

Certicom Security for VoIP Devices

secure voice communications for enterprise VoIP deployments

THE PROBLEM

The deployment of Voice over IP (VoIP) in the enterprise is growing rapidly. IP based telephony systems are replacing traditional PBX systems. With this new technology comes new challenges for protecting the mission critical voice network from malicious attacks. Legacy PBX systems were relatively immune to such attacks due to the isolation of the physical network. With IP based systems, the voice devices are subject to the same sort of attacks that are well known for data networks. Additionally, attackers may be able to steal service, resulting in fraudulent long distance usage.

To thwart these attacks, it's not enough to secure the network itself using standard mechanisms such as Firewalls and Session Border Controllers. Vendors of IP telephony equipment must select from among a wide range of technologies to secure the VoIP device, while maintaining the voice quality users have come to expect.

The signaling channel is implemented using the session initiation protocol (SIP), and is responsible for making sure a call is properly directed to the correct IP address. The signaling protocol is also responsible for providing services such as call forwarding, call transfer, call hold, and caller ID. Although SIP can run over UDP, TCP or SCTP connections, it is usually run over a reliable transport layer such as TCP or SCTP.

Once a VoIP call is set up using the signaling channel, the media channel is established. The media channel converts the analog voice signals to digital data streams using any one of several codec technologies. This data stream is then transmitted across the IP network using the real-time transport protocol (RTP), which provides an efficient, highly reliable mechanism for exchanging voice packets.

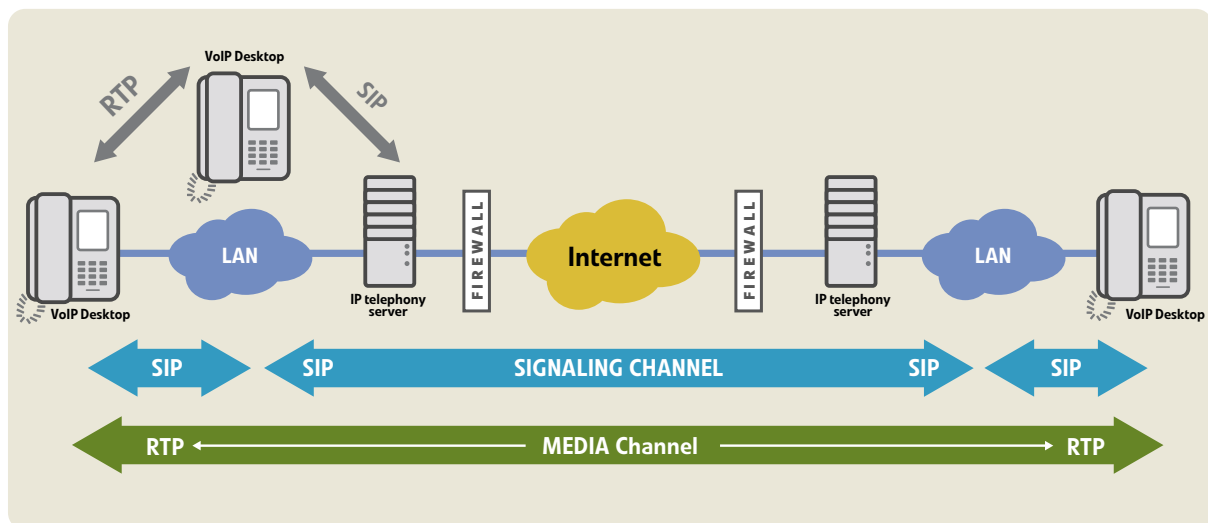


FIGURE 1

As with any emerging and expanding technology, VoIP devices should be built with the expectation that they will need to be updated in the field, and for system management, they should be capable of being provisioned centrally. These capabilities create additional opportunity for attackers to compromise the VoIP device.

The Developer needs to make decisions on if and how to secure the signaling channel, media channel, and the device itself.

New threats and vulnerabilities are identified all the time. Meanwhile the VoIP market evolves, with new and revised standards and protocols, creating a real requirement to securely update software in field deployed phones.

Finally, in today's multi-vendor environments, interoperability between devices is more pronounced than in legacy 'closed' environments.

SOLUTION

Security needs to be designed in, not added on. To achieve strong security, device manufacturers need to consider five elements:

- **Securing the signaling channel**
- **Securing the media channel**
- **Securely provisioning the device**
- **Securely updating the software**
- **Protection from malicious code**

There are several approaches available to the developer, and there is no single correct solution. If you are building a VoIP devices to work with an existing SIP server, and that server only supports SSL for securing the signaling channel, your decision is pretty clear. If, on the other hand, you are designing a complete system, then you have choices to make. Let's examine the options available to achieve the goals listed above.

Signaling Channel

Security protocols introduce some level of latency and throughput degradation on the data channels they secure. The signaling channel is not significantly affected by this, since signaling messages are generally short, and infrequent.

Both IPSec and SSL/TLS can be used to secure the signaling stream. Both can work with reliable transport mechanisms such as TCP and SCTP, and this adds additional reliability to the overall signaling solution. Both can support the same strong cryptographic algorithms. There are pros and cons to each solution, and both have been successfully used.

Media Channel

Unlike the signaling channel, the media channel is susceptible to excessive throughput delays and latency, which can cause reduced quality in the voice service. For low end devices, memory and CPU costs are a key design criteria, so the solution needs to take into account the constraints of the device. For higher end devices, memory and CPU power may not be as critical.

Since security protocols can degrade performance, the developer needs to be more careful in the selection of a security solution. Providing very strong IPSec security, can degrade the media stream to an unsatisfactory level. SSL/TLS may also have similar issues, which are compounded by the fact that it runs over a reliable transport (TCP), which can degrade performance due to retransmissions.

The Datagram Transport Layer Security (DTLS) protocol was developed to address the issue of performance. DTLS is essentially a specialized implementation of TLS that is designed to operate over UDP, and is optimized for securing media packets.

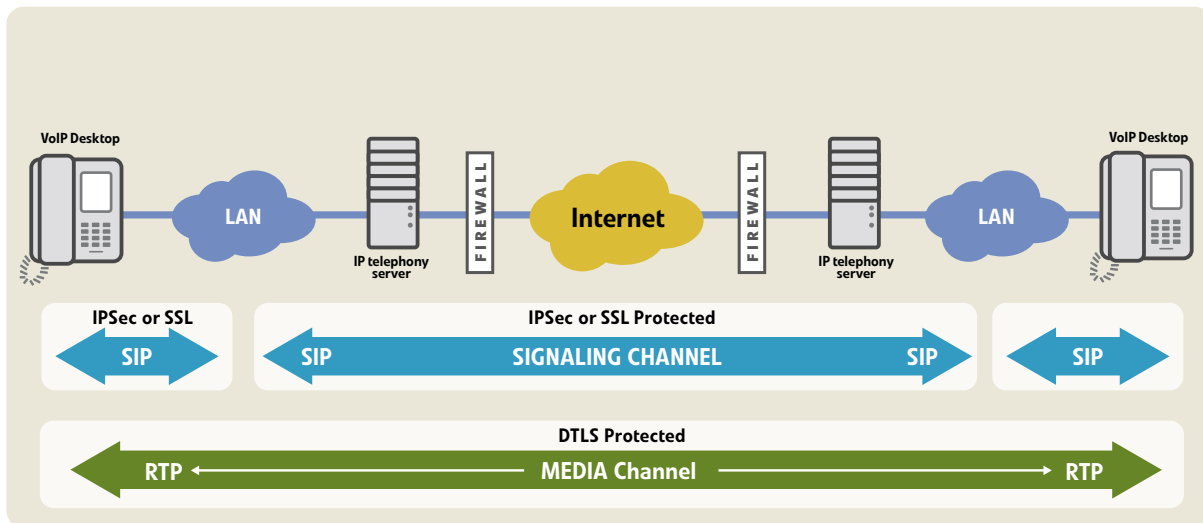


FIGURE 2

Provisioning

It is often necessary for VoIP devices to be provisioned by the network administrator. This provisioning includes information required to authenticate with the service provider. It is not uncommon for someone to try to copy the configuration files from one device, place it in a second device, thereby gaining access to services gratis.

To thwart this process, device manufacturers can include in the provisioning code a “salt” that is used to modify the user’s password before it is stored securely on the device. This salt is sometimes a hardware serial number, or some other mechanism that is unique for each device.

The salt ensures that no two devices can have the same password, thus preventing the cloning that might occur if a user’s password is somehow discovered. This also prevents a legitimate user from duplicating the provisioning file on his device and creating several copies to give to friends.

Software Updates

Device manufacturers should implement a code signing process to protect against the introduction of malicious code. Code signing is the process of digitally signing files so that their authenticity and integrity can later be verified.

Consider the scenario where a bug is found in a VoIP phone. As the manufacturer, you create a software update, and put it on your web site. Users can then use the download capability that you built into the phone to update their device. As long as everyone plays by the rules, there are no problems.

However, it’s not uncommon to see these patches copied to a corporate server, and enterprise users pointed to the local copy. Friends pass them along to others. Pretty soon, there are dozens of copies floating around. What happens if someone alters this software? An unsuspecting user could grab it, and introduce all sorts of malicious demons into the network.

By signing the original image, and using the proper verification processes in the phone, the user can be assured that the code that is being installed is authentic.

Malicious Code Protection

By employing trusted boot procedures, device manufacturers can ensure that the image that is loaded at boot time is valid and has not been altered. Trusted boot procedures establish a root of trust on the device, usually by the use of protected RAM or other locked hardware storage. This root then validates the rest of the image before it is loaded at boot time.

IMPLEMENTATION

Vendors who are designing VoIP desksets must choose a security solution that offers:

- **Security for the signaling and media channels, as well as device security**
- **A common security framework that enables easy integration of a wide variety of security protocols and crypto algorithms**
- **Strong, future-proof security**
- **Optimization for constrained and embedded devices**
- **Conformance to industry standards for security and interoperability**
- **FIPS validated algorithms and NSA Suite B conformant cryptography for devices being deployed in government applications**

It is unrealistic to expect a product development team to implement the various security protocols and algorithms required by VoIP devices. Standards-based toolkits exist that allow you to quickly and easily add the required security functionality, speeding time to market and lowering development costs.

Certicom has more than 20 years of experience providing standards-based developer toolkits that meet these requirements. The Certicom Security Architecture is a comprehensive platform that offers all the protocols needed for VoIP devices in a common framework. The modular design of the platform allows you to incorporate only those algorithms and protocols that are required for your application, yielding the optimal performance and footprint.

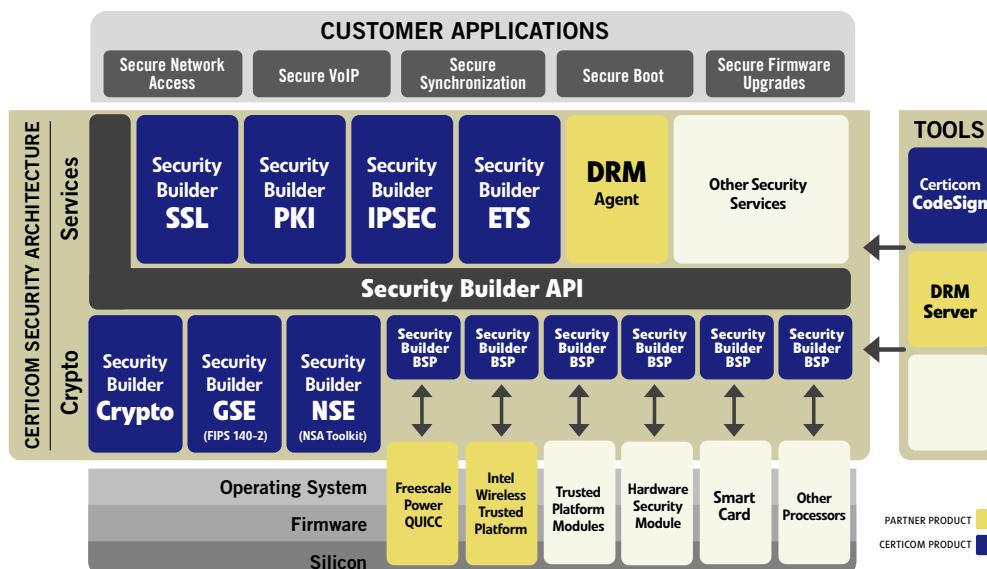


FIGURE 3. The Certicom Security Architecture

The Certicom Security Architecture consists of:

Cryptographic Providers

- **Security Builder® Crypto™**: High performance cryptographic module that includes a comprehensive suite of algorithms
- **Security Builder® GSE™**: A **FIPS 140-2 validated/NSA Suite B enabled** cryptographic module
- **Security Builder® BSP™**: Board Support Package providing an optimized abstraction layer for interfacing to other crypto providers, such as hardware based crypto algorithms.

Security Services

- **Security Builder® SSL™**: Complete protocol module for implementing the Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS) protocols
- **Security Builder® IPSec™**: Client side Virtual Private Network module including IPSec, IKEv1 and IKEv2, with support for all major VPN Gateways
- **Security Builder® PKI™**: Comprehensive digital certificate management module
- **Security Builder® ETS™**: Embedded Trust Services module that provides secure boot, key storage, key management, and authentication services for trusted platforms.
- **Certicom® CodeSign**: Application for digitally signing firmware and code updates

Since all projects do not have the same security requirements, the components of CSA are modular, allowing the developer to select only those modules necessary to provide the optimum security solution.

RESULTS

The Certicom Security Architecture provides all the protocol support necessary to secure the signaling and media channels for VoIP devices, and also provides the necessary functionality to secure the device by adding code signing and secure boot and provisioning capabilities.

By taking advantage of the synergy of the various components in CSA, VoIP device vendors can take advantage of these additional benefits:

- All of the modules use a common API – the Security Builder API – which allows vendors to leverage one common security architecture for cost effective software development and faster time to market with lower project risk.
- All of the modules are optimized for constrained environments, providing strong security with minimal impact to the VoIP device footprint and performance.
- By incorporating advanced Elliptic Curve Cryptography (ECC) into the solution, VoIP vendors can achieve a significant performance increase while increasing the overall strength of the security solution.

about certicom

Certicom protects the value of your content, software and devices with government-approved security. Adopted by the National Security Agency (NSA) for classified and sensitive but unclassified government communications, Elliptic Curve Cryptography (ECC) provides the most security per bit of any known public-key scheme. As the undisputed leader in ECC, Certicom security offerings are currently licensed to more than 300 customers including General Dynamics, Motorola, Oracle, Research In Motion and Unisys. Founded in 1985, Certicom's corporate offices are in Mississauga, ON, Canada with worldwide sales headquarters in Reston, VA and offices in the US, Canada and Europe.