LiteScape Secure Profile Management (SPM)

Whitepaper: Secure and personalized access to VOIP services
Identity Management solution for VOIP devices

LiteScape Technologies Inc.
April 2010

Summary

Providing **Secure Access** to applications and services has rapidly become mandated within most large organizations.

According to a Garner Group report on application security, enterprises currently spend approximately $20 billion per year on IT security. Still, over 50 percent of all security breaches are caused by workers within the enterprise. Even so, just 30 percent of all security issues are actually reported.

As a result large organizations with important security and intellectual properties must implement security measures for any communication device that can access enterprise services and information.

The tremendous adoption and growth rate of VOIP (Voice over IP) based solutions are changing the very way we communicate. VOIP products have expanded communication solutions for IP phones, providing even wider user access to the internal networks of the enterprise.

IP phones are typically at fixed locations and naturally 'always on'. Unlike computers and PCs, these IP devices are widely available at various public environments (conference rooms, lobbies, front-desks, security check-points, flex-office, etc) and can be used by multiple users. Accordingly securing these devices from unauthorized use and the risk exposure these devices can have for an organization are of key importance.

It is essential to provide appropriate security, access, and control mechanisms to manage user access to the breadth of features available on these kinds of IP devices. For example: access to collaborative communications features (such as an employee joining an IP phone-based conference-call in progress), or the ability to place IP phone-calls to normally restricted locations, and access to corporate and personal directories and information.

Currently available solutions that provide a means for users to authenticate themselves using a mix of existing verification methods (RFID/Smart/Magnetic card readers, bio-metrics and passwords) in order to access VOIP services can effectively address the ongoing security concern.

LiteScape's **S**ecure **P**rofile **M**anagement (**SPM**) solutions offers the enterprise the secure environment needed to allow safe and secure access to the communication features of VOIP enabled phones.

This paper discusses the various aspects of the **SPM** solution as applies to the Cisco VOIP infrastructure (Cisco CallManager and Cisco VOIP phones).

Physical Security and multi-method authentication

The compliance of an effective identity management solution, in terms of access to a secure application, involves ensuring that physical access to the application infrastructure is properly managed. This is done best through; restriction, control and monitoring.

Established industry guidelines provide a range of flexibility from standard password protection protocols (***1. what the user knows***) to sophisticated biometric identification (***2. who the user is***). Multi-method verification/authentication systems can also leverage RFID/magnetic/smart-card

readers (***3. what the user has***). The specific implementation blend of these methods is largely dependant upon the level of security that is required or makes sense to have within each organization.

LiteScape SPM verification can combine any of the 3 following primary identification factors, in any combination:

- Biometrics: Who the user “Is”
- Password: What the user “Knows”
- Magnetic/RF-ID card: What the user “Has”

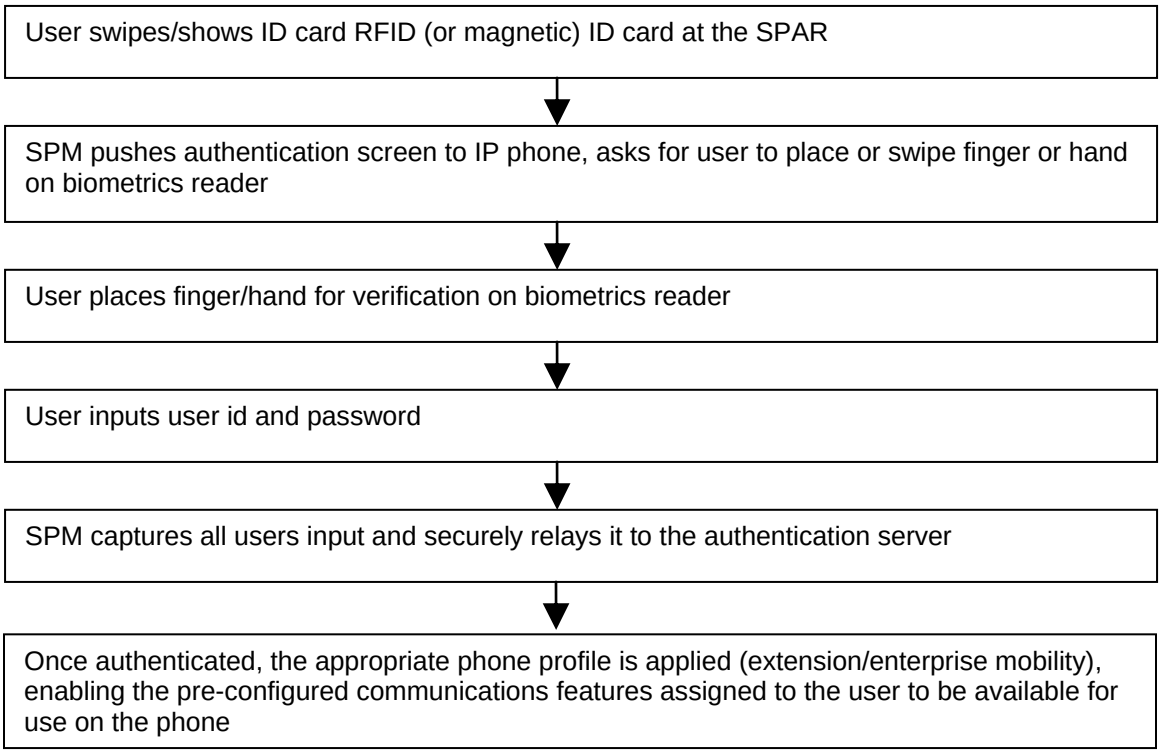
Once the user has logged into the phone/device, SPM maintains an active “session” until either the user logs out or the session times out.

SPM pairs standalone IP phones with a physical device, a **S**ecure **P**ersonal **A**uthentication **R**eader (**SPAR**). These devices provide an interface for users to interact with such as swiping their company-provided ID-badges, pass their proximity access or "smart" cards across, or even use bio-metrics such as fingerprint or other sensors to “log-in” to and access the IP phone.

The IP phone screen/keyboard combination is used by SPM to enable a secondary authentication method by allowing entry of alpha-numeric passwords.

SPM usage Scenarios

A typical usage scenario for the SPM Verification Method would be as follows:



For example, the user can now place long distance calls within their assigned territory on a phone that was previously restricted to other users. In addition, the same SPM transaction enables extension mobility. This means that callers that are trying to reach this user will be directed to the authenticated IP Phone.

The same log-in could be used to establish a firm point of presence. Alternatively, a Time-Card tracking application can be notified to establish check-in/check-out time for the users.

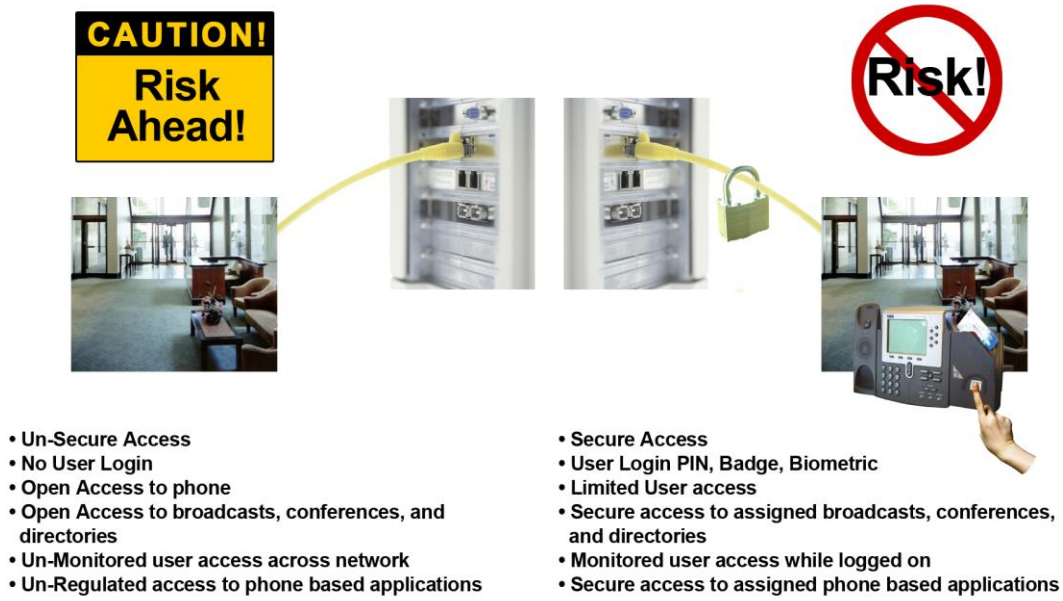
Service lock-down/authentication proxy

Once a user logs in using SPM, they can use applications from the VOIP phone enabled to provide the capabilities available to the user's profile. Restrictions to place calls, send/receive broadcasts or participation/organize conference calls are all controlled based on central policies and group/individual profile management.

Multi-site CallManager access to extension mobility

As users move from location to location within an organization, (such as large campus or multi-building facilities) they can use SPM to authenticate themselves and access their personalized services at any IP device. For example:

- By default a typical office lobby phone in a building is inert or provides limited extension access and little or no outside communication services to the user.
- User 'logs' in using SPM
- All calls can now be routed to the VOIP phone
- Night-time or upon completion of the task, user logs off using SPM
- SPM adjusts the users communication profile to use an Interactive Voice Response (IVR) application
    - This application can either route all calls for this user to voicemail or to his/her mobile or other alternate phone as appropriate.
- The IVR application can selectively route calls based on user log-in status (night-time vs. day-time service) to various locations.



Session and presence management

SPM acts as a proxy between SPAR, the authentication server, the IP PBX (for example, Cisco Unified Call Manager) and existing business or collaborative applications (such as Directory

servers, presence servers, Time-tracking or Customer Relationship Management (CRM) solutions).

In addition, SPM can publish the user's current 'Present & Available' status. This specific IP terminal information can be shared with common off-the-shelf presence servers throughout the enterprise.

The same information can also be shared with time-management applications for the purpose of check-in/check-out services, for part-time, or increasingly common, contract employees.

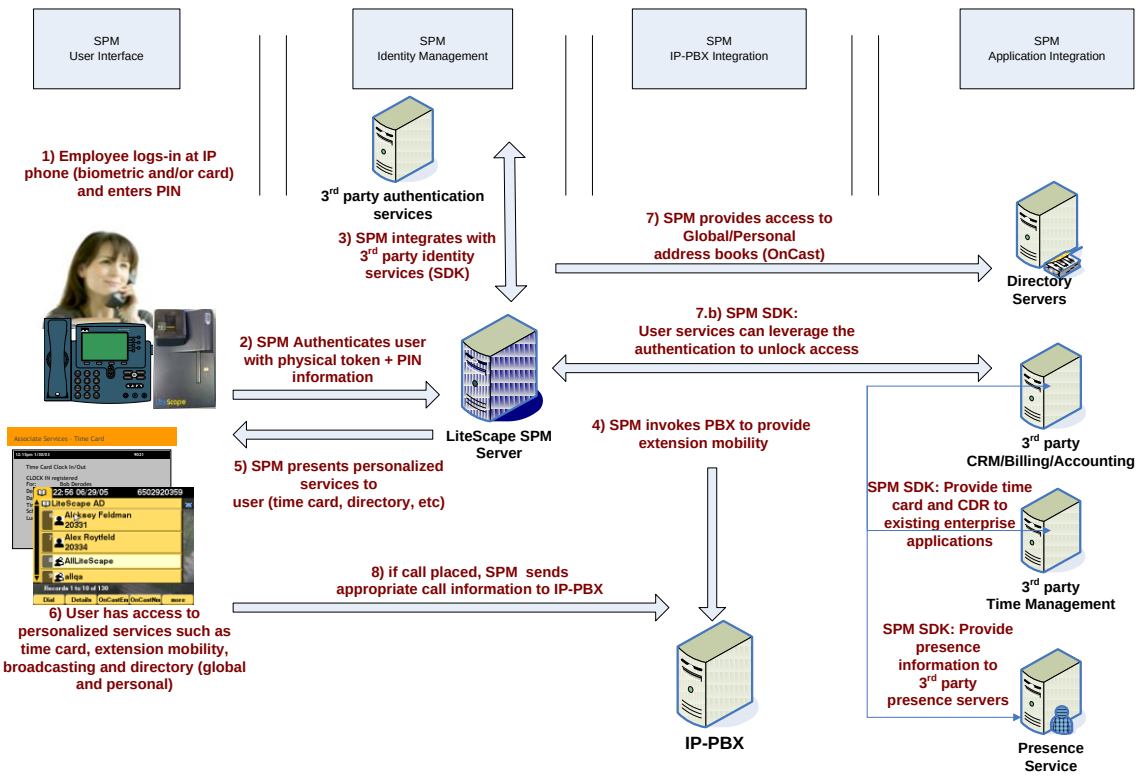
The ability to transfer session information to applications like CRM or call-centers is tremendously useful in that, by using already-captured 'session' information, a service agent does not have to collect information from the caller when accepting a service request. Previous session information is transferred to the agent with the call when it is answered.

A recent study by LiteScape has shown that the trusted and secure transfer of this kind of session information lowers the length of a customer service call by an average of 2 minutes.

Services Personalization

SPM can also effectively integrate with 3rd party application services on a user-by-user basis. Some examples of such services are timecard applications, reminders, urgency or matter specific ring-tones, etc.

The following diagram shows the overall interaction of SPM with various service components.



SPM solution features and characteristics

SPM includes the following functional features and characteristics:

SPM authentication & security features

- Supported communications encryption protocols:
  - Transport layer security (TLS),
  - Internet protocol security (IP-Sec)
  - XML-Encryption
  - Cryptographic message syntax (CMS)
  - **Cryptography:** Digital signatures
  - 128 bit secure SSL HTTPS
  - 802.1X Port Based Network Access Control
- Identification, Authentication and Authorization:
  - Authentication management via single sign-on (SSO) or reduced sign-on (RSO) and in support of Advanced Encryption Standard (AES) FIPS 197
  - Support of Federated trust services for communication of security assertions to provide access privileges for cross-application using.
- Support of **FIPS** (Federal Information processing Standard) 140-1/2 for validated encryption algorithms
- Support of **DISA FSO STIG** (Field Security Operation Security Technical Implementation Guidance)
- Configurable **False-Acceptance-Rate** (FAR) and **False-Rejection-Rate** (FRR)
  FAR < 1 in 100,000
- Rejection of **exact matches**
- SPM follows the **DOD 8500.1** information assurance directive
- Integrates with PKI based encryption for digital identities using certificates
- Multi-method authentication and policy-based conditional access control components and subsystems
- Encrypted and secure storage of sensitive credentials data and data-repositories (e.g. password encryption or hashing, private key protection and bio-metric patterns data protection, database content)
- Transaction integrity measures to avoid transaction replay and masquerading
- Rules based automatic-logout of users to control access duration
- Scales to support simultaneous access of SPM during busy periods (e.g., morning login, afternoon logoff) within organization

SPM application level features

- Support for multiple off-the-shelf 3rd party bio-metrics based authentication servers, solutions and devices
- Integrated support of access (search and lookup) on directories (personal, corporate, global) on a policy basis
- Support of policy based dialing, conferencing and broadcast services
- Support of multiple versions of Cisco CallManager and Cisco VOIP phones
- Support of multiple VOIP platforms including Avaya Communication Manager and Nortel Communication Server
- Presence server integration with MS-LCS and IBM SameTime
- Integrated support of time-management applications

- Integrated support of session transfer for CRM integration
- Integrated support of IVR integration for mobile applications

SPAR device characteristics

- POE supported Ethernet interface
- Fingerprint biometric reader
- RFID reader. 13.56Mhz ISO 14443/ISO-15693/TI-Tag-It
- Scanner I/F
- Three track Magnetic card reader. (track 1+2+3)
- Single port Hub (to connect another IP device)
- Data Cable (between Phone and reader)
- +5 volt supply brick
- RS-232 interface for management
- Device can be inactive on the network until user initiates transaction (swipes card/shows badge/uses fingerprint for biometrics recognition)
- Extra IP port can be disabled (statically configured or based on authentication result)
- Cisco side-car integration with Cisco 7940/60/70 IP phones
- Integration with other phone types (Avaya 4600 series and Nortel 2000 series)

Biometric Authentication

Manageability & serviceability

- Multi-access-level **administration** and **monitoring**
- Logging and tracing:
  - Guaranteed transaction logging;
  - Secure activity and event logging that prevent sensitive data (e.g. user credentials or account numbers) from being included in operational logs (e.g. in violation of privacy policies or regulations).
  - Information collection, processing and distribution management, logging and auditing for privacy regulatory compliance
- Segregation of operational management roles:
  - Sufficient segregation is in place,
  - Enforced by the application system

- Enforced within the software development life-cycle (SDLC)
  - No single engineer has the capability to control, monitor and audit the process from start to finish

SPM technology background

SPM is built on LiteScape's **M**ulti-modal **A**pplication **P**latform (MAP).

This powerful and scalable platform enables real-time management of interactive multi-modal sessions over a convergent network. Such sessions are comprised of voice, data, graphics and media streams that can be coordinated and simultaneously delivered to users of IP phones, IP soft-phones, and IP smart devices.
Unique aspects of the MAP platform are:

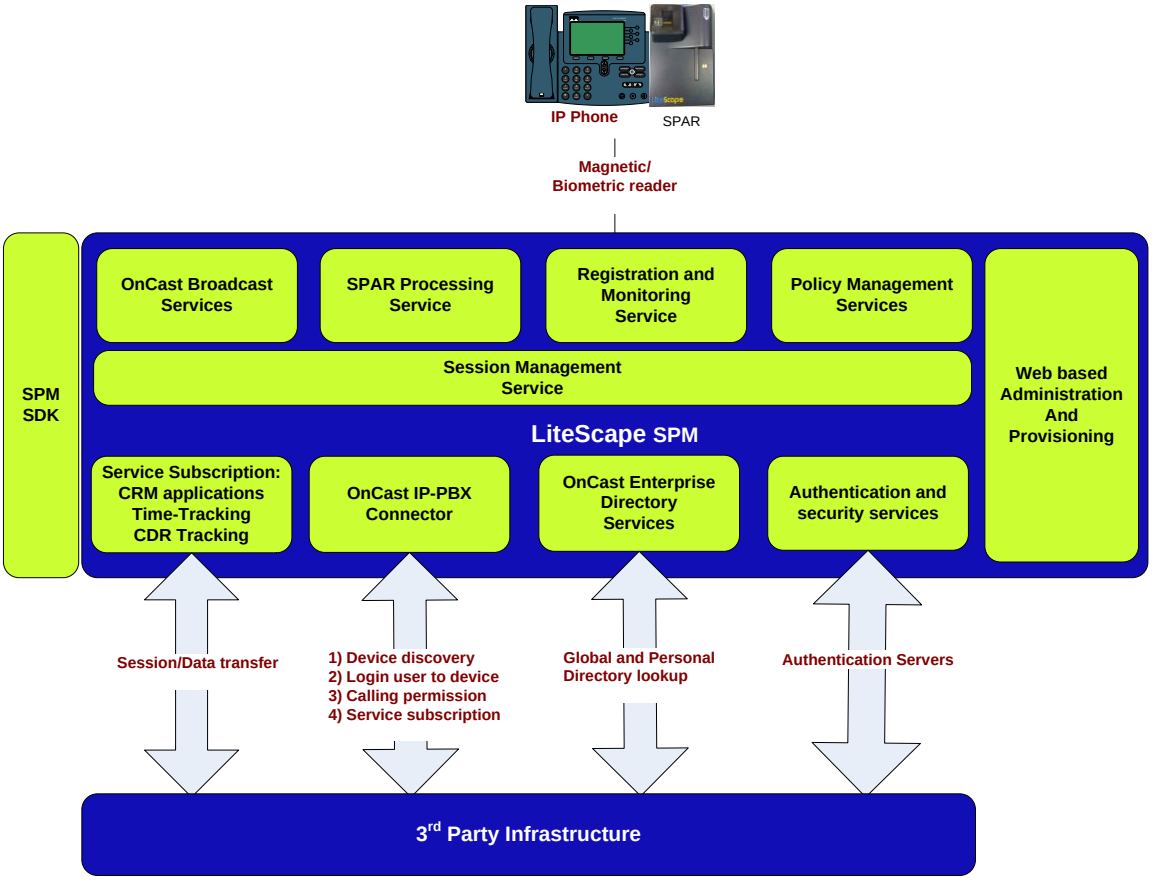
- A rich set of flexible business rules and configurable policies,
- Strong security, authentication, access control,
- Comprehensive real-time multi-modal interaction capabilities

These key advantages allow enterprises to leverage their investment in converged infrastructures to enhance and improve their existing business processes with real-time communications and collaboration.

The MAP platform enables various modes of authentication at the very outer edge of the network. Magnetic card-readers touch key screens, biometric readers and smart-chip card-readers can be used to determine and authenticate the registered identity of the employee requesting services from an accessible IP-phone.
This enables rapid and secure authentication and personalization of users compared to the currently used methods (keying in information manually, or announcing credit-card and other personal information loudly in a public place for all to hear).

This kind of "Point-of-Service" terminal effectively has many benefits for the employee and provides the enterprise with significant advantages over traditional business processes:

• Simplified Secure Authentication – uses the employee's ID card which is preferred method of identifying and authenticating them today.
• Minimization of Authentication Errors – once authenticated, the system knows the employee's accounts and does not require the keying in of long numbers.
• Personalization – information is personalized to the employee based on their account data.
• Re-use of Existing Applications – leverage existing investments in applications by making them available to all employees.
• Extended Reach – enterprises can extend the reach of their existing applications, such as ERP and benefits software, to the edges of their network where PCs are not readily available.
• Single button "Help" can default the employee to a service representative at any time.
• "Enterprise Directory" – function allows employees to find and connect with enterprise personnel by searching Active Directory, DC Directory, LDAP based directories and personal address books.



Certification requirements

Various organizations and industries have established certification requirements for solutions that provide security and authentication access.
SPM will comply with independent third party accreditation requirements.
This is a vital process for adding checks and balances and achieving industry assurance.
The LiteScape MAP platform closely follows ISO 15408 process standards.
LiteScape closely follows the Federal Information Processing Standard (FIPS), the Federal Information Security Management Act (FISMA), and the Defense Information Technology Security Certification and Accreditation Process (DITSCAP).
As of this writing, the SPM solution has been awarded FIPS 140-2 Non-Proprietary Security Policy for LiteScape SPAR & JITC IA accreditation certifications and is actively pursuing other necessary certification and accreditation processes.
As various SPM-based solutions extend to magnetic card based authentication in public/consumer environments, the solution should comply with the credit card company security certification process EMV (Europay, MasterCard, Visa (EMV) as well.

Risks and challenges

Physical access security vs. application security

Although SPM provides authentication and session management for access to services to on VOIP phones, this does not remove the need for implementing sound measures to secure the applications themselves.
A 2003 Garner report shows that over 75% of attacks against applications come at the application layer itself and not lower infrastructure and network layers.

References

CSI/FBI: Computer Crime and Science survey, 2003
Garner Group report Application security, 2003
LiteScape Financial Service Point White-Paper, 2005
NIST SPAR Security Policy Revision 1.8, NIST.gov web site
DISA: Reference: (a) DoDI 8100.3, "DoD Voice Networks," 16 Jan 2004.

About LiteScape

LiteScape's ServicePoint™ solutions deliver simultaneous and secure voice, text and image for seamless and economic collaboration. LiteScape transforms IP phones into standalone, always available, self-service devices. Employees can use LiteScape empowered IP telephones to check in, access accounts, updates, alerts and training. Customers can quickly query product availability and location, account information or instantly talk to support.

For further information on LiteScape Technologies, Inc.:

LiteScape Technologies, Inc.
info@litescape.com
www.litescape.com
Toll Free: 800-617-0917