ESI eCloud

VoIP Enhanced Call Security using Encryption

This document discusses what VoIP is and what can be done to increase its security.

Enhanced Call Security

With the proliferation of Voice over IP (VoIP) systems, eavesdroppers have come up with new ways to listen in on private conversations. Because VoIP communications are digital, they rely on software and data networks to facilitate voice exchanges, making them susceptible to many of the same types of threats found in other digital systems. Someone who hacks into a VoIP network can use a protocol analyzer to intercept and record phone conversations without callers knowing.

Those customers that have particular concerns about the confidentiality of the calls between their users, such as banks, medical, and legal businesses, would benefit from this optional feature. This document will explain how this feature works.

Understanding VoIP

To understand how enhanced call security works and is beneficial it's best to understand how VoIP works. Voice over Internet Protocol (VoIP) is a form of communication that allows you to make phone calls over a broadband internet connection instead of typical analog telephone lines. Basic VoIP access usually allows you to call others who are also receiving calls over the internet.

VoIP utilizes these protocols to make a phone call possible:

- SIP (Session Initiation Protocol) is a signaling and call setup protocol for IP-based communications supporting the call processing functions and features present in the public switched telephone network (PSTN). SIP is also used for other multi-media sessions such as video, messaging, etc. In this particular context, we're looking at voice sessions only.
- SIP can be carried over the internet by several transport layer protocols including TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
- RTP (Real-time Transport Protocol). Once SIP has established a session for a VoIP call, the payload of that session – i.e. the voice – is packetized using RTP throughout the duration of the voice call session.

As VoIP usage has increased, so have the potential threats to the typical user. While VoIP vulnerabilities are typically similar to the ones users face on the internet, new threats, scams, and attacks unique to IP telephony have emerged lately.

What can be done to increase security?

Concerns about the security of calls via the public Internet have been addressed by encryption of the SIP protocol for secure transmission. TLS (Transport Layer Security) is the top and most powerful transport layer that protects your VoIP calls from hackers and eavesdropping attacks. Using TLS/SSL certificates for SIP voice configurations, you can easily protect your communications by encrypting data and securing channels between two endpoints.

TLS helps safeguard your SIP voice in the following ways:

- **Encryption:** Calls are transmitted over the internet using ciphertext (a random string of text) to shield data from unauthorized sources.
- **Authentication**: Process of authenticating parties exchanging calls and messaging.
- **Verification**: Process of verifying that call data wasn't compromised and a secure SIP delivery took place.

The SRTP (Secure Real-Time Transport Protocol) is a security profile for RTP that adds confidentiality, message authentication, and replay protection to that protocol. Once the TLS session is established, the SIP session will now take place where the negotiation of media will also be handled. Note that, with SRTP, the encryption parameters for the RTP are contained within the SIP signaling (which is why TLS should be used for SIP in the first place). SRTP therefore encrypts the call's payload.

Do all endpoints support TLS/SRTP?

Not necessarily. In the initial session initiation, one of the first checks done is if both endpoints involved in the call support TLS. If one of them does not, then the call is completed as usual using TCP or UDP as the transport protocol and therefore the call is not encrypted.

How ESI supports Call Security

Security and privacy are very important issues in today's public communications. ESI has been working hard to address those issues, and make sure our products and solutions offer measures that support security and privacy and therefore offers today the Enhanced Call Security for all our endpoints (desk phones and the *ePhoneGO 2™* mobile app.) utilizing TLS and SRTP. This is an optional feature that can be enabled across an entire domain. Please contact ESI Sales for details - https://www.esi-estech.com/contact-us.

Notice that the ESI Webphone uses HTTPS (web security protocol), not TLS/SRTP and is therefore not associated with the Enhanced Call Security feature.

Important Note: Once the feature has been ordered and activated for a domain, for changes to take effect, desktop phones should be unplugged and plugged back in to update the phone. *ESI ePhoneGO 2™* users must logout to reset the application, and then log back into the mobile app.

How can I explain Enhanced Call Security in a simplified manner to a customer?

Alright, let's imagine you're sending a secret message to your friend over the internet. You don't want anyone else to understand it, so you use two special helpers to keep it safe: TLS and SRTP.

TLS, which stands for Transport Layer Security, is like having a magical envelope for your message. When you put your message inside this envelope, it locks itself automatically. This means that only your friend, who has the special key, can unlock and read the message.

Now, SRTP, or Secure Real-time Transport Protocol, is like a special language you use when talking on the phone or through video chat. It ensures that your conversation stays private and no one else can understand what you're saying. It's like having a secret code for your words.

So, with TLS and SRTP working together, your internet messages and conversations are like secret letters and codes that only you and your friend can understand. They help **keep** your online communication safe and private!