Pipeline
Knowledge Is Power

www.pipelinepub.com Volume 4, Issue 11

Vandals at the Gate:
The Realities of Modern Web Application Security

by Tim Young

Do you lock your car doors? If you've driven into a major downtown area, do you hit the lock button on your keyless entry and make sure you don't have any valuables lying out on your back seat? How about if you're just running into a neighborhood coffee shop? In your own garage? According to the Insurance Information Institute, in 2006, just under 1.2 million cars were reported stolen in the United States. That's substantial, but rather weak compared to the 15 million cases of identity theft that took place between mid-2005 and mid-2006, according to a Gartner report. No doubt a great many of these cases were the result of online fraud or intrusion.

However, awareness about security on the consumer end is growing every day. Desktop firewalls and anti-virus software are ubiquitous. Awareness about phishing and other common fraud is growing. It must be a very difficult time to be Nigerian royalty attempting to involve a lucky stranger in a legitimate monetary exchange. The public is getting savvy. Still, many of us put far more care in protecting our cars, which are less likely to be stolen, than our identities, which are easy prey.

However, we should go a step further. Let's look at the implications of wider security. Not security on the consumer end. Security that will protect private information after it has left the users safe little desktop lockbox. Security that will protect consumers from dangers they don't even know pose threats.

One area that is particularly vulnerable to outside attacks is the growing world of web applications. Web applications are commonplace for millions of users. From webmail to e-commerce, to wikis and online games, it's rare for a user to navigate an entire day without using a web application, including applications that deal with sensitive personal data.

"Today, virtually every application is a Web application," says Ryan Barnett, Director of Application Security for Breach Security, a firm dedicated to security for webapps. "Business-essential Web applications require automated, application-specific tailored security with visibility into the SSL encrypted traffic to effectively secure Web applications." The ubiquity of web applications is certainly not going anywhere anytime soon, either. Users clearly enjoy the quick response time and ease of accessibility that webapps offer.

However, doesn't excessive security run counter to those very selling points for webapps? "Any feasible security solution for protecting Web applications must not affect the availability of the Web application or hurt the user's experience," Barnett concedes. Security measures must be unobtrusive and low-impact. A difficult duality, perhaps. Still, one that is necessary to provide if at all possible.

Back in 2003, Yankee Group estimated that by 2007, the web application security market would be worth 1.74 billion dollars. That was arguably before web applications had shown themselves to be quite as indispensable as they have proven to be. Last year's acquisitions of SPI Dynamics by HP and Watchfire Corp by IBM prove that web application security is on the minds of many larger software players.

The truth is that the growth of web applications has changed the game. "As hackers have shifted their strategy for attacking organizations from searching for vulnerable servers to compromise," Barnett says, "to *targeted* attacks against Web applications, often rife with defects, companies are learning that Web application security is no longer an option, but an essential part of doing business on the Web."

The location of the information, in short, is much less important than it once was. "Before Web applications became so popular, sensitive information was stored in databases and applications on internal networks," says Barnett. "Hackers would have to gain access to this data by breaking into servers deeper and deeper within an organization's network until they found something useful."

Traditional network security solutions were up to the task of facing such challenges. Firewalls and intrusion detection systems could prevent entry or notify administrators of such entry and ensure that future incursions were more difficult to execute and less common overall. "However," Barnett asserts, "as web applications evolved from simple sites containing non-critical information to complex multi-tiered applications at the forefront of business, these network solutions are no longer

sufficient."

Furthermore, there is the problem of the double-edged sword of user-friendly applications. Not only do well-laid-out and easy-to-navigate sites aid users in gaining value from webapps, the resources are far easier for hackers to navigate, as well. "IDS and traditional network security systems are not designed solely for these constantly changing web applications," says Barnett, "and hackers no longer need to search through a network to find the valuable data; they simply browse an organization's Web site."

"Additionally," continues Barnett, "each Web application is different and cannot be protected by generic measures as is possible with network security such as the network firewall or the network IDS/IPS system." There is no simple blanket solution for web applications. However, solutions do exist, and should be considered a priority for anyone involved with webapps. The increasing complexity of such applications will make them even more valuable to the end user, and likely more vulnerable to intrusion.

In short, any organization or enterprise that is interested in maintaining security within the context of a web application should take note of advances in web application security. Most desktops are well equipped with firewalls and detection software. Users are more vigilant than ever. Furthermore, a look at some of the other articles in this month's issue of Pipeline will underscore the fact that security on the network itself is becoming more common and more effective. Careful monitoring of all traffic is allowing carriers to see intrusions and anomalies in real time. Tools abound to proactively confront malice in a real and effective way.

The network and those accessing it are thicker-skinned than ever. The web application cannot afford to be the chink in the armor that causes the entire process to become less secure.

If you have news you'd like to share with Pipeline, contact us at editor@pipelinepub.com.