On the Trust of Trusted Computing in the Post-Snowden Age

Feng Hao

School of Computing Science,
Newcastle University, UK
feng.hao@ncl.ac.uk

Abstract

Revelations in the Snowden case have raised hard questions about the trust of Trusted Computing (TC). When the software is encapsulated within tamper resistant hardware (e.g., TPM) and it is impossible for users to access the internal code, how can we be sure about the integrity of the code (e.g., there is no built-in trap-door)? One may say this question is irrelevant so long as the hardware device is "trusted", which is what the term "Trusted Computing" (subtly) implies. Arguably there appears no incentive for the TPM manufacturers to compromise the security of their own products. But, as revealed in the Snowden documents, a state-funded adversary may have the incentive to coerce manufacturers to add trap-doors, e.g., in order to possess the exclusive power to break a system. Is this a fact or rumour? How can one tell?

In this position paper, I argue that neither of the existing black/white assumptions about TPM (i.e., complete trust or total distrust) is adequate in capturing realistic requirements. Instead, I propose a third assumption that sits in between: namely, "trust-but-verify". Based on this new assumption, many of the existing TPM APIs need to be re-designed to allow public verification of the integrity of the internal software without having to access its source code. The essence of this proposal is consistent with the "software independence" principle, which was first proposed by Ron Rivest to address a similar trust crisis on e-voting systems. Here, we extend the same principle to the research on API security. As a concrete example, I will explain how to apply the trust-but-verify principle to design a TPM-based secure data storage and erasure system (based on [1]). This is however only a small step in a long journey towards addressing many trust issues about TPM (and TC in general) in the post-Snowden age when the threat from state-funded adversaries needs to be accounted.

References

[1] Feng Hao, Dylan Clarke, Avelino Zorzo, "Deleting Secret Data with Public Verifiability," accepted by IEEE Transactions on Dependable and Secure Computing, In press, 2015. Available at http://eprint.iacr.org/2014/364.pdf.