

comp.security.unix: Our Data : an appeal – a "Plimsoll line" for computer security

Our Data : an appeal – a "Plimsoll line" for computer security

Source: <http://www.derkeiler.com/Newsgroups/comp.security.unix/2002-06/0080.html>

From: David Mohring (heretic@heretic.ihug.co.nz)

Date: 06/13/02

From: heretic@heretic.ihug.co.nz (David Mohring)

Date: Thu, 13 Jun 2002 17:28:42 +0000 (UTC)

An invitation to discussion in comp.os.linux.security.

However relatively bad the security of Microsoft's products are in comparison to what the free licensed and open source communities (as well as practically every other vendor on the planet) provide, Microsoft is not alone in the presence of vulnerabilities, this is a major issue for Linux/BSD and Unix as well as ever other OS and vendor.

>*From the Plimsoll Club history*

<http://www.plimsoll.com/history.html>

+Samuel Plimsoll, M.P.

+(1824–1898)

+

+Samuel Plimsoll brought about one of the greatest shipping
+revolutions ever known by shocking the British nation into making
+reforms which have saved the lives of countless seamen. By the
+mid-1800's, the overloading of English ships had become a national
+problem. Plimsoll took up as a crusade the plan of James Hall to
+require that vessels bear a load line marking indicating when they
+were overloaded, hence ensuring the safety of crew and cargo. His
+violent speeches aroused the House of Commons; his book, Our
+Seamen, shocked the people at large into clamorous indignation.
+His book also earned him the hatred of many shipowners who set in
+train a series of legal battles against Plimsoll. Through this
+adversity and personal loss, Plimsoll clung doggedly to his facts.
+He fought to the point of utter exhaustion until finally, in 1876,
+Parliament was forced to pass the Unseaworthy Ships Bill into law,
+requiring that vessels bear the load line freeboard marking. It
+was soon known as the "Plimsoll Mark" and was eventually adopted
+by all maritime nations of the world.

The risks,issues and solutions for providing a more secure
operating and application enviroment have been known for decades.

Those who do not already comprehend the issues and are willing to learn, should take some time out to listen to some of the speeches at Dr. Dobbs Journal's Technetcast security archives...

http://technetcast.ddj.com/tnc_catalog.html?item_id=502

..., starting with Meeting Future Security Challenges

http://technetcast.ddj.com/tnc_play_stream.html?stream_id=411

by Dr. Blaine Burnham, Director, Georgia Tech Information Security Center (GTISC) and previously with the National Security Agency (NSA)

The design and implementation of some applications and servers are just too unsafe to use in the "open ocean" of the internet.

Numerous security experts have railed against Microsoft's lack of security, best summed up by Bruce Schneier Founder and CTO Counterpane Internet Security, Inc who rightly said ...

<http://www.counterpane.com/crypto-gram-0201.html#1>

+Honestly, security experts don't pick on Microsoft because we
+have some fundamental dislike for the company. Indeed, Microsoft's
+poor products are one of the reasons we're in business. We pick on
+them because they've done more to harm Internet security than
+anyone else, because they repeatedly lie to the public about their
+products' security, and because they do everything they can to
+convince people that the problems lie anywhere but inside
+Microsoft. Microsoft treats security vulnerabilities as public
+relations problems. Until that changes, expect more of this kind
+of nonsense from Microsoft and its products. (Note to Gartner: The
+vulnerabilities will come, a couple of them a week, for years and
+years...until people stop looking for them. Waiting six months
+isn't going to make this OS safer.)

However Microsoft's products are not alone in the presence of vulnerabilities, this is a major issue for Linux/BSD and Unix as well as any other OS and vendor.

In a recent speech "Fixing Network Security by Hacking the Business Climate", also now on Technetcast

http://technetcast.ddj.com/tnc_play_stream.html?stream_id=700

, Bruce Schneier claimed that for change to occur, the software industry must become libel for damages from "unsecure" software, however historically, this has not always been the case, since most businesses can insure against damages and pass the cost along to the consumer.

The Ford Pinto and more recently the Ford Explorer's tires are two examples of public and media pressure being more successful than just threat of lawsuits. Even so, just as with the automotive industry, eventually though public pressure the governments around the world have to step in and pass regulations that set up a minimum set of requirements an automobile has to meet to be deemed

"road worthy". This includes crash testing as well as the inclusion of safety equipment on all models. The requirements are not constant and change to meet the expectations and demands of the public and lawmakers.

The onus is not only on the automotive industry itself but also on the users. Most countries require that all automobiles undergo regular inspection and maintain an up to date "Warrant of Fitness".

In the same way, if you want a secure IT infrastructure, eventually the software design, implementation and each deployment will have to undergo the same type of regulation and scrutiny.

Unix, Linux, BSD and especially OpenBSD are currently far superior in terms of security, both in closing the vulnerabilities in applications before they have the chance to be widely exploited and implementing more secure access subsystems (SELinux/LSM etc).

However, should the Unix, open source and free licensed communities and vendors be taking a more active approach, including lobbying government, to

- 1) set up a minimum set of expectations, in the design and implementation of internet "accessing" software ; and
- 2) ensure that all deployments are more securely implemented ; and/or
- 3) remove inherently insecure products from the marketplace,

IMO the above three are preferable to all software vendors, including Microsoft, than attempts to allow liability lawsuits against vendors for deployments which the vendors do not necessarily have any control over.

David Mohring – Any constructive comments welcome.

- ***Next message:*** Juergen P. Meier: "Re: NAT – Network Address Translation"
- ***Previous message:*** Barry Margolin: "Re: NAT – Network Address Translation"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]