

Enterprise Security for Web 2.0

Mary Ann Davidson, Oracle
Elad Yoran, Security Growth Partners



Security 2.0 means securing all data, end points, and networks and perimeters.

Web 2.0 is among the most talked-about, highest-buzz IT constructs of late, the subject of numerous articles and blogs and, since 2004, multiple conferences.

While in many respects an Internet phenomenon, Web 2.0 is quickly gaining a beachhead against the legacy “stovepiped” way in which users manage and disseminate information of all kinds within the enterprise. It’s also an outside-in revolution: Technologies developed and explored outside the enterprise are migrating inside it. People who’ve gotten hooked on Web 2.0 demand the same user experience, tools, and networking in their work that they’ve experienced at play.

The good news for enterprise security practitioners is that the impact of Web 2.0 has thus far been evolutionary. However, Web 2.0 growth is accelerating, and it’s doing so for reasons as varied as compliance, privacy, and protection of corporate assets.

Organizations considering deployment of Web 2.0 capabilities must exercise caution and control, just as

they do with non-Web 2.0 technologies. What’s needed, in short, is Security 2.0.

WEB 2.0 ATTRIBUTES

Web 2.0’s nature calls to mind the story of the blind men and the elephant: What you “see” depends on your personal experience. For some, Web 2.0 is smooth and graduated, like an elephant’s tusk; for others, it’s rough and random, like an elephant’s trunk. However, Web 2.0 has several attributes that clearly set it apart from the current Web.

Active, collaborative information

Web 2.0 encompasses active, collaborative information rather than passive, receptive information—users are contributors and creators, not just “information sinks.” A wiki, for example, is multiauthored and dynamic instead of monoauthored and static. Even applications can become dynamic in Web 2.0: Disparate components combine to form entirely new mashups, in contrast to the Web’s static, form-based applications.

Ubiquitous data access

Another major attribute of Web 2.0 is ubiquitous data access. Users to date have been limited in their data access by device, protocol, and location, such as whether or not they’re inside the corporate network. With Web 2.0, users expect whatever data, music, pictures, and videos they want, wherever and whenever they want them.

Even the number of devices is collapsing: Users want their phone, personal Web access devices, MP3 players, and PDAs to shrink to a single device even as the breadth and depth of the applications they’re using and the amount of information they access grows exponentially.

Rationalized data

On the application side, users “pedal faster” to keep up with the volume of information, but they also want data more rationalized—hence, wikis and mashups instead of endless links that users click on, evaluate, and mentally discard if irrelevant. Web 2.0’s premise is that users can combine “all information, all the time” in new ways that let them actually do more with it instead of combing through mounds of composting links in search of a pony.

The greater mobility that rationalized devices represent also will provide an impetus to telecommuting. For most bankers at one global investment bank, the new device of choice is no longer a laptop but a smart phone that supports various modes of communication and a wide range of needed applications. More radically, the bank encourages its employees to work from home at least one day a week.

However, the bank’s IT and security organizations, which are jointly responsible for secure telecommuting, struggle to separate the “bank network” (as extended to the home) from the “home networks.” Employees expect that their home network will be designed to suit not only the bank’s needs, but also the needs of their families. After all, who wants two entirely separate home networks?

ADAPTIVE SECURITY

User expectations for ubiquitous and rationalized access appear to be at odds with the increasingly centralized and compliance-driven direction of enterprise computing.

The key to Security 2.0 is finding an adaptive security model that will facilitate collaboration without making it the fatally weak link in the security chain. The implications of Security 2.0 will be felt in virtually every dimension of IT, ranging from data security to device security (on all end points) to connectivity security (all networks and perimeters).

Security 2.0 must adapt to reflect the new reality: Data is no longer locked up behind multiple portcullises and moats. Rather, it strolls out of the gates of a fortified castle and camps with other data in “mashup tents” that fold or are rolled out elsewhere with apparent ease.

We create larger encampments, not exactly on the fly but in a “prefab” way using Web services. At the same time, enabling broader access to selected bits of data can’t mean providing privileged data to anyone who happens to wander into a mashup tent.

Network perimeters haven’t vanished; in fact, they must—paradoxically—both expand and shrink. They must expand to encompass all network players, even temporary ones, instead of relying on a few trusted gatekeepers. At the same time, every network component must have its own defensible security perimeter, and each perimeter must therefore shrink to fit the size of the item protected, whether that is an individual laptop, smart phone, or any other end point.

Connectivity in Security 2.0 will also follow the collaborative usage patterns of Web 2.0. No longer will it be sufficient for enterprises to maintain the traditional hub-and-spoke approach to networking. Remote users will want to connect simply and securely to other remote users, peer-to-peer and point-to-point, ensuring the confidentiality and integrity of the communication, whether data, video, voice, or images.

Strong authentication and encryption technologies must operate in peer-to-peer formats and be able to scale to orders of magnitude—many tens of millions of devices, far larger than the operational threshold of current technologies.

SECURING END POINTS

As smart phones become the primary platform for Web 2.0 access, the devices themselves must be secured, including encryption of basic voice communications. Unfortunately, users don’t think twice about using cell phones to discuss sensitive company business such as mergers, intellectual property, and important transactions.

Connectivity in Security 2.0 will also follow the collaborative usage patterns of Web 2.0.

This trend is particularly worrisome in that in today’s global economy, enterprises often do business over insecure cell phones in parts of the world where commercial and government eavesdropping is a way of life. One global energy company recently lost a multibillion-dollar deal because its employees discussed secret information over their cell phones.

Universal devices

As smart phones and other end points increasingly make up greater portions of our computing lives, enterprises are migrating e-mail, calendar, and complex custom applications to them. Further, since no one likes to carry around more than one device, cell phones will be both enterprise access devices and personal communication devices. They might also be digital cameras, music players, or even the means by which users control their digital homes.

Security 2.0 will thus need to enable a single device to serve both personal and professional needs. End-point devices also will need the same “friend

or foe” challenge, virtual moats, and armed responses as the old armed data fortresses lest data be compromised on these new end points, or the end points themselves become compromised and serve as platforms for attacking other systems. In some cases, applications on smart end points might be firewalled from one another to prevent a single compromised application from taking over the entire device.

Cyberhealth maintenance

Maintaining the health of each end point is also important. Having a regular physical is the best way to catch an illness in its earliest phases. Likewise, most states have some sort of regular safety and emissions testing requirements for automobiles. In Security 2.0, each end point must be regularly checked for its cyberhealth, echoing the deployment of PC-based firewalls and network access control. Similarly, the system should check an end point’s cyberhealth every time it connects to either a network or another device.

SECURING DATA

Data itself will need active protection as it migrates from device to device. Security 2.0 will include teaching new tricks to some already high-IQ dogs.

Intelligent search engines

Search engines will be both smarter and more selective inside the enterprise than generic Web search engines. Smarter in that, absent the marketing activity of purchased keywords, an enterprise search engine can return results that are more relevant and that match the searchers’ intent more clearly. More selective in that, depending on corporate security policies, search results might not include a particular result, depending on the searcher’s need to know.

For example, in some cases, even a document’s name—such as a company’s merger and acquisition plan—is highly confidential; the search engine shouldn’t disclose that this

document even exists to anyone except named individuals in the M&A department. In other cases, an intelligent search engine could indicate that a document exists but require the searcher to obtain additional privileges to view it.

An intelligent search engine could also become the compliance officer's best friend by being used in "privileged mode" to map all information on the network, just as security practitioners map their networks regularly.

Information rights management

IRM will be another weapon in the Security 2.0 enterprise security arsenal.

Data-driven collaboration in a compliance-driven environment will include—in addition to data and document time-to-live as well as auditing who accesses what and when—control of data extending even beyond the firewall.

Rights management, however narrowly or broadly deployed, must also apply to "all data, all the time." That is, where IRM is used, it must apply to multiple forms of information exchange—e-mail, instant messaging, documents, spreadsheets, presentations, and so on—regardless of where the data lives, how and where it travels, and what devices it resides on.

Data migration

Another reason to have self-securing data, and not merely self-securing applications, is that it's difficult enough to secure all of a network's elements, such as operating systems, routers, and multiple types of applications. Expecting a mashup creator to also be a security expert inadvertently weakens security because one person's mashed-up application could all too easily become a messed-up application by giving transitive privileges to someone who shouldn't have them.

Just having access to an application module or to privileged data through that application module doesn't mean the user should be able to pass that access to another person through a mashup. Enterprises don't want critical

data to migrate like a cold virus—that is, to pass with every "data touch." If the system enforces security at the data level, wherever and however it migrates, controlled collaboration doesn't become uncontrolled data leakage.

In the enterprise computing realm, Security 2.0 means securing all end points; establishing simple, secure peer-to-peer connectivity between these end points; and controlling all data, in whatever form it lives and morphs, throughout its entire life cycle, wherever it goes and however it gets there. It also means that each network entity must self-defend because network and application perimeters themselves have become mutable and collaborative.

Security 2.0 must also be easy for users. Firewalls and network-based intrusion-detection systems were king and queen of the Security 1.0 realm, but security often failed through its own complexity and lack of "invisibility." Users often bypassed security because it was too hard to use or it wasn't "just there" and they had to enable it, often painfully.

Web 2.0 is transforming computing from complexity—too many devices, too many stovepipes, too much "uncollated" information—to a collaborative phenomenon that seems natural and intuitive. Security 2.0 must be equally natural and intuitive to unleash the next great wave of innovation and business growth. ■

Mary Ann Davidson is chief security officer for Oracle. Contact her at mary.ann.davidson@oracle.com.

Elad Yoran is CEO of Security Growth Partners. Contact him at eyoran@securitygrowth.com.

Editor: Richard G. Mathieu, Dept. of Computer Information Systems and Management Science, College of Business, James Madison Univ., Harrisonburg, VA; mathierg@jmu.edu

The magazine that helps scientists to apply high-end software in their research!



Peer-Reviewed Theme & Feature Articles

2008

| | |
|----------|--------------------------------------|
| Jan/Feb | SDSS Archive |
| Mar/Apr | Usable Community Grid |
| May/June | Combinatorics in Computing |
| Jul/Aug | Computational Astrophysics |
| Sep/Oct | Computational Provenance |
| Nov/Dec | High-Performance Computing Education |

Top-Flight Departments in Each Issue!

- Books
- Computer Simulations
- Education
- Scientific Programming
- Technology
- Visualization Corner



Subscribe to CiSE online at <http://cise.aip.org/cise> or www.computer.org/cise