

SINGLE FAIL-ON: PREVENTING AN ENTERPRISE MELTDOWN

This paper is written for senior managers alerting them to significant enterprise risk by poorly planning and architecting enterprise single sign on systems.

Copyright, 2003. [Guy Huntington, HVL](#).

HERE'S A SCENARIO

60% or more of your enterprise applications are tied into web application security software providing single sign on. The web security servers come under internal electronic attack and go down. As a result, users cannot access any resource or application protected by the security servers. In effect, most of the enterprise shudders to an electronic halt.

What did that just do to your bottom line, productivity and relationships with your customers, business partners and employees tied into your systems? How much does it cost you for every minute you're down? Is this a sky is falling scenario or, is it realistic?

It's my experience from deploying single sign on and application security systems that the possibility of this happening is a lot higher than it should be. The point of this paper is to alert enterprise executives to the possibility of this happening to your systems and indicate some steps to prevent a catastrophe before it occurs.

SINGLE FAIL-ON

Today's modern enterprise systems are becoming highly integrated as a result of the drive for efficiencies in B2B's, B2C's and intranets. Essentially, enterprises are creating a spider web of interconnectedness between most systems.

Systems that were formerly independent with only a handful of super users, are now becoming routinely accessed by hundreds, thousands or millions of users. The users want a limited number of authentication mechanisms to have to memorize and/or use. The benefits of single sign on then are obvious at the end user level. However, what is maybe not so obvious is the potential single point of enterprise failure being created.

The common point between all these systems, networks and applications is becoming the web based identity management and access control security system. It's the heart of the spider web where all system access threads are essentially connected. If it goes down, it takes down all the other systems making up the system spider web of connectedness. Why?

Each application, web or portal server protected by the web security software will have a security agent on it. The security agent checks to see if the resource or application requested is protected and if so, what are the authentication and authorization requirements to allow access. To do this, the security agent in turn talks to the enterprise security servers to determine authentication and authorization success or failure. If the security agent can't talk to the downed security server(s), no authentication or authorization is provided and hence, no access granted to users. So, if the security servers go down, you potentially have a single point of enterprise failure or what I call "single fail-on".

HOW IT MIGHT HAPPEN

I have seen in my own practice where one of the many different types of enterprise application, web, portal, reverse proxy or network servers, routers or bridges for whatever reason begins to essentially and unwittingly create an internal denial of service attack on the security servers. For example, the server turns rogue and starts bombarding a security server with requests. While the enterprise usually has good firewall protection from external denial of service attacks, the enterprise is usually poorly prepared for attacks originating internally within their networks.

Additionally, what I have also found is that web security vendors usually lack a web security management console that alerts security managers to such an attack or, other major problems in the making before the servers go down. For instance, if the number of authentication requests suddenly climbs by 70-90% when not anticipated or, the number of failed authentications or authorizations suddenly climbs in a given set of seconds, most vendors do not have the tools to alert the security managers to an attack or problem in progress.

Furthermore, when the servers do go down and an effort is being made to diagnose the problem, I've also found that some of the security server audit logs are insufficient, cryptic or poorly documented. The response time to bring up the system is then hampered by the quality of diagnostic tools available.

It's only a matter of time until malicious competitors, inside users or intelligence agencies use this knowledge and purposefully create these kind and other forms of internal attacks on the security servers and related infrastructure such as the LDAP directories to try and bring the enterprise to its electronic knees. It's often not that hard as it should be to gain access to an internal server.

Perhaps a higher risk of going down is just from plain ignorance of how critical infrastructure hardware and software systems is. For example, at a recent university security conference I attended, one system administrator told the story of a water leak occurring in the network room. Water was pouring down onto the servers. One directory server was down. What about the backup directory server? It was located in the same rack underneath the primary server!

Make sure that all mission critical infrastructure hardware is in proper data centers, with fail-over schemes such that the fail-over is in another data center. Don't take it for granted that the directory and security servers are secure. Find out for yourselves. Also make sure the systems are tested so you can sleep easier at night.

APPRAISING THE RISK

A quick check is to write your own script mimicking extensive authentication or authorization requests to the security server and/or LDAP directories to see if you can create a successful internal denial of service attack on your servers. If successful, that should be a strong wake-up call to your system and security managers.

Next, you should ask your web security managers to demonstrate they are monitoring authentication and authorization requests for patterns such as suddenly high levels of authentication/authorization requests and/or failures. They should be able to show you how they determine the levels and conditions to monitor for. Next, they should be able to show you how they set this up. To implement this, the web security software system will have to be parsing the audit logs from the security servers in near real time.

There are many other things to check into. Most enterprises are usually better prepared for preventing physical attacks to the security servers, trying to get at master administrative security system passwords, intercepting passwords and usernames traveling in the clear, etc. There should be a formal risk assessment done to ensure you have properly identified the possible threats and addressed them to the degree you feel comfortable with.

Finally, you need to ask yourself a fundamental question before you architect your web single sign on solution. Does the risk warrant interconnecting the security of all or most of your systems or, should some of them remain independent?

Vendors are quick to tell you how fast you can deploy web single sign on using their products. What is often left unaddressed is the risk of architecting a solution where so many formerly independent systems are now interconnected.

This brief paper is not to infer that you shouldn't trust web security software or its implementation into your enterprise for things such as single sign on. What's important is that you, your staff, the web security vendor and your project consultants have properly addressed the issues raised in this paper. With proper steps, planning and tools, you can ensure your enterprise has the benefits of integrated enterprise application security and not the unwanted results of enterprise single fail on.

USEFUL REFERENCES

[“Single Sign On Underneath The Hood” - What Senior Managers Need To Know - \(pdf\)](#).

This paper covers the areas of planning for a Web Single Sign On project that senior managers should be aware of before starting a project.

[Successfully Managing A WSSO Project - \(pdf\)](#)

Addresses the practical issues of successfully managing a web single sign on project in a heterogeneous environment.

[Five Minute CEO/CIO Briefing on Web Security- \(pdf\)](#)

The first in a series of papers covering web security by Guy Huntington, HVL. This briefing covers seven questions CEO/CIO's should be able to answer to understand web security.

[Reducing Total Cost of Ownership in Web Security- Six Points to Saving Money \(pdf\)](#)

The second in a series of briefings on web security by Guy Huntington, HVL. This briefing is designed to quickly educate senior managers where to look for cost savings in web security deployments.

[Web Security PowerPoint Presentations \(www.hvl.net/ebusiness.htm\)](#):

Put together by Guy Huntington, HVL and Derek Small, [Nulli Secundus](#) from their web security, directory and ERP experiences, these presentations cover general and specific issues in web security, identity management, single sign on, LDAP directories, PeopleSoft LDAP integrations and PeopleSoft Oblix integrations.

[“Secrets and Lies: Digital Security in a Networked World”](#):

Bruce Schneier, CTO of CounterPane and a noted cryptography expert wrote an excellent book covering the issues of digital security. It's a must read for IT managers.

[“SAML” \(Security Assertion Markup Language\)](#):

This is the emerging standard for authentication and authorization. It's being put together by OASIS, the Organization for the Advancement of Structured Information Standards. OASIS is a nonprofit, international consortium that creates interoperable industry specifications based on public standards such as XML and SGML, as well as others that are related to structured information processing.

ABOUT THE AUTHOR

Guy Huntington, President of [HVL](#), recently was the project manager for Boeing's global single sign on initiative. He specializes in leading enterprise re-engineering projects including B2B's, B2C's and intranets integrating web security and LDAP directory infrastructure into the many disparate systems within each enterprise including data warehouses, ERP's, etc. Guy has lead many projects over the years, authored numerous papers, on-line presentations, written an electronic book and given many speeches on the use of the web in business. Guy can be contacted at 604-921-6797 or email guy@hvl.net or www.hvl.net.