User credentials to access web based applications is well known by the public and are composed of a UserID/Password combination. Enterprise IT organizations will require frequent/regular password updates from users as well as a complexity that lessens the possibility of someone getting the password by guessing or unauthorized access (a.k.a. hacking) into the Enterprise accounts.

Certain web applications utilize external web services to deliver the intended service. These web services are provided by other organizations which specialize in the information or service required by the application. These external web services also have credentials composed of an ApplicationName/Password combination. However, these credentials are not user based but application based and are managed in a similar manner as User credentials. These credentials are also important to change since unauthorized access to the web service can result in:

- Unauthorized access to web services
- Lost revenue by the web service
- Unwanted charges to the enterprise application
- Unwanted network traffic resulting in application latency and cost
- Unauthorized access to sensitive web services

Application service code is usually written in programming languages such as C, C++, Python (Shaw 2014), Java and Ruby and access to external web services using RESTful APIs (Vaqqas 2014). Updating the password of a web service is more complex than those used for humans in that the change requires a modification of the application code (a.k.a. software).

Changes to application software requires a complex process of change, testing and deployment by the application developers and their IT organizations as well as a coordination with the IT organizations of the web service.

A solution to enforcing and updating the credentials of the application server was designed and resulted in US Patent 9,154,482, Secure Access Credential Updating (Dudziak 2015).

An email notification along with a change identifier token is sent to the administrators of the application requiring a password change within a certain time period. The token identifies any attempt to change the password as that coming from the authorized user and will expire after a predetermined time period. Using the token the application developers can make the change to their code within their internal change, testing and deployment process. If any issues are encountered the original password can be restored and the change process can be repeated until it is working properly with the new password.

**Technical Term Definitions**

- **RESTful APIs** - Application Programming Interfaces that allow programmers to access complex, specialized services provided by companies that specialize in certain kinds of information. Some examples of Network based APIs include census data, marketing data, image recognition, media uploading and downloading (Flickr), voice mail access, voice to text services and location based information. Network APIs are used by web, mobile and platform based software developers and allow them to develop applications faster than if they had to create the services themselves.

- **RESTful APIs** are a software architectural style that allows both simple and complex web services and information to be accessed and manipulated using HTTP. HTTP or HyperText Transfer Protocol is the most commonly used over the Internet to enable web pages to be created on a mobile device or computer using web browsers. However, RESTful APIs are normally relegated to server based software applications due to the security issues with accessing them.

**Conclusion**

A means of updating application credentials for using Network based APIs was discussed. The design allows notification of the need to update the credentials to the application developers as well as allows the change to be made asynchronously with their internal software development change process.

The design resulted in US Patent 9,154,482 titled Secure Access Credential Updating. This patent was issued in less than 2 years illustrating the scarcity of Network Security Intellectual Property within the patent system.

The importance of having the credentials changed on a regular basis is to lessen the possibility of the following from occurring:

- Unauthorized access to web services
- Lost revenue by the web service
- Unwanted charges to the enterprise application
- Unwanted network traffic resulting in increased application server latency
- Unwanted network traffic resulting in increased application server cost
- Unauthorized access to sensitive web services

**Literature Cited**


**Acknowledgements**

Paul Schultz, PhD, Distinguished Member Technical Staff, Verizon, Co-Inventor

Robert Sartini, Distinguished Member Technical Staff, Verizon, Co-Inventor

David O’Neil, J.D., Assistant General Counsel, Verizon Communications, Patent Attorney