Friday, February 8. 2008

Less known Solaris Features: Signed binaries

One of problems in computer security is the validation of binaries: Is this the original binary or is it a counterfeit binary? Since Solaris 10 Sun electronically signs the binaries of the Solaris Operating Environment. You can check the signature of the binaries with the elf-sign tool.[root@gandalf:/etc]$ elfsign verify -v /usr/sbin/ifconfig
elfsign: verification of /usr/sbin/ifconfig passed.
format: rsa_md5_sha1.
signer: CN=SunOS 5.10, OU=Solaris Signed Execution, O=Sun Microsystems Inc.Obviously you have to trust the elfsign. But you can check it, when you boot the system from a trusted media (like a original media kit or a checksum validated iso-image. This enables you to check the signature of the elfsign independently from the system.

By the way: This certificate and the signature is very important for crypto modules. The crypto framework of solaris just loads modules signed by Sun to prevent the usage of malicious modules (for example to read out the key store and send it somewhere) into the framework.

Posted by Joerg Moellenkamp in English at 11:23