Analysis of Pin and TPM for Microsoft Laptops

Example Policy Brief, September 2015

Marshall Kuypers (mkuypers@stanford.edu) and Elisabeth Pate-Cornell (mep@stanford.edu)

COMPANY X uses full disk encryption (FDE) to secure information on all of its devices. However, certain FDE implementations are still vulnerable to a small group of advanced attackers. Tradeoffs need to be made to balance security and usability to ensure the success of COMPANY X employees while safeguarding their information.

COMPANY X is considering different implementations of FDE solutions for laptops running a Microsoft OS.[1] There are two alternatives under consideration:

1. **Implement Pin[2] + TPM on laptops.**
   Under this alternative, a user will be prompted for a Pin before the computer boots. Once the user authenticates, they will be prompted for the OS password to gain access to the computer. This authentication scheme is very strong, but is slightly disruptive because users may need two credentials instead of one to access their device.
2. **Implement TPM only on laptops.**
   Under this alternative, the user is prompted only for the OS password. The information on the device is still fully encrypted, but the device becomes vulnerable to a small set of attacks. For example, if an attacker can exploit a vulnerability in a service that boots before the OS password prompt, a skilled attacker could possibly gain access to the data on the device.

It is important to note that both alternatives protect devices from the vast majority of cyber attackers. The decision should therefore be framed as weighing the user's additional cost for using Pin + TPM versus the added security against an advanced attacker. Further, this decision centers on what security procedures result in a sufficiently low probability of exploitation. For example, even Pin + TPM could be broken by a persistent attacker by monitoring an employee as they enter their passwords in a public space, brute forcing the login, or by kidnapping the employee to elicit the password. However, these scenarios are of sufficiently low probability that organizations accept these risks. Here, we assess the probability an attacker compromises information given devices use TMP only to determine the additional risk of this policy.

Quantitative Analysis

[1] OS X has a native FDE implantation called FileVault 2, which integrates pre-boot authentication into user login. Therefore, COMPANY X is concerned with only with Microsoft devices here.

[2] The term 'pin' is used to denote the pre-boot authentication credential. This credential can still incorporate numbers, letters, and symbols.

COMPANY X has good situational awareness about device type, information distributions, and lost device rates. First, it is important to note that roughly 50% of laptops at COMPANY X use a Microsoft OS, meaning that the decision is only relevant to half of the organization's devices. Of these devices, we estimate that 20% have sensitive data.[3] Lost laptops occur rarely at COMPANY X, at an average rate of around 20 devices per year. This translates into roughly a 0.4% probability that a given laptop is lost in a one year timeframe.[4]

Pin + TPM are consistent with industry best practices for securing information. Currently, there is little guidance on the effectiveness of TPM only[5]. Directly comparing Pin + TPM to TPM only can determine how much additional risk is accepted when moving between the policies. Figure 1 shows a decision tree for the two alternatives. The probability of a device being lost in one year is not changed by the alternative chosen.[6] Another important factor is the attacker's ability to obtain a laptop that is shut down or in standby mode versus in sleep mode. Computers in sleep mode are vulnerable to attackers, even if they have Pin + TPM, because the user will not be prompted with pre-boot authentication if a computer is in sleep mode. We estimate that 50% of lost laptops are in the vulnerable 'sleep mode' and 50% are in the secure 'shut down' or 'hibernate' mode.[7]

Significant uncertainty surrounds the issue of sleep mode versus hibernation/ shut down. To our knowledge, NIST has not published a best practice or specified if data on a device with FDE (pre-boot authentication) that is lost while in sleep mode is considered vulnerable and requires a data breach notification. While sleep mode does increase the probability that a sophisticated attacker can obtain information from an encrypted device, we believe that the increased risk is minimal. The decision tree in figure 1 illustrates that roughly 50% of laptops using Pin + TPM have security comparable to TPM only, given the rate of devices in sleep mode.

The last relevant uncertainty is the probably that information is obtained given each scenario. Here, we note that while it is easier for a sophisticated adversary to obtain information if TMP only is implemented, data recovery is still very difficult and requires advanced skills, possibly including access to zero-day vulnerabilities. Further, COMPANY X does not have evidence that laptop theft is a preferred attack

[3] 20% comes from a COMPANY X incident database records lost devices. Historically, roughly 20% of lost devices have sensitive information.

[4] We assume that there are roughly 5,000 laptops at COMPANY X.

[5] NIST SP 800-111 'Guide to Storage Encryption Technologies for End User Devices' (2007) says that authentication after the OS boots is weaker than pre-boot authentication, but does not say more on the subject.

[6] Here, we have made the assumption that persistent adversaries will not begin stealing more laptops if COMPANY X implements TPM only. There are a number of reasons that we believe this is unlikely, which are address later in the paper.

[7] This number is informed by a COMPANY X incident database that records lost devices.

vector for persistent adversaries, and the vast majority of historical lost laptops can be attributed to misplacements or untargeted thefts[8].

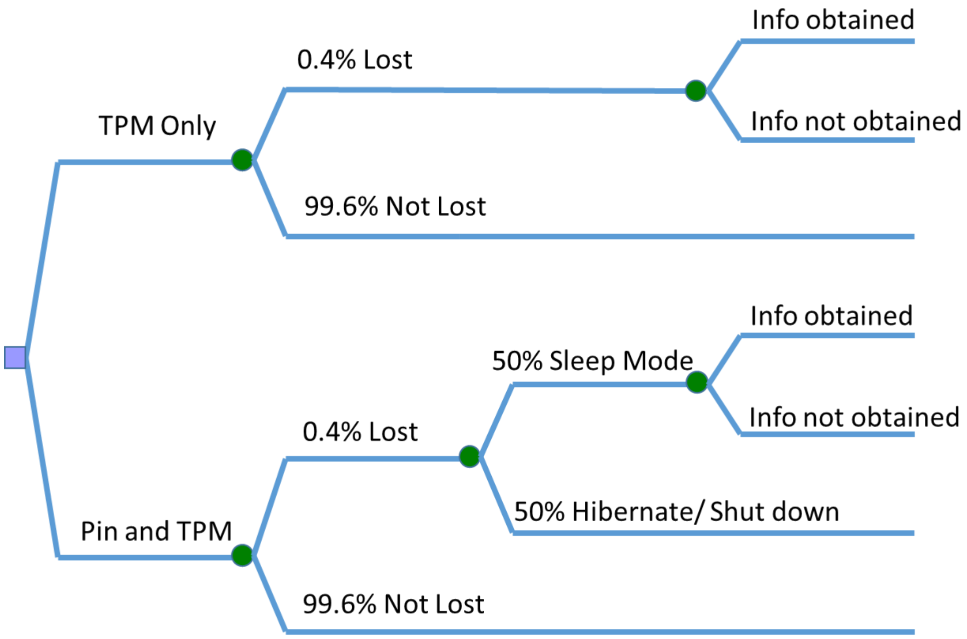

Figure 1: A notional decision tree for TPM only versus Pin + TPM.

The impact of each prospect needs to be evaluated as well. Pin + TPM presents a disruptive user experience, which could lead to an increase in the proportion of devices that are kept in sleep mode.[9] The impact of information being obtained can be compared to historical incidents, but is not discussed here for security reasons.

Other Considerations

COMPANY X does not have evidence that laptop theft is a common attack vector for sophisticated and persistent attackers. First, other attacks including website hacking and phishing have a much lower risk for an adversary, since attackers can remain in their home nation. Further, laptop theft has a very uncertain payoff, since it would be difficult for an attacker to know what devices contain valuable information and which do not a priori. Finally, we simply do not have evidence that targeted laptop thefts have occurred at COMPANY X, while significant evidence exists that adversaries are actively attacking via other vectors (e.g. websites and email).

Conclusion

[8] It is possible that this will change, although COMPANY X assesses that it is unlikely.

[9] Disabling sleep mode is not feasible at COMPANY X, since users may have legitimate reasons to keep a computer in sleep mode, or even 'awake' when a laptop lid is closed. For example, hibernate or shut downs could disrupt data processing and simulations runs.

Overall, COMPANY X assesses the likelihood of data disclosure given a laptop has Pin + TPM or TPM only to be extremely low. Further, we believe that a laptop's state (shut down, sleep, or hibernate) does not significantly change the probability of data disclosure if a laptop is lost. Therefore, COMPANY X does not consider the information on a lost laptop with FDE to be compromised unless evidence exists that the information has been obtained.

Given all of the information available, the risk between the two alternatives is small, primarily because Pin + TPM and TPM only both protect data from the vast majority of attackers. Therefore, taking into account the qualitative features of the decision, including user experience, is advised. The decision should be revisited as standards are updated, but until a more streamlined, user friendly implementation for Microsoft OS is produced, TPM only remains a feasible alternative for COMPANY X.