Toward Transparency:

Setting Standards for Security

The computing industry is setting security standards through consensus, which helps promote transparent security implementations. By offering factory-installed operating systems preconfigured with security settings based on Center for Internet Security (CIS) benchmarks, Dell demonstrates its commitment to consensus-driven security standards.

BY J. CRAIG LOWERY, PH.D., AND CRAIG PHELPS

Technology generally tends to mature in phases. Initial proofs of concept are followed by explosive innovation, then a cooling-off period in which society assesses the full effects of a technology, identifies the advantages and disadvantages, and then integrates the technology into mainstream processes. Computer technology has been no different. Although innovation continues, many agree that new hardware and software features are less important than solving outstanding problems. Security is one such problem.

Computer users demand products that are secure by default and employ transparent security measures that do not make a product more difficult to use. Dell incorporates such customer requests into its product development cycles, but it must respond without increasing cost or complexity. For guidance, Dell turns to consensus-driven security standards.

Consensus-driven standards lead to transparency

When a broad set of stakeholders can contribute to a standard, they capture and consistently document best practices and solutions; everyone involved knows what to expect. A dearth of security standards leads to confusion and complicated, proprietary security implementations—the antithesis of transparency. Agreement on how best to achieve secure computer systems is just beginning. Best practices as communicated through nonprofit organizations such as the SANS (SysAdmin, Audit, Network, Security) Institute are prime examples of industry efforts to consolidate opinion on security topics.

Perhaps the most notable example of successful security through consensus is the work performed by the Center for Internet Security (CIS). CIS is a consortium of security specialists from nearly all sectors, including government, higher education, finance, and health care. Although many organizations have stepped forward with recommended security settings, CIS approaches this problem by first achieving a consensus among security professionals on proper configuration settings, and then providing a tool that measures how closely a system comes to meeting those settings.

CIS benchmarks reflect security recommendations

CIS provides a library of configuration standards known as benchmarks. Volunteer CIS members identify a system for which no consensus benchmark currently exists, gather recommendations concerning the best way to configure such a system so that it is more secure, and write a document that, after intense review and scrutiny by the members, achieves CIS benchmark status.

CIS benchmarks fall into two categories: Level I and Level II. Systems that meet Level I benchmarks achieve what CIS calls a "prudent level of minimum due care." Most security professionals would agree that these settings achieve a baseline for a reasonably secure system. Level I settings and actions require no special expertise to apply and usually will not diminish system usability. Many of the settings disable services that are not needed in most environments. Other settings disable features that are convenient but generally unnecessary. Level II benchmarks are much more complex; they further increase system security, but require more expertise in their application because they can affect usability.

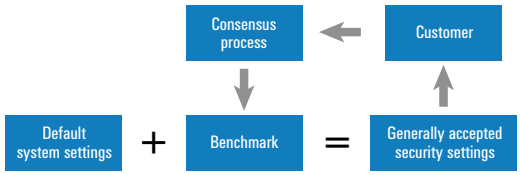
Each benchmark has an associated scoring tool to help assess system compliance. When run on a target system, the tool produces a numeric score from 0 to 10—0 meaning no compliance and 10 indicating full compliance. Attaching a defined metric to security compliance enables system administrators to track improvements in overall security preparedness.

CIS initially focused its benchmark evaluation on operating systems but has expanded its scope to include firewalls, routers, and applications, among other targets. Because CIS is an open forum, anyone in the industry has access to the benchmarks and scoring tools at no charge through the CIS Web site at http://www.cisecurity.org.

Dell makes sense of the consensus

Dell believes in disseminating information such as best practices by promoting standards. The CIS benchmark model, shown in the top half of Figure 1, exemplifies this philosophy in the security arena—being user-driven, it is particularly suited to the Dell™ direct model, which places high importance on quickly integrating customer feedback into products.

CIS benchmark model



Ideal model

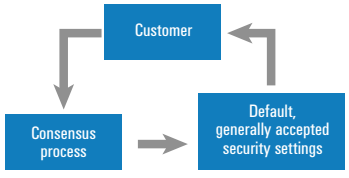


Figure 1. Achieving consensus: two models

Products such as Dell systems with CIS benchmark settings can help bring widely accepted security improvements to market now, while computer users wait for software releases that already incorporate these benefits.

Through its factory build-to-order and custom factory integration services, Dell offers Microsoft® Windows® 2000 operating systems preconfigured with CIS Level I benchmark settings. Although this offering resulted from suggestions by government customers, anyone can request it on Dell OptiPlex™, Dell Precision™, and Latitude™ desktops and laptops. Customer acceptance and further demand may prompt offerings for other operating systems and hardware platforms in the future.

By delivering systems preset to CIS benchmarks, Dell illustrates the viability of the consensus mechanism. Ideally, the consensus settings will be incorporated into software products at the source, as shown in the lower half of Figure 1, rather than being achieved through post-installation configuration changes. Dell believes this is beginning to happen, and offers as evidence the new "secure by default" philosophy that influenced the default configuration settings for the Microsoft Windows Server 2003 operating system. Products such as Dell systems with CIS benchmark settings can help bring widely accepted security improvements to market now, while computer users wait for software releases that already incorporate these benefits.

J. Craig Lowery, Ph.D. (craig_lowery@dell.com) is chief security architect and a software architect and strategist in the Dell Product Group—Software Engineering. Craig has an M.S. and a Ph.D. in Computer Science from Vanderbilt University and a B.S. in Computing Science and Mathematics from Mississippi College. His primary areas of interest include computer networking, security, and performance modeling.

Craig Phelps (craig_phelps@dell.com) is security brand manager in the Dell Public Sector Marketing Group. Craig has an M.B.A. from the Marriott School of Management at Brigham Young University (BYU) as well as a B.S. in Psychology and B.A. in English from BYU. His primary focus is identifying security measures for the public sector and then implementing them across Dell product lines.

FOR MORE INFORMATION

Center for Internet Security: http://www.cisecurity.org

SANS Institute: http://www.sans.org