

SINGLE FAIL-ON – PREVENTING AN ENTERPRISE MELTDOWN

Here's the 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 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.

The Risk

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 are 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 problem 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.

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 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 back-up 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 wakeup 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.

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 this issue. 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.

About the Author:

Guy Huntington, President of Huntington Ventures Ltd, has many years of experience leading large, complex, Fortune 500 identity projects. His work has included leading Boeing's single sign on, Capital One's single sign on, Capital One's Sarbanes-Oxley provisioning project and Kaiser Permanente's web single sign on review.

He maintains a website on authentication at www.authenticationworld.com . He also maintains an authentication blog available off his website. He can be reached at guy.huntington@authenticationworld.com or by phone at 604-921-6797.