Ivan Buetler

From: musnt live [musntlive@gmail.com]
Sent: Mittwoch, 15. Dezember 2010 02:36
To: bugtraq@securityfocus.com
Subject: OpenBSD's IPSEC is Backdoored

Original e-mail is from Theo DeRaadt

http://marc.info/?l=openbsd-tech&m=129236621626462&w=2

I have received a mail regarding the early development of the OpenBSD IPSEC stack. It is alleged that some ex-developers (and the company they worked for) accepted US government money to put backdoors into our network stack, in particular the IPSEC stack. Around 2000-2001.

Since we had the first IPSEC stack available for free, large parts of the code are now found in many other projects/products. Over 10 years, the IPSEC code has gone through many changes and fixes, so it is unclear what the true impact of these allegations are.

The mail came in privately from a person I have not talked to for nearly 10 years. 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.

Of course I don't like it when my private mail is forwarded. However the "little ethic" of a private mail being forwarded is much smaller than the "big ethic" of government paying companies to pay open source developers (a member of a community-of-friends) to insert privacy-invading holes in software.

From: Gregory Perry <Gregory.Perry@GoVirtual.tv>
To: "deraadt@openbsd.org" <deraadt@openbsd.org>
Subject: OpenBSD Crypto Framework
Thread-Topic: OpenBSD Crypto Framework
Thread-Index: AcuZjuF6cT4gcSmqQv+Fo3/+2m80eg==
Date: Sat, 11 Dec 2010 23:55:25 +0000
Message-ID: <8D3222F9EB68474DA381831A120B1023019AC034@mbx021-e2-nj-5.exch021.domain.local>
Accept-Language: en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
MIME-Version: 1.0
Status: RO

Hello Theo,

Long time no talk. If you will recall, a while back I was the CTO at NETSEC and arranged funding and donations for the OpenBSD Crypto Framework. At that same time I also did some consulting for the FBI, for their GSA Technical Support Center, which was a cryptologic

reverse engineering project aimed at backdooring and implementing key escrow mechanisms for smart card and other hardware-based computing technologies.

My NDA with the FBI has recently expired, and I wanted to make you aware of the fact that the FBI implemented a number of backdoors and side channel key leaking mechanisms into the OCF, for the express purpose of monitoring the site to site VPN encryption system implemented by EOUSA, the parent organization to the FBI. Jason Wright and several other developers were responsible for those backdoors, and you would be well advised to review any and all code commits by Wright as well as the other developers he worked with originating from NETSEC.

This is also probably the reason why you lost your DARPA funding, they more than likely caught wind of the fact that those backdoors were present and didn't want to create any derivative products based upon the same.

This is also why several inside FBI folks have been recently advocating the use of OpenBSD for VPN and firewalling implementations in virtualized environments, for example Scott Lowe is a well respected author in virtualization circles who also happens top be on the FBI payroll, and who has also recently published several tutorials for the use of OpenBSD VMs in enterprise VMware vSphere deployments.

Merry Christmas...

Gregory Perry
Chief Executive Officer
GoVirtual Education

"VMware Training Products & Services"

540-645-6955 x111 (local)
866-354-7369 x111 (toll free)
540-931-9099 (mobile)
877-648-0555 (fax)

http://www.facebook.com/GregoryVPerry
http://www.facebook.com/GoVirtual