

White Paper

Privileged Account Management

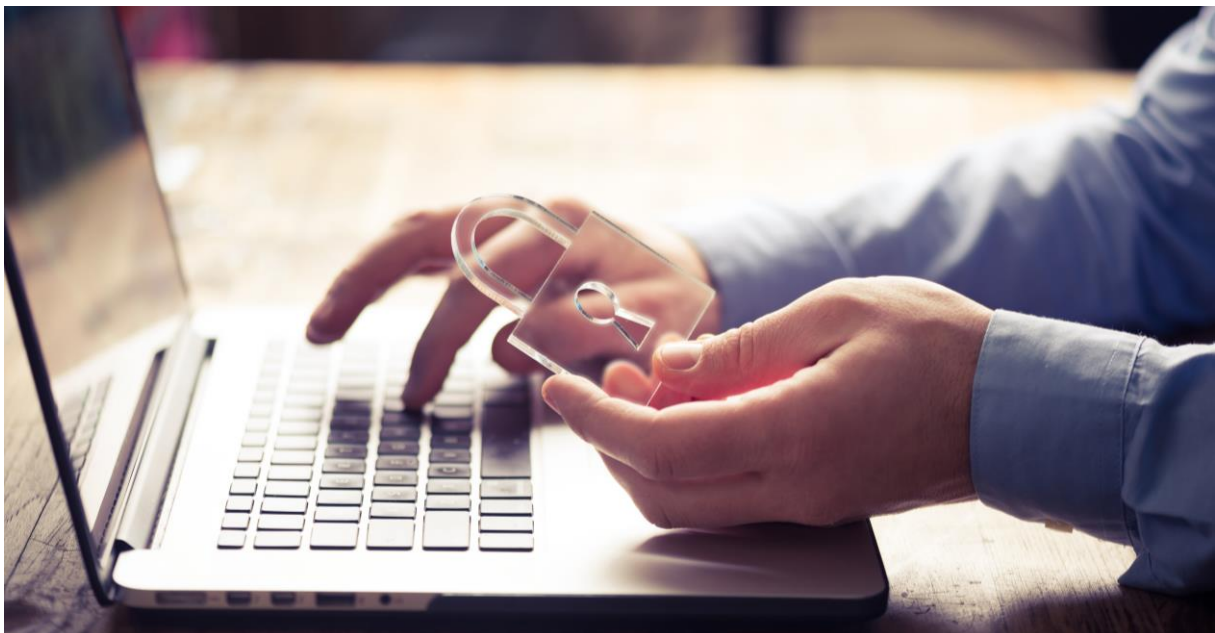
What it is

All computer accounts give the account holder various rights to specific resources or capabilities. Some of these resources may be physical in nature (e.g. folders or files stored on a hard drive), others may be more virtual in scope (e.g. ports or interfaces).

Normal user accounts give the account holder access “to their own stuff”, i.e. their files, their email, their own user data.

When an account gives the user access to other people’s stuff, or to features or capabilities that could cause issues if the feature is abused, then the account should be seen as “privileged”.

Overlaying the concepts of normal and privileged is ‘role’. Most ‘privileged’ accounts are such because the holder of the account represents a role. A Database User Administration role gives the account holder the rights to add or delete database users. Rather than force the employee to have two accounts, however, the role is assigned to the employee’s normal user account, and from then forward that normal account is “privileged” to also be a Database User Administrator.



Folders and files, and applications that can be configured via the file system are usually governed by ‘access control lists’ (ACLs). While ACLs are very useful for file-system protection, they aren’t designed to protect resources or capabilities outside the role of the file system. A file may provide the configuration for a webserver, or it might prevent a user from using a web client, but an ACL will not, generally, prevent a normal user from accessing pages on a website if the client use is granted.

Because privileged accounts are created, coordinated and manipulated based on corporate policy, it may be that a single user account has cross-functional roles that give it greater or lesser access to corporate data, individual personally identifiable information (PII), banking information and so on. And, those roles may be applied or removed from an account over time, and the roles themselves may be created, altered or deleted as time passes.

The process of managing and auditing the rights and responsibilities of a role, with regards to its data access, process control and resource management, as well as to whom they are assigned or retracted, and when, is called **Privileged account management**.

What are the risks?

If a privileged account is compromised, the account can be used to affect changes that might best be described as counterproductive.

If an account has the rights to effect the transfer of funds, and if the account is compromised, then the person using the credentials can embezzle or steal funds, with the blame falling on the employee to whom the credentials belong. If the account has access to the PII of the human resources in the company, sufficient information can be extracted to engage in tax fraud, or could even blackmail employees or the company itself.

And risk is not limited to things that are happening inside the enterprise. If an enterprise builds a computer-controlled "IoT" device, which is then sold to the public, or installed in public areas, it risks having these devices compromised. A hacker, or hacker group, does not care about the individual unit, they want to compromise the entire model run. One way of doing this is to compromise the over-the-air update facility, such that they can convince the deployed devices to accept rogue code as legitimate.

Security and Privileged Account Management

The management of account roles can be simplified using enterprise "Privileged Account Management" or PAM software. Various companies provide methods to define roles, give the roles access to resources based on policies, manage who in the organization will fulfill the roles, and provide full audit capabilities for everything.

In most cases, these packages work on the premise of a single System Key, which is used to protect everything below it. Compromise of the System Key is necessary to take complete control of the PAM, and while this is usually accomplished via compromise of the PAM Manager role, it is also possible to steal the System Key outright if it is stored on a hard-drive someplace.

Preventing exposure or compromise of the PAM system key is a primary requirement for the protection of corporate resources and data.

A much better method is to store the System Key in a NIST FIPS 140-2 certified Hardware Security Module (HSM), such as the Utimaco CryptoServer. Hardware Security Modules are designed to securely store cryptographic keys and other secrets, by

- Allowing for four-eyes (or greater!) requirements for use of the secrets contained,
- Providing policies around (not) allowing the export of secrets (if not permitted, the keys must be used in situ -- input is sent to the HSM, which uses the key and returns just the results. The key never leaves the protection boundary), and
- Providing for physical protection of the secrets (in the event of physical attack, well-designed HSMs will erase the key material, preventing its compromise).

Use of an HSM-protected primary system key should also be protected by policies and procedures, implemented using the HSMs own user management scheme.

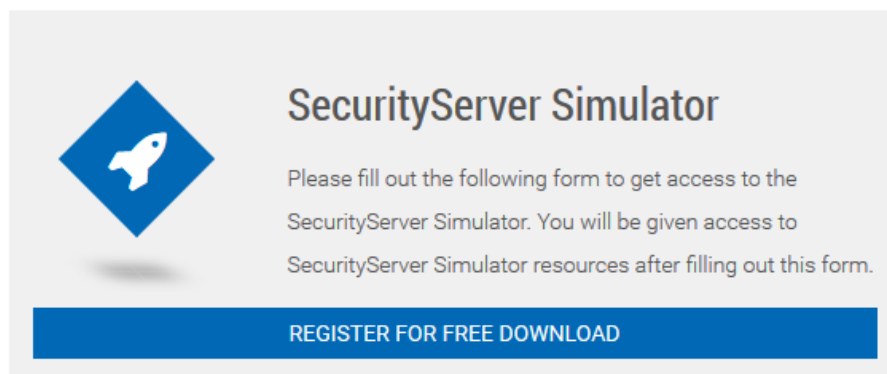
About Utimaco

Utimaco is a leading manufacturer of hardware security modules (HSMs) that provide the Root of Trust to the IoT. We keep cryptographic keys and digital identities safe to protect critical digital infrastructures and high value data assets. Our products enable innovations and support the creation of new business by helping to secure critical business data and transactions. Founded in 1983, Utimaco HSMs today are deployed across more than 80 countries in more than 1,000 installations. Utimaco employs a total of 170 people, with sales offices in Germany, the US, the UK and Singapore. For more information, visit hsm.utimaco.com



Download the Utimaco Software HSM Simulator to get started immediately learning about HSM devices. It is a FREE fully functioning Software version of the Hardware HSM. The download package includes documentation on our product. Here is the link to register for the download.

<https://support.hsm.utimaco.com/hsm-simulator>



The banner features a blue diamond icon with a white rocket ship on the left. To the right, the text reads: "SecurityServer Simulator", "Please fill out the following form to get access to the SecurityServer Simulator. You will be given access to SecurityServer Simulator resources after filling out this form.", and a blue button with the text "REGISTER FOR FREE DOWNLOAD".

The Simulator download includes tools for creating user accounts, sample code and libraries for PKCS#11 Microsoft CNG, Java JCE and the Utimaco CXI API to link and test your code. The Simulator will run on a Windows or Linux platform. This is your opportunity to try out the Utimaco HSM technology easily and without initial cost.