



GORE™ Secure Plug-On Module

Protect Your Crypto Keys, Critical Program Information, or Intellectual Property From Physical Hackers

Electronic modules often store highly sensitive information. Communication devices store cryptographic keys and software waveforms, handhelds can store passwords and records, and embedded systems maintain sensitive algorithms in memory. These devices can easily fall into the wrong hands.

Attackers can gain access to your information in many ways. Once inside, information stored in solid state memory can be read even if the device is inoperable. A proven means of defense against these attacks is volume protection.

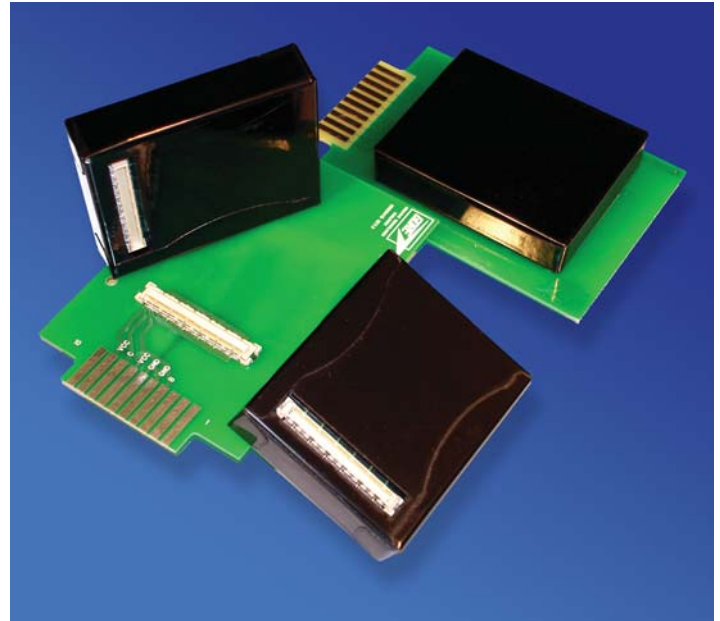
A GORE™ Tamper Respondent Envelope can surround and protect your electronic module. Acting as an anti-tamper sensor, this specialized envelope is designed to detect any means of entry into the module. With such protection, the attacker comes up empty as the module automatically erases the target of his attack.

PRODUCT SUMMARY

The GORE™ Secure Plug-On Module is Gore's latest offering from a broad range of unique tamper respondent sensors and technology.

GORE™ Tamper Respondent Technology offers secure, yet easy-to-adopt solutions to volume tamper protection. The new GORE™ Secure Plug-On Module detects physical intrusions by sensing attempts to penetrate or unwrap the envelope that it forms around the mezzanine card module. Detection typically triggers erasure of critical security information such as cryptographic keys or sensitive algorithms. The GORE™ Secure Plug-On Module is designed to achieve a strong level of physical security in a convenient and friendly format.

The sensor is extremely low power and, being non-metallic, is impossible to analyze by X-ray. It is designed to detect penetration by drills and probes as well as by erosive and chemical attacks.

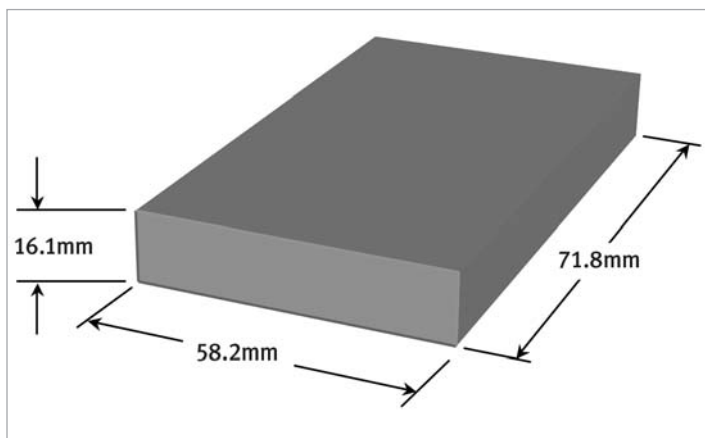
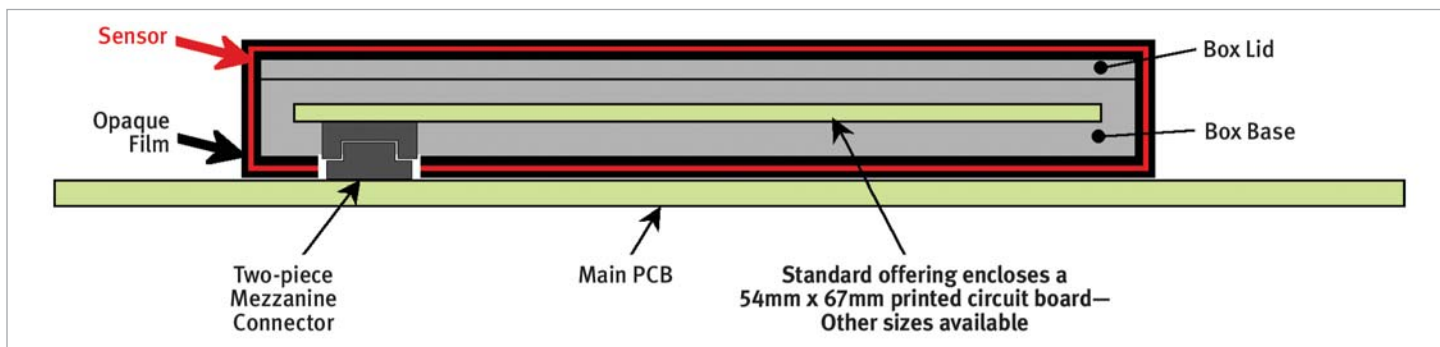


FEATURES AND BENEFITS

- Provides anti-tamper volume protection in a convenient plug-on form factor
- Initial offering protects a 67mm x 54mm printed circuit board—Other sizes available
- Incorporates a low profile mezzanine connector for module input/output and attachment
- Enclosure acts as a tamper sensor that enables zeroization of critical keys or information stored within the protected volume
- Attempted penetration (cutting, drilling) or unwrapping causes detectable permanent change in electrical state
- Minimizes size and space
- Modular format allows for re-use in multiple end products
- All-polymer sensor construction precludes X-ray analysis by an attacker
- Two product variants targeting:
 - FIPS 140-2, Level 3, 3+, and USPS security requirements
 - Payment Card Industry PED security and other high-level security applications
- Easy to monitor with low power consumption
- OEM needs only simple design rules
- From the only commercial supplier of protection of secure electronics having many independent certifications



GORE™ Secure Plug-On Module



APPLICATIONS

- Embedded cryptographic security processors
- Secure radios and wireless devices
- Point of sale and PIN entry terminals
- ATM PIN entry units
- Postal security devices
- Secure handheld devices
- Biometric security devices
- Access control systems

GORE and designs are trademarks of W. L. Gore & Associates, Inc. ©2007 W. L. Gore & Associates, Inc.

W. L. GORE & ASSOCIATES, INC.

402 Vieve's Way • Elkton, MD 21921 • USA
Phone: 1.800.445.4673 • Phone: 1.302.292.5100
E-mail: electronics.usa@wlgore.com

gore.com

W. L. GORE & ASSOCIATES (U.K.), LTD.

Mariner Drive • Dundee Technology Park
Dundee DD2 1JA SCOTLAND
Phone: 44.1382.561551

