Advanced Intrusion Detection

Peter Liao  
Hewlett Packard Enterprise

Eason Chen  
Hewlett Packard Enterprise

Geoffrey Sun  
Hewlett Packard Enterprise

Mealy Cheng  
Hewlett Packard Enterprise

Chuan-Yu Lin  
Hewlett Packard Enterprise

Follow this and additional works at: http://www.tdcommons.org/dpubs_series

Recommended Citation
Liao, Peter; Chen, Eason; Sun, Geoffrey; Cheng, Mealy; and Lin, Chuan-Yu, "Advanced Intrusion Detection", Technical Disclosure Commons, (August 16, 2017)  
http://www.tdcommons.org/dpubs_series/624

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.
Advanced Intrusion Detection

An Advanced Intrusion Detection (AID) feature provides improvements and flexibility on existing chassis intrusion designs, while reducing component costs, and software development efforts.

Chassis Intrusion Detection is a feature on server and PC systems used to detect if a system’s chassis cover has been opened or improperly closed. This feature can notify users of events, such as if an unauthorized user has tampered with the system, or if a user has insufficiently or forgotten to re-attach the cover of the system, which may eventually cause a thermal overheating event. While this feature is easy to implement, it adds an additional cost burden to the system’s overall cost, regardless if it is used or not (in an age where declining sales margins makes every cost adder an additional burden). The design may also need to be modified based on the physical characteristics of different systems, further compounding costs to implement it. Additionally, due to simplicity of the switch design, a user with familiarity of the system could easily employ methods to bypass it, or if the switch were to fail, the feature would not work as designed.

The left diagram of Figure 1 shows one of the many typical circuit designs to implement the chassis intrusion feature. A switch is used to detect the physical event of a chassis cover being open. When there is a change in state, a signal is outputted to the system chipset and a programmable FPGA or BMC which logs the event. Whether or not the chassis intrusion feature is implemented, the circuit adds cost to the total material cost. Different physical dimensions of each system may also require the use of different switch types for each system, which further compounds the development costs to implement the chassis intrusion feature on all system types.

Machine Learning is a sub-field of Computer Science maintaining big utilization growth in software programming. Through machine learning, a system gains the ability to recognize patterns and analyze statistical data to modify its own programming in order to recognize stimuli and return a desired response. Through the implementation of Supervised Machine Learning, presented below is an Advanced Intrusion Detection (AID) feature that can cut costs of physical electronic circuits and components, while also reducing software development efforts in implementing the AID to any system type. The right portion shows how the physical Intrusion Detection subsystem can be simplified with the utilization of Machine Learning.

The flowchart in Figure 2 shows the software flow for the Intrusion Detection feature when Machine Learning programming is implemented in the programmable microcontroller/FPGA chip. Instead of using a physical switch to indicate the chassis intrusion event, the controller recognizes other stimuli. In this case, the stimulus is the change in internal chassis temperature when a cover is removed and air is no longer confined to a closed space.
Figure 3 shows how Supervised Learning is utilized to train the microcontroller to recognize stimuli indicating that a Chassis Intrusion event has occurred. In Supervised Learning, a computer is presented with example inputs and desired outputs, with the goal of the Machine Learning algorithm to create a general rule mapping inputs to outputs. The controller is presented with a series of cases of sample events where the chassis cover is removed. When the cover is removed, sensors indicate temperature changes, and the algorithms for determining fan speeds will also cause the fans to spin at a higher rate, which serves as an example input. When the system is provided with a sample size of inputs, the desired output, a Chassis Intrusion event, is selected by the user as the output to be generated.

1. Cost adder on mechanical and hardware design.
2. SW implementation needed.

Figure 1
Implementing the Advanced Intrusion Detection over a traditional chassis intrusion provides the following benefits:
a. Cost savings from physical circuit components reduction.
b. Cost savings in material costs of electrical traces reduction.
c. Software development cost reduction. A basic Machine Learning code can be utilized on all system types despite differences in thermal detection and fan spin thermal algorithms. The existing Chassis Intrusion design requires custom programming for each distinct system.
d. Circuit Design can be leveraged on all system types despite differences in physical characteristics. Current designs require different switch types for each system, and potential costly modifications to a mechanical chassis.
e. No additional cost burden on systems not requiring a chassis intrusion feature
f. Design is not dependent on a switch, so it will not fail to function when switch fails or when unauthorized users physically depress the switch.

Disclosed by Peter Liao, Eason Chen, Geoffrey Sun, Mealy Cheng and Chuan-Yu Lin, Hewlett Packard Enterprise