



SECURITY

[LinuxInsider](#) > [Security](#) | [Read Next Article in Security](#)

February 25, 2009 03:15:41 PM

Please note that this material is copyright protected. It is illegal to display or reproduce this article without permission for any commercial purpose, including use as marketing or public relations literature. To obtain reprints of this article for authorized use, please call a sales representative at (818) 461-9700 or visit <http://www.ectnews.com/about/reprints/>.

Superuser Privilege Management: It's Not About Trust



By Tom Kemp
LinuxInsider
02/25/09 4:00 AM PT

[Back to Online Version](#)
[E-Mail Article](#)
[Reprints](#)

The logic bomb episode at Fannie Mae is an illustration of the destruction that's possible when enterprises fail to properly monitor user privileges. IT managers must be aware of who has what privileges and determine the appropriate level of access for all users.

Though "everyone knows" the threat and consequences of insider attacks, it was still shocking to read the headlines that a former Unix engineer at mortgage giant Fannie Mae was charged in federal court with allegedly planting a logic bomb that would have effectively shut down all 4,000 servers at Fannie. The FBI alleges that this logic bomb planted in a script would have "caused millions of dollars of damage and reduced if not shut down operations" for at least one week. And it was "only by chance" that another Unix engineer spotted the logic bomb a week after it was planted and prior to its detonation.

This incident reveals the imperative to implement what IT analysts refer to as "superuser privilege management." The "root" of this potential problem that can have such a catastrophic impact on the operations of an organization lies in the fact that most operating systems, applications and databases have an administrative account to enable installation, configuration and management of those platforms. These administrative accounts are used and shared by multiple personnel (e.g. systems administrators, database administrators, developers, etc.), resulting in the situation whereby multiple people in your organization have the privilege of carrying the proverbial "keys" (i.e. administrative access) to your "kingdom" (i.e. the systems and applications that power your business).

Keep an Eye Out

If IT organizations don't properly manage these privileged people an IT staffer can either accidentally or maliciously compromise or destroy the operations of the business. This is even more critical in today's economy, where a growing number of layoffs [increase](#) the probability

that some of today's superuser "key holders" may not be with your organization tomorrow.

In order to implement a robust set of superuser privilege management processes and technologies you must take the following steps:

- know which users have elevated privileges;
- understand whether or not these privileged users are sharing common accounts;
- determine how much privileged access is appropriate for each superuser and if effective delegation and separation of privilege is in place amongst superusers;
- figure out whether or not a user's access and the corresponding privileges can be completely and immediately removed when a user departs an organization (as opposed to still being an operational "orphaned account");
- enforce accountability and detect potential threats in real time by monitoring and reporting what these users are doing.

The Fannie Mae incident shows what can go wrong if proper superuser privilege management processes and technology are not in place. The FBI Affidavit regarding Fannie Mae reveals that on Oct. 24, 2008, a Unix engineer was terminated between 1 and 1:30 p.m., and was told between 2 and 2:30 pm that all of his equipment (including his laptop) needed to be turned in by the end of the day. He did not turn in his laptop until 4:45 pm and presumably left soon after. After the engineer was terminated, his computer access was still active until late that evening.

This time window gave him the opportunity to try to inflict serious damage when, at 2:53 p.m., he remotely logged into a development [server](#) as the "root" user. He modified a legitimate maintenance script to include some malevolent logic that would run on all of the 4,000 Unix systems that support Fannie's operations. The script itself would run on Jan. 31, 2009 (a weekend, and well after the Unix engineer had left the premises), replace all data on all the systems with zeroes, block access to the servers so other superusers could not stop the script, attempt to destroy all the backup software making recovery more difficult, and then power the servers down.

Potential Disaster

The FBI asserts that this script would have knocked Fannie offline for a week and the remediation would have included "cleaning out and restoring all 4,000" of Fannie's [servers](#) as well as "restoring and securing the automation of mortgages, and restoring all data that was erased." This damage is puny when compared to the devastation of Fannie Mae's reputation if this had happened. A week after this script was planted, another engineer found "by chance" the logic bomb embedded in a standard maintenance script.

Given this stark example of an insider attack, how can organizations avoid a similar situation? Here are some ideas:

- **Don't share privileged accounts.** IT organizations need to break the bad habit of IT staff sharing the Unix root password (which the Fannie Mae Unix engineer had access to) and the passwords to other privileged accounts. People should log in with an account that clearly identifies who the user is. This provides more accountability and makes user actions easier to trace; it also means when an IT staffer is terminated, you don't have change the root password on 4,000 systems.
- **Move to a single directory that spans multiple platforms.** A single directory that can span multiple [operating system](#) platforms (e.g. Unix, Linux, Windows, Mac, etc.) and applications (e.g. [SAP](#) (NYSE: SAP), [Oracle](#) (Nasdaq: ORCL), Apache, etc.) provides the ability to immediately disable a given user's access across the enterprise (i.e. all Unix and Windows systems) from one place. For example, a popular and widely deployed directory such as [Microsoft](#) (Nasdaq: MSFT) Active Directory (which is focused on the Windows platform) combined with third-party "Active Directory bridge" products that tie-in non-Microsoft systems can provide a central identity store. In minutes you can immediately disable a user's accounts across the enterprise, while in the case of Fannie Mae it took over 10 hours to disable the Unix engineer's access. This centralization is essential because access to Unix systems is typically managed locally (i.e. the local /etc/passwd text file), and it may take many hours (if not days) to check and turn off a user's access to 4,000 systems.
- **Implement access control and authorization management technologies to enforce the principle of "least privilege."** Organizations need to limit which users with privileged access can authenticate to which particular systems or groups of systems. They should also ensure users run with as few privileges as possible. For example, the popular sudo utility on Unix can manage and enforce fine-grained control over user access and privileges on their systems.
- **Implement user-level auditing and forensic tools on critical servers.** Just as security cameras are deployed at banks and casinos, software auditing tools can be deployed on mission-critical systems to help IT organizations view who has been accessing what systems, what commands are being executed, and what changes are being made to key files and data. If a forensic tool to capture user-level activity had been deployed at Fannie, the Unix engineer's every keystroke and the actual text of the script he was editing would have been captured. The FBI would then be able to "playback" (like [TiVo](#) (Nasdaq: TIVO) or a VCR) in court the login session in which the Unix engineer created the logic bomb and implanted it in the maintenance script.

Fortunately, this incident at Fannie was prevented, and we hope it will serve as a wake-up call to organizations to make sure they are properly managing who has privileged access to their systems and applications. Given the keys that these personnel hold, a philosophy of "trust but verify" should be implemented that is backed up by a set of superuser privilege management procedures and technologies that enforce the essential protections required. **ECT**

Tom Kemp is CEO of [Centrify](#), a leading provider of Microsoft Active Directory-based auditing, access control and identity management solutions for non-Microsoft platforms.

Social Networking Toolbox: [ShareThis](#)

Next Article in Security:
[1234567890 Day and a Hot Job at Microsoft](#)

Copyright 1998-2009 ECT News Network, [Terms of Service](#) | [Privacy Policy](#) | [How To Advertise](#)
Inc. All Rights Reserved.