Optical Tamper Detection Technology Leaves Criminals in the Dark

Ahsan Javed, Silicon Laboratories, www.silabs.com

The Rising Threat of Public Access Terminal Tampering

On June 3, 2011, three men in their early 20s were arrested in Derbyshire, England, on suspicion of tampering with a co-op cash machine by taking money before it actually reached the external cash tray.[1] On August 4, 2011, Alin Zele, an Irish youth, was charged with three instances of tampering with ATM machines to steal money from high-traffic ATMs [2] On May 12, 2011, five debit card pin pads were tampered with at a Lynnwood, Washington, department store with the intention of stealing customer pin information. This was one of 90 reported tampering incidents for the nationwide chain, resulting in all of the department store pin pads being replaced at all U.S. locations.[3]

Figure 1. ATM machine card readers are key targets for intrusion.

Illegal tampering and sabotage have plagued public access terminals or interactive kiosks for many years. The word “sabotage” has been around for more than a century. During a French railway strike in 1910, striking workers brought railways to a halt by knocking out wooden shoes call sabots that held the rails in place, hence sabotage.

Over the last few decades, there has been a dramatic rise in the number of tampering cases for electro-mechanical systems such as ATMs (as shown in Figure 1), electronic voting machines, vending machines and casino slot machines. While these systems contain sophisticated security software and anti-corruption countermeasures, the physical chassis and systems remain vulnerable to tampering. These vulnerabilities are being exploited widely, and as “hacking” instructions proliferate over the internet, incidents of tampering and theft are sure to rise. A simple web search reveals hundreds of pages dedicated to ATM skimming, slot machine cheats and voting machine vulnerabilities. Electronic system hacking has mushroomed into a very serious problem causing significant monetary losses to large corporations. In developing countries such as India, utility meter hacking is on the rise, becoming a large source of lost revenue for local and provincial governments.

Overview of Anti-Tampering Technology

Efforts to thwart criminal activities have given rise to a growing industry devoted to tamper detection and prevention. Microcontroller (MCU) suppliers already offer secure system MCUs with cryptography-enabled memory access to prevent malicious code from being programmed into systems. Physical enclosures and chassis are also secured by complex and proprietary locks, mechanical tamper detection systems and even optical systems such as lasers. One tamper detection patent for a utility meter cites a “plurality of tampering sensors sensing tilt, electric field, magnetic field, temperature, sound, reverse rotation of a moving element, and excessive difference between metered consumption and an approximate actual consumption.”[4]

Casino slot machines are among the most secure systems in the world, equipped with multiple safeguards to prevent intrusion and tampering. A key element to having a secure but flexible system is allowing routine maintenance while safeguarding vital system components from unwanted access. The control processor of modern electronic slot machines will not power up if there has been any unauthorized access to the system memory or modifications to the hardware. In addition, various keys are required to access different areas of the slot machine, and different personnel carry these access keys, thereby distributing the risk of complete system access. Slot machines are generally networked and can generate a system-wide alarm if any tampering is detected. Finally, casinos have deployed a plethora of visual surveillance systems around slot machines to confirm that only authorized access is taking place. The hierarchy of slot machine security can be abstracted to apply to any secure system as shown in Figure 2.

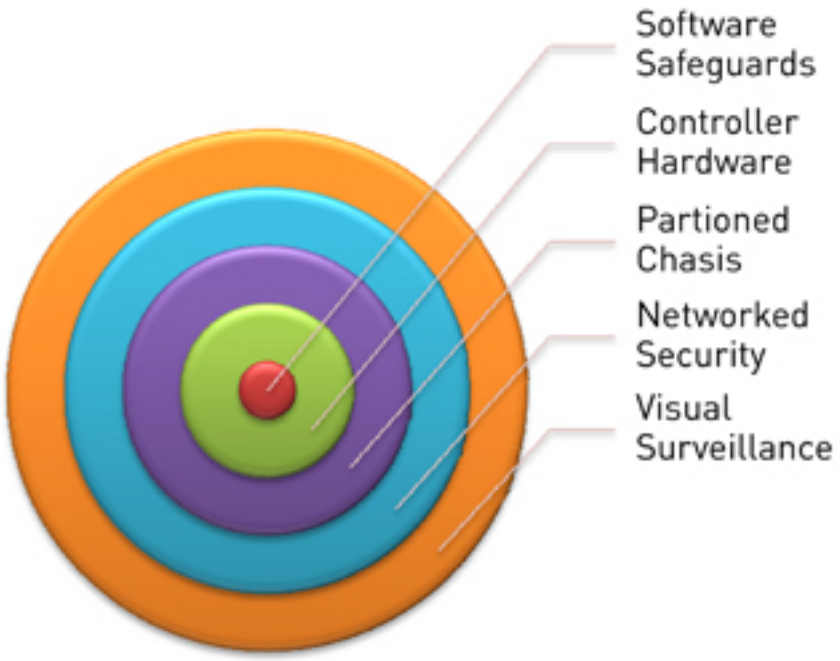

Figure 2. Hierarchy of system security.

Environmental Awareness

Infrared (IR) proximity-based tamper detection circuits offer another layer of

protection for electronic systems, in addition to various existing security methods available today. Proximity sensing enables environmental awareness that can notify a system administrator if physical tampering has occurred, providing the number of times a portion of the chassis has been accessed as well as time-stamps. This additional layer of protection can especially help systems that do not have networked security or visual surveillance such as remote ATMs or vending machines. The biggest issue with tamper detection is recognizing when unauthorized access has been made and when to conduct a full system security check. A context-aware system can aid in alerting system administrators in the event of unauthorized access.

The benefits of IR proximity-based security systems include:

* “Invisible” implementation: Operation in the IR spectrum makes such systems invisible to the human eye unlike mechanical or laser-based systems. Furthermore, objects that are opaque to visible light can often pass infrared light, offering tamper detection abilities behind visually opaque covers. This is a key advantage in thwarting criminals who otherwise are aware of how to bypass visible security measures.

* System flexibility: Multiple irLED sensor implementations can offer tamper detection redundancy over single irLED implementations. Combination proximity sensors and ambient light sensors can use both visible and infrared light to identify potential tamper events.

* Small form-factor: Small-footprint optical sensors and surface-mount irLEDs make implementation discrete, cost-effective, and difficult to detect and defeat.

* Reliability: An optical-based tamper detection system, unlike a mechanical-based system, employs no moving parts and improves reliability and minimizes the need for maintenance.

Silicon Labs’ Si114x QuickSense family of multi-LED proximity sensors is ideally suited to tamper detection applications. The Si114x proximity and ambient light sensors have the ability to drive up to three irLEDs, and the high sensitivity photodiodes feature the industry’s longest sensing range and fastest single-pulse sensing architecture. The integrated ambient light sensing photodiode provides visible light measurements. The Si114x proximity sensors are also highly configurable via an I2C interface. Silicon Labs’ QuickSense Studio provides a common development environment that supports real-time reflectivity measurements and enables rapid code development and prototyping.

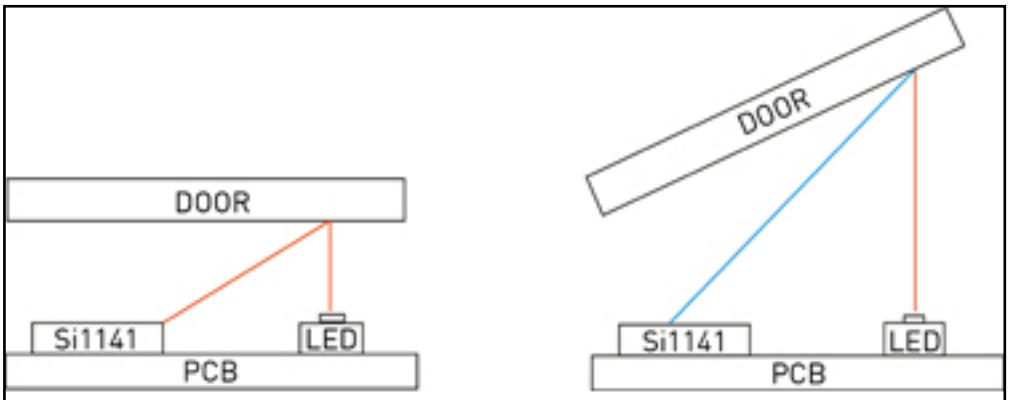

Figure 3. Concept of secure access using Si1141 proximity sensor.

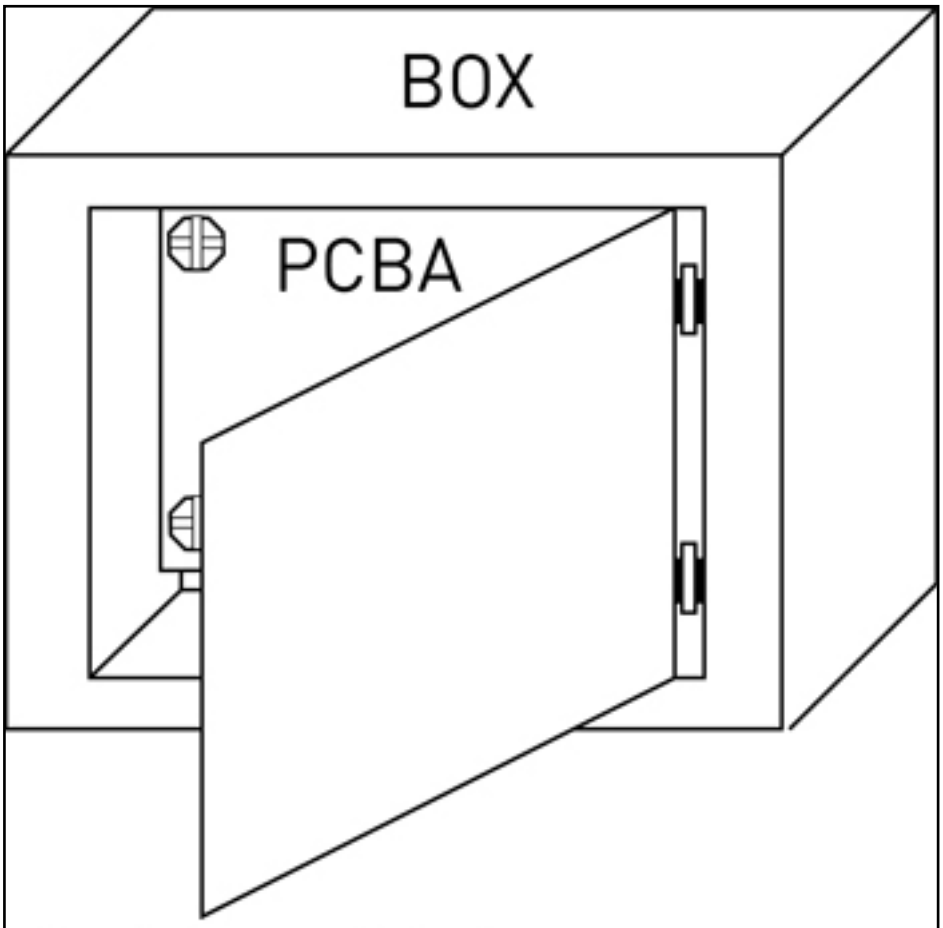

Figure 4. Secure metal chassis.

Proximity Sensing Proof of Concept

The sample tamper detection circuit shown in Figure 3 uses the Si114x proximity sensor as the basis of operation. Although this example shows a single irLED implementation, there are many instances where a multiple irLED system would provide additional security layers. The system concept is designed to detect whether a system chassis, represented by a metal enclosure shown in Figure 5, has been opened. The proximity sensor PCB is housed within the metal chassis as indicated by “PCBA” in Figure 4.

Note that this access awareness could be achieved using simple ambient light sensing, but this approach would not be robust since many chassis experience external light leakage and contain blinking LEDs as part of their internal systems, which would result in false readings. Another way to achieve this awareness involves using mechanical intrusion detection, but that method is not as discrete and has inherent wear-out mechanisms that require maintenance.

This sensor-based system works by measuring the minimum and the maximum values of reflected light when the door is open and closed respectively. When the door is closed and in close proximity, the sensor measures a maximum reading, and when the door is open the sensor will read a minimum reading (see Figure 4). The system uses minimum and maximum readings only to ensure robust operation across temperature since LEDs inherently have temperature-dependent light outputs.

Because infrared reflectance is affected by the surface being detected, the system was evaluated using different patterns on the interior of the door: the bare metal interior, a checkerboard pattern, and a dark to light radial pattern as shown in Figure 5.

Figure 5. interior door reflectance patterns.

The best results were achieved with the checkerboard pattern, then the unpainted metal door, and finally the radial pattern. However, each system provided ample margin between minimum and maximum readings to measure the system access robustly. The system uses a maximum LED drive current of 359 mA and a minimum current of 22 mA, although these values can be modified depending on the end system’s power

constraints. System auto-ranging is also implemented to adjust the Si1141 sensor's sensitivity based on the ambient infrared light level and to eliminate photodiode saturation in direct sunlight conditions.

Figure 6 shows an example of a complete tamper detection system, which includes the IR proximity sensor, MCU, USB bridge chip and other components. In this example, Silicon Labs' C8051F996 ultra-low power MCU serves as the system controller, ensuring minimal power consumption. A CP2102 USB to I2C bridge MCU enables communication between the detection system and host application on the PC. The irLED is an OSRAM SFH4056 22 degree half-angle LED. The system operates by tallying the number of times the door has been opened and could be easily modified to add timestamps to show when the access occurred.

System Security Is a Necessity

Hacking into electronics systems for criminal activities is on the rise. Witness the number of major hacking cases this year involving high-profile establishments such as Sony, the RSA and even the FBI. Given the growing threat of hacking and tampering, system security is much more than a desirable differentiating feature for electronics systems. It is a must-have capability – especially for publically accessible interactive kiosks such as ATMs and vending machines.

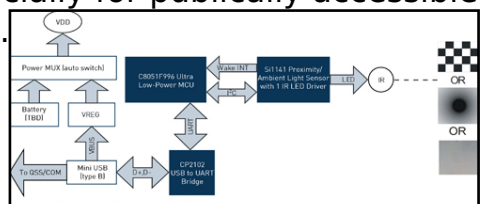

Figure 6. Example of tamper detection system.

As devices become increasingly networked, criminals can break the weakest link in a system security chain to attack the host or steal data. One method of minimizing the damage from attacks is to detect and prevent the attacks from happening. IR proximity sensor-based tamper detection provides a cost-effective and discrete technology that can be easily deployed to detect potential tamper events. Preventing an embedded device chassis from being compromised can help provide a first line of defense against illegal tampering. Ultimately, a consolidated approach to security that includes tamper detection is essential to providing comprehensive, robust and fail-safe protection for today's electronic systems.

Bibliography and Further Reading:

1) ADT Banking Security and Financial Security Solutions - http://www.adt.com/commercial-security/solutions/industry/banking
2) Hosting a Cash Machine at Your Business Location - http://www.mastercard.com/za/merchant/en/security/what_can_do/hosting_ATM.html
3) How does ATM skimming work? - http://money.howstuffworks.com/atm-skimming.htm
4) ATM security - http://atmsecurity.pcifraud.com/
5) How E-voting Works? - http://people.howstuffworks.com/e-voting.htm
6) Changing Slot Payouts - http://mitchell.casinocitytimes.com/article/in-reply-to-changing-slot-payouts-12640

1 http://www.bbc.co.uk/news/uk-england-derbyshire-13637666
2 http://www.herald.ie/news/courts/man-is-accused-of-tampering-with-bank-cash-machines-2839884.html
3 http://www.king5.com/news/cities/everett/PIN-pads-tampered-with-at-5-Western-Wash-Michaels-stores--121738234.html
4 http://www.google.com/patents?hl=en&lr=&vid=USPAT5086292&id=gx0aAAAAEBAJ&oi=fnd&dq=optical+tamper+detection&printsec=abstract#v=onepage&q=optical%20tamper%20detection&f=false

Source URL (retrieved on *09/17/2014 - 3:00am*):
http://www.ecnmag.com/articles/2011/11/optical-tamper-detection-technology-leaves-criminals-dark