Chapter 7

Addressing Evil Maid Attacks

Originally the term Evil Maid Attack [11] was used to describe attacks on the full disk encryption schemes. In such scenarios the attacker (the Evil Maid) was replacing or infecting part of the code which was asking the user for the disk decryption passphrase. Once the passphrase was obtained from the unsuspecting user (who thought they provided it to the legitimate system software), the malicious code could have store it somewhere (e.g. save on unused disk sectors), or leak through networking, allowing the attacker to decrypt the laptop once the attacker somehow got access to it subsequently (e.g. after physically stealing it from the user, or perhaps covertly making a copy of the hard disk).

But the old Evil Maid Attack concept can be easily generalized and applied to the stateless laptop scenario. Now the Evil Maid would be replacing the whole laptop, rather than just the software on it (because there is no software to be replaced on the laptop in this case, of course). The new, fake, laptop would look identical to the user from the outside, but might be a completely different machine on the inside. E.g. it might be full of persistent memory, and also feature an army of wireless devices to leak all the user secrets to everybody in a radius of miles.

A special case of such an Evil Maid attack would be when the laptop was replaced during shipment, or simply if the vendor of the laptop turned out to be (or was forced to be) malicious.

What could we do about such attacks?

First, we should stress the primary reason behind introducing the stateless laptop idea is *not* to prevent sophisticated physical attacks, such as "full" Evil Maid attacks which replace the whole laptop with an identically-looking one.

Having said that, the author is of the opinion that the stateless laptop design