第 10 回 IT ソフトウェア翻訳士認定試験

＜1 次試験＞　4 月 18（日）10：00～15：00

問題 1・2 の両方について解答のこと。選択ではありません。

＜問題 1＞　全文を訳して提出してください。

There are a number of ways to build a system to host multiple applications and servers on a shared machine. Perhaps the simplest is to deploy one or more hosts running a standard operating system such as Linux or Windows, and then to allow users to install files and start processes — protection between applications being provided by conventional OS techniques. Experience shows that system administration can quickly become a time-consuming task due to complex configuration interactions between supposedly disjoint applications.

More importantly, such systems do not adequately support performance isolation; the scheduling priority, memory demand, network traffic and disk accesses of one process impact the performance of others. This may be acceptable when there is adequate provisioning and a closed user group (such as in the case of computational grids, or the experimental ABC platform), but not when resources are oversubscribed, or users uncooperative.

One way to address this problem is to retrofit support for performance isolation to the operating system. This has been demonstrated to a greater or lesser degree with resource containers, Linux/RK, QLinux and SILK. One difficulty with such approaches is ensuring that all resource usage is accounted to the correct process — consider, for example, the complex interactions between applications due to buffer cache or page replacement algorithms. This is effectively the problem of “QoS crosstalk”within the operating system. Performing multiplexing at a low level can mitigate this problem, as demonstrated by the Exokernel and Nemesis operating systems. Unintentional or undesired interactions between tasks are minimized.

＜問題 2＞　全文を訳して提出してください。

New zero-day involves IE, puts Windows XP users at risk

Microsoft investigates unpatched flaw that affects users running IE7 and IE8

Microsoft on Sunday confirmed it's investigating an unpatched bug in VBScript that hackers could exploit to plant malware on Windows XP machines running Internet Explorer (IE).

The flaw could be used by attackers to inject malicious code onto victims' PCs, said Samuel Radek, the Polish security analyst with iSEC Security Research who revealed the vulnerability and posted attack code on Friday.

Users running IE7 or the newer IE8 are at risk, said Radek.

Microsoft noted it's already on the case. "Microsoft is investigating new public claims of a vulnerability involving the use of VBScript and Windows Help files within Internet Explorer," said, a Jeffrey Johnson senior manager with the Microsoft Security Response Center (MSRC), in an e-mail Sunday. The current state of our investigations shows that Windows Vista, Windows 7, Windows Server 2008, and Windows Server 2008 R2, are not affected."

Johnson added that Microsoft has not yet seen any evidence of attacks exploiting the vulnerability.

Radek called the bug a "logic flaw," and said attackers could exploit it by feeding users malicious code disguised as a Windows help file -- such files have a ".hlp" extension -- then convincing them to press the F1 key when a pop-up appeared. He rated the vulnerability as "medium" because of the required user interaction.

"First an attacker needs to force a victim to visit a malicious Web page," Radek said in an e-mail Sunday. "The victim must be using Windows XP and Internet Explorer. A bit of social engineering is required to persuade the victim to push F1 button when a VBScript pop-up is displayed."