

## Blogs: Sue Marquette Poremba



## Data Security

Securing your data and network, inside and outside the perimeter

About this Blogger  RSS

## Subscribe



Sign up now and get the best business technology insights direct to your inbox.

Daily Edge

Business Tools & Templates

Aligning IT & Business Goals

Maximizing IT Investments

IT Careers

## Most Popular Posts

[Generation Y Employees and Privacy](#)

[Bulletproofing Your Data](#)

[The U.S. Leads the Way in Credit/Debit Card Fraud](#)

[Thinking Like a Cyber Criminal to Prevent Cyber Crime](#)

[Seven Improved Security Features in Windows 7](#)

## Recent Posts

[2011 Saw Change in Approach to Cyber Crime](#)

[Bulletproofing Your Data](#)

[The U.S. Leads the Way in Credit/Debit Card Fraud](#)

[When the Security Policy Works](#)

[New Adobe Flaw Affects Computers Across Different OS Platforms](#)

[Thinking Like a Cyber Criminal to Prevent Cyber Crime](#)

[Federal Agencies Struggle to Define Their Cybersecurity Work Forces](#)

[No Such Thing as Privacy When It Comes to Smartphones](#)

## Cookies as a Security Tool

Posted by [Sue Marquette Poremba](#) Sep 8, 2010 4:43:41 PM

Computer [cookies](#) have a mixed reputation. As the folks at [Mykonos Software](#) told me:

First-party cookies are an understood and accepted part of using many of today's Web applications. When you go back into Amazon, for example, the site remembers you because you have a cookie on your machine. These cookies are not really controversial per se and anyway they are easily cleared. Third-party cookies, where companies share your purchasing practices across sites, using some form of advertising tracking cookie, allow Web applications to serve up personal content based on your behavior. This type of cookie raises some concerns about privacy because the behavior of the user is being tracked and stored.

Now Mykonos has come up with another use for cookies, this time definitely for good -- security cookies. According to Al Huizenga, director of product management, the cookies are used to protect enterprises' public-facing websites from abuse. The focus is to monitor user behavior and learn the patterns used to manipulate the website's applications to bypass the original intent. One of the examples of sites where security cookies are useful sites is where customers are buying tickets or booking a reservation. Abusive users, said Huizenga, will manipulate the sites to order more tickets or book more sites than allowed by the original application, which shuts out legitimate customers and hurts the overall business.

The security cookies allow the business to track the communications between the users and applications, and Mykonos specifically looks for abusive behavior at the site. Huizenga said:

Usually patterns and signatures are used to point out a situation that looks like an attack or if someone is in-putting code when they should actually be inputting text. We're trying to go a step further and recognize when a user is being abusive. We'll inject detection points into the application points that allow us to see if the user is trying to manipulate the forms or messing around with the URL string to see if they are doing something bad. That information gets added to that user's profile, and allows the company to track the user over time.

As threats get more sophisticated, Huizenga added, security organizations need more weapons and new approaches to fighting them. Tracking user behavior is a new tool to add to the more traditional security tools.

 SHARE

 Print

 0 Comments

## Related Content

Browse

Topic: [Usage Management and Monitoring](#)

Usage management and monitoring tracks who is using the network and what they are doing

Blog: [Built-in Security Soon to Be Available to PCs](#)

Article: [IT Security Only as Strong as Your Weakest Link](#)

White Paper: [Shrink Your Internet Exposure: Nine Totally New Ways to Lower Your Network Risk](#)

Related Topics

[Application Security](#), [Data Security](#)



## White Papers, Events, and Resources



### Ten Database Activities Enterprises Need to Monitor

Read this analyst report to learn the ten critical database activities and behaviors enterprises should audit now.



### Are Proxy Anonymizers Putting Your Enterprise in Peril?

This white paper explores a Web filtering solution that identifies and filters HTTPS requests, a strategy that enables monitoring of the non-standard ports proxies can sometimes

use.

## RECENTLY RELEASED

### 2011 Gartner Magic Quadrant for Business Intelligence Platforms

Download the full report in convenient PDF format.



DOWNLOAD NOW