Operating systems homework/assignment #7

18. Give one case where a translated code can be faster than the original code in a system using binary translation

A translated code can be faster than the original code if the binary translation system performs optimization during the translation process. For instance a dynamic binary translator might recognise frequently executed code blocks and apply performance improvements or optimizations; one example is instruction reordering eliminating redundant operations or inlining function calls. This often leads to fewer instructions executed or more efficient CPU usage compared to the original non improved binary. As a result the translated version may ran faster especially in performance critical sections or blocks.

24. One way to handle guest operating systems that change their page tables using ordinary (nonprivileged) instructions is to mark the page tables as read only and take a trap when they are modified. How else could the shadow page tables be maintained? Discuss the efficiency of your approach versus the read-only page tables.

A different type of approach is to use instruction trapping and emulation, where the hypervisor intercepts a number of specific instructions that the guest OS uses to modify its page tables. Instead of marking the page tables as read only and relying on hardware traps when they are written to, the hypervisor monitors and interprets updates to the guest's page tables directly, using binary translation or virtualization extensions.

This method can be more efficient overall than using read only traps in environments where page table writes are common. By avoiding a full trap and context switch each time, the system reduces computational overhead. However, this comes at the cost of added complexity in the hypervisor, which will now need to handle instruction interpretation. More often than not the best method will often depend on the given workload: frequent writes benefit from emulation, while infrequent updates may still perform well with the read-only trap method.

34. Migrating virtual machines may be easier than migrating processes, but migration can still be difficult. What problems can arise when migrating a virtual machine?

Migrating a virtual machine VM involves transferring an entire software stack including the operating system, applications, and associated memory states etc…. to a different physical or virtual host. While this can be more simple than migrating individual processes (because you do not need to rebuild process states from scratch) significant problems will still remain. One notable issue is data consistency. During a live migration, active memory pages and I/O buffers will be copied over carefully to ensure that no data is lost or corrupted. If the VM runs a database or has large in memory data structures. synchronizing those resources can become complex and time-consuming.

40. We have seen that hypervisor-based virtual machines provide better isolation than containers. This is clearly an advantage from a security point of view. However, can you thnk of any security advantages that containers might have over virtual machines?

Some security advantages that containers have over VMs are that containers usually have a smaller runtime footprint, so they have fewer system components and libraries that can be taken advantage of this more cut approach means the general attack surface is reduced: a container often includes just the application code and minimal OS level dependencies, whereas a full virtual machine carries a complete OS stack.

Another security advantage is that containers have the benefit of a rapid deployment and patching model. It is relatively easy to rebuild container images and deploy them to production servers when security updates become available. In contrast doing that with the more time-intensive process of patching and updating a full guest OS for a VM. Although not as foolproof as a fully separate kernel, these container tools can limit the damage caused by a compromised container offering a layer of security that is quick to implement and manage.