DOCKETED	
Docket Number:	14-AAER-02
Project Title:	Computer, Computer Monitors, and Electronic Displays
TN #:	206315
Document Title:	Information Technology Industry Council Comments: ITI & Technet Comments: Security Features Appendix
Description:	N/A
Filer:	System
Organization:	Chris Hankin/Information Technology Industry Council
Submitter Role:	Public
Submission Date:	10/9/2015 8:08:10 AM
Docketed Date:	10/9/2015

ITI & Technet Comments: Security Features Appendix

Additional submitted attachment is included below.

CEC Draft Computer Standards (Docket #14-AAER-2)

2014 Appliance Efficiency Pre-Rulemaking

ITI/TechNet Comments on Aggios Security Features paper, Appendix B of the CA IOUs and NRDC August 2015 CASE Response

Date: October 9, 2015

Authors.

The Information Technology Industry Council ("ITI"; http://www.itic.org) and the Technology Network ("TechNet"; http://www.technet.org).

The contacts for our organizations are: Christopher Hankin, 202-626-5753, chankin@itic.org and Andrea Deveau, (805) 234-5481, adeveau@technet.org

Comments on Appendix B, "Power Requirements of Security Features in Business Desktop Computers", included with the

CA IOUs and NRDC August CASE Response

<u>Discussion.</u>

ITI and Technet have a number of concerns with the Paper and its initial findings. These include the following:

1. The authors seem to assume that evaluation of vPro /AMT and TPM BIOS and software features on one assembled system and 2 unidentified systems is an adequate evaluation of energy demands of security features in PC products worldwide.

2. The authors mistakenly assume that configured vs. not configured are sufficient system changes to determine/measure the energy consumption related to AMT/ vPro. Their analysis is based upon the mistaken conjecture that the changes being made between tests will yield power measurements indicative of the energy consumption of these hardware features in the platform.
    a. The power adder for this feature can only be determined by comparing one system with power applied to the feature vs. the same or an identical system without power applied to the feature. Not configured vs. "configured with nothing to do" effectively leave the AMT/ vPro controller in states with very similar energy use. The device will consume virtually the same power in both tests.
    b. As a result, the authors effectively compared a system with vPro to a system with vPro and determined that vPro does not contribute to energy consumption.

3. The authors state, "Another technology that all vPro-enabled PCs offer is TPM (Trusted Platform Module), enabling hardware-accelerated encryption and decryption as well as secure key storage."
    a. This conclusion cannot be reached unless the authors have conducted an exhaustive evaluation of PC's in the market to determine if there is a match between vPro and TPM. If such an evaluation has been completed, we ask that it be shared.

4. Within the measurement results section of the paper, the authors state: "When conducting the same power measurements after configuring AMT remote management we obtained the same measurement results in the idle states. We did however observe a slight increase in power consumption (1.05W vs 0.65W) in the

OFF-state, when AMT was enabled and configured, compared to when AMT was disabled in the BIOS."

    a. While in the conclusions section the authors state: "Similarly, the presence of remote management functionality should only have minimal impacts on power draw in the idle modes, considering that even without AMT an active network connection is already accounted for in the short-idle and long-idle states. Even if AMT does require a dedicated management and control processor to be running at all times, such small processors typically have very low power requirements (below 100mW)."

    b. The authors provide measured data that the AC power contribution for vPRO/AMT is at least 400mw yet state the contribution will be less than 100mW in the conclusion in spite of their own measured data to the contrary. Some systems are designed such that the vPro/AMT engine does not receive power in the sleep and or off modes unless it has been configured and enabled in the BIOS. The delta being measured is due to the energy consumption of the vPRO/AMT controller being powered vs. not powered. The above measured data is conclusive evidence that a powered vPro/AMT engine consumes at least enough power to cause a 400mW delta at the power cord when powered vs. not powered.

5. In the conclusions section the authors state: "Our preliminary observations presented above seem to be in contrast with the position taken by ITI in their response to the CEC Staff Report (2015). It would be helpful if ITI would additionally quantify the impact of security/manageability features on desktop idle power draw and provide information on the devices tested and the measurement setup and procedures followed."

    a. The ITI/Technet submission identified a lack of consideration of critical end user features in the CEC Staff Draft and did not identify the appropriate power levels for any given subset of those features. The Staff Draft stated that idle power adders are not necessary for any features. ITI/Technet identified security capabilities as critical customer required features that definitely have an idle power impact greater than zero as even the poorly designed experiments carried out in the paper show.

    b. At the F2F in Folsom on June 10th, industry demonstrated two micro form factor systems: one with no security features having an idle power of 9W; and, one with vPRO/AMT, a TPM and a discrete hardware encryption engine with an idle power of ~12W. Detailed system information was provided, and is linked below. Both systems were operating, instrumented for power measurements and available for inspection at the June 10th meeting. Purchase information and detailed specifications for the two systems can be found at the following web links:

      • The baseline system was the Dell 3020 Micro available here:

        o http://www.dell.com/us/business/p/optiplex-3020m-desktop/pd?oc=sso3020mw7p0023&model_id=optiplex-3020m-desktop

      • The high security system was the Dell 9020 Micro available here:

- http://www.dell.com/us/business/p/optiplex-9020m-desktop/pd?ref=PD_OC
   c. It would be helpful if the authors followed their own request for adequate information by providing sufficient information for someone to duplicate the tests they performed. Two of the systems are not identified other than a limited set of system configuration data. The built configuration identifies the motherboard but ignores other key elements such as chassis and fan. None of the actual measurements are provided. No before and after measurements are provided and the only useful information regarding the actual delta in measurements do not identify which system exhibited the delta.

Conclusion.

Based upon the power measurements in this paper and the June 10th demos provided by industry, it is clear that vPRO/AMT and TPM have at least a 400mW adder at the power cord and these in combination with a discrete encryption engine would require at least 3W at the power cord.