



A White Paper

Elevating Existing Infrastructures to Tomorrow's Security Standards

...without the overhaul.

KoolSpan, Inc.
11134 Stephalee Lane
North Bethesda, MD 20852
+1 (301) 468-9434
www.koolspan.com

THE PROBLEM

Why is it that stronger security systems always seem to require major changes to existing applications and infrastructure? At best, these changes are even possible—current systems can be extended to support the new security and there is available budget for the modifications. At worst, and is often the case, these changes are wholesale. Otherwise operable systems undergo a forklift upgrade to meet increasingly stringent security requirements.

The problem is complex and in constant motion influenced by a number of forces. First, businesses are always changing. New business lines, new offices, new business process are just a few realities that drive the need for regular application and infrastructure adoption. Second, technology is, of course, always evolving. Consider the rapid rise of Wi-Fi and its impact on existing infrastructures, or VoIP and its protocol which challenges traditional firewalls. Third, security threats are always changing as hackers and their tools evolve in parallel with each new technology advance. Fourth, the regulatory environment is ever changing, making compliance efforts ongoing and often fluid.

THE NEED

What is needed is a strong security solution that doesn't drive the replacement of otherwise useful infrastructure, but rather drives the ROI of existing applications, networks and systems. Key requirements for such a system include:

- Strong Authentication, multi-factor and mutual, without key exchange
- Strong Encryption, 256-bit AES with per-packet keying
- Support for securing applications and networks without any modification
- Native operation in wired and wireless environments
- Native operation inside and outside the firewall
- Future system support, again without modification
- No negative impact on deployment environment
- Automatic and transparent operation
- Highest common denominator security standard
- Flexible deployment and re-deployment options

Meeting these requirements enables the continued use of existing systems with the benefit of the strongest security commercially available. The bottom line, a stronger ROI for existing systems and more budget available for other projects.

THE SOLUTION

KoolSpan elevates existing infrastructures to the highest standard of security. Operating independently of the application, networks and systems it protects, KoolSpan establishes trusted user and network connections.

Taking a unique approach to network security and connectivity, KoolSpan simplifies network design. It operates without modification to the applications it protects and is transparent to the network itself. In addition to a more fortified network, it delivers cost savings in network management and end user support, reduced infrastructure related capital expenditure and an increased ROI on the applications it secures.

The solution is based on the pioneering use of a proven security technology—Smart Cards. Implemented on *both* sides of the communications link, the Smart Cards are enabled to compute with each other (not a server farm) to establish strong authentication and security. Smart Cards are embedded into a network-based KoolSpan “Lock” and user “Key” respectively. The Lock authenticates and bridges users with Keys onto the network. Multiple Locks can be used to connect multiple networks. To connect users, they are provided small USB “Keys” that allow a device such as a laptop to bridge onto the network. No servers or other infrastructure is required. Access into the network is provided through a single port in the firewall protected by the KoolSpan Lock. Rather than proxy (typical of a VPN), KoolSpan establishes a secure Layer 2 Ethernet bridge whether inside or outside the LAN over any network link. This breakthrough approach, delivers unprecedented benefits as legacy infrastructures, can be seamlessly protected by today’s strongest security architecture.

HOW IT WORKS

Smart Card-to-Smart Card Architecture

The KoolSpan Platform consists of three components, each containing a Smart Card. KoolSpan “Locks”, “Keys”, and management application work together to provide an unmatched security model, without servers or user complexity. Whether in the Lock-to-Key or Lock-to-Lock configuration, the KoolSpan platform solution is powered by the same Smart Card-to-Smart Card architecture.

Smart Cards contain an embedded microprocessor, non-volatile tamper-resistant secure memory, and additional functionality including encryption algorithms. Typically, Smart Cards are employed to provide trusted identification, verifying that a user has the right to certain network-based services, and has emerged as the dominant physical token for authentication and security. The strength of Smart Card security is time-tested and trusted to provide revenues by most wireless phone providers and satellite television operators throughout the world. It should be noted that KoolSpan loads no application on the Smart Card, so there’s no application to attack.

Implemented on both sides of a network link, KoolSpan uniquely enables the Smart Cards to communicate and compute with each other. This architecture provides a platform for a variety of security applications and solutions. KoolSpan Locks can be deployed centrally or at the network edge, but at all times are centrally managed.

Authentication: Bi-Directional & Keyless

KoolSpan enforces two factor authentication without requiring the end user to input or otherwise manage One Time Passwords (OTP). When a user plugs in a KoolSpan Key, he/she is prompted for a user-defined eight character password which simply identifies the user to his/her Smart Card, not to the network. Now, without further user action, the Smart Card generates an OTP which is automatically sent to the network Lock. The OTP process takes place entirely within the Smart Card, both simplifying the user experience and eliminating the exposure of a user’s secret network key. Upon receipt of this single OTP packet, the Lock writes the OTP into its Smart Card where it is automatically decrypted, authenticating the user. In reply, the Lock then generates its own OTP (again, entirely internal to its Smart Card) and returns it to the user’s Key to properly authenticate the network. Now,

both sides have only exchanged two packets, an OTP in each direction. Mutual authentication has been established, without ever exposing network secret keys. In short, all communications are pre-encrypted before the data transfer is commenced.

With OTPs and network keys generated, encrypted and decrypted entirely internal to the Smart Cards, they are known to nobody, not even the network administrator who has complete control of the system.

Encryption & Per Packet Keying

With OTPs mutually exchanged to establish bi-directional authentication, the Smart Cards are then used as active elements in the encryption process. On each side of the link, the respective Smart Cards simultaneously and independently compute the same 256-bit AES session key, using, in part, the two authentication OTPs unique to the user and that session.

To further strengthen the communications, this initial AES key is never used directly. Instead, the Smart Cards, again independently and simultaneously, compute an offset to yield a new 256-bit AES key which is then changed with every single packet transmitted. The per-packet key can be created anywhere within the 256-bit key space to ensure maximum strength. This robust data protection is provided without the exchange of network keys and without the related risk of interception and attack.

Administration & Key Management

KoolSpan is administered by an Enterprise Management application and a Smart Card designated as the "Master Key". At the time of set-up, the Master Key is initialized and it generates a unique set of keys for the network. This process is performed entirely internal to and protected by the Smart Card. User Keys (which generate their own unique network keys at the time of initialization) and back-up Master Keys (which are 'cloned' from the Master Key) are similarly Smart Card protected.

The Enterprise Manager and Master Key together securely communicate with network based Locks to transfer the enciphered secret key of trusted users. After this initial set-up the management application only needs to run when a change is required, adding or deleting users, and not on a highly available basis.

As the network keys can never be read directly, are unknown to even the IT Administrator (who otherwise has complete control of the system) and are not stored on a central server for authentication, the enterprise essentially operates as its own "root authority".

Layer-2 Operation

Whether operating inside or outside the LAN, KoolSpan operates at Layer 2 providing its users with a true LAN-peer experience. The KoolSpan Lock does not proxy users onto the network. Instead, it operates as a secure bridge for trusted users and is an end-point for all others. Operating at Layer 2, KoolSpan security is transparent to the network, devices, applications and other assets it protects.

When connections are made across the Internet, a Layer 3 network, KoolSpan still delivers a Layer 2 link. Here's how:

1. The KoolSpan Key and driver send an OTP to the public IP address of the remote network. This is done, of course at Layer 3.
2. The Lock receives the OTP and validates the user and returns an OTP in response to the user, again at Layer 3.
3. The KoolSpan driver then establishes a virtual Ethernet adapter and all traffic to/from this virtual interface is encrypted at Layer 2 and then tunneled over the Layer 3 connection.
4. All network services, DHCP etc, are provided securely to the remote user by the network (not the Lock) where the Lock is installed.
5. The Lock decrypts the user's encrypted Ethernet packet and deposits it on the local LAN. The LAN sees an Ethernet packet from a "local" user—establishing a Layer 2 connection.
6. In reverse, the remote user receives encrypted Ethernet from the far network. It's decrypted and presented to the computer for "local" network or Layer 2 processing.

In short, KoolSpan establishes an Ethernet bridge not an IP bridge. As a result, the user connection appears to be local to both the user and the destination network. Security is automatically and transparently applied to all the user's operations, applications and network services accessed.

HOW IT'S DIFFERENT

KoolSpan Compared to a Layer 3 VPN

Typical VPNs establish an IP bridge. In contrast, KoolSpan establishes an Ethernet Bridge. KoolSpan operates without a client application, just a standard driver. No certificates or user specific data is stored onto machines using KoolSpan, all unique user information is generated and stored within the KoolSpan Key, more specifically its Smart Card.

After mutual authentication, the KoolSpan Lock and Key or Lock and Lock respectively, work to tunnel Ethernet packets to the other side. The tunnel is independent of IP traffic and, in fact, can handle NetBIOS and other protocols that ride on top of Ethernet. Unlike IPSec, which is a unicast protocol, KoolSpan's Layer 2 operation provides secure unicast, secure multi-cast and broadcast capability. This enables the simultaneous and secure one to many communications. It also permits broadcast network services such as Windows' network neighborhoods.

The KoolSpan Lock simply deposits all decrypted Ethernet packets on the LAN without modification. By contrast, a typical VPN gateway acts as a proxy between the Firewall and the LAN. As such, the user authenticates and tunnels traffic to the gateway and is assigned a local IP address by the gateway. The gateway in turn talks to the local network, vice versa back to the remote user. This can often be problematic as the gateway changes the IP address between the remote user and the LAN confusing applications and protocols.

KoolSpan vs. Other Token-Based Solutions

KoolSpan makes use of off-the-shelf Smart Cards, not proprietary hardware chipsets, and its design is very different from other token implementations in a number of ways.

- Active processing component in the Authentication and Security process
- Two Smart Cards - one on each side of the communications link
- Uniquely combines: Authentication, Security and LAN/WAN/WLAN/Remote Access

Rather than use the token for simple user identification, KoolSpan uses Smart Cards to actively and securely compute the information necessary to establish bi-directional authentication and AES security. For example, KoolSpan uses the following on-chip Smart Card capabilities:

- Key generation (write only, cannot be read from card)
- Encrypted Random number generation
- 3DES encryption/decryption authentication keys (protect keys and random numbers)
- Secure storage (protect keys)
- Secure encrypted hash (SHA1)

By employing Smart Cards on both sides of the communication link and enabling them to compute together, KoolSpan has obviated the need for a server-based authentication infrastructure.

KoolSpan loads no application on the Smart Cards, so that there is no application to attack. Instead the card is simply formatted in a certain way and its logic fully leveraged. Further, a single KoolSpan Key provides support for connections to up to 16 discrete networks—most token systems only work with one network. From the user perspective, this provides a simple, consolidated and consistent way to securely access multiple network environments as permitted by one or more administrators.

The KoolSpan Key hides all complexity from the user. Rather than having to read and type a time sensitive password, the Smart Card internally and automatically generates and transmits the OTP. As this OTP is invisible to the user, it is impossible for the user, if a rogue party, to share the credential electronically, by phone or otherwise. Physically a KoolSpan key operates without a battery which wears out or a LCD display which may break.

ELEVATING EXISTING INFRASTRUCTURES

With KoolSpan, users keep what they have and add what they need to elevate their existing infrastructure to the strongest security standard. Business applications, internal and inter-office network links, high value assets and more can be instantly fortified without modification, simply install KoolSpan and access is restricted to secured trusted users.

By example, existing firewalls are strengthened as port ranges can be closed, with networked applications serviced via a single port secured by a KoolSpan Lock. As all connections are made at Layer 2, users and applications always interact as if they are inside the LAN, regardless of location. No changes need to be made to these applications, they just work.

Or consider high value assets/applications which can be easily protected, made available only to trusted users, and only on an encrypted basis. This is again with modification to the assets/applications and without impacting the host network.

Whether they are internal LAN/WAN links, wireless connections inside or outside the firewall, KoolSpan's Smart Card to Smart Card architecture with its native Layer 2 operation delivers strong security. Transparent to the network, network gear and applications it protects, KoolSpan elevates existing infrastructures to tomorrow's security standard and drives the ROI of the environment in which it is installed.