

True vulnerability analysis finally comes into its own

There's vulnerability assessment and penetration testing, but what about vulnerability analysis? Before you tell me that I'm just playing with words, stop for a sec and consider: it's one thing to assess what vulnerabilities may be in a system. It's quite another to analyze and understand them. Sometimes assessing is enough. All you really want to know is if the vulnerabilities are there. Certainly, you may want to attempt to exploit the vulnerabilities and see if they can lead to penetration. That's today's standard practice.

However, suppose you want to perform a full analysis of how your system will respond to various types of anomalous input. That's a nice way to say "attacks" but, really, it is quite a bit more. A bit over a year ago, researchers at a Finnish university discovered a fundamental flaw in the ASN.1 formalism. This formalism defines the protocol. If the formalism — and, by extension, the protocol — is flawed, any implementation of it will be flawed as well.

The researchers developed a set of test cases to analyze the flaw. These test cases consisted — although the researchers didn't use the term — of protocol mutations. These mutations, directed against software that implemented the protocol, cause systems using it to crash. That was a surprise since the initial hypothesis was that the attacks would allow penetration. If they had used the new Mu 4000 from Mu Dynamics, they would have known exactly what to expect.

The Mu 4000 is an analysis tool, perhaps the most robust analysis tool of its type that I ever have seen. This is not your average scanner, nor is it a penetration tool (although to a limited degree and can do both). This is a tool that you can use to perform a full range of vulnerability analyses on everything from a firewall to a piece of security software. In a nutshell, the Mu 4000 performs a wide variety of vulnerability tests from simple scans to protocol mutations.

The scans use only vulnerabilities from the past three or so years — sort of like using the WildList (www.wildlist.org) as an anti-virus benchmark. The protocol mutations are every-

thing from malformed packets to dangerous payloads and beyond. I usually hate that type of generalization, but this tool deserves it. As soon as you think that you've figured out what to do with it, you discover a new capability that lets you probe deeper into the system under test.

This is a true industrial strength tool. It will tell you quickly and positively how your system will behave under a wide variety of attacks and security-related failures or errors. If the protocol mutations provided (and updated periodically) are not enough for you, write your own. And, if the system under analysis crashes as a result of the testing, the Mu will restart it automatically and resume testing.

This is not a tool for the faint-hearted, however. While it is not difficult to use, for it to be effective you need to understand exactly what you are trying to learn. And, above all, you need to understand protocols.

The heart of the Mu 4000 is its ability to exercise software that is supposed to be implementing a protocol in just about every way imaginable. The result is that you know, in advance, how the protocol implementation will respond to almost any kind of attack. You know because you have presented it with just about every conceivable type of error, stress or exploit. And, you have done this at the protocol level. So, if the software is not implementing the protocol correctly — and, by extension, may be subject to exploit — you'll know it. The benefit? Goodbye zero-day exploits.

We married up the Mu 4000 with another tool I wrote about a few months back — the Amenaza SecureITree — and together they enabled solid, formal testing. With SecureITree we set up an attack tree and then executed it with the Mu. While our test case was simplistic, the power of this combination was obvious.

Here's the point: when you have sophisticated, mission critical testing to do on a large scale network, go big or stay home. The old paradigms of running a scanner and calling it a day are gone. When the survival of your organization depends on keeping your assets secure, the big guns are the order of the day. Mu 4000 certainly fills that bill. — *Peter Stephenson*

AT A GLANCE



Product Mu 4000

Company Mu Dynamics, Inc.

Availability Now

Price Price starts at \$50,000 for a usable configuration with on the order of 10 protocols. A full protocol license for 12 months, including all protocols shipped in those 12 months, is \$250,000. There are about 50 protocols supported today, plus published vulnerabilities (priced separately at \$15,000). The base price includes ARP, IPv4, ICMPv4, TCP, UDP, TFTP, as well as the appliance, automated test harness, power restarters and 150 GB RAID array.

What it does Industrial strength vulnerability analysis at the protocol level.

What we liked This is the most powerful vulnerability analysis tool I have ever used. Combined with complementary tools, such as Core Impact, SecureITree and I2's link analyzer, there is just about no security analysis you cannot perform on a system, device or software. This is a true, complete automated test bed for security analysis of protocol-based systems.

What we didn't like There really was nothing I didn't like; however, I had to struggle with the high price of this product until I realized that in a very large network, one protocol-related flaw that allowed a zero-day exploit to succeed could cost the organization everything. In that context, the price is very reasonable. Also, if you do not understand how networks work at the protocol level, this tool will just frustrate you. Bottom line is the usual: if you want to solve very difficult problems, you first must understand the problem in depth. This tool is no exception.

We award the Mu 4000 our SC Magazine Lab Approved award, the highest we offer.

SC
MAGAZINE
Reprints

 **Mu Dynamics™**

web: www.mudynamics.com | email: info@mudynamics.com
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
phone: (866)276-4640 or (408)329-6330 | fax: (408)329-6317

Part # RPT0700108D