

Re: [Full-disclosure] Remote Desktop Command Fixation Attacks

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-10/msg00427.html>

- *From:* "James (njan) Eaton-Lee" <james.mailing@xxxxxxxxxx>
 - *Date:* Mon, 15 Oct 2007 17:03:17 +0100
-

You can take defence in depth too far (or misinterpret it and implement something that's just overcomplex)... actually, I think this e-mail demonstrates how not to do defence in depth. Here's my take on this approach:

gjpgowey@xxxxxxxxxxxxxxxxxxxxx wrote:

If you want my take on how to secure a wireless network I'd approach it like this:

- 1) wpa2 (of course)
- 2) mac restrictions (yes, keeping a list of legitimate mac's will be required, but if you don't have an automated inventory system in this day and age then how are you ensuring nothing goes missing to begin with?).
- 3) ipsec VPN connections from all systems that connect via the wireless (this is in addition to the wpa2) using a unique cert per system (not the typical shared password setup that I am still amazed passes for secure in some peoples minds).
- 4) all traffic must go through a proxy server that sits right behind the VPN concentrator)

If you're running an MS based setup:

- 5) necessary GP modifications to enforce all this and more (if you study all the options available to be forced, xp, w2k, and w2k3 really can get quite secure at the protocol level).
- 6) force kerberos authentication everywhere possible with absolutely no client side caching of the credentials allowed. Reason: even if someone gets all the way through to the proxy server level ISA can still stop someone cold if their machine doesn't have a machine account on the domain (good luck spoofing that).

Basically you're looking at layers of authentication and encryption with no way around any of them (even if you do plug in a NIC on one of the systems that's on the wireless) and this really doesn't take a lot of hardware or software to pull off. Example setup: in front would be your WAP behind that would be a Cisco pix fw with a Cisco VPN concentrator behind it and a MS w2k3 box running ISA behind that. 4 devices basically providing a very solid wireless infrastructure.

=> Broadly...

This set of steps is redundant in many places, and it's also enormously expensive, since you're using no less than three different expensive bits of networking hardware (AP, PIX, VPN Concentrator), in addition to a bunch of x86 server hardware, windows server licenses, and at least one ISA license.

Re: [Full-disclosure] Remote Desktop Command Fixation Attacks

When you consider that anyone with a serious need for such a "secure" infrastructure also probably has very high requirements in terms of reliability and redundancy, you're going to have to double that cost to cover cisco/windows licenses and the cost of provisioning physically redundant kit and inter-site supporting connectivity.

=> Specifically...

VPNs-over-wireless is very 2001, and is worth avoiding, unless you have very good reasons for it, and WPA2-Radius and EAP-TLS should strongly be considered as an alternative. Here are some specific disadvantages of the approach you've outlined, and of VPNs employed thusly in general:

i) Your computers necessarily don't have full access to your network infrastructure when they aren't logged on, so GPOs, software updates, etc can't be applied at the times you want them to be applied (when the PCs aren't in use). Either:

- * You accept you won't have any, and push updates / update GPOs after users authenticate (obvious disadvantages for management/performance)

- * You decide you want wireless clients to update GPOs, carry out software updates, etc. when no-one's logged on, when the VPN drops etc. In this case, you have to provision a mezzanine network infrastructure just for this – which requires protection (and exposes an attack surface). Since your laptops are probably domain clients you're necessarily going to have a route back to the network behind the VPN required to make this approach work via infrastructure exposed to the wifi network pre-VPN, and even if you fast forward to 12 months time and use a Read-Only w2k8 DC or similar, the attack surface and complexity involved really questions why you're bothering with the VPN anyway.

ii) Users can't roam between Access Points (the VPN connection falls over)

iii) The logon process becomes complicated and unfriendly, and is different from working non-wirelessly, as you're going to need to configure machines with VPN Connectoids that enable the "logon using dialup connection" option in the login screen. You'll probably have to roll some custom code / script to poll the up-ness of the VPN frequently and force it to be re-established when it goes down. (see (ii))

iv) If any one of your pieces of infrastructure fall over (Wireless APs, VPN Servers, Proxy Servers, and probably CAs, LDAP Servers, or Webservers used to check the CRL, since you're using x.509 certs for authentication) you lose the entire infrastructure, and your users can't logon or do any work. That's a long string of dependencies.

v) Significant performance hit due to the use of VPNs tunneling traffic over wireless.

vi) Your users aren't going to be able to do *anything* that won't go over a proxy server, since you've said "all traffic must go through a proxy server". This means one of the following things:

- * Only Web/FTP Traffic is allowed

- * You're going to allow HTTP CONNECT tunneling on all ports, obviating the proxy server entirely and making life for your users hellish as you try and force a whole load of traffic to go over a web proxy

- * You're going to use SOCKS (similar to the previous)

- * You're going to use the ISA Firewall Client, which does in effect allow you to authenticate all traffic going via your ISA Servers, but renders the VPN pointless, and is very difficult to firewall.

- * Only selected traffic is *actually* going to traverse the proxy server when you realise it isn't a panacea (again, obviating the need for it). Since you've specifically highlighted authentication as the main reason for the "proxy server" here, and you've mentioned kerberos as a protocol that is traversing your wlan, you can't simply mean "application-layer firewall", and I must only assume you want to use the firewall client (or don't

Re: [Full-disclosure] Remote Desktop Command Fixation Attacks

understand what ISA does).

vii) Probably other stuff I didn't think about in the 10 minutes it took me to write this e-mail.

Many elements of the policy are pretty pointless given the number of other restrictions you have in place, such as:

MAC Filtering – when you consider what a tiny hurdle MAC spoofing is compared to your VPN infrastructure, proxy infrastructure, kerberos, etc and the overhead associated with this, it really seems quite pointless.

The Cisco PIX – Why? To filter the one or two ports hitting the VPN Concentrator? Even if you had this after the concentrator and not before, sitting a PIX (which is a firewall) in front of an ISA Server (which is a firewall) and behind a VPN Concentrator (which probably does basic firewalling itself) is pretty redundant, especially given the bandwidth your LAN clients likely use and the cost of Cisco Firewalls. If you're going down the Firewall Client route, firewalling the traffic between ISA and the VPN Concentrator is almost entirely pointless anyway.

Turning on, enabling, and implementing every possible security setting and device you think of is not defence in depth, and will probably only have two effects – your users won't use your wireless network, and you'll burn so much cash you won't have any left to spend on *useful* security measures.

=> Alternatively...

You can do some extremely nice things with WPA2–Radius, it can be authenticated in a very similar way to VPNs, using 802.1x and EAP–TLS with certificates, and you can even dump users into different VLANs over wifi depending upon who they authenticate as. It can be implemented for the price of a \$300 entry–level enterprise–grade AP such as those from HP and Cisco, using existing licensed Radius software on your Windows DCs, and an existing licensed Enterprise CA with autoenrolment.

If that's not good enough, and you simply must have encryption and authentication over the top of your encrypted, authenticated wifi lan, why not use IPSec? This provides a performance benefit over a VPN (no tunneling), is far more granularly configurable (across your whole AD estate via GPOs), and won't automatically break when users roam across Access Points. It also provides security for *all* users, not just VPN users, and generally hardens the soft underbelly of your internal network infrastructure rather than relying on an overcomplex outer shell which, once breached, exposes your (probably under–hardened) internal network.

This approach makes it substantially easier to provision new wireless access points too (since they no longer have connectivity requirements tied to your proxy/VPN infrastructure or carry the requirement to provision additional VPN Servers / PIXes / ISA Servers / etc). At worst you may have a few trunked vlans.

There is obviously a performance and management hit associated with this approach (IPSec), but I think it's a more balanced one based on the nature of the threat, and it provides a greater return than just wifi security.

If you're looking to step it up further you can go with MS SMS server and shavlik netchk to manage and audit the laptops.

If you were going to take this a step further, I'd suggest using one of the many NAP–like platforms currently out there, doing some sensible application–layer firewalling, or waiting until w2k8 came out and using NAP

Re: [Full-disclosure] Remote Desktop Command Fixation Attacks

itself. You've already got NAQC, since in your hypothetical scenario you've already bought some ISA Licenses – you may as well actually use them.

– James.

-----Original Message-----

From: "pdp (architect)" <pdp.gnucitizen@xxxxxxxxxxxxxxxx>

Date: Sun, 14 Oct 2007 21:59:19 To: "C Q" <kyle.c.quest@xxxxxxxx>

Cc: full-disclosure@xxxxxxxxxxxxxxxx, bugtraq@xxxxxxxxxxxxxxxx

Subject: Re: [Full-disclosure] Remote Desktop Command Fixation Attacks

CQ,

maybe I am making a huge mistake for responding to your message, but let see. this is what I think about security in depth in a bit more detail.

let say that we have a wireless network which is guarded by "security in depth" network administrators. the first thing they will do is to secure the actual network by some massive segmentation exercises... then the connection with enhanced privacy/encryption schemes (WPA2). They will put more layers on the top of that. For example, the users need to authenticate with client-side certificates. Now the network and the connection is secure (sort of), they enforce group policy for all laptops so that these laptops cannot connect to any other network (sending probe requests, rogue access points). Right! But now they also kill the ethernet since a laptop cannot be connected to the wireless and the wired network since it is also a risk (stepping stone attacks). Each client has a firewall on the top of that. The firewall blocks everything that comes in and lets only the browser to go out through a proxy which requires authentication (NTLM, Basic Auth, etc). The user of the laptop runs with the least possible privileges and they cannot install software. They cannot use the CD (Sonny Rootkits), they cannot use the USB (endpoint security). The laptop has a boot password as well so in case it is stolen the attackers cannot crack open the disk.

My question is the following: does this sound sane to you? Do you really believe that someone will let you do all that, without causing chaos? Laptops are good because they are mobile. You are allowed to take them out and work from home. At home you have your own network which you would like to connect to. Even if you use a different account on that same laptop to connect to that network, the risk is still there. A system is as secure as the weakest link.

Companies don't like to hear how you are going to solve all problems once and for all with some killer security in depth solution because it is not possible. in order to make things work you have to leave

Re: [Full-disclosure] Remote Desktop Command Fixation Attacks

various doors open. At GNUCITIZEN we have one maxima.. "Be legitimate!" If the attacker try to be a legitimate user as much as possible they will stay unnoticed and they will get in.

Now how do we handle security in 21st century the way I see it (btw, I am not interest in selling any services, in fact, GNUCITIZEN is not that type of organization)? First of all, careful planning – the system has to be as secure as flexible and usable even if this means that you need to have a shared key for all of your wireless networks. Second, you need a crisis management plan. Natwest got hacked by a MP3 player.. how many of you have heard of it and for how long this story was on the news? Third, you need to calculate the risk. Example? Credit card fraud! We know that cards are getting stolen but the calculated risk is %2 out of the whole, which can be easily compensated. Etc, etc, etc!

As you can see it is not just technical when it comes to the real world. In the real world the management gives you instructions and you have to implement them in the best possible way. Projects stack up. People leave, new people join in and work on the networks that have been given. Chaos is the norm! How many of you have seen a network that is done right? Yeh, there are a few of you, but you are probably talking about your home network which does not exceed more then 20 machines. How come I have never seen a security in depth in practice. You guys are more experienced then me, that's for sure... but I've done quite a few tests in the past 4 years and I know what I've seen. It is bad, but it is OK, because then we can sit together and walk through the entire process.

I expect more flames for which I am not planning to respond. If you think that security in depth works for you... do it! personally, I will offer something additional to my clients. something, that gives them that extra safe net, which has nothing to do with security in depth.

cheers,
pdp

On 10/14/07, C Q <kyle.c.quest@xxxxxxxx> wrote:

I guess there's some logic in spreading FUD about security in depth not working. It might be a nice way to scare potential customers who don't know much about security into whatever services GnuCitizen team sells. However, these kind of tricks simply won't work with any seasoned security professional. It'll actually backfire if you are not careful... because you won't be taken seriously in the industry. I'm pretty sure Pdp's rating in the books of many security professionals went down quite a few notches :-). It's a small world... and most likely it'll affect your and your company's future... because you'll need to do business with

Re: [Full-disclosure] Remote Desktop Command Fixation Attacks

people like Thor (who gave a great and very logical description with proper supporting examples of what security in depth is and what's mean to do).

The chances are that they'll simply choose to work with someone else... who betters understands the big picture in security :-)

CQ

Full-Disclosure – We believe in it.

Charter:

<http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

--

pdp (architect) | petko d. petkov

<http://www.gnucitizen.org>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

--

James (njan) Eaton-Lee | UIN: 10807960 | <http://www.jeremiad.org>

"All at sea again / And now my hurricanes
Have brought down this ocean rain / To bathe me again"

<https://www.bsrp.org.uk> | ca: <https://www.cacert.org/index.php?id=3>

--

Attachment: *smime.p7s*

Description: S/MIME Cryptographic Signature

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

Re: [Full-disclosure] Remote Desktop Command Fixation Attacks