



*Chris Christiansen
Program Vice President, Security Products and Services*

Decru Tightens Storage Security with Security Analyzers from Mu Security

October 2006

Security vulnerabilities are a major concern for enterprise, government, product developer, and service provider organizations. For example, according to IDC's 2005 Enterprise Security Survey, although 66% of attacks on enterprises are reported foiled, more than 40% of survey respondents who knew about attacks reported at least one successful breach of security to their networks. Because vulnerabilities are now exploited within days, hours, or even before formal disclosure, security preparedness is critical. Moreover, proactively finding and remediating vulnerabilities is important for vendors of IT products because the sooner a security vulnerability is discovered in the product-development cycle, the less it costs to fix. But IT product developers are overloaded with the growing complexity of products and security management options. Security solutions tend to come in two classes: brawny prevention products or brainy management products. Security analyzers, however, represent the integration of brains and brawn. Analyzers that perform vulnerability testing are helping drive the convergence of the three "S's" — Security, Systems, and Storage — as evidenced by the experience of Decru, a NetApp company and vendor of storage security systems.

The following questions were posed to Kevin Brown, Vice President of Marketing at Decru, a NetApp company, by Chris Christiansen, Program Vice President of IDC's Security Products and Services Group, on behalf of Mu Security.

Q. Can you describe the overall storage-security goals of Decru and the reasons for these goals?

A. We're the security arm of Network Appliance, but we actually run as a separate subsidiary. So, while we operate with all of NetApp's products, our products also work with all of NetApp's competitors' products.

The big trends we're addressing are encryption, privacy, and compliance. Until a few years ago, the approach was to build a big fence around the perimeter of your company and focus on protecting that perimeter with firewalls, etc. It was assumed that all the bad guys were on the outside and the good guys were on the inside.

However, the perimeter security model is no longer sufficient to protect against certain types of threats, particularly internal. So the focus has shifted from device-centric and network-centric security to a more data-centric security model — essentially protecting the data as it flows through the IT infrastructure. Data-level security requires a combination of encryption, key management, access controls, and authentication. It's a set of different technologies that have to be integrated together in order to harden and protect data-at-rest.

Historically, the big frame-array storage systems and file-based systems as well as tape back-up systems had no security — all the data was sitting there in clear text format. Today, if you scrolled a terabyte of data onto a single tape, you could fit every credit card in the world on it. And if you were to print it out that tape, it would produce about 20 million pounds of paper. So the magnitude of the amount of data being stored, the value of that data, and the insecure environment in which it has historically resided makes for a big and important market. There's \$100 billion worth of installed base storage systems sitting out there, with essentially no native security.

Decru specializes in applying security to those storage environments — that is, how to cost-effectively retrofit strong security into millions of heterogeneous, multi-vendor storage devices out there in the enterprise.

Q. How does security analyzer technology help Decru achieve its security goals?

A. Traditionally, most QA testing of products has relied on reliability or functional testing. Security testing is very different because of the way that hackers think, and the way that products are attacked — i.e., by operating them in unexpected ways.

As a result, very few companies are expert in understanding how to test unexpected usage cases, and most companies in fact do a poor job of security testing. This fact has contributed to the high number of vulnerabilities out of the marketplace. Enterprise networks have dozens of different products strung together in different ways, so the testing that's needed to validate their security has been beyond the reach of most companies.

Meanwhile, many users are realizing that if they buy a new product for their network, they could be opening up new vulnerabilities. The new product could, in fact, become a gateway for the bad guys. So, we as vendors need to demonstrate a commitment to secure development processes, as well as having multiple mechanisms including detailed analysis reporting and remediation tools for ensuring the quality and security of products that our customers are deploying.

Decru is using Mu Security's products in our development process to enhance the overall security testing that's applied to our product. For example, we already participate in a number of government and private certifications, and we regularly update our FIPS 140-2 Level 3 certifications. We're engaged right now in Common Criteria, working with the various intelligence sponsors with a target assurance level of EAL-4+. We are also DOD 5015.2 certified. We've done classified penetration testing, along with source-code review with multiple government customers. So security certification and testing is a very large area of investment for Decru.

In the past, we've used a variety of homegrown security test processes, but what we really like about Mu Security's analyzer is that it enables us to easily automate and extend certain types of internal testing that we've traditionally done using a powerful Web-based product. The Mu-4000 essentially automates the Security, Test, and Evaluation (ST&E) functions, enabling more comprehensive testing in advance of certification and accreditation. It's a great way to extend our coverage and inject it into earlier phases of our development process.

The upshot is, we're more likely to catch security issues or vulnerabilities much earlier in the development process, which saves money and results in more secure products. This is really important because we don't just sell any IT products, we sell security products. Secure development processes are essential, especially when you're dealing with something as sensitive as encryption and key management. Encryption technology has a giant target painted on it. If you're a bad guy, this is where the keys to the kingdom are literally stored.

The ability to take Mu Security's device, point it at our products, and execute a large set of automated attacks that look at different likely failure cases is a very useful way to truly operationalize that testing. It does a very nice job of assuring that our IP-enabled devices, for instance, don't inadvertently introduce weaknesses into critical infrastructure.

An interesting trend we're seeing is that the government certifications we've invested in for our military and intelligence customers are now being requested by private-sector customers. Banks, for example, are asking us about the details of our FIPS 140-2 Level 3 certifications, and what our protection profile is for Common Criteria. Over time, we expect that enterprise customers will be asking more detailed questions about our security testing and development process, and Mu Security provides an automated platform for addressing these requirements.

ABOUT THIS ANALYST

Chris Christiansen is the Program Vice President for IDC's Security Products and Services group. He conducts in-depth primary research and provides insight and analysis on a variety of evolving security markets. Mr. Christiansen delivers critical market intelligence to technology vendors, IT professionals, and the financial community.

ABOUT THIS PUBLICATION

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

COPYRIGHT AND RESTRICTIONS

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the GMS information line at 508-988-7610 or gms@idc.com. Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC visit www.idc.com. For more information on IDC GMS visit www.idc.com/gms.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com