



## ▶▶ RECENT NEWS

### SecTor event highlights holes in DNS, databases

Experts explain rebinding attacks on domain name servers and how to stop them.

Plus: SQL Server forensics...

11/22/2007 12:25:00 PM

by Kathleen Lau

**Toronto** -- The Web was originally designed for housing public content, but the fact that it's now used to build applications housing private data make it a ripe platform for malicious attacks, according to one speaker at the SecTor 2007 conference in Toronto this week.

“The Web is where the wild things are nowadays,” said Dan Kaminsky, director of penetration testing at Seattle-based security consultancy IOActive, during a session on Domain Name Server (DNS) rebinding attacks.

Essentially, DNS translates human-readable computer hostnames into IP addresses. But the DNS rebinding attacks subvert the DNS same-origin policy that assumes information stemming from the same origin must be trusted identically, said Kaminsky, but the reality is, the translations during this process can change at any time.

DNS rebinding attacks take advantage of this fundamental Web design flaw, breaking the Internet's security policy and converting browsers into open network proxies, said Kaminsky, adding that this ultimately exposes every corporate network. “Corporate firewalls are bypassed via lured browsers.”

One of the contributing issues is people tend to use DNS TTL (Time to Live) - which defines how long records should live before getting discarded - as a security technology, he said, when in fact overriding the TTL can be “quite trivial”.

Considering that in DNS, multiple IP addresses can be transmitted besides the genuine one, it's possible to create a VPN (virtual private network) into a corporation, said Kaminsky.

Kaminsky acknowledged the challenge facing organizations given the wide variety of DNS rebinding mechanisms out there, but he did share some suggestions that might help corporations, including configuring corporate servers to not transmit valuable information back to unrecognizable host systems.

Also, he said, it's useful to perform external to internal routing checks to stop sites on the Internet from routing to internal targets on the corporate Intranet.

Also at SecTor 2007, challenges around corporate database attacks and methods to perform forensic investigation on SQL Server 2005 systems to determine possible data breaches were discussed.

The database has become a critical asset to organizations because of the critical information it holds, like financial, healthcare and human resources data, said Kevvie Fowler, manager of managed security services at Longueuil, Quebec-based healthcare and financial technology provider Emergis Inc. "All this critical stuff that organizations need to share, maintain, process."

Besides that, there is an industry trend toward scaling down to fewer consolidated systems, given the high cost of maintenance of databases, said Fowler.

Given these single mission-critical systems are often targeted by attackers, he said, it's important for organizations to secure and log underlying database transactions upon which to perform forensics.

However, traditional forensic investigations typically exclude the plethora of evidence housed in databases probably because people fear what they don't understand, he said.

Furthermore, most organizations' database servers, said Fowler, are ill-equipped for potential forensic investigations, but there are available methods that can be applied "without the dependency on shiny appliances, logging appliances, or apps."

Internal IT staff can take advantage of certain repositories - like transaction log files and volatile database data files - within the database that contain valuable evidence of potential breaches, he said.

The transaction log files, for instance, he said, aren't so complex to be useful as most people think. Each transaction can have up to 101 different data elements logged, he said. "That's 101 different chances to have critical data that you need to support an investigation that you're working on."

But before collecting this data, organizations should first determine the scope of the investigation and how much information is required to be collected, said Fowler, adding they should factor in the "relativity of the data based on the investigation you're investigating."

[Close Window](#)