout seznam v menu nastavení sdílení.

Závěr

Toto by bylo asi vše co bych mohl o programu říct. Určitě se stane užitečným tam, kde se kloubí požadavek na vysokou bezpečnost komunikace a možnost sdílet data, která jsou také šifrovaně přenášena. Užijte si ho! ;o]



[9]

kdysi dávno na oknech..

Odkazy

Nový projekt odvozený od WASTE - WASTE again http://wasteagain.sourceforge.net/ [10]
Stránky projektu WASTE - http://waste.sourceforge.net/ [11]
Official download - http://sourceforge.net/project/showfiles.php?group_id=82356 [12]
WASTE Nullnet - http://www.wasteuser.com/soft/WASTE_NULLNET.rar [6]

URL článku:
https://security-portal.cz/clanky/waste-komunika%C4%8Dn%C3%AD-program-sd%C3%ADlen%C3%AD-soubor%C5%AF-pro-paranoiky

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/anonymita
[3] https://security-portal.cz/category/tagy/encryption
[4] https://security-portal.cz/category/tagy/recenze
[5] https://security-portal.cz/category/tagy/security
[6] http://www.wasteuser.com/soft/WASTE_NULLNET.rar
[7] http://www.security-portal.cz/img/clanky/90/2.png
[8] http://www.security-portal.cz/img/clanky/90/1.png
[9] http://www.security-portal.cz/img/clanky/90/3.png
[10] http://wasteagain.sourceforge.net/
[11] http://waste.sourceforge.net/
[12] http://sourceforge.net/project/showfiles.php?group_id=82356

CC-BY-SA Security-Portal.cz | secured by paranoid sense | we hack to learn