

Re: National Security Backdoor in telnetd – all versions.

Source: <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2003-08/0737.html>

From: Nico Kadel-Garcia (nkadel_at_verizon.net)

Date: 08/28/03

Date: Thu, 28 Aug 2003 13:17:21 GMT

Au Naturel Productions wrote:

> *On Thu, 28 Aug 2003 01:42:50 +0000, Nico Kadel-Garcia wrote:*

>

>

>>*Horse pockey. They're a federal agency, they are constrained by
>>constitutional limitations. They *violate* them, and are difficult to
>>prosecute under the auspices of "national security".*

>

>

> *Do you really know what you are talking about? Have you ever done anything
> within the National Security field? From what I have see you write: I
> highly doubt it.*

Follow the lawsuits.

>>*That would be *GREAT*. It would provide additional constitutional
>>grounds to have the courts yank the teeth out of these business and
>>freedom crippling regulations.*

>

>

> *You must feel the military and government shouldn't have any secrets huh??*

Sure, they should. They need to have a half-life. The Swedish model is far superior here, where all governmental documents are public by constitutional statute, and those which need to be restricted must be declared so if asked for. And even then, there has to be an expiration date.

I'm living in Boston. We've **seen** what happens when federal "security" agencies are allowed to operate in secret. Heck, have you even followed the efforts trying to find the name of the judge who signed the warrants for the "Sun Devil" raids? That was a raid on a bunch of high-school crackers, and the warrants are all sealed!

>>*Now try to provide a secure password, and make sure it doesn't get
>>sniffed when you have to reconfigure your switch from offsite.*

comp.os.linux.security: Re: National Security Backdoor in telnetd – all versions.

>

>

> *You allow remote root logins?*

You ever tried to administer a switch on the other coast that is part of your network, especially for VPN use? Building the tunnels is a pain in the ass, and many sites do it through extremely poor obscurity protection.

Not me: secure tunneled access, baby!

>> *Whoops. Can't be done without building an SSL/SSH tunnel, which costs*

>> *another \$5000 in rack space and setup time to make reliable.*

>

>

> *Vendor is your problem, not government. Vendors claim government, because*

> *they are lazy themselves.*

Horse shit. The vendors themselves have been screaming about the export regulations for decades now, because it forces them to ship "crippled" versions of their product by default and make the customer apply "security upgrades" after the fact to bring them up to the security level *allowed* by US export regulations.

If you've ever tried to reprogram the BIOS of a high-end switch to add features, it's non-trivial. Instead, we get pitiful end-to-end ethernet encryption techniques such as the EEpro100 "s" chipset, which was never a stable piece of hardware.

>> *That's right, you can download it. You can't have it *already built in*,*

>

> *<snip>*

>

>> *real-time, as we can now crack the old 'crypt' by raw brute force"?*

>

>

> *Vendors are your problem, or are you just lazy to do the work yourself? As*

> *to you histroy, read The Puzzle Palace. You might get an idea of my*

> *experience.*

That's nice. Try reading the Cuckoo's Egg, which is far closer to mine.

> *Then blame the cell phone makers for not helping secure their phones.*

They *can't*. Didn't you read the Telecommunications Privacy Act? If they incorporate new, non-tappable at the switching office telephone technologies, that act fined them quite a lot of money every day for operatinig it.

Even with parts of that legislation dropped since then, after court challenges of various sort, the FCC refuses to allow licensing of the airwaves or creation of new telephone systems that don't provide

Re: National Security Backdoor in telnetd – all versions.

comp.os.linux.security: Re: National Security Backdoor in telnetd – all versions.

man-in-the-middle access for law enforcement.

>> *The encryption was apparently solid. The *patent violations* were done*
>
> *<snip>*
>
>> *your own genuinely private session keys in roughly 45 minutes.*
>
>
> *NSA development? Where did you get that information? VChip had nothing to*
> *do with what you are claiming?*

Start with Google searches on "Clipper Chip", "Skipjack", and "patent violation". Here's a good start:

http://www.eff.org/Privacy/Key_escrow/Clipper/ for the history of the legal issues.

<http://www.rsasecurity.com/rsalabs/faq/6-2-4.html> for the LEAF vulnerability allowing use of genuinely private keys.

And yes, the chip was originally designed for voice transmission use.

>> *This is what "security by federal mandate, it's a secret and we can't*
>> *tell you, p-b-b-b-b-t-h" gets you. Illegal behavior and stupid designs.*
>
>
> *Do you know what sets how this nation sets its classifications? Probably*
> *not.*

No, considering that it's been modified at least twice since Sept. 11 by the Department of Reich^H^H Homeland Security. I can't keep up with Ashcroft playing dodgeball with constitutional rights....