

CSO

SECURITY AND RISK

Blogs

Newsletters Dashboard RSS Solution Centers White Papers Webcasts Podcasts Video Events Magazine


Google Custom Search

GO

Data Protection Identity & Access Business Continuity Physical Security Security Leadership Basics Tools & Templates Security Jobs Blogs

Blog Topics

Data Protection Identity Management Business Continuity Physical Security Leadership Career



An FBI backdoor in OpenBSD?

by Robert McMillan, Security Blanket

Wed, 2010-12-15 09:06

Topic(s): Data Protection

You have to give Theo de Raadt credit: he's into openness. What other software product would take serious, but questionable allegations about an FBI-planted back door in its code and just go public with them?

That's what OpenBSD's de Raadt did Tuesday after a former government contractor named Gregory Perry came forward and told him that the FBI had put a number of back doors in OpenBSD's IPsec stack, used by VPNs to do cryptographically secure communications over the Internet.

The allegations could make many people think twice about the security of OpenBSD, but the way de Raadt handled the matter will probably have the opposite effect -- giving them another reason to trust the software.

Here's what de Raadt said:

I refuse to become part of such a conspiracy, and will not be talking to Gregory Perry about this. Therefore I am making it public so that

(a) those who use the code can audit it for these problems,

(b) those that are angry at the story can take other actions,

(c) if it is not true, those who are being accused can defend themselves.

I contacted Perry about his email, and while I couldn't get him on the telephone, he confirmed that his letter to de Raadt was published without his consent. He gave a few more details on his involvement with the FBI (which, by the way, has no immediate comment on this).

Hello Robert,

I did not really intend for Theo to cross post that message to the rest of the Internet, but I stand by my original email message to him in those regards.

The OCF was a target for side channel key leaking mechanisms, as well as pf (the stateful inspection packet filter), in addition to the gigabit Ethernet driver stack for the OpenBSD operating system; all of those projects NETSEC donated engineers and equipment for, including the first revision of the OCF hardware acceleration framework based on the HiFN line of crypto accelerators.

The project involved was the GSA Technical Support Center, a circa 1999 joint research and development project between the FBI and the NSA; the technologies we developed were Multi Level Security controls for case collaboration between the NSA and the FBI due to the Posse Comitatus Act, although in reality those controls were only there for show as the intended facility did in fact host both FBI and NSA in the same building.

We were tasked with proposing various methods used to reverse engineer smart card technologies, including Piranha techniques for stripping organic materials from smart cards and other embedded systems used for key material storage, so that the gates could be analyzed with Scanning Electron and Scanning Tunneling Microscopy. We also developed proposals for distributed brute force key cracking systems used for DES/3DES cryptanalysis, in addition to other methods for side channel leaking and covert backdoors in firmware-based systems. Some of these projects were spun off into other sub projects, JTAG analysis components etc. I left NETSEC in 2000 to start another venture, I had some fairly significant concerns with many aspects of these projects, and I was the lead architect for the site-to-site VPN project developed for Executive Office for United States Attorneys, which was a statically

RECENT COMMENTS

May god help us if such an

1 week 5 days ago

Murder, mayhem, Orwellian

4 weeks 19 hours ago

Murder, mayhem, Orwellian

4 weeks 19 hours ago

what exactly are you suggesting?

4 weeks 6 days ago

Illegal

5 weeks 20 hours ago

RECENT POSTS

» more posts

Patch Tuesday panic not necessary. Or is it?

Siberian exploit kit circumvents traditional security

An FBI backdoor in OpenBSD?

Sixth Circuit Makes it Harder to Get Cloud E-mail

Gawker fallout: Mel Brooks warned us

WEBCASTS

60 Minutes: The Future of the Perimeter

Smart Techniques for Application Security

The Business Case for Data Protection

Utility Mandate: Software Security for the Smart Grid

CyberAttacks ... Are you protected or prepared to pay?

» View All Webcasts

WHITE PAPERS

The Business Case for a Next-Generation SIEM: Delivering operational efficiency and lower costs through an integrated approach to network security management

IDC Technology Spotlight: Leveraging the Benefits of Cloud Computing with Specialized Security

http://blogs.csoonline.com/1296/an_fbi_backdoor_in_openbsd[12/15/2010 9:43:20 AM]

keyed VPN system used at 235+ US Attorney locations and which later proved to have been backdoored by the FBI so that they could recover (potentially) grand jury information from various US Attorney sites across the United States and abroad. The person I reported to at EOSUA was Zal Azmi, who was later appointed to Chief Information Officer of the FBI by George W. Bush, and who was chosen to lead portions of the EOUSA VPN project based upon his previous experience with the Marines (prior to that, Zal was a mujadeen for Usama bin Laden in their fight against the Soviets, he speaks fluent Farsi and worked on various incursions with the CIA as a linguist both pre and post 911, prior to his tenure at the FBI as CIO and head of the FBI's Sentinel case management system with Lockheed). After I left NETSEC, I ended up becoming the recipient of a FISA-sanctioned investigation, presumably so that I would not talk about those various projects; my NDA recently expired so I am free to talk about whatever I wish.

Here is one of the [articles I was quoted in from the NY Times](#) that touches on the encryption export issue:

In reality, the Clinton administration was very quietly working behind the scenes to embed backdoors in many areas of technology as a counter to their supposed relaxation of the Department of Commerce encryption export regulations – and this was all pre-911 stuff as well, where the walls between the FBI and DoD were very well established, at least in theory.

Some people have decided that Perry's claims are not credible, and at least one person named in his email has [come forward to say it's not true](#). But at this point, it seems that nobody but Perry really knows what's going on.

It's hard to really know what to say at this point. We're talking about backdoors that probably just look like regular old bugs in code that was written 10 years ago.

» [read more from Robert McMillan](#) | [post a comment](#)

POST A COMMENT

Subject:

Username:

E-mail:

The content of this field is kept private and will not be shown publicly.

Homepage:

Body: *

- Allowed HTML tags: <a> <cite> <code> <dl> <dt> <dd>
- Lines and paragraphs break automatically.

* Denotes a required field



WHITEPAPER	WHITEPAPER
3 Strategies to Protect Endpoints from Risky Applications	Guide to Proactive Threat Protection

[Strong Authentication for the Here and Now](#)

[Addressing the Grand Challenge of Cloud Security](#)

[Securing Virtualization In Real World Environments](#)

[Business Resilience: The Best Defense is a Good Offense](#)

» [View All White Papers](#)

CSO Corporate Partners



organizational endpoints and mitigate the rising risk from these applications.

» [View this Webcast](#)



and increased sophistication of cyber attacks and discusses the value of integrated threat intelligence.

» [Read More!](#)

SPONSORED LINKS

- ▶ [Best practices in email security and security software as a service. Read more >>](#)
- ▶ [RSA Archer gives you one smart choice for security, risk & compliance](#)
- ▶ [Download the Forrester Study to learn how 305 IT decision makers are protecting their corporate secrets](#)

RESOURCE CENTER

[buy a link »](#)



[Home](#) | [About](#) | [Privacy Policy](#) | [Terms of Service](#) | [Subscription Service](#) | [Advertising](#) | [Events](#) | [Site Map](#)

THE IDG NETWORK

[CIO](#) | [Computerworld](#) | [CSO](#) | [DEMO](#) | [GamePro](#) | [Games.net](#) | [IDC](#) | [IDG](#) | [IDG Connect](#) | [IDG Knowledge Hub](#) | [IDG TechNetwork](#) | [IDG Ventures](#) | [InfoWorld](#) | [ITwhitepapers](#) | [ITworld](#) | [JavaWorld](#) | [LinuxWorld](#) | [Macworld](#) | [Network World](#) | [PC World](#)



© 1994 - 2010 CXO Media Inc. a subsidiary of [IDG Enterprise](#)