Is the Operating System Dead?

by Gordon Merrill, MSIA &
M. E. Kabay, PhD, CISSP-ISSMP

Gordon Merrill, MSIA has been thinking hard about security aspects of operating systems mobility and the cloud. This article and the next four in the series are based on some of the papers Mr Merrill wrote during his studies for the MSIA< http://infoassurance.norwich.edu > degree at Norwich University< http://www.norwich.edu >. Everything that follows is Mr Merrill's own work with minor edits.

* * *

One of the problems dismaying information assurance professionals today is the avalanche move towards mobile devices< http://www.usatoday.com/money/workplace/2011-05-30-mobile-devices-in-the-workplace_n.htm > taking over computing for most users. A recent study predicts "U.S. mobile handset data traffic will grow from 8 petabytes per month this year [2010] to 327 petabytes per month in 2015."< http://econsultancy.com/us/blog/5683-study-mobile-Internet-traffic-is-set-to-grow-400-by-2015 > That would translate to an annual compound growth of about 110% per year.

The PC is no longer the primary device for accessing the Internet.< http://www.networkworld.com/news/2010/120910-top-stories-2010.html > The ratio of mobile devices to PCs used for daily computing is no longer even 1-to-1.< http://www.networkworld.com/columnists/2010/121610-andreas.html > The days of telling employees that they will connect only to corporate-issued Internet devices are soon to be over as well. With more than a billion mobile devices estimated to be in use before the end of 2013, our users will be doing business with several mobile devices.< http://www.informationweek.com/news/Internet/Webdev/showArticle.jhtml?articleID=222001329 >

In a posting by a criminal-hacker-supporter, "Cheesemunk" wrote, "So say somehow somewhere we ended up choosing a target to start wreaking havoc upon. All we need is an IP Address."< http://meussententia.wordpress.com/2008/06/14/hacking-101-hacking-using-ip-address-of-the-victim/ > The writer then goes on to post details of how to execute simple hacks on any site on the Internet whose IP address is accessible.

[MK adds: everyone reading this article should be familiar with – and periodically use – Steve Gibson's "ShieldsUP!!" port scanner< https://www.grc.com/x/ne.dll?bh0bkyd2 >; your system should result in a solid-green matrix, indicating that all ports from 0 to 1055 are in Stealth mode and do not respond to probes.]

Information assurance was a daunting enough task when we had one operating system (OS), or maybe two, and one standard issue mobile device. The biggest concern with the move to mobile interconnectivity is how we can protect our information in the face of the combinatorial explosion resulting from the manufacturers, models and software versions. < http://www.networkworld.com/news/2010/120910-top-stories-2010.html >

Here's a hypothetical illustration of that combinatorial explosion. Suppose there are

- 10 different mobile device manufacturer
- 20 models per manufacturer
- All devices are available on any mobile network
- Each device has its own OS
- Most users will not upgrade as needed so there may be up to 5 versions of each in use.

So in this scenario, we would have to cope with

- 10 x 20 = 200 possible devices
- Each of which is tailored to 10 different networks = 200 x 10 = 2,000 and
- Up to 5 different versions of OS = 5 x 2,000 = 10,000 variations of hardware and software.

How do we control 10,000 different device/OS connection configurations and maintain our sanity? We don't.

We must redesign of our concepts of inside and outside in our infrastructure. Rather than trying to enforce uniformity on our users' mobile devices, we should supply appropriately restricted data to mobile devices with authenticated users. Instead of trying to dictate specific configurations, we should focus on testing compliance with functional security requirements. The industry is going to have to develop the equivalent of network access controls for mobile devices so that we can verify compliance with minimum security requirements such as resistance to malware and to interception. Examples of highly rated mobile-device management software from a recent report by a research organization that declined to have its name included in this article include AirWatch< http://www.air-watch.com/ >, Good Technology< http://www.good.com/ >, MobileIron< http://www.mobileiron.com >, Sybase< http://www.sybase.com >, and Tangoe< http://www.tangoe.com >, but these companies seem to focus on specific brands and models of mobile devices. Some of the products use the Open Mobile Alliance (OMA)< http://www.openmobilealliance.org > Device Management< http://www.openmobilealliance.org/Technical/DM.aspx > developments.

We need security-software professionals to focus on what it will take for *any* mobile device to prove it is trustworthy for connection to our systems.

Part two of this series will discuss whether our data systems are ready for 4G connectivity.

* * *

Gordon Merrill, MSIA,< mailto:merrill.ia@gmail.com > currently lives and works in Tennessee. His career< http://www.linkedin.com/in/gordonmerrill > has taken him to 48 of the 50 states and to six foreign countries. Gordon's information assurance background has included working for major computer companies such as IBM, managing IT projects for Fortune 250 companies in the risk management field, owning his own business, and working as a private consultant. He was Chair of the School of Information Technology at the ITT Technical Institute in Chattanooga< http://www2.itt-tech.edu/masgoogle/campus/school.cfm > for three years.

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of

Adaptive Cyber Security Instruments, Inc.< http://acsi-cybersa.com/ > and Professor of Information Assurance< http://norwich.edu/academics/business/infoAssurance/index.html > & Statistics< http://www.mekabay.com/courses/academic/norwich/qm213/index.htm > in the School of Business and Management< http://norwich.edu/academics/business/faculty.html > at Norwich University.< http://www.norwich.edu > Visit his Website for white papers and course materials.< http://www.mekabay.com/ >