wave™

Technology Brief

# Spotting Advanced Persistent Threats Early

*Using the TPM to Monitor the Security and Health of the PC Boot Environment*

With the influx of laptops, smartphones, and tablets joining the corporate WiFi, IT managers have realized that traditional perimeter security isn't enough to prevent data leakage. The sheer amount of applications, both sanctioned and unsanctioned, has become unmanageable and is getting worse every day. In this environment, corporate IT relies heavily on behavioral anomaly detection, that is, the ability to spot anomalies or changes to the benchmarked traffic on their corporate networks. With advanced persistent threats (APTs) appearing as normal traffic, new malware often goes completely unnoticed for long periods of time and causes severe damage in the form of infected systems and data loss.

### Twelve PCRs:

- **PCR 0**: CRTM, BIOS and Platform extensions
- **PCR 1**: Platform and Motherboard configuration and data
- **PCR 2**: Option ROM code
- **PCR 3**: Option ROM configuration and data
- **PCR 4**: MBR code
- **PCR 5**: MBR partition table
- **PCR 6**: State transition and wake events
- **PCR 7**: Computer manufacturer specific
- **PCR 8**: NTFS sector
- **PCR 9**: NTFS boot block
- **PCR 10**: Boot Manager
- **PCR 11**: BitLocker Access Control

Almost a decade ago, the computer industry recognized these growing threats and in response formed the Trusted Computing Group (TCG), an international industry standards body. In short, the TCG encompasses a range of technologies and standards intended to make computers secure, more reliable and less prone to viruses and malware. One such TCG standard outlines the specifications for an embedded security chip, called the Trusted Platform Module (TPM). Fortunately, nearly all business class PCs have been shipping with TPMs for several years. In fact, companies like Dell, HP and Lenovo include TPMs as part of their standard hardware configurations and have shipped hundreds of millions of TPM-equipped systems — ready to defend organizations against APTs and other types of sophisticated threats.

Amongst other capabilities, the TPM provides tamper-resistant storage locations called Platform Configuration Registers (PCRs). There are twelve primary PCRs that can be used to securely collect information about a computer's pre-OS environment, as the system powers-on. Of these twelve, PCR 0 which measures the Core Root of Trust for Measurement (CRTM), BIOS, and platform extensions and PCR 4 which measures the Master Boot Record (MBR) code are especially useful for detecting malware that has been known to evade traditional anti-virus tools.

## WORLD-WIDE GOVERNMENT AGENCIES RECOMMEND TRUSTED COMPUTING

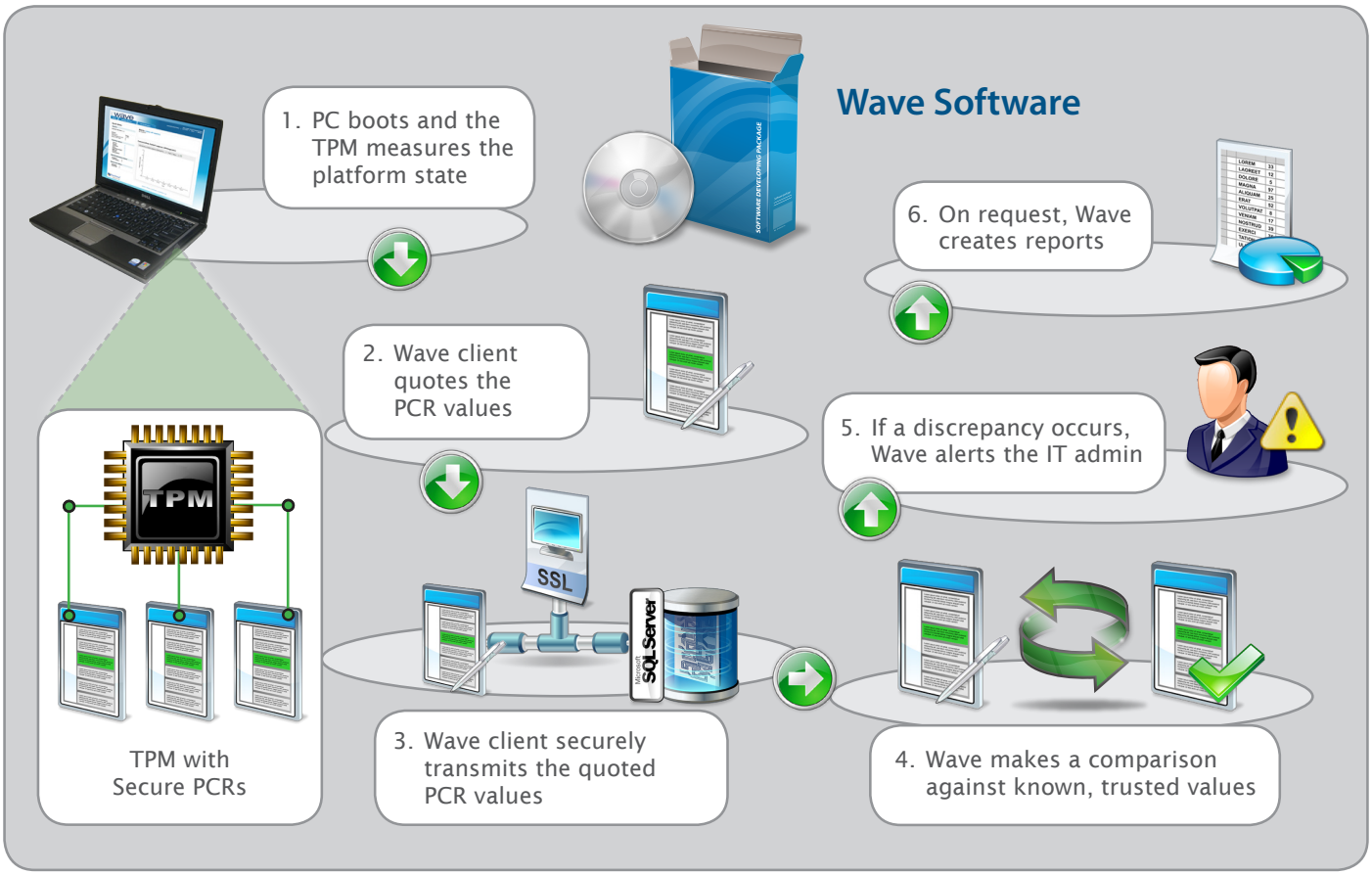
The US National Security Agency (NSA) now recommends that TPMs be turned on in the BIOS to secure VPN access. They further advise that "Trusted Computing technologies can provide network administrators with basic information about host integrity without expensive hardware or excessive administrative overhead. Hosts that support TPMs should have their TPMs turned on and activated from the BIOS."

CESG, the UK Government's National Technical Authority for Information Assurance, recently published guidance for the use of TPMs. Most notably, CESG declared that

"TPMs can provide additional security and assist with device management at low cost." They further suggested that "Government departments should consider whether cost savings can be made by introducing TPMs."

Organizations interested in detecting and mitigating Advanced Persistent Threats are advised to perform comprehensive scanning for anomalous behaviors across their organizations to allow for early detection. Wave's software adds an additional layer of anomalous behavioral scanning at the endpoint that can discover rootkits by detecting changes in the master boot record or BIOS. In addition to activating and managing TPM policies and keys, Wave software collects PCR values each time a system powers-on and compares these against a known, trusted set of values. Further, Wave software provides customizable alerts and granular reports so that administrators can be warned in real-time, and take action, in the event an anomaly is detected.

## Steps to detecting Advanced Persistent Threats




## Wave Systems EMEA

**Northern Europe**
104a Park Street
London W1K 6NG
United Kingdom
+44 1235 520956
emea@wave.com

Netherlands
Jan Pieterszoon
Coenstraat 7
2595 WP The Hague
Netherlands
+31 (0) 70 799 9326
emea@wave.com

**Central/Eastern Europe**
Excellent Business Center –
Westhafen Tower, Westhafenplatz 1
D-60327 Frankfurt am Main
Germany
+49 69 959 32 393
emea@wave.com

**Southern Europe, Africa & Middle East**
La Grande Arche-Paroi Nord
92044 Paris La Defens, France
+33 1 40 90 33 44
emea@wave.com

Israel
32 Habarzel Street
Tel Aviv 69710, Israel
+972 3 6442662
emea@wave.com

03-000290/ version 2.02 Release Date: 10-08-2012



Wave Systems Corp.
480 Pleasant Street, Lee, MA 01238, USA
+1-877-228-9283 · Fax +1-413-243-0045
www.wave.com