8.5 Secure Communication

Intent

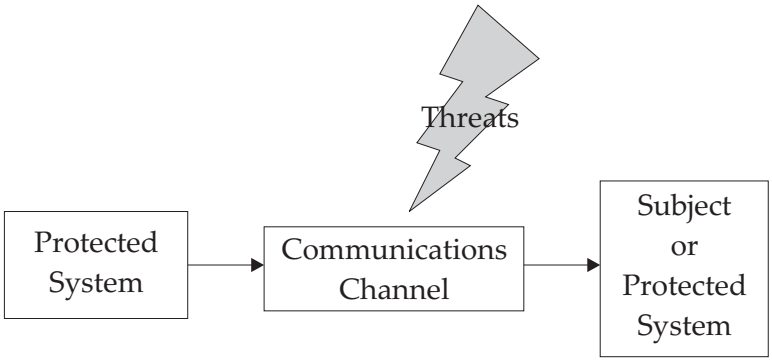
Ensure that mutual security policy objectives are met when there is a need for two parties to communicate in the presence of threats.

Also Known As

None known.

Motivation

A communications channel between two Protected Systems or between a subject and a Protected System may be subject to various security threats. The security provided by the sending Protected System will not be effective if it can be subverted by attacks on the communications channel. Therefore it may be desirable or imperative to protect the channel.



Threats against the communications channel may include:

- Unauthorized disclosure of traffic
- Impersonation of a party to the communication
- Unauthorized modification of traffic
- Diversion or interdiction of traffic

The Secure Communication pattern protects against threats by employing security countermeasures to protect traffic in the communications channel.

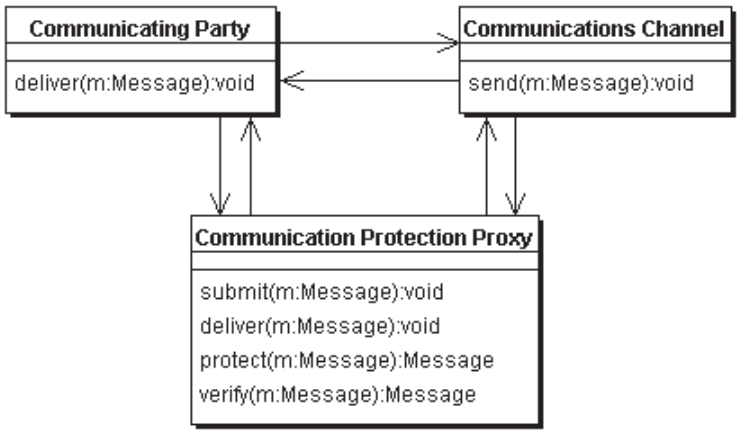
Applicability

Consider using the Secure Communication pattern when:

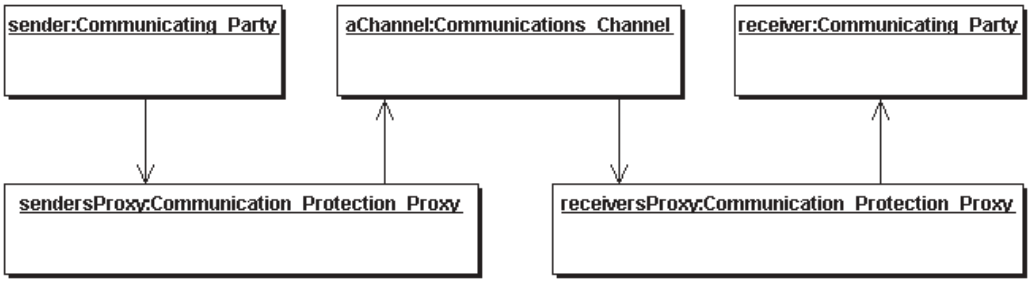
- A Protected System needs to communicate sensitive information with subjects or with other Protected Systems over a communications channel.
- Traffic in the communications channel may be subject to security threats.

Structure

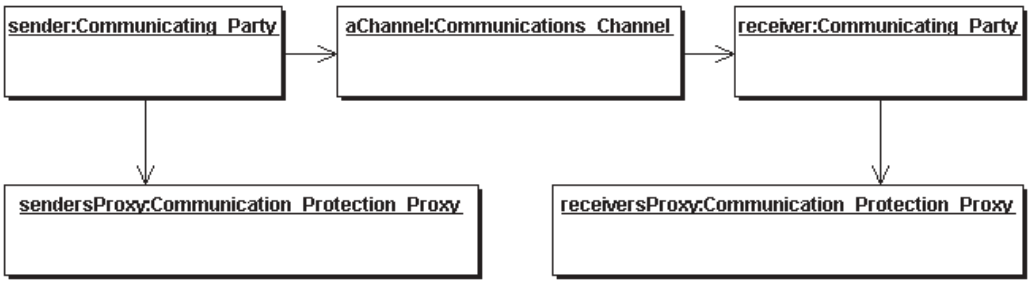
The Secure Communication Pattern has two structural variants.



In the first variant, a Communication Protection Proxy is an inline proxy between the sender/receiver and the communications channel.



In the second variant, a Communication Protection Proxy is an out-of-band service which is used by senders and receivers to protect traffic which they submit to or receive from the Communications Channel. (Note that this variant is more appropriate for use with non-session-oriented or store-and-forward communication protocols.)



Participants

- Communicating Party

  The source and/or destination of messages to be sent over a communications channel.

- Communications Channel

  Carries information exchanged between a message sender and receiver.

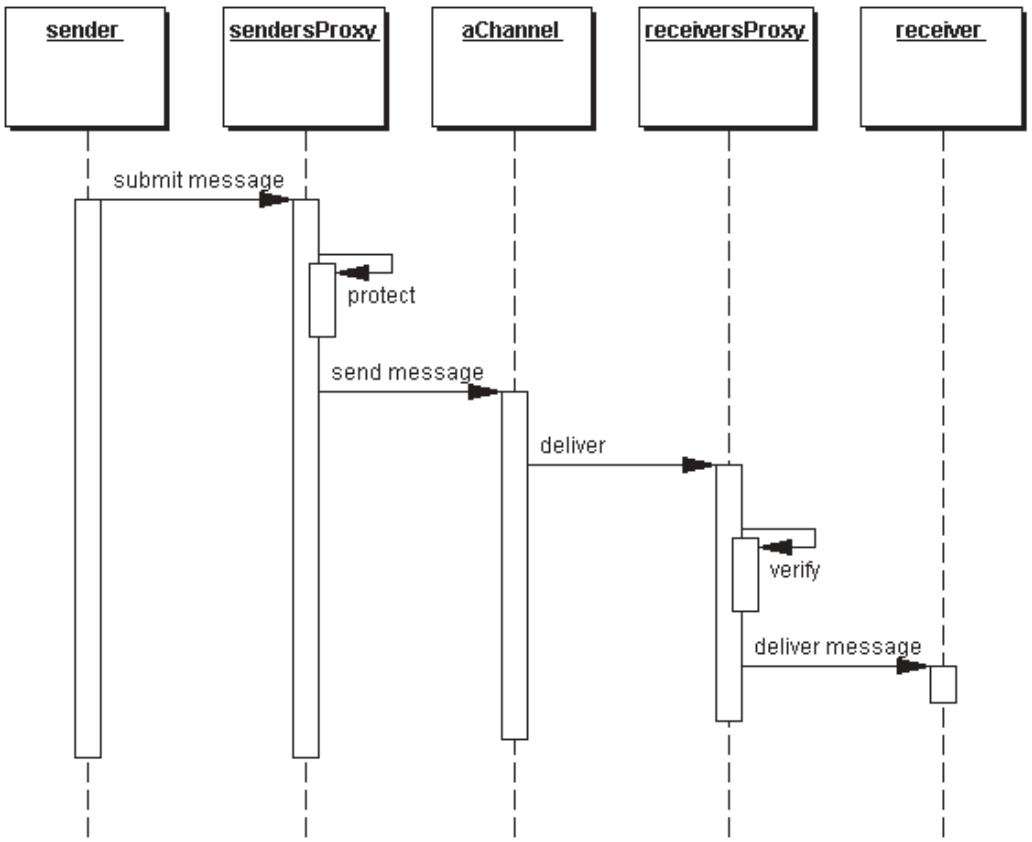
- Communication Protection Proxy

  Protects traffic sent over the communications channel using one of a variety of protection mechanisms.

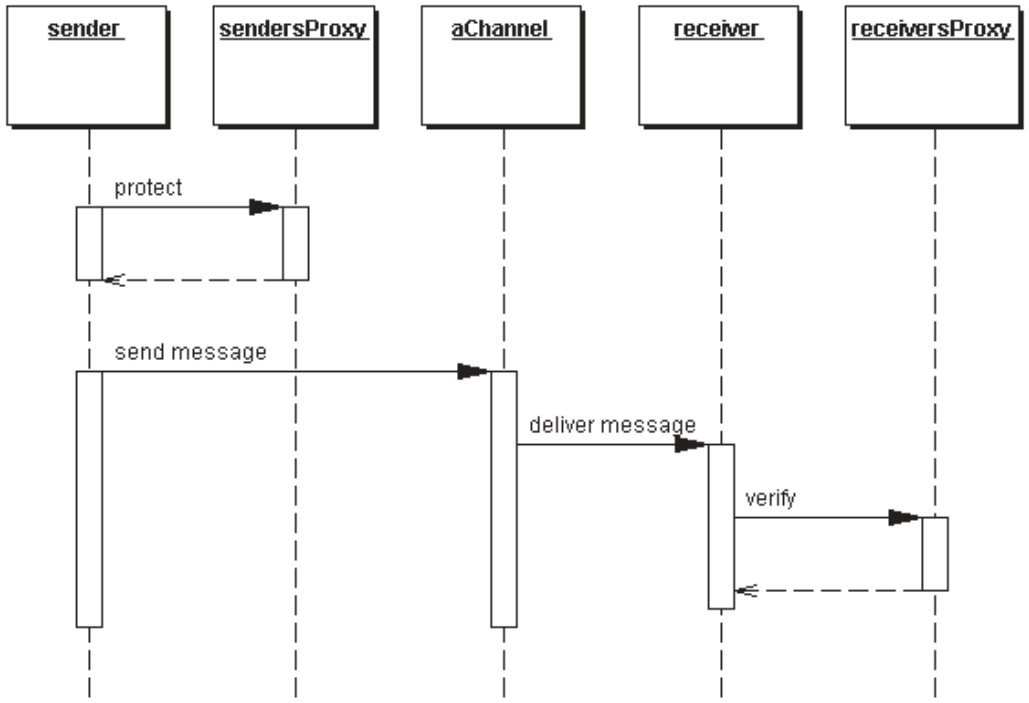
Collaborations

- A sending Communicating Party submits a message to its Communication Protection Proxy for protection.
- The Communication Protection Proxy applies appropriate protection to the message.
- If the Communication Protection Proxy is functioning as an inline proxy (variant 1 above) then it uses the Communications Channel to transmit the message to the Communication Protection Proxy of the receiving Communicating Party.
- If the Communication Protection Proxy is functioning as an out-of-band service (variant 2 above) then it returns the protected message to the sending Communicating Party, which uses the Communications Channel to transmit the protected message to the receiving Communicating Party.
- The receiver obtains messages sent over the Communications Channel; if the receiver's Communication Protection Proxy is serving as an inline proxy, then the message's protection will already have been verified and any necessary decryption will already have been done by the Communication Protection Proxy. If the receiver's Communication Protection Proxy is serving as an out-of-band service, then the receiver will pass the protected message to its Communication Protection Proxy, which will verify the message's protection, do any necessary decryption, and return the verified message to the receiver.

The figure below illustrates the interactions for variant 1 (inline proxy) of the Secure Communication pattern.



The figure below illustrates the interactions for variant 2 (out-of-band service) of the Secure Communication Proxy.



Consequences

Use of the Secure Communication pattern:

- Ensures that data communicated over a potentially insecure communication channel is protected against a known set of threats.
- May reduce communications throughput or increase communications latency.
- May require the use of cryptography (and therefore may require consideration of international deployment issues related to cryptography).
- May interfere with the use of other services (for example, content scanners, proxies, filtering routers) which depend on access to message content between communications endpoints.

Implementation

Secure Communication Proxies may need to apply one or more of the following types of protection to messages in order to counter threats anticipated in the Communications Channel:

- Data Origin Authentication protects against misrepresentation of the identity of a sender of a message.
- Peer Entity Authentication protects against impersonation of parties to the communication.
- Data Integrity protects against undetected, unauthorized modification of data in transit in the communications channel. Data integrity services may provide additional services, including:

  — Replay detection

  The ability to detect that some unauthorized party that captured a sequence of communication exchanges subsequently tried to replay that exchange.

— Sequence ordering

The ability to detect missing or reordered elements of a communication.

- Data Confidentiality protects against disclosure of message contents to unauthorized parties.

One or more of following mechanisms is used to implement the protection features listed above:

- Cryptography
- Cryptographic Key Management
- Hash Functions
- Secure Protocol Handshake Exchanges

For the data content that is to be passed across a communication channel the pattern implementor will need to identify:

1. The protection services and mechanisms that need to be applied in the context of a security policy appropriate to use of the communication channel, and the strength of mechanisms which will be required to counter anticipated threats.
2. The granularity of protection services and mechanisms to be applied (for example, whether protection characteristics will be able to be changed on a per-message basis or only on a per-session basis).
3. What key management and key exchange functionality will be required to support the necessary protection services and mechanisms.

Known Uses

The following are instances of Secure Communication (variant 1, inline proxy):

- Secure Sockets Layer (SSL) and Transport Layer Security (TLS) [IETF RFC 2246 and others]
- Internet Protocol Security [IETF RFC 2401 and others]
- IEEE Standard for Interoperable LAN / MAN (SILS) [IEEE Std 802.10-1998]

The following are instances of Secure Communication (variant 2, out-of-band service):

- Secure Multipurpose Internet Mail Extensions (S / MIME) [IETF RFC 2311]
- Cryptographic Message Syntax [IETF RFC 2630]
- Generic Security Service (GSS-API) [IETF RFC 1508 and others]
- Independent Data Unit Protection (IDUP-GSS-API) [IETF RFC 2479]

Related Patterns

- Protected System [TG_SDP] instances use Secure Communication to protect messages transmitted between their guards.
- Secure Communication uses Security Association [TG_SDP] to store state information about the security parameters to be used to protect messages.
- Single sign-on, role-based access control [APLRAC].
- Authenticated session [NAI].
- Pattern language for cryptographic software [Tropyc].
- Enabling application security, session [Yoder-Barcalow].