Entrust Technologies White Paper

EntrustIPSEC Negotiator Toolkit Overview

Author: Nigel Johnson
Date: March 1997
Version: 1.0

1. Introduction

Entrust® is a family of computer network security products. Designed to be the single security infrastructure for organizations, Entrust provides numerous security services to system administrators, network users, and applications. In particular, Entrust provides automatic and transparent key management so that neither developers nor end users need to understand the details of cryptography to take advantage of Entrust security services.

This document provides an overview of EntrustIPSEC Negotiator Engine, the shared library that allows third-party IPSec (IP Security) applications to take advantage of an Entrust security infrastructure. The EntrustIPSEC Negotiator library is accessed though a set of Application Programming Interfaces (APIs) that are defined and described in the EntrustIPSEC Negotiator Toolkit.

EntrustIPSEC Negotiator implements the Internet Security Association Key Management Protocol (ISAKMP) for IP Security. It is widely recognized that the Internet needs data protection and strong authentication before it can be fully utilized as a business tool. The IETF (Internet Engineering Task Force) has created a Security Working Group that creates standards for the protection and authentication of data packets flowing over the Internet.

These standards are the AH (Authentication Header) and ESP (Encapsulated Security Protocol) standards which specify exactly how to implement the wrapping of the packets, and the ISAKMP standard which describes how to perform the key negotiation and authentication for the AH and ESP. To date, there is no standard for how security credentials are to be created or maintained. In other words, while there are standards for key exchange, there are no standards for key management.

This is where EntrustIPSEC Negotiator is valuable. Since the EntrustIPSEC Negotiator provides ISAKMP key negotiation services and Entrust key management services, vendors who use EntrustIPSEC Negotiator can have a scalable IPSec solution.

EntrustIPSEC Negotiator can be used for any application that requires strong authentication using TCP/IP. Two examples are Internet remote access and single sign-on applications.

2. EntrustIPSEC Negotiator Engine

The EntrustIPSEC Negotiator is an application-layer shared library that provides Entrust key management and ISAKMP/Oakley key negotiation and authentication services.

In order for two parties to communicate using AH (Authentication Headers) and ESP (Encapsulated Security Protocol), each party must know the symmetric (or secret) keys required for these two protocols.

ISAKMP provides a means of negotiating the symmetric keys and making sure that the negotiation is done with the correct party. This is also known as key exchange and authentication.

ISAKMP/Oakley does this using the Diffie-Hellman algorithm for key negotiation and RSA public-key authentication. ISAKMP/Oakley assumes that each end of the negotiation has traded certificates through an out-of-band communication, and therefore trusts the certificates that are passed in the ISAKMP negotiation.

It is this assumption that creates the need for EntrustIPSEC Negotiator. Key management is the most complicated and difficult part of security to implement in an application. For a large-scale system, one cannot presume that every end entity will be able to pre-share its public key with the other party before a communication starts.

The EntrustIPSEC Negotiator uses the Entrust Public-key infrastructure (PKI) to create security credentials for each entity on the network. These entities can be people or processes. These credentials are known as Entrust profiles (epfs) and contain important and sensitive information such as the private RSA keys. The Entrust profiles are stored securely by the EntrustIPSEC Negotiator.

The key management portion of the EntrustIPSEC Negotiator works with the Entrust PKI to perform the following services:

- Security credential initialization
- Certificate generation
- Certificate revocation list (CRL) generation
- CRL checking
- Certificate validation
- Automated key rollover
- Cross-certification
- Authority revocation list (ARL) generation
- ARL checking
- Key recovery

3. Typical Use of EntrustIPSEC Negotiator

Currently, the most common use for the EntrustIPSEC Negotiator is Internet remote access. Internet remote access can support thousands of users trying to connect to a corporation. Each of these users needs to be authenticated and have his/her data protected.

The EntrustIPSEC Negotiator works in concert with an AH/ESP Engine to provide full IPSec services. The advantage of IPSec is that security

and authentication can be implemented without any changes to the applications on the desktop.

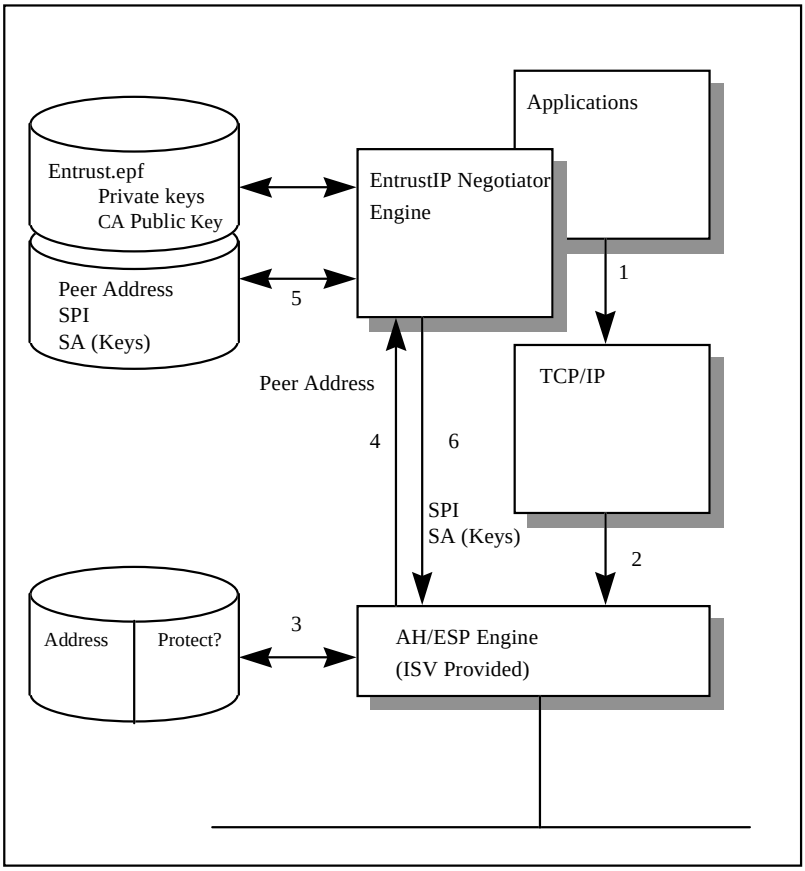

Figure 1: Steps involved in IPSec Communication

Figure 1 shows the information flow in a typical outbound message using the EntrustIPSEC Negotiator and a third-party AH/ESP Engine. As an example this could be the client end of an Internet remote access solution connecting to the corporate gateway. The following is a detailed description of Figure 1:

1) The application calls the TCP/IP stack
2) The TCP/IP packet is captured by the AH/ESP Engine.
3) The AH/ESP Engine decides whether traffic going to that specific address needs to be protected. If not, the packet is sent with no modification.
4) If the packet needs to be protected, the AH/ESP Engine passes the address to the Negotiator and requests the Security Association (SA) and Security Parameter Index (SPI) for that address.
5) The Negotiator looks up the SA and SPI in its internal database. If an SA has not been negotiated for that specific address, then the EntrustIPSEC Negotiator initializes an ISAKMP/Oakley negotiation with the peer address.
6) Once that negotiation is complete, the SPI and SA are passed to the AH/ESP Engine. Now all packets sent to that address are

protected by the AH/ESP Engine with keys negotiated by the EntrustIPSEC Negotiator.

Figure 2 shows the information flow in a typical inbound IPSec packet. An example of this would be the gateway of an Internet remote access solution.

If the arriving packet has an SPI (Security Parameter Index) associated with it, the SA (Security Association) associated with that SPI is retrieved from the EntrustIPSEC Negotiator database. If the SPI is not in the database then the packet can be rejected.

If the arriving packet does not have an SPI embedded in it, the AH/ESP Engine can presume that the packet doesn't have an SA associated with it. Since there is no SA associated with the packet it can be rejected.

If the incoming packet comes in to the port reserved for ISAKMP negotiation then the AH/ESP Engine will pass all of the ISAKMP packets to the EntrustIPSEC Negotiator. The Negotiator will pass the reply packets through the AH/ESP Engine

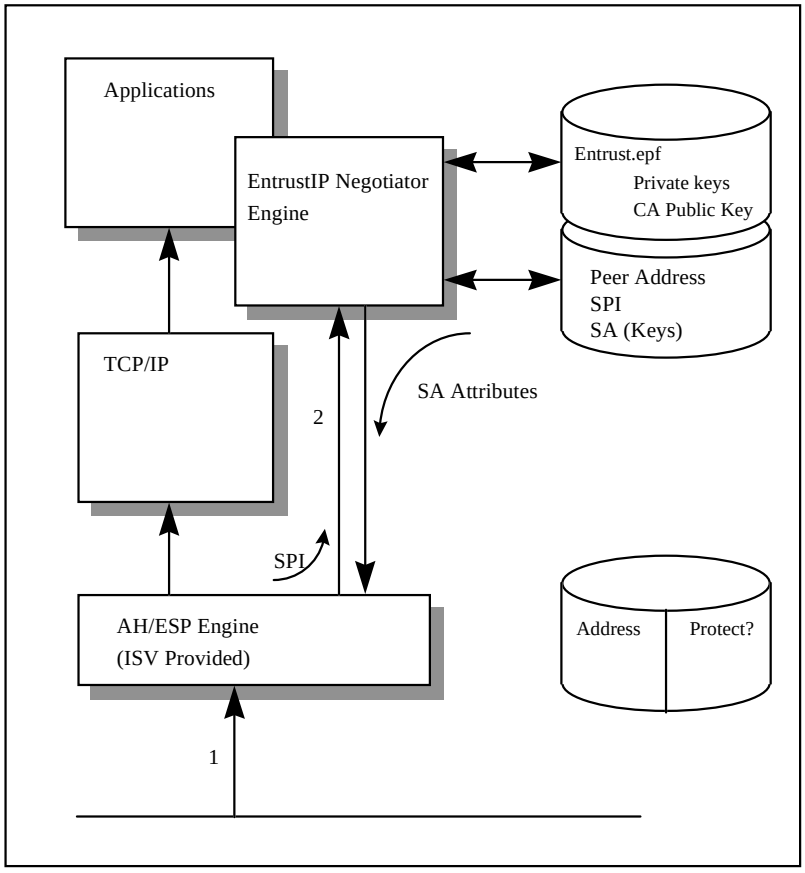

Figure 2: Steps involved in Processing Incoming IPSec Packets

4. Interoperability

The EntrustIPSEC Negotiator will interoperate with any other implementation of ISAKMP/Oakley that complies to the standards, no matter what CA the other ISAKMP application uses.

The Negotiator has an interface that will allow the user to list certificates that should be trusted, no matter under which Certification Authority (CA) domain they fall. However, these CAs must produce X.509 version 3 certificates.

This means that any vendor or customer that uses EntrustIPSEC Negotiator will be able to communicate with any other application using ISAKMP Oakley.

5. Scalability

Since the EntrustIPSEC Negotiator is based on Entrust key management, it can scale up to hundreds of thousands of users.

There are many application vendors that are offering IPSec services. However, any IPSec product being used by more that several hundred users will need a key management infrastructure in order to remain secure and easy to use. The vendor of any IPSec product should be able to provide clear, simple answers to these questions:

- How do the security credentials get to each person or machine?
- How are these credentials managed over time?
- How do I manage trust in my network?
- Is there a PKI in place?
- What happens if somebody leaves my organization?

6. Related Articles and Web Sites

IETF IPSec Working Group Home Page:
http://www.ietf.org/html.charters/ipsec-charter.html

Internet Security Association and Key Management Protocol (ISAKMP)

IP Encapsulating Security Payload (ESP) (RFC 1827)

IP Authentication Header (AH) (RFC 1826)

7. Definitions

AH	Authentication Header: The mechanism for ensuring that each packet is authenticated as coming from the expected location or indivdual
ESP	Encapsulating Security Protocol: The mechanism for encrypting the data with TCP/IP packets
ISV	Independent Software Vendor
SA	Security Association: This defines the keys and algorithms to be used for the AH and ESP
SPI	Security Parameter Index: This is a number created by the AH/ESP Engine to keep track of which SA should be used with which incoming packets.

Printed in Canada.