CALEA Compliant Encryption Without Backdoor Security Vulnerabilities

TECHNICAL WHITE PAPER

Cory Beard, PH. D.
Associate Professor
University of Missouri-Kansas City

Hien Van Nguyen
SIPbiz CTO & Co-owner
SIPbiz.net

01/23/2018

SIPbiz.net
Cyberspace Identity System

Summary of Contents

Executive Summary

Court orders mandate surveillance operations by law enforcement agencies. But it is difficult if not impossible for certain organizations to comply because of the types of communication systems they use. And frequently their users utilize third-party tools entirely outside their control.

This paper presents one solution to solve two problems: the "Front Door" CALEA approach to support law enforcement and "Going Dark" problems when communication is encrypted.

The solution provides a rich suite of communications and workgroup tools. It designates one of the organization's user sign-in identifications as the Registrar. By design, this user id cannot participate in any group communications, but when requested by law enforcement agencies it can be used to access the private and encrypted communication data of a member or members of the organization.

The solution is CALEA compliant because the Registrar has access to and can report the data to the law enforcement through a "Front Door" solution, and it fixes the "Going Dark" problem because the Registrar can decrypt the communication data.

I. Introduction

The Communications Assistance for Law Enforcement Act (CALEA) of 1994 was designed to preserve the longstanding ability of law enforcement agencies (LEAs) to conduct electronic surveillance under court order. Previously this had been accomplished through ports on telecommunications switches, but this capability was at risk as new digital technologies and wireless services were deployed.

> CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance while protecting the privacy of information outside the scope of the investigation.
>
> Federal Communications Commission

Without new mechanisms to provide the same type of access, communications were "Going Dark" to LEAs. Investigators encountered an increasingly diverse range of communication systems, social networking mechanisms, and operating systems.

Recent events have shown that it is certainly in the public interest for electronic surveillance to continue in certain dire circumstances. But it is also clear that providing such access to any system should not be accomplished through a hidden "back door" entry into a system. This creates vulnerabilities that could be exploited by attackers.

Instead, CALEA advocated a "Front Door" approach where under court order an authorized user in a system would access potential evidence and hand over the information to authorities in a controlled manner. This special authorized user should be able to decrypt communication as necessary; communication should not be "dark" to that user. And some communication could be archived for potential future investigations, but again only decrypted by the special user under court order.

Here we present a solution that accomplishes exactly these objectives: a system that provides "Front Door" authorized access to encrypted communication.

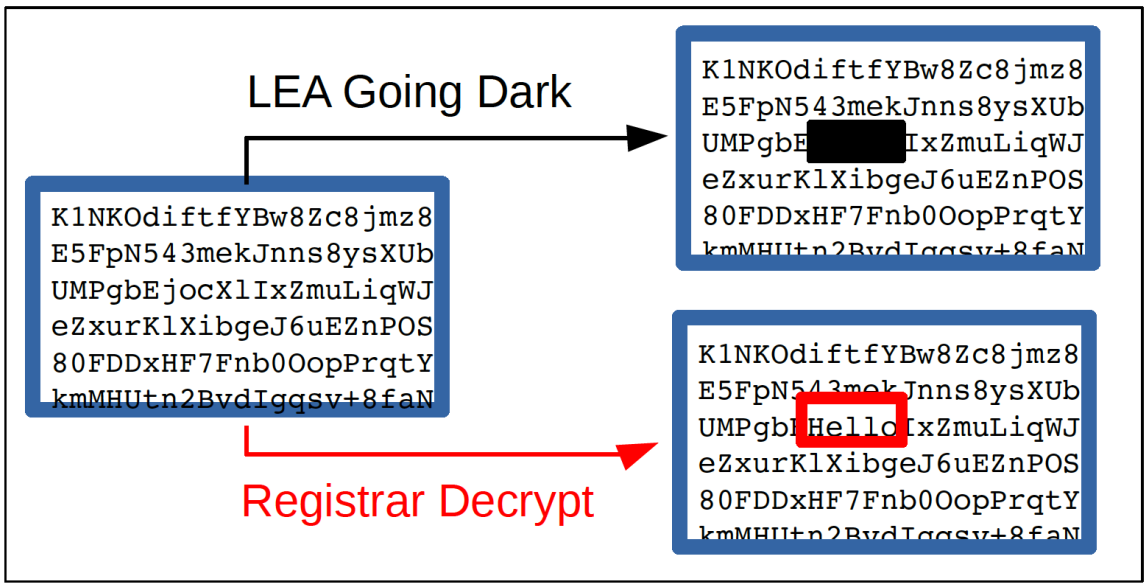

Figure 1: Registrar can decrypt strong encryption.

The solution is not architected with a "Back Door." Instead it builds trusted communities of users based on mutually agreed connectivity and unbreakable strong encryption, while working together to exclude inappropriate membership and intruders.

II. Solution

The key to our solution is for any organization to have its users communicate within a system where a key authorized user, who we call the Registrar, creates, organizes, and can potentially observe strongly encrypted communication within the organization's workgroups. The system should provide a rich suite of strongly encrypted data communication and workgroup functionalities.

This paper presents what we believe is the only such solution available.

The Registrar depends on the Cyberspace Identity System (CIS) to identify and manage system users. The CIS assigns user identity and validates it each time the user accesses the system.

Once identified by CIS, the user can build inner circles of contacts and communicate with others using the encrypted text messaging system. This encrypted text message system includes chat rooms that are created by the users. Any user can create a chat room and invite their contacts to participate. Only invited members of the chat room can read and write messages and attachments, which are encrypted during transit and at rest.

A. CALEA Compliant Registrar

Each organization of users has a Registrar. The Registrar can decrypt and view the communications of any chat room. The organization's Registrar can add or remove users and perform other administrative functions of a system administrator.

One special administrative function of the Registrar is to create connections with other organizations. The Registrars of two organizations may agree to create a secure channel for members of their organizations to communicate. Once a secure channel is established, members of one organization can request to add members of the other organization as contacts.

The Registrar differs from a regular administrator in the ability to provide "Front Door" access for LEA's and to decrypt strong encryption. The Registrar can read and decrypt the encrypt the text messages created by member users of its organization. The Registrar depends on Cyberspace Identity System (CIS) to identify system users.

CALEA "Front Door" Access for LEA's

The user id of the Registrar is configured to have read access to the data in the database of all organization members and is equipped with necessary keying materials to decrypt the encrypted text messages created by the organization members.

Because of this important role, the Registrar can only sign-up once from one device. In the sign-up device, some information about the Registrar id is kept so as to be used to validate a future sign-in.

To be sure that the Registrar can only sign-in at one device, the CIS applies a secure hash using a 256bit secret key to the Registrar's public key and keeps the result in the device. Each time the Registrar signs in, the public key, which is kept in the server, is hashed using the same secret key and the result is compared against the value stored in the device.

The secret key is hidden in the server and the hashing algorithm is randomly selected, by the device, from the set of most recently developed standard hashing algorithms.

The Registrar will not be allowed to sign-up or sign-in at another device. The Registrar can sign-off and sign-in with a different user id and use it to communicate with other users.

The Registrar id is not allowed to participate in any communication with members of the organization. This prevents the Registrar id from being logged in for long periods of time or from being inadvertently used for non-Registrar activity.

No “Going Dark” and No “Back Door” Breaches

“Going Dark” happens when the communication individuals ordered under surveillance cannot be read. LEAs (or even administrators within an organization) cannot decrypt strong encryption. As discussed above, the Registrar is designed to decrypt the encrypted text messages of its organization’s users.

The role of the Registrar in the system creates a solution to the “Going Dark” using a “Front Door” approach. No “Back Door” breaches will be possible since no back doors would even exist.

> Make no mistake, the FBI supports strong encryption, and we know firsthand the damage that can be caused by vulnerable and insecure systems. ...The government uses strong encryption to secure its own electronic information, and it encourages the private sector and members of the public to do the same.
>
> ….And as for a perceived conflict between keeping people safe and protecting their privacy, “it isn’t a question of conflict,” according to Comey. “We must care deeply about protecting liberty through due process of law, while also safeguarding the citizens we serve...
>
> FBI – Going Dark

B. Strong Encryption Users

The solution is built on the principle of strong end-to-end encryption. First, the end-user has to be identified and verified. Then we apply the most recently developed industry and government standard strong encryption technologies to methods of data encryption and transmission.

The messages are encrypted and transported using AES-GCM, an authenticated encryption algorithm designed to provide both data authenticity (integrity) and confidentiality. All keys are wrapped using AES-256 before stored in the server. Elliptic curve technology, Curve25519, is used in creating the PKI keypair and in Diffie-Hellman (ECDH) key agreement to create session keys. All keying materials are secure hashed (SHA-3) with secret keys or using the Extract-and-Expand Key Derivation Function (HKDF).

Cyberspace Identity System

Before a user can use the system, the user id must be registered with the CIS. During the sign-up session, the user id that is being used to sign-up is validated and will not be allowed to sign up if it cannot be validated. Once signed up, the user is assigned a CIS identity which includes a set of keying materials and a PKI key pair (public key and private key).

During the sign-up session, the device information is added to the user CIS identity and kept in the server to assure that the same user id cannot be signed up from another device. And the user CIS identity is also kept on the device. For example, the user public key is secure hashed using a 256bit secret key and the result is kept in the device. Each time the user signs in, the public key, which is kept in the server, is hashed using the same secret key and the result is compared against the value stored in the device.

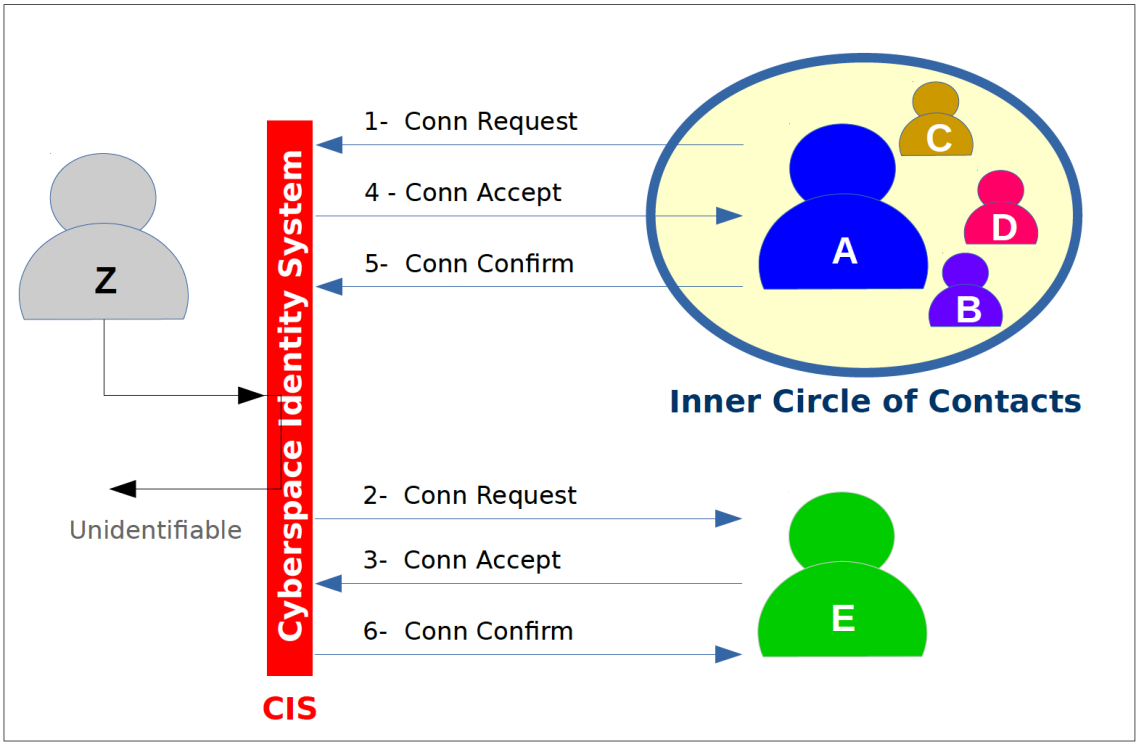

Figure 2: Building up identifiable inner circle of contacts.

Inner Circle of Contacts

A user first must build a list contacts. From that list of contacts, a user picks a contact to add to a private messaging session.

When a user wants to add another user to the contact list, there are a few secure processing and checking operations from both sides to confirm the user identity.

To secure communications between users, they exchange their credentials to create a secure channel between them. The secure channel is created using PKI public/private key pairs which are then used by the parties to encrypt the exchanged messages to confirm their identity. They also exchange mutual keying materials for future uses, like when there is need for an invitation to a private messaging session.

Private Messaging Session

The encrypted text messaging system includes chat-rooms that are created by the users. Any user can a create chat-room and invite members to participate. The invited members are picked from the contact list. Only invited members of the chat-room can read and write messages and attachments, which are encrypted during transit and at rest.

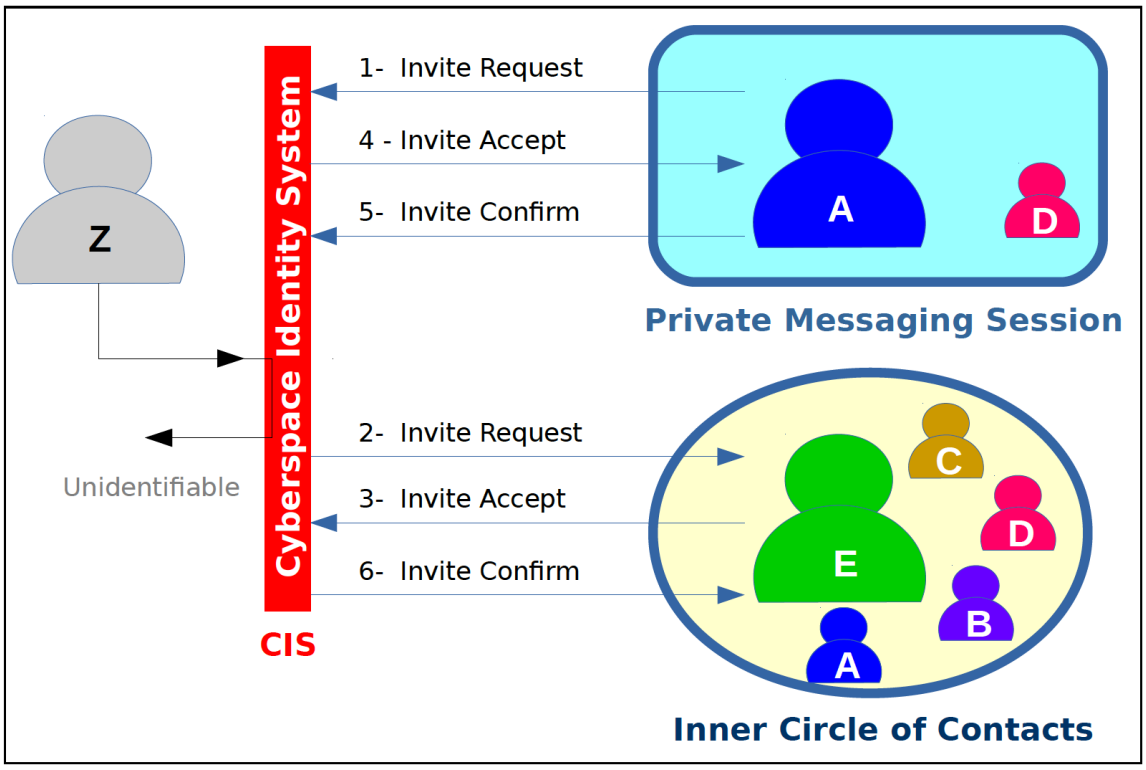

Figure 3: Invitation to participate in private messaging session.

The goal of secure communication is not only applying strong encryption technologies to encrypt data, as described in previous sections, but also in distributing session keys.

The distribution of a session key to a contact as a new member of the chat-room requires looking into the inner circle for the contact's secure channel. The secure channel is then used to send the session key, after wrapping it with a wrap-key that is only known to the sender and receiver.

III. Conclusion

This solution is CALEA compliant because the Registrar has access to the data and can report it to law enforcement through a "Front Door" solution. It fixes the "Going Dark" problem because user interactions and chat-rooms conversations occur inside the system, which the Registrar can decrypt.

The solution is not architected with a "Back Door." Instead it builds trusted communities of users based on mutually agreed connectivity and unbreakable strong encryption, while working together to exclude inappropriate membership and intruders.

References

[1] Communications Assistance for Law Enforcement Act

https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

[2] Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications

https://dspace.mit.edu/handle/1721.1/97690

[3] CALEA II: Risks of Wiretap Modifications to Endpoints

https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf

[4] Going Dark

https://www.fbi.gov/services/operational-technology/going-dark