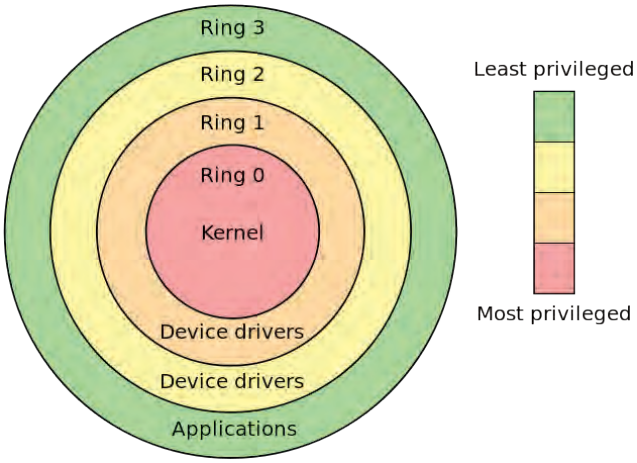
Introduction to ACS Keystroke Transport Layer Security™ (KTLS™)

Up until now, enterprises and government agencies have lacked the ability to fully protect their endpoints from a zero day keylogger, the single biggest threat that is leveraged in the first stages of almost all advanced threats. A keylogger, a primary component of all malware and advanced persistent threats, is a type of surveillance software that has the capability to record every keystroke an employee makes on their keyboard. In addition, most keyloggers come with the ability to change their form (polymorphic) and go on undetected as they quickly spread between the endpoints within the Enterprise. KTLS ™ Protocol's basic premise is that strong cryptography should always begin at Ring 0 and not only at Layer 4, Transport Layer, of the OSI.

KTLS™ Overview:
Keystroke Transport Layer Security™ (KTLS™) is an ACS patented cryptographic protocol that provides for the encryption and transport of keystrokes originating from the kernel at the time of secure boot, entry in to any application, web application or web browser. While SSL and TLS enable strong encryption in network transport (Layer 5 of the OSI model), KTLS begins strong encryption from the kernel level at ring 0 within the operating system; KTLS encrypts all keystrokes at the moment of press, before network transmission.

KTLS™ protocol can be utilized in both endpoint desktop (Windows) and endpoint mobile (IOS and Android) environments as a primary component of endpoint security. Endpointlock™ is the commercial product name by which KTLS™ protocol is implemented within an enterprise.

The primary goal of the patented KTLS™ protocol is to provide strong cryptography at the time of keystroke entry to protect the initial transmission of usernames and passwords (as required by HIPPA, PCI 8.2.1 and 8.2.1a and Homeland Security's Critical Infrastructure Protection Guidelines ("CIP") and subsequent keystrokes entered in to any program or application.



Advanced Cyber Security

3880 VETERANS MEMORIAL HIGHWAY, BOHEMIA, NY 11716 | p: 1-866-417-9155
WWW.ADVANCEDCYBERSECURITY.COM

KTLS™ Overview continued

When secured by KTLS™ protocol, connections between the keystroke and applications have the following properties:

• Keystroke Cryptography begins within the kernel at Ring 0.

• Both encryption and decryption occur directly within the application without any modification to the application required.

• The keys for this symmetric encryption are generated uniquely for each connection and are based on a shared secret that is generated directly from the Trusted Platform Module (“TPM”).

• The negotiation of a shared secret is both secure (the negotiated secret is unavailable to Keyloggers and cannot be obtained, even by an attacker who places himself in the middle of the connection) and reliable (no attacker can modify the keystroke transmission during the negotiation without being detected and kernel layer alerts being generated).

• The Key management is the management of cryptographic keys. KTLS™ uses the AES algorithm with a key size of 256 bits to encrypt keystrokes. AES is a symmetric encryption scheme. The same key is used to encrypt and decrypt.

• The Session key is generated once per session (KTLS™ loaded/unloaded). It can be generated either by a TPM chip (if it is there), or else by a built-in Random Number Generator.

• If a TPM chip is available for access to the KTLS™ system components, the Session Key is encrypted/decrypted by a TPM Master Key Pair (RSA 2048 public key cryptosystem), which resides on the TPM chip (and never leaves it).

• The encrypted Session Key is stored in secure memory shared by all KTLS™ system components. The TPM Master Key Pair is generated by the TPM chip every time the computer is powered up. This can be accessed via the NULL hierarchy.

• If a TPM chip is not available for access to the KTLS™ system components, the Session Key is encrypted/decrypted by a Storage Master Key (AES 256 Key) comprised of a combination of a hard coded part and a randomly generated part.

U.S. Department of Defense TPM Requirements

The United States Department of Defense (DoD) specifies that "new computer assets (e.g., server, desktop, laptop, thin client, tablet, smartphone, personal digital assistant, mobile phone) procured to support DoD will include a TPM version 1.2 or higher where required by DISA STIGs and where such technology is available." The TPM is anticipated to be used for device identification, authentication, encryption, measurement, and device integrity.

KTLS™ utilizes Intel’s TPM chip for enterprise endpoint desktop deployments. If Intel (or other) TPM is available for mobile devices KTLS™ protocol can be deployed.