Contribution ID: **44** Type: **Oral Presentation**

Smooth migration of a feature-rich vulnerability analysis engine within a security portal for users with divergent skill levels

Thursday, 4 April 2019 14:30 (30 minutes)

Vulnerability management is useful for maintaining security with keeping the flexibility of the network environment, especially for the DMZ network that allows connections from the Internet.
We have been operating a vulnerability management portal site named DMZ User's Portal for 13 years.
In KEK, all of the host administrators in DMZ network (DMZ admin) have their own accounts for the portal site, and they can manage the vulnerabilities by themselves.
Moreover, the portal site was also adopted to other two sites with different operation policy, and they are also now in operation.

In DMZ User's Portal, we have adopted the same series of vulnerability analysis engine which has many advantages, and it has offered a lot of benefits to us for 13 years.
Now, all of DMZ admins came to deal with the serious vulnerabilities detected by the engine promptly.
On the other hand, the inspection performance of the engine gradually came to be degraded.
Now, we decided to replace the engine into a more powerful and complex one.

In the replacement, it is desirable to continue the successful experiences and contributions within the portal site.
One of the important contributions covers divergent skill levels among DMZ admins in KEK, by simplification of the intricate usage of the vulnerability analysis engine that is designed for network security experts.
The other is that the portal site has accumulated a lot of know-how gained from the operation of the portal site that includes user-response of DMZ admins.
It is a difficult task to continue these contributions of the portal site when replacing the vulnerability analysis engine, without the design and development of the modules carefully in advance.

This talk presents the design and methods for smooth migration of a feature-rich vulnerability analysis engine within the security portal site mentioned above.
The key point is that module dependency has been carefully considered among essential functions of vulnerability analysis engine, web interface, email notifier, and database.
To achieve the lower degree of module dependency, the techniques of O/R mapping, code generation, wrapper architecture, template engine consolidation, and test case were leveraged.
The combinational use of these techniques brought not only modularity but also maintainability to the modules for the essential functions above.
Consequently, it enabled us to replace the vulnerability analysis engine with minor modifications of user interfaces within web and email.
In this way, we can continue to operate the portal site with inheriting the successful experiences, along with gaining the benefits of a new powerful vulnerability analysis engine.

Primary author: Dr MURAKAMI, Tadashi (High Energy Accelerator Research Organization (KEK))

Presenter: Dr MURAKAMI, Tadashi (High Energy Accelerator Research Organization (KEK))

Session Classification: Networking, Security, Infrastructure & Operations

Track Classification: Network, Security, Infrastructure & Operations