CHEAP HACK
by Larry Seltzer

All Blogs • eWEEK • BASELINE • CIO INSIGHT • GOOGLE WATCH • LINUX WATCH • RESOURCE LIBRART

ADVERTISEMENT

INTERNET ARCHIVE
WayBackMachine BETA

http://ad.doubleclick.net/adi/entzd.eweek/blog/cheap_hack;sz=728x90;o

Latest

Show All

Page cannot be crawled or displayed due to robots.txt.

See ad.doubleclick.net robots.txt page. Learn more about robots.txt.

The Wayback Machine is an initiative of the Internet Archive, a 501(c)(3) non-profit, building a digital library of Internet sites and other cultural artifacts in digital form. Other projects include Open Library, nasaimages.org & archive-it.org.

Your use of the Wayback Machine is subject to the Internet Archive's Terms of Use.

ADVERTISEMENT

http://blogs.eweek.com/cheap_hack/content/border_security/blog_skypetunnel_a_horrifying   Go

42 captures

6 Jun 07 - 15
Jun 09

OKT   **JUN**   JUL
15
2008   **2009**   2010

http://ad.doubleclick.net/

Latest

Show   All

**Page   cannot
be   crawled   or
displayed
due   to
robots   .txt .**
See   ad .doubleclick   .net
robots   .txt   page   . Learn
more   about   robots   .txt .

The Wayback Machine is
an initiative of the
Internet   Archive , a 501 (c)
(3) non -profit , building a
digital library of Internet
sites and other cultural
artifacts in digital form .
Other   projects   include
Open   Library ,
nasaimages   .org &
archive -it .org .

Your use of the Wayback
Machine is subject to the
Internet Archive 's Terms
of Use .

Home | Got a Tip ? | Archive | All Blogs

SEARCH

Home >> Border Security >> Skypetunnel: A Horrifying Idea

Tuesday, May 29, 2007 10:07 PM / EST

Skypetunnel: A Horrifying Idea

Just what corporate network administrators needed to hear: Let's turn Skype into a VPN tunnel.

Peeter P. Mõtsküla in **his Skype Developer Blog proposed** using the Skype client API (ap2 ap) to tunnel other services over the network . Since all Skype traffic is encrypted , an admin would have no way to know what was going on.

Some admins already do what they can to root Skype out of the network , but if you aren't blocking it, this notion should be reason enough to do so, even if you think it's futile to try. Skype is not a controllable application. At least not the free personal Skype. The business Skype version is supposedly manageable to allow blocking of the client API.

TECH SECURITY NEWS

It May Be Time to Abandon Adobe

Apple Fixes AirPort Base Station, Time Capsule Security Flaws

Security Report Ignites Firefox vs. Internet Explorer Feud
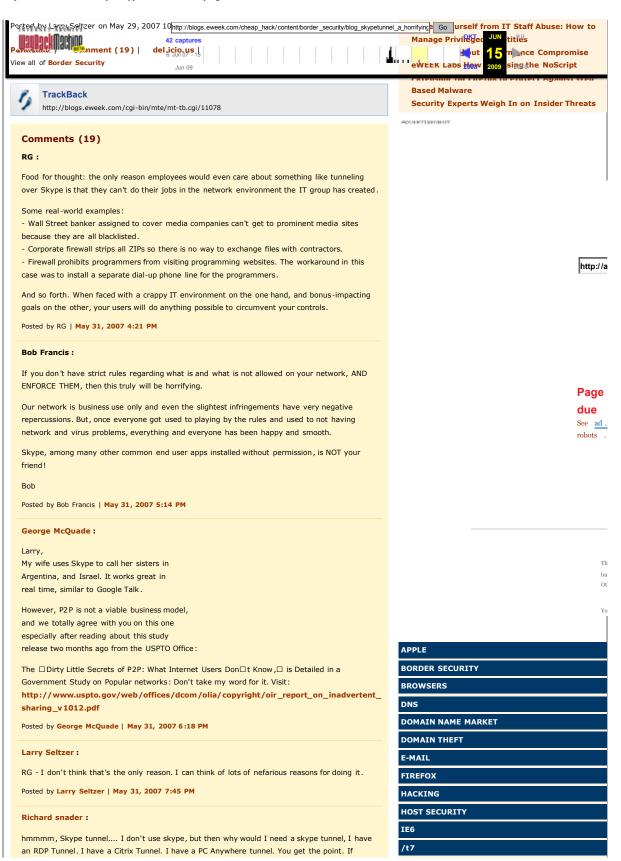
Microsoft Plans Three Security Bulletins for Patch Tuesday

How to Match Your Security Needs to Your IT Infrastructure Budget

Security Consultant Turned Hacker Gets Prison for Running Botnet

Posted by Larry Seltzer on May 29, 2007 10

Permalink / Environment (19) | del.icio.us |
View all of **Border Security**

TrackBack
http://blogs.eweek.com/cgi-bin/mte/mt-tb.cgi/11078

Comments (19)

RG :

Food for thought: the only reason employees would even care about something like tunneling over Skype is that they can't do their jobs in the network environment the IT group has created.

Some real-world examples:
- Wall Street banker assigned to cover media companies can't get to prominent media sites because they are all blacklisted.
- Corporate firewall strips all ZIPs so there is no way to exchange files with contractors.
- Firewall prohibits programmers from visiting programming websites. The workaround in this case was to install a separate dial-up phone line for the programmers.

And so forth. When faced with a crappy IT environment on the one hand, and bonus-impacting goals on the other, your users will do anything possible to circumvent your controls.

Posted by RG | **May 31, 2007 4:21 PM**

Bob Francis :

If you don't have strict rules regarding what is and what is not allowed on your network, AND ENFORCE THEM, then this truly will be horrifying.

Our network is business use only and even the slightest infringements have very negative repercussions. But, once everyone got used to playing by the rules and used to not having network and virus problems, everything and everyone has been happy and smooth.

Skype, among many other common end user apps installed without permission, is NOT your friend!

Bob

Posted by Bob Francis | **May 31, 2007 5:14 PM**

George McQuade :

Larry,
My wife uses Skype to call her sisters in
Argentina, and Israel. It works great in
real time, similar to Google Talk.

However, P2P is not a viable business model,
and we totally agree with you on this one
especially after reading about this study
release two months ago from the USPTO Office:

The Dirty Little Secrets of P2P: What Internet Users Don t Know, is Detailed in a
Government Study on Popular networks: Don't take my word for it. Visit:
**http://www.uspto.gov/web/offices/dcom/olia/copyright/oir_report_on_inadvertent_
sharing_v1012.pdf**

Posted by **George McQuade** | **May 31, 2007 6:18 PM**

Larry Seltzer :

RG - I don't think that's the only reason. I can think of lots of nefarious reasons for doing it.

Posted by **Larry Seltzer** | **May 31, 2007 7:45 PM**

Richard snader :

hmmmm, Skype tunnel.... I don't use skype, but then why would I need a skype tunnel, I have an RDP Tunnel. I have a Citrix Tunnel. I have a PC Anywhere tunnel. You get the point. If

| APPLE |
| BORDER SECURITY |
| BROWSERS |
| DNS |
| DOMAIN NAME MARKET |
| DOMAIN THEFT |
| E-MAIL |
| FIREFOX |
| HACKING |
| HOST SECURITY |
| IE6 |
| /t7 |

price :

You already can use Skype for application tunneling. Timbuktu, the remote control application can already use the Skype API and run remote control sessions through a tunnel.

While interesting, based on my use of Timbuktu, the performance of running any apps through the tunnel is shaky at best. It is very, very slow, even on fast links.

If you need an 'on-demand' private VPN, use Hamachi.

Posted by price | **May 31, 2007 8:30 PM**

Jim Noble :

Why is skype getting all of this fear mongering?

The Onion Router (TOR - **http://tor.eff.org**) is a fantastic way of circumventing IT controls in just about ANY network. I can run TOR with my altirus software virtualization tool (free), and i can do it from my 4GB USB Thumbdrive.

I have worked in environments where the IT security and network staff felt that they knew exactly what was going on, however, since all of my outbound network traffic was tunneled over TOR, (at least the information that I didn't want them to see), I could still perform any feat or action that I desired on the internet.

My main point here is not to run away from these applications. They have their place. I use TOR primarily to surf competitors web sites, when I don't want my company's IP Address showing up in the web logs, however, when draconian rules are applied as described by the previous posters, these people need to understand that "tightening the screws" will only make people find these tools, and deploy them.

For those of you who want a real experience with something truly scary, take a look at Anonym.OS, a bootable ISO image, that is a hardened BSD, not allowing any ingress traffic, that can stealthily enter most networks, and communicate to the internet anonymously... (btw, it was released to the general public on Thursday, 23 February 2006, at ShmooCon in Washington DC), you can find it here... **http://sourceforge.net/projects/anonym-os/**

Posted by Jim Noble | **May 31, 2007 9:33 PM**

Diogenes :

As in many such matters, it's easy to blame guns (or tunnels) for the disasters, when we should be educating and making more honest the people who handle them.

Tunnels don't kill systems; users kill systems.

Posted by Diogenes | **June 1, 2007 2:04 AM**

RG :

RG - Please. I.T. environments are locked down because users will happily surf porn sites, download games, forward virus laden jokes and click on anything that looks remotely interesting. if user requests access to a specific web site (business related of course) they are granted access.
stop complaining that IT is making your job impossible, they are protecting your sorry ass. another RG.

Posted by RG | **June 1, 2007 7:13 AM**

An 'IT' man :

For the 'Jim Noble's' out there..

How far do you want to take that game?? - Is it really worth your job?

Even booting into an alternate OS, there are ways of spotting you out of the herd.

Posted by Lit IT man | June 1, 2007 8:34 AM

DC :

RG2 - I couln't agree with you more! Users are simply selfish - they will click anything without forethought. Here's a big 'Atta Boy' for you!

Posted by DC | **June 1, 2007 9:35 AM**

Mark :

And to think most SMB executives complain that too much money is spent on IT! They have NO idea of what we are saving them from...even when we try to tell them in simple language.

The most common reaction is: Find sand, dig hole, insert head, cover up head.

Later, after the disaster, fire somebody and call an ultra expensive security contractor when if they had just listened in the first place...

Posted by Mark | **June 4, 2007 3:38 PM**

Larry Seltzer :

I'd like to apologize for a technical problem we had over the weekend with the blog. A couple of comments may have been lost.

Sorry.

Posted by **Larry Seltzer** | **June 4, 2007 3:54 PM**

Les :

The people in the IT department always know what is best for the company. Their decisions should never be questioned by the management or other employees they are "saving".

It seems the biggest problem most IT departments have is with the internet. If they could just find a way to shut it down except for about 10 minutes a day, they would not have to deal with all those people who keep coming up with ways to get around the safety net the IT has built around it.

I don't know why more companies don't just shut it down. Just think of the IT headaches that would stop.

Of course, it could be that the IT department at your company has an open mind and realizes that the internet is a tool to help people with their work, and that even though some people want to play and download porn, most do not. At many companies, the management let's it's employees know that certain things will be monitored and will get you fired.

Skype is just a tool. Perhaps the IT department should teach people how to use it for the benefit of the company, instead of worrying about it's abuse.

Posted by Les | **June 4, 2007 7:08 PM**

Gary Rathwell :

Skype is a useful productivity tool, but just like the telephone that it supplements, it can be abused. However, it is not the role of the IT Manager to control who a user calls on his telephone, his Skype, or file sharing utility. It is the responsibility of the business management of the company to ensure that employees' efforts are focussed, that they observe the company's policies, and that they contribute to the bottom line.

By the same token, IT provides a service that should be purchased, or not, at the discretion of business management. If the manager responsible for a business unit choses to use Skype or other tool that is not approved by corporate IT, that should be within his (or her) authority. He (or she) is responsible for the performance of the business unit, not the IT manager.

This places the responsibility on the IT manager to offer productivity tools, monitoring systems, consulting services and training that business management want to buy.

Page due

See ad .
robots .

Posted by Gary Rathwell | June 5, 2007 2:

Vincent Biggar :

I am far from a security expert. My understanding of TOR is that it
creates a tunnel where the data is encrypted once it hits the first
router and is passed to multiple routers and handed back off to the
destination unencrypted of course. Basically this ensures your privacy
from the far end web site. Your data and URL history (Destination IP
address and or DNS
name) still passes through your corprate network and DNS servers or
local internet service provider unencrypted. You aren't hiding
anything,
this is simply securing your privacy from the far end.

The bad thing is that all of your internet traffic will use the TOR
network and you don't know who the owners of the TOR routers are. In
the
work environment this is a serious problem because you could be
compromising your companys security and your own. I take pride in my
work and who I work for. If you don't you should find a better job.
Your
company is supporting you. The better job you do for your company the
better they can support you.

Posted by **Vincent Biggar** | **June 5, 2007 5:36 AM**

RJ :

An additiaonal to J.N.'s

The thing you violate by going around IT is trust. Sure people in your department may think it is
cool that you can do stuff like that, but in reality they will trust you less if you blatently violate
compnay guidelines. If you work in a place that this is the 'norm', then there are larger issues
where you work. That situation isn't the case most places. In no way have I ever seen the end-
run on IT perceived by managers as a trait that will lead promotions. More generally it is
perceived as 'If cant maintain trust for something simple, we are not going to trust them with
something complex.' Once you violate trust it is almost impossible to get it back to the level it
was at when it was lost. The thing that happened will always be in the back of the managers
mind...

Depending on where you work, the thing you are doing may violate a contract the company has.
Should your 'tricks' come to light they could loose the contract, lots of people would loose their
jobs, not just you and some in IT. It may take more work, but getting buy in to get restrictions
modified for legitimate business use is the way it (and IT) works in the real world. Usually people
doing the end-run on IT think that work is the right place to be IM'ing their friends from, visiting
dating sites on the internet, trying to steal company proprietary information, or any other of a
host of 'legitimate company use items'. Don't be so selfish that you think you know what is best,
or why a particular rule is implemented. Be part of the solution to change, not part of the
problem.

As for fear mongering around skype...I think the fear part should be how well is it encrypted. You
can tunnel over other protocols. SSH for instance allows you to tunnel multiple ports though a
single link. Those connections are secure between your host and the remote one. NO routers
between you and the destination see the traffic, period.

If this had been marketed as Skype VPN would it have been spoken of differently? Yes, I know
the only private part is to the skype server. Functionally there isn't much difference -- just a
distinction of where the encryption/service stops.

Posted by RJ | **June 7, 2007 7:05 PM**

David Marshall :

Most arguments used above are intended to instill or allay fear of the process used by Skype.
Any business that is sincere should ask its IT department to create dedicated homemade
standalone networks and hardware that do the job.

Because all commercial, and most private access they are unsuitable for secure work. A properly outfitted IT department will have no problem designing and installing basic sy of external support. Those systems will be able to network within the dedicated environment paradigms will ensure no one can listen in.

The current spending habits of most corporations include upgrading software and hardware, neither of which are under the control of the buyer. Then the upgrades are tested, sometimes for nearly a year before the upgrades are installed. The expense for doing these upgrades and tests are enormous, especially when you consider the end result is that someone else's product has been tested and not the corporation's own. That is a huge waste.

Get the work done first, then use the outside systems for research but keep the two separate behind very high walls. Employees were hired to work, not play with externals, and they do not need outside access if the corporation provides all the necessary materials and data. Data mining the outside world should be done by purchasing agents who buy the product, verify its accuracy, clean and disinfect it, and then mold it for internal use.

All the above can be done in a nearly real-time basis if the companies are sincere about security. I believe it is already being done. The fact you don't know about it means their systems are working. Check it out.

Posted by **David Marshall** | **June 15, 2007 12:57 PM**

---

jt :

DC's comment that "Users are simply selfish - they will click anything without forethought" reminds me of finance executives who say, "This would be a perfect business if we could just get rid of all the f!@#g people." And Customer Support would like to do without customers, and IT would like to do without users.

I see lots of whining from IT types who'd like to lock down the environment, and I think we all understand how much more safe & manageable that would be. But RG's comment stands: "The only reason employees would even care about something like tunneling over Skype is that they can't do their jobs in the network environment the IT group has created."

There's going to be tension between IT & users about this. Hopefully creative or positive tension, depending on how you deal with it, but until users stop having very good reasons to do things that IT doesn't support, IT had better remember that they're a service dept, there to support, enable, facilitate - not get in the way. Firms are in business to get things done to make money, not to build circumscribed networks that are safe because they're disconnected from the outside world.

Try this: Imagine someone just invented the telephone and your IT dept's reaction to it: "Sure users do business with it, they'll call Mom, or a phone sex line... they'll talk to competitors, headhunters, who knows what!" Wouldn't IT race HR to ban it completely? Wouldn't IT build Private Phone Networks so users could talk just with other internal offices? Everything would be safe. And IT would realize what they need next is to put a lock on the door to stop anyone ever leaving the building...

Posted by jt | **June 27, 2007 2:53 PM**

Post a Comment

Name: [   ]

Email Address: [   ]

URL: [   ]

[ ] Check to remember personal info

Comments:

HTML tags
for style)

http://blogs.eweek.com/cheap_hack/content/border_security/blog_skypetunnel_a_horrifying   Go

42 captures

6 Jun 07 - 15

Jun 09

OKT   JUN   JUL

15

2008   2009   2010

PREVIEW   POST

Cheap Hack   **Contact Us** | **Advertise** | **Site Map**

eWEEK QUICK LINKS

Enterprise Security
Network Security
Infrastructure Security
How To: Data
IT Security News
Cheap Hack Blog
Security Watch Blog

Data Storage
Cloud Storage
Storage Virtualization
Network Access Storage
Storage Reviews
Data Storage News
How To: Storage
Storage Station Blog

Apple OSX
Linux Systems
Windows Vista
Managed Print Services
Cloud Computing
PC Reviews
Microsoft Watch Blog
Apple Watch Blog
Google Watch Blog

VoIP Solutions
Wireless Technology
Messaging Software
Web Services
Mobile Applications
Wireless News
Mobile Reviews

Application Development
SAAS
Search Engines
Database Software
Web 2.0
IT Project Management
Emerging Tech Blog
CIO Insight Blogs
CIOs

enterprise

OKT   **JUN**   JUL

Federal Government 21 captures   **15**
Health Care IT   6 Jun 07 - 15   **2009**
Finance IT   Jun 09   **2008**   2010

Mid-Market
Channel Partners
Careers Blog
Value Added Resellers

Tech Knowledge Center
Tech Newsletters
Tech RSS Feeds
White Papers
Tech Podcasts
Tech Videos
eWeek Magazine Subscriptions

ZDE Home
Baseline
Channel Insider
CIO Insight
eSeminars
eWeek Mid-Market
Publish Online
Web Buyers Guide

Dev Shed
DeveloperShed
ASP Free
MS DevSource
SEO Chat
Codewalkers
Tutorialized
Scripts.com
Dev Mechanic
Dev Articles
Web Hosters
Dev Hardware

Device Forge
Desktop Linux
Linux Devices
Windows for Devices
iGrep Search Engine
PDF Zone
Linux Watch