

Re: Open source firewalls

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-07/3784.html>

From: RVK (rvk_at_prodmail.net)

Date: 07/14/05

Date: Thu, 14 Jul 2005 19:34:19 +0530
To: Helge Hafting <helge.hafting@aitel.hist.no>

Helge Hafting wrote:

> *RVK wrote:*
>
>> *Proxies can be a good way of filtering but it can't avoid buffer*
>> *overflows.*
>
>
> *Yes they can – did you read and understand my previous post at all?*
> *A proxy _can_ avoid a buffer overflow by noticing the*
> *anomalously large data item and simply refuse to pass*
> *it on to the real server! The proxy can terminate the tcp*
> *connection and throw away the data.*
>

Some of the validations can be done at proxy end. But there are more invisible scenarios than the simple visible ones. And its definitely much preferable to use Apache like stuff then using our own.....I hope u agree with me...

I don't disagree on proxy doing the filtering and validations what I mean to say is it can't guarantee avoiding buffer overflows. As it itself can be a source for it.

>> *It can only increase it. More code more bugs.*
>
>
> *Of course the proxy can be buggy too, but it is easier to*
> *avoid problems there:*
> *1. The server was written to perform a service, perhaps with*
> *security thrown in later. (Yes, that's bad design.)*
> *A firewall proxy is written for security, so buffer overflows*
> *are usually avoided in the firewall proxy itself. Because this*
> *is exactly what the firewall writer is thinking about.*
> *2. The proxy may be much smaller and simpler than the server*
> *it protects, it is therefore much easier to audit for security*
> *problems.*
> *3. Fixing the server is indeed best, but not necessarily an option.*
> *It could be proprietary, or written in a unknown language.*

Linux–Kernel: Re: Open source firewalls

>

No. As ur the only user of ur program, means resources is limited to visulize all senarios for all protocols. No one would like to keep on adding the proxies for the sake of buffer overflow. Is basically taken as a facility for filtering.

>> *If it is running on a hardware firewall as a service then its more*

>

>

> *"Hardware firewall" ???*

>

Yes embedded firewall. When ur gateway is protected by firewall device. Another one is a software firewall sol'n.

>> *dangerous as once it is compramisid then IDS signatures also can be deleted :-). No use of IDS the right ?*

>

>

> *A compromised firewall is of no use – sure. So what? That applies to any firewall, any IDS, or any server for that matter.*

>

No its not true as one ur frewall is compramisid, it can effect other services also. But at the same time if any of the servers is compramisid only that server is effected.

>> *So the best way is either make your code free of buffer overflows or*

>

>

> *Yes, but the server may not be "my code" at all. Can't you see that problem? It may very well be someone elses code. I may not have the source, or the source may be useless for a number of reasons, such as:*

> *1. being written in a language I don't understand*

> *2. Have a licence that forbids change*

> *3. Need compilers/tools I don't have*

> *4. Being such a nasty mess that writing a proxy is much easier*

> *than fixing the bloated ill–designed server code one*

> *unfortunately depends on for the time being.*

>

> *In these cases, I can still protect my server with a proxy firewall, although I can't fix the server itself.*

>

Again it will be ur own code with limitation of taking care of all scenarios. Take an example....Id we are trying to add a web proxy and using apache as our server. Do u say that code written by us will be more safe than apache ? :-)

>> *use some library which controls the attack during any buffer overflow*

>> *or use Stack Randomisation and Canary based approaches.*

>

>

Linux-Kernel: Re: Open source firewalls

> *A library that controls any buffer overflow doesn't exist at all.*

>

Its there and available. Just need to search.

> *Stack randomization helps but don't solve all cases, the attacker*

> *simply need code to search for randomly moved parts he need, pad with*

> *a few megabytes of NOPs and things like that. Of course, a proxy*

> *can easily detect megabytes of NOPs and kill that connection . . .*

>

Its not easy to have an attach with Stack Randomization. Like TCP syn randomization.

Regards

rvk

> *Helge Hafting*

> -

> *To unsubscribe from this list: send the line "unsubscribe*

> *linux-kernel" in*

> *the body of a message to majordomo@vger.kernel.org*

> *More majordomo info at <http://vger.kernel.org/majordomo-info.html>*

> *Please read the FAQ at <http://www.tux.org/lkml/>*

> .

>

-

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@vger.kernel.org

More majordomo info at <http://vger.kernel.org/majordomo-info.html>

Please read the FAQ at <http://www.tux.org/lkml/>