From: Interoperable Networks
for Secure Communications (INSC)
Symposium 4-6 November 2003

DRDC Ottawa SL 2003-113

An Analysis of the INSC Key Management Infrastructure

Dr. Steve Zeber
DRDC Ottawa
Steve.Zeber@drdc-rddc.gc.ca

Abstract

This paper analyses the key management infrastructure implemented and demonstrated in INSC. The principal conclusion is that the integration of IPsec/IPv6 with PKI services has yet to be achieved. This will require substantial progress in both IPsec and PKI product implementations.

1. Introduction

The goal of the Interoperable Networks for Secure Communications (INSC) project is to investigate and demonstrate the use of a secure IPv6 network infrastructure and applications that could be used to support a coalition joint task force operation. The infrastructure must be able to support communications and information sharing in a secure manner both within the coalition command structure and between the coalition members and their national headquarters.

This paper analyses the key management infrastructure that was implemented and demonstrated in INSC to support the network security services and draws conclusions regarding the maturity of the technology and the effectiveness of the solution.

2. INSC Network Architecture

The INSC network model assumes three operational components: a joint command (JC) component, a land (L) tactical component and a maritime (M) tactical component. Therefore, the INSC network comprises three corresponding wide-area components (JCWAN, LWAN and MWAN) each of which interconnects with one or more national[1] and/or coalition LANs (CLANs) supporting the corresponding operational component (Fig.1).

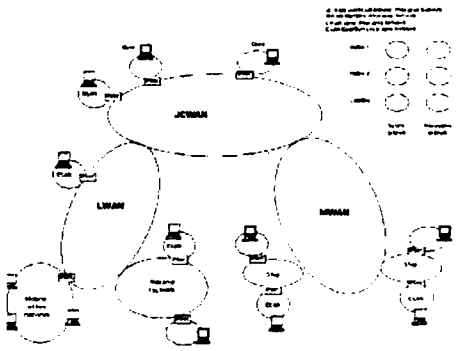

Fig.1

3. INSC Security Architecture

The INSC security architecture defines two coalition security domains: a "black" unprotected domain and a "red" protected domain. IPsec devices are used to separate the coalition red domain from the wide area transit (black) domain and from national security domains. Each CLAN connects to wide area network services through an IP security gateway (IPsec GW). Coalition communications between CLANs are protected by virtual private network (VPN) connections tunneled across the transit networks, which may include national security domains as well as unclassified public domains (Fig. 2)

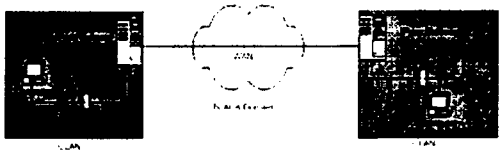

Fig. 2

4. Requirement for Key Management Infrastructure

IPsec security mechanisms require cryptographic keys to be issued and managed in a secure and trusted manner in

[1] Although at least one nation has implemented secure communications to national LANs, multi-level security is beyond the scope of INSC and is an area for further research.

accordance with a specified security policy. The INSC security policy did not address key management, nor did it explicitly delegate responsibility for this policy. As a result, policy on key management evolved through pragmatic ad-hoc decisions made as implementation and testing required.

Initial testing of the IPsec GWs and VPN connections was performed using manual distribution of preshared symmetric keys. However, the final testing and demonstration was done using X.509 public key certificates to provide authentication when establishing security associations (SAs) between IPsec GWs. This necessitated a public key infrastructure (PKI) to generate, distribute, and manage the certificates.

A typical PKI includes a Certificate Authority (CA), one or more Registration Authorities (RAs), an X.500 or LDAP electronic directory service to store and distribute the certificates and certificate revocation lists (CRLS), and possibly client software for the systems or devices using the keys and certificates. Well-defined policies and procedures are also essential in providing the basis for the trust associated with the PKI services, which include key generation and distribution, and certificate enrolment, renewal, and revocation.

The following sections describe how PKI services were integrated into the INSC infrastructure.

5. Certification Authority

The main problem was to find a CA/RA implementation that operated over IPv6. Since none of the leading commercial PKI products were enabled for IPv6[2], the adopted solution was to implement a CA using OpenSSL. Five nations in total (CA, DE, FR, UK, US) implemented an OpenSSL CA. Canada implemented an off-line CA with integrated RA functions. With an off-line CA it was necessary to provide the CA services to the client devices using manual procedures. Certificate requests and signed certificates were transferred between the CA and the devices manually using diskettes.

The manner in which CA operations were executed was determined locally. The Canadian CA implemented shell scripts which a system administrator executed manually to provide CA operations. The CA was initialised using a script that first removed all files from any previous CA, and then generated a CA private key, a self-signed root certificate and an initial signed but empty CRL. Additional scripts were executed as required to sign a certificate, revoke a certificate, and issue a CRL. There was no automated service for certificate renewal or CRL update.

6. Directory Service

As with the CA, there was no commercial IPv6-capable X.500 or LDAP directory server product, so OpenLDAP, an open source implementation was used for the directory server. Three nations (CA, DE, and US) implemented OpenLDAP directory servers in the black domain interconnected by the JCWAN. A combination of LDAP commands, a Java client, and a free version of a commercial IPv6-capable LDAP client were used for Directory administration. Nations that did not operate a directory server arranged with a nation operating a server to host their entries.

The main purpose of the directory service in the black domain was to store the IPsec GW certificates and the CRLs. Certificate and CRL information was transferred between the CA and the local directory server manually using diskettes. Directory entries were updated using shell scripts. Each server replicated all of the information it mastered to every other server so that each server held a complete copy of the INSC directory database to provide robustness and survivability. Replication, triggered by any change to the directory database on a server, maintained synchronization with all other servers.

7. Operating Policy and Procedures

No formal policy was developed for the PKI services and procedures. Procedures were developed or adopted in a pragmatic manner to achieve an operational capability

[2] Much later, the project became aware of an IPv6-capable PKI implementation from the University of Murcia in Spain.

within the time and resource constraints of the project. The following subsections summarize the policies and procedures as implemented in INSC. In cases where the particular details of a procedure differ among the INSC nations, the description reflects the implementation in Canada.

7.1 Trust Model

With multiple CAs issuing device certificates the ideal would be to establish cross-certification agreements among all CAs. Because INSC was conducted in a closed environment, it was agreed that certificates signed by any INSC CA would be trusted. The root certificates were published in the directory and were circulated by an out-of-band procedure (i.e., e-mail) to all national testbeds as well. These certificates were also loaded manually into the IPsec GWs.

7.2 Certificate Profiles (CPs)

Certificate profiles were defined and agreed in the INSC project for both root and device certificates. The key length was not specified in the profile but it does affect the certificate size, which can affect interoperability.

7.3 Certificate Policy (CP)

A formal CP was not developed for INSC. Since the goal of INSC was to investigate and demonstrate the operation and use of the technology, developing a formal CP was not a priority.

7.4 Certification Practices Statement (CPS)

A formal CPS was not developed for INSC. The sum of the operating procedures described in Section 7 comprises the CPS for INSC.

7.5 Device Key Generation

IPsec device keys were created locally on each IPsec GW using a script to generate a private key and a public key certificate request file. The private key was stored in a local directory and always remained on the GW device.

7.6 Certificate Enrolment

The certificate request file was transferred manually on a diskette to the CA where the certificate was signed. The signed certificate was then transferred to the LDAP directory on a diskette and was added to the corresponding device entry using a script. The certificate was also loaded manually from the diskette onto the IPsec GW.

7.7 Certificate Revocation

A device certificate was revoked by executing a script on the CA. The script generated an updated CRL which included the revoked certificate ID and a file to update the CRL information in the LDAP directory. The new CRL was transferred to the directory on a diskette and the directory information was updated by executing a script on the directory server.

No policy was defined governing certificate revocation nor were operating procedures defined for requesting a certificate revocation. The only reasons for revoking a certificate were certificate renewal and to demonstrate the effect of certificate revocation within some operational scenario.

7.8 Certificate Expiry and Renewal

There was no automated mechanism to check for, and renew, certificates about to expire. A certificate about to expire had to be renewed by revoking the certificate and issuing a new certificate using the manual procedures previously described.

7.9 Certificate and CRL Caching

No policy was defined regarding certificate and CRL caching or the use of cached entities. The IPsec GW procedures for negotiating and establishing a security association with a remote IPsec GW assumed that the certificates were stored in locally on the GW. Consequently, the device certificates were copied into a local directory on each IPsec GW. As no external directory service was assumed, the IPsec implementation did not include any capability to retrieve certificates or CRLs from the directory. Scripts were developed to retrieve and check CRLs but these were not implemented uniformly.

7.10 Certificate Validation and CRL Checking

Certificate validation and CRL checking was left as the responsibility of the local IPsec GW administrator due to the lack of uniform support for retrieving and checking CRLs across different IPsec implementations. In some cases, CRLs were cached locally on the IPsec GW, but refreshing the CRL was the responsibility of the IPsec GW administrator. The FreeS/WAN default policy was to accept expired CRLs, but it could be configured to require a valid CRL to establish an SA. However it still lacked a dynamic CRL retrieval capability.

8. Conclusions

The principal conclusion drawn from the INSC experience is that the integration of current IPsec/IPv6 implementations with electronic key management is minimal to nil and remains to be achieved. Most IPsec implementations do not support the use of X.509 certificates for authentication. For example, in the IABG FreeS/WAN implementation, the capability was provided using an independently developed patch. Nevertheless, even with the patch, the implementation did not provide automatic CRL retrieval and checking, which would be required for policy–based certificate validation.

In those cases where the IPsec/IPv6 implementations do support the use of X.509 certificates for authentication, the integration is incomplete because the support for processes such as the dynamic retrieval of certificates and CRLs from an external directory server is not implemented uniformly, and the implementations do not support a standard API to request and receive PKI services, such as certificate enrolment. The lack of an API makes integration with particular commercial PKI products difficult. Commercial products that only support proprietary APIs also make integration difficult.

Because IPsec does not perform fragmentation, certificates that are too large can result in IP packets larger than the maximum supported size and thus prevent the successful establishment of SAs. This problem was encountered at least once during testing in Canada. The solution was to reduce the key length, indicating that policy decisions on key length and other aspects of the certificate profile have performance implications that must be taken into account.

Security policy was also a weak aspect of the INSC infrastructure, as it was not addressed in any detail. Security policy and operating procedures must be well planned and in place before deployment of the security infrastructure to provide the desired level of trust in the security services and mechanisms. Furthermore, the operation of the security services and mechanisms should be tightly coupled to the security policy.

The INSC trust model may also not be the best solution for a coalition operation. A better trust model would be that provided by a single coalition PKI with one root CA administered by the coalition command in accordance with a coalition security policy. This would obviate the need for multiple cross-certification agreements, enhance the achievable trust level, and simplify certificate management. An operation involving several disconnected security domains would possibly require multiple subordinate CAs, but they would still be subordinate to a single coalition root CA.

Automated key management for IPsec in a tactical environment also poses other operational problems that INSC did not address. Some of these include operation with limited bandwidth, communicating with mobile users, and CRL checking and the renewal of expired certificates and CRLs under electromagnetic emission control (EMCON) conditions which may preclude communications with a remote LDAP server or CA.

Finally, INSC did not address the issue of evaluation and the trust levels that can be achieved with the IPsec and PKI security technologies.

The highest priority challenge for the future, highlighted by INSC, is to achieve the integration of IPsec with electronic key management. A second challenge will be to tailor implementations to work in a tactical

environment that requires mobility and imposes bandwidth and EMCON constraints. This will require substantial progress in both IPsec and PKI implementations and the cooperation of the commercial vendors. Until this is a reality, a scalable manageable security infrastructure will not be possible.

#522076

CA024498