WHITE PAPER

Securing Wireless Voice

KOOLSPAN®

Securing Wireless Voice

Wireless voice communication is increasingly the lifeblood of enterprise, government and industrial workflow. But as mobile phones, smartphones and voice-enabled PDAs become more and more like full-fledged computing platforms (e.g., mobile Linux, Java, Symbian, Windows), they are exposed to vulnerabilities that were previously associated only with wired IT systems, such as eavesdropping on calls and data sessions (mobile intercept), user masquerading, theft of service, theft of personal data, session spoofing, device cloning, backdoors and mobile identity theft.

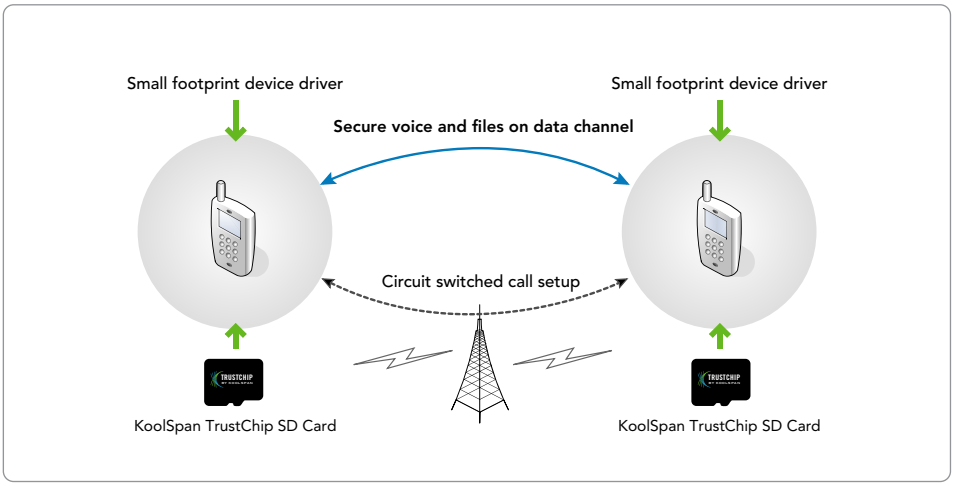
Like any IT resource, smartphones, mobile phones and PDAs are potentially vulnerable to viruses, worms, Trojans and spyware. Malware threats that were once targeted at LAN-based desktop and data center computers are now attacking mobile devices and mobile service provider networks. Mobile malware has been found to be very effective at attacking mobile voice and data sessions through open protocols and services.

With conventional security software, encryption routines running on mobile platforms are largely defenseless and vulnerable to a large number of hacker exploits and viral threats at the application, operating system and network levels. In the current era of escalating cyber threats, mobile platforms need a better approach to network encryption and authentication. This new approach must shield device-based security software from the vulnerabilities of open platforms and networks, so that wireless mobile CDMA and GSM voice traffic can be fully protected, end to end.

KoolSpan for end-to-end wireless voice device security

In response to the growing array of mobile device malware and hacker threats, and the security deficiencies of enterprise and wireless operator networks, KoolSpan delivers plug-and-play secure connections for wireless productivity devices, including smartphones, PDAs and various ruggedized mobile voice platforms (e.g., Symbol Technologies and Motorola).

Figure 1. *Secure mobile voice sessions with AES 256-bit encryption and mutual authentication*



KoolSpan's solution is end to end from the originating mobile device, through the network, to the destination device. This can be visualized as a two-way secure tunnel that encrypts and continuously authenticates traffic, regardless of vulnerabilities in underlying cellular networks.

KoolSpan crypto software and hardware can be easily embedded by OEMs in mobile devices, mobile application servers, wireless portals and VoIP systems. Crypto processing hardware in the form of the KoolSpan TrustChip is embedded through the industry-standard SD Card form factor. To complement the TrustChip silicon, KoolSpan crypto software is available in quickly deployable API libraries that can be added to mobile devices and management platforms as a driver that is loaded during boot-up. KoolSpan management console software is also available for integration and OEM product development.

KoolSpan hardware and software
KoolSpan's award-winning enhanced 256-bit AES cryptographic algorithms run on hardened silicon hardware with on-board crypto processing and secure memory operations. The crypto card platform creates an ideal tamper-proof, tamper-evident environment for running advanced encryption routines, and storing keys and other security data. KoolSpan offers a vast improvement over conventional security software products that store secret keys on end-user or server hard disks that are vulnerable to human and malware attacks, including a wide range of Trojan Horses, backdoors, rootkits, etc.

The memory and processing resources on crypto cards and embedded silicon are hardened to defend against digital and physical attacks. By running encryption processing on specialized hardware, KoolSpan off-loads computationally intensive CPU demands and storage overhead from the mobile device. This approach ensures minimal device footprint and high performance, even on resource-constrained mobile device platforms.

KoolSpan encryption software sets up an AES 256-bit secure tunnel between end points without any need for public keys or certificate management (PKI, IKE, Keberos, RSA, etc). KoolSpan authentication is conducted bidirectionally at three levels: 1) at the device level, 2) at the session level, and 3) continuously on a per-packet basis, which ensures that hackers cannot conduct man-in-the-middle attacks, dictionary attacks, replay, and cloning or spoofing exploits.

KoolSpan's powerful encryption technology is necessary for protection of critical infrastructure, but many attack vectors aren't directed exclusively at the encrypted data in transit. Hackers and blackhats will also hack into end devices and servers via internal backdoors, rootkits, bots, or through VPN tunnels. Badly implemented IT security infrastructure and misconfigured security settings are of great assistance to hackers and many types of malware. In contrast, KoolSpan encrypted and authenticated connectivity is, by design, an out-of-the-box security solution. KoolSpan requires little or no setup and completely isolates critical device traffic and operator console traffic from outside attack, end to end.

In operation, KoolSpan's integrated TrustChip crypto hardware and proprietary software together provide a hardened and dedicated "security engine" in each mobile voice device, enabling a very wide range of secure wireless voice interactions for corporate, industrial and government users. KoolSpan's high-performance security engine supports encryption, authentication, user identification, mobile device PINs, and key management services for popular mobile phones and wireless voice devices. When the TrustChip is inserted in a mobile device via standard SD card slot, it enables device-to-device 256-bit AES encrypted TrustedConnections, which fully protect end-to-end voice traffic. The KoolSpan engine grants mobile devices membership in a virtually limitless number of security groups - referred to as TrustGroups. In peer-to-peer mobile device communities, TrustGroups do not require central administration after initial installation. In centralized configurations, security groupings and associations within TrustGroups can be managed from a central KoolSpan console on an ongoing basis.

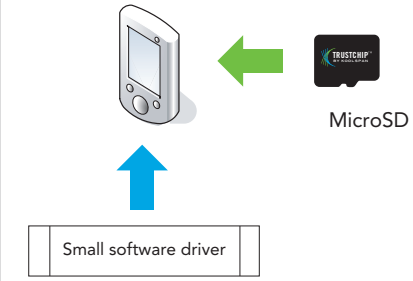
KoolSpan's streamlined mobile device service API makes it easy for developers and OEMs to deploy product that support very scalable communities of secure mobile voice devices. The KoolSpan TrustChip is the optimum approach to secure mobile voice for popular cell phones, smartphones and PDAs that don't have the processing power, memory or built-in crypto processing capabilities that are necessary for simple, secure voice communications.

Peer-to-peer or centralized
Security relationships between mobile devices can be either peer-to-peer or centrally administered. In the central KoolSpan model, a management console function allows network administrators to dynamically create security groups and permit/deny security associations for participating users and client mobile devices. Managing KoolSpan centrally presents an opportunity to create a granular set of privileges for mobile devices and mobile application servers. Access rights for secure KoolSpan connections can be defined for each device and each upstream application. This means that corporate mobile users will have connectivity only to mobile devices and services for which they have explicit rights.

In the peer-to-peer version, all the necessary authentication keys, identity codes and crypto algorithms are pre-loaded into the KoolSpan TrustChip or SD Card hardware during installation. From that point on, mobile devices authenticate sessions and set up secure end-to-end tunnels automatically. Once peer-to-peer devices are installed and operational, they can continue to dynamically form secure connections within their security groups for an indefinite amount of time without operator intervention.

In both the peer-to-peer and centralized versions, KoolSpan secure mobile device connectivity is essentially plug and play, requiring none of the complex configuration, administration and network architecture modifications that are associated with conventional IP firewalls and VPNs.

KoolSpan strengths and benefits
In non-traditional IT spaces where special-purpose online machines and terminals (enterprise, government and other mission critical voice communication environments) need improved end-to-end security, the KoolSpan connectivity solution delivers a wide range of benefits including:



Scalability. KoolSpan's significant advantage in scalability means there's no need to create complicated traffic management rules or security key administration procedures and policies. KoolSpan-protected security devices can authenticate and encrypt sessions with little or no centralized administration across all types of CDMA and GSM networks. KoolSpan security scales seamlessly to a very large number of devices/end points that all benefit from simple plug-and-play connection protection.

Secure processing and storage. Often, the open nature of Linux, Java and Windows systems, which all have many well-known components including network ports/sockets, operating software libraries, I/O architectures and application interfaces, hampers conventional network security. Hackers and blackhats take advantage of vulnerabilities in open security device platforms to compromise and defeat VPNs and firewall perimeters on a regular basis. KoolSpan avoids these problems by running its routines on hardened, tamper-proof crypto hardware. Critical data and application sessions are fully authenticated and encrypted end-to-end on a packet by packet basis, leaving no holes in security for traffic that is inside or outside the firewall.

Device footprint. Today's desktop and data center systems feature ever-increasing amounts of disk and memory space to accommodate more and more robust applications and operating systems. Infinite storage space is not always the case with online security devices that often have constraints on memory and disk resources. KoolSpan is ideal for constrained devices because it has a very small footprint on end devices in terms of how much code space is required. KoolSpan encryption and authentication routines run on TrustChip hardware in SD Cards. Along with the TrustChip hardware, a small software driver is loaded into each mobile device, which means that the footprint is minimal and non-intrusive, requiring no expensive upgrades to systems or operating software.

Device processing demand. IPsec and related IT security programs typically run on the main memory and processors of client and server computer devices, which is known to cause substantial overhead in terms of memory and processor usage. Mainstream IT security methods can rob horsepower and code space from online security devices with computationally intensive processing and contribute to reduced performance. In contrast, KoolSpan runs its routines using the advanced dedicated crypto processor that is available in TrustChip SD Cards and related embedded hardware that KoolSpan and partner OEMs manufacture.

Network latency and overhead. Many security device applications require real-time or near real time network communications to support point of sale transactions, financial services, and other interactive applications. Due to the complexities of the key exchange, encryption and security handshaking, VPNs and other conventional IT security methods can introduce substantial network latencies during session initiation and traffic forwarding. KoolSpan, by contrast, minimizes network overhead and session start-up time, introducing an absolute minimum delay into secure connections.

Simplicity and ease of use. KoolSpan-protected security devices can set up P2P security associations that require no external key management administration or certificate servers. The KoolSpan end-to-end security model allows highly automated authentication and encryption in an extremely scalable plug-and-play, peer-to-peer security architecture—without complex configuration and administration. If centralized controls are needed, they can be deployed without the major administrative and policy burdens that are associated with VPNs and PKI.

Conclusion

Our current climate of heightened security demands for a more proactive and comprehensive approach to providing wireless voice device users with secure network communications. KoolSpan has responded to this need with advanced crypto software and hardware that is specially designed to easily integrate into existing mobile devices in enterprise, public and government voice networks. The KoolSpan solution provides machine and terminal applications with end-to-end encryption and authentication that is not readily available from conventional security software solutions. Whether you are an OEM, systems integrator, consultant or enterprise end user, please contact KoolSpan for detailed information on how your specific online machine or terminal application can benefit from simple secure connectivity today.

For more details on the underlying security technologies please see KoolSpan's Foundation Technology white paper

For More Information

Please call 240.880.4400, or go to www.koolspan.com