White Paper: Could Government Subversion Affect your Business?

Introduction

The Internet is awash with speculation following allegations that the IPSEC cryptographic stack in OpenBSD was furnished with a backdoor at the behest of the Federal Bureau of Investigation (FBI).

The allegations were made by Gregory Perry in an e-mail to one of the founders of NetBSD - Theo De Raadt – and were published on the BSD mailing lists so that a code audit can be undertaken by those with an interest in doing so.

If such a backdoor does exist, it could allow the FBI (and conceviably others) to decrypt communications between servers, whether those communications take place over a Virtual Private Network (VPN) or over a Secure Shell Connection (SSH).

This whitepaper will examine the precedents for this allegation as well as the potential impact that such a revelation could have on businesses around the world.

NSAKey

Although the OpenBSD allegation is being widely discussed, it would not be the first time that a security agency has been accused of attempting to install a 'backdoor' into an operating system.

In August 1999 a security researcher located a cryptographic public key in Windows NT 4 (Service Pack 5) named _NSAKEY. It was assumed, from the name, that the key had links to the US National Security Agency (NSA). If true, the NSA would be able to subvert the security of any Windows system.

Microsoft denied the allegations and claimed that the name had been chosen because the NSA were responsible for vetting for compliance with US export controls. Microsoft claimed that the key was used in order to ensure compliance with these controls.

Shortly after NSAKEY was discovered, a third key was also found, to the apparent surprise of Windows developers attending the conference.

Although the allegations were never fully answered, _NSAKey remains in current versions of Windows, albeit under a different name.

Lotus Notes

The once popular productivity suite, Lotus Notes, was also subverted by the NSA. Due to export controls, Lotus sold international customers a different version of it's suite to the offering available in the US.

Prior to striking deals with a number of European Governments, Lotus had published details of the NSA 'trapdoors' built into it's international package.

When sending encrypted e-mail, the International version of Notes included the first 24-bits of the 64-bit key in the e-mail headers. This information was encrypted, for security, using a NSA Public Key. This meant that whilst the system remained secure (computationally, at the time) the NSA could easily retrieve the first 24 bits of the key. This weakness would allow the NSA to decrypt intercepted e-mail some 16 million times faster than another attacker!

Indeed, it was estimated that the NSA would be able to calculate the final 40-bits of the encryption key within seconds.

Once the weakness became widely reported, steps were taken to prevent the 'trapdoor' from being disabled. Notes was updated so that if the field containing the first 24-bits was incorrect, the e-mail would not open. This prevented users from replacing the NSA's key with one of their own.

Although Lotus quietly removed the relevant documentation from their website, they never denied the allegation. Instead, they opted to spin the claims as being of benefit to European customers (US Strength encryption protecting your e-mails from everyone, except the NSA)

IBM still carry information on the trapdoor.

Huawei Based Infrastructure

Strong concern developed in the UK when it was discovered that British Telecom PLC (BT) had purchased equipment used in their telecoms infrastructure from the company Huawei. Concerns arose over Huawei's intimate relationship with the Government of the Peoples Republic of China (PRC).

The concern was that Huawei may have been pressured to include a backdoor allowing the PRC access to the UK's telecoms infrastructure. Such a backdoor would allow an unprecedented level of espionage to take place, not to mention the critical repercussions if the system were to be utilised in a time of war.

Concerns still exist, despite efforts by Huawei to convince the populace that their concerns are unfounded. The company has offered to allow independent inspection of it's source code, which conveniently overlooks the fact that backdoors can be both in hardware and software.

At time of writing, these concerns remain unresolved.

OpenBSD

As discussed in the introduction, allegations have been made that the FBI subverted the IPSEC stack in OpenBSD. This crucial function is responsible for handling cryptography within the Operating System, and communications that had been assumed to be secure could be available for easy decryption by US Security Services.

Although the backdoor was allegedly planted in OpenBSD, the possible impact is not limited to this Operating System. The OpenBSD IPSEC stack was the first to be freely available and portions of it have been used in other operating systems, including GNU/Linux.

Because the allegations have not specified the nature of the subversion, it may take some time to adequately resolve the matter. Indeed, as conspiracy theories abound, it's highly likely that every bug or fault found in the code is likely to be seen, by some, as 'proof' of the subversion. The prevalence of such theories may ensure that the truth of the matter may never come to light.

Impact on Business

If we assume that all allegations of subversion are true and/or that similar tactics have been employed but not yet detected, then the potential impact on privacy and security is very difficult to overstate.

If the NSA/FBI truly do have backdoors in a variety of Operating Systems, this would allow them unrestricted access to the data stored and transmitted by business worldwide (Well, outside the US at least). How they would access this depends on the nature of the backdoor in question.

From a European perspective, the biggest concern would surely be that of political and economic espionage. If the NSA/FBI are able to access encrypted communications then they would potentially be able to view anything our Politicians, employee's and customers encrypt and send.

Suitable Responses

As the recent outrage has shown, it's very easy to develop a knee-jerk reaction to such allegations. Whilst the recent allegations are both concerning and controversial, they remain unproven. It's important to remember that, given the wide influence of the US Government, there's no guarantee that other OS' and applications have not also been subverted.

It'd be easy to claim that the only solution is not to use computers for anything remotely sensitive, but in today's world this is not only an excessive response, but one that would be very difficult to effectively implement.

Those handling *very* sensitive information should already be aware that such systems should not be connected to, or accessible from, the Internet. If the network being used is truly inaccessible to outside users then the potential ramifications of such a backdoor are largely negated.

In reality, no encryption system used today is 100% cryptographically secure (despite claims by LogMeIn and competitors). Many of the encryption algorithms used today are, however, considered computationally secure (i.e. the computing time required to crack the encryption is so excessive as

to ensure that most attackers would be unable to compromise the communication within a reasonable period of time).

This means that whilst it is concerning that the NSA/FBI *could* have a means to decrypt 'secure' communications, in reality anyone with the computing power required could also complete the same task. Admittedly, If a backdoor does exist, it would allow the NSA/FBI to retrieve the plaintext far more expediently (as seen in the Lotus Notes controversy).

Those concerned about the existence of NSAKEY are able to remove/replace the key without suffering any issues with the related functions in Windows.

Long Term Reactions

Although most of the current cryptographic algorithms originated, or are derived from algorthims originating, in the US, there's very little to prevent new algorithms from being developed outside of the US. Indeed, the inclusion of _NSAKEY in Windows actually undermined the claimed goal of the key, because users were able to replace NSAKEY with a more secure cryptographic key.

FreeBSD is developed primarily in Canada, so the influence of the US Government and it's agencies is already weakened somewhat. Whilst the FBI could repeat their alleged actions, it is far harder for the US Government to attempt to include backdoors in Operating Systems not developed on US soil.

In the future, those requiring 'secure' systems may develop a bias towards Operating Systems not developed in territories open to US interference, and the focus of cryptographic development may also become more focused outside of the US.

Open Vs Closed Source

Many had assumed that, due to it's open nature, Free Software was immune to such subversion. The recent allegations of FBI subversion cast doubt on this assumption, although the reader should be aware that this may be the very intent of those making the allegations.

However, regardless of immunity, it remains more difficult to find evidence of such subversion in closed systems. Open Source, by it's very nature, allows any interested party to perform a code audit, raising the possibility of any backdoor being discovered. It is this principle which has led Theo De Raadt to criticise GNU/Linux users for allowing closed source drivers to be used on their systems (the drivers being binary implementations with full kernel access, i.e. quite easy to hide a backdoor in).

If the recent allegations are proven, it may be used as 'proof' by proprietary vendors that Open Source software (OSS) is no more secure than proprietary. In reality, it should be remembered that *any* user has the ability to run a code audit on any OSS.

Conclusion

The recent allegations have generated a wide amount of controversy across the internet, but, for many businesses, they change very little. Even if the allegations are proven, proprietary applications have been (allegedly, in some cases – Proven in others) subverted by US security agencies for many years.

Businesses handling *truly* sensitive data are those most likely to be affected by US subversion, but these same companies are those most likely to have already taken the steps which can help negate the consequences of these backdoors.

Whilst the debate over the alleged OpenBSD subversion will doubtlessly provide entertainment for many, the weakness (if one exists) is likely to be found and patched very quickly. Other Operating Systems that may have been affected will doubtlessly be pursuing their own Code Audits in the meantime.

Until the allegations are proved, there's very little that businesses can do in the meantime. Those with the resources, may wish to perform an internal code audit. Other businesses, however, will have little choice but to monitor the news to ensure that they apply and resulting updates promptly.

The truly paranoid, of course, may choose to cease sensitive communications until the issue is resolved. It seems unlikely, however, that the debate will end any time in the near future.

About the Author

Ben Tasker is an IT Manager & Linux Specialist at Virya Technologies. He has substantial experience within the IT Industry, and a keen interest in Network security.

More whitepapers and free resources available at http://www.viryatechnologies.com/