A Composite Architecture for Network Security at JPL

Robert B. Mead, Tom G. Dearmond, and Joseph S. Sherif

JPL, California Institute of Technology
Pasadena, CA., 91109

Abstract:

We advance a tentative composite model for computer security at JPL, together with inter and intra networking with other NASA centers and overseas clients. JPL for the past two years had been involved with the Distributed Computing Environment (DCE) as a security infrastructure. Other NASA centers may be using Entrust (PKI) Public Key Infrastructure as their security architecture in the near future. To alleviate the problems of incompatibility, we propose a composite model that allows JPL to continue utilizing DCE, and at the same time plan to implement Entrust (PKI) for secure e-mail between NASA centers at the near future and then integrate DCE and Entrust in a composite infrastructure that supports authentication, authorization, privacy, integrity and non-repudiation.

Background:

A. DCE

1. Elements of DCE

The Open Software Infrastructure (OSF) Distributed Computing Environment (DCE) is a package of technologies and tools that support vendor-neutral distributed computing. DCE provides security (Authentication, Authorization, Privacy, and Integrity) and is highly scaleable. It is designed to support distributed applications in heterogeneous hardware and software environments. DCE is a key technology in three of today's most important areas of, computing security, the World Wide Web and Distributed Objects. DCE security services are provided by servers running on machines in different geographic locations. This provides redundancy if one fails. The default is to select a security server randomly from those available until an active server is found.

At JPL, the DCE security service includes the security registry database, the authentication service and the privilege service. The security registry database is structured in such a way that allows a single DCE cell to simulate multiple DCE cells. The authentication service uses Kerberos V5 to authenticate clients' identity with servers. The privilege service creates Privilege Access Certificate (PAC) which contain a listing of clients' identity and roles. Roles based authorization help protect resources based on a client's job classification. The JPL DCE environment may contain many cells. All users and groups are registered in a single cell (called the authentication cell) containing people, groups, server principles, accounts, etc. All users and groups are therefore foreign to the JPL working cells. This means that the authentication cell must be part of the principal name when the users login into a working cell. Server applications execute on machines that are part of a work cell therefore the authorization cell contains security and identification information and the work cell contains servers, server bindings, server groups and server profiles[1].

2. Potential Users of DCE

- An organization consisting of multiple computing sites that are already interconnected by a network can use DCE to tie together and access resources across the different sites. The different sites can be in different countries, or even in different continents.
- Any computing organization comprising, or expecting to comprise in the future , more cooperating hosts than can be easily administered manually can benefit from the administrative support afforded by a DCE environment. For example, in DCE the database of computer users and their associated information (such as passwords) can be administered centrally, removing the need for an administrator to update information on every single node in the network each time a new user is added.
- Organizations that wish to participate in networked computing on a global basis. Since DCE supports standard directory services that will be used throughout the world, a site that participates in DCE will be able to plug into that worldwide directory service database, allowing it to both "see" and access information about other sites and organizations around the world. In turn, it will be able to add itself to the directory service, allowing itself to be "seen" and accessed, if desired, by other sites worldwide.
- Organizations that write distributed applications can use DCE as a platform for their software. Applications that are written on DCE can be readily ported to other software and hardware platforms that also support DCE.
- Organizations that would like to make a service available over the network on one system (for example, VMS), and have it accessible from other kinds of systems (for example, UNIX based workstations).
- An office with isolated computing resources can network the computers together and use DCE for data and resource sharing.

3. How DCE Security Works (Kerberos Model)

- When a DCE cell is first created, the DCE security administrator runs a program to create an initial security database. The administrator then starts up a DCE Security Server, called **secd**, on the same machine as the database. Using the **rgy_edit** command, the administrator creates user accounts in the security database. (please see Figure 1).

- After the administrator has created an account for a user, the user can participate in a secure DCE system. Typically a user logs in at the beginning of the session. The Login Facility interacts with both the Authentication Server and the Privilege Server. It sends a request for the authentication credentials to the Authentication Server. The Authentication Server sends back the authentication credentials, called a **Ticket**. The Authentication Server's reply is encrypted using the user's password, so if the user can supply the right password, the reply can be decrypted and the Ticket can be accessed. Tickets are used by clients to authenticate themselves to servers; that is, to prove that clients are really who they say they are.
- Next, the Login Facility sends the Ticket to the Privilege Server. The Privilege Server returns authorization credentials, called a PAC (Privilege Attribute Certificate). The PAC contains authorization information specific to the user, such as which groups the user belongs to. PAC's are used to authorize users; that is, to help a server decide whether users should be granted access to resources that the server manages. When the Login Facility has finished running, the user has a security environment and can communicate in a secure way with application servers.
- For example, if the user runs an application client, the application client can use Authenticated RPC (Remote Procedure Call) to communicate with the application server. The application server receives the RPC-based request, which includes the user's PAC. The server inspects the user's authorization credentials and the Access Control List (ACL) associated with the resource the user wants to access. If, for example, the ACL says that any user in the group **friends** can access the resource, and the user's PAC shows that the user is in the **friends** group, then the server will give the user access to the resource.

  The authentication and authorization information that is sent over the network is all encrypted so that only the intended recipients are able to decrypt and read the messages. If desired, the application data can be encrypted as well. This prevents any unauthorized user from being able to read data that is sent over the network.

B. Entrust (PKI)

1. Elements of Entrust (PKI)

Entrust is the only complete Public-key Infrastructure (PKI) that provides end-to end security (Privacy and integrity) through encryption, authentication, authorization and non-repudiation. It is a fully managed environment that embraces revocable electronic identities, digital signatures, message encryption in transmission and storage, along with assured delivery, decryption and verification upon receipt. Its software uses 1024-bit digit signature, which extends the life span of digital signatures.

Entrust runs on Microsoft Windows 3.1, NT/95. Macintosh 7.1 and 7.5, HP-UX 9.03 and 9.0, SunOS 4.1.0, Solaris 2.4 variants of UNIX. Entrust software uses RSA technologies, which is a part of existing and proposed standards for the Internet and World Wide Web, CCITT, ISO, ANSI, IEEE, and business, financial and electronic commerce networks around the globe.

Entrust can also use DES, DSS, CAST, and NIST DSA-SHA. Entrust also enables organizations to communicate over the Internet privately and affordably by providing a single security infrastructure shared across a variety of applications. Organizations need to define security provision only once rather than separately for each individual application[2].

1.Potential Users of Entrust

- Organizations that deal with deployment of mission critical applications.
- Organizations that deal with Electronic Mail, Electronic Commerce (EC), Electronic Data Interface (EDI), and Financial Communications such as:
    - S.W.I.F.T (Europe)
      Society For Worldwide Interbank Financial
      Telecommunication
      5800 Institutions
      156 countries
      688 Million messages per year (1996)
    - IBM, Lotus Development Corp., Jet Form, HP, Harbinger Corp.
    - Organizations that deal with:
        - Electronic Mail over the Internet
        - Data Archival
        - Transaction Routing
        - Secure Mail Boxing
        - Internet and Intranet Security
        - Smart Card Management Systems

3. How Entrust Security Works (Public Key Infrastructure(PKI))

- Each user has two pairs of keys: one encryption key pair and one signing key pair. Each key pair consists of a private key and a public key. The encryption key pair consists of an encryption public key and a corresponding decryption private key. The signing key pair consists of a signing private key and a corresponding verification public key.(please see Figure 2).

Users' encryption public keys are widely known and publicly available so that any user can encrypt data for others (known as *recipients*) using those keys. Recipients can decrypt encrypted data that was intended for them using their decryption private keys. Since only the recipients have the appropriate decryption private keys, nobody else can decrypt the data. Users' decryption private keys must never be revealed.

A user's signing private key is used to sign data. The user's corresponding verification public key (certified by an appropriate authority for integrity) is included with the signed data to allow others to verify the signature and the integrity of the data.

- To sign and encrypt a file, the Entrust/Client application proceeds as follows:

1. The Client takes the signing private key of a user and digitally signs a file. The user's corresponding verification public key (certified by an appropriate authority for integrity) is included with the file to allow others to verify the signature.
2. The Client generates a random symmetric key and uses it to encrypt the file. The symmetric key is used only once to encrypt this particular file and it is never used again.
3. The Client searches an online directory for the encryption public keys of the intended recipients and uses these keys to encrypt the symmetric key (that was used to encrypt the file). Therefor, the symmetric key is encrypted as many times as there are intended recipients.
4. The Client includes copies of the encrypted symmetric key (with the names of the corresponding recipients) at the beginning of the encrypted file.
5. The end user gives a copy of the encrypted file to the recipients.

- To decrypt the file and verify the digital signature, Entrust/Client proceeds as follows:

1. The Client locates the name of the recipient and the corresponding encrypted symmetric key in the list of recipients included with the encrypted file.
2. The Client decrypts the encrypted symmetric key using the recipient's corresponding decryption private key.
3. Using the symmetric key, the Client decrypts the encrypted file.
4. The Client takes the verification public key of the user who signed the file and uses it to verify the signature. If the protected file has not been altered since it was encrypted and signed, the signature is accepted.

C. Analysis

1. DCE:

- DCE per se can support authentication and authorization only. However with the utilization of SNARE software [3], and/or other available plug-ins, DCE can support secure E-mail, data and full session encryption.

- For DCE client/server to provide authorization, authentication, privacy and integrity, all systems must be in a DCE cell.
- For generic client/server, with client not in DCE machine but server is on DCE machine, DCE SNARE software should be used to ensure privacy and integrity together with private key.
- DCE uses Kerberos V5 to provide authentication and authorization. The kerberos algorithm is continuously in a state of improvements and change.

2. Entrust (PKI)

- Entrust (PKI) is a stand alone bona fide complete security infrastructure that can provide authentication, authorization, privacy, integrity, and non-repudiation at the machine, network and inter-networking levels.
- It uses a defacto government encryption standard Rivest, Shamir, Adleman (RSA)and/or DES-3.
- It supports secure FTP file transfer, Telnet session (login/logoff), electronic mail, and Electronic Data Interchange (EDI), along various telecommunications media including the Internet.
- Entrust can also use DSS, CAST and NIST/SHA encryption technologies
- Entrust conforms to NASA policies concerning telecommunications security.

3. DCE and Entrust

- It is not impossible to use DCE and Entrust together as viable security architecture for JPL. In this case we will use three DCE cells, one for authorization (people), one for engineering (machines) and the third for everything else (client systems). TMOD together with Goldstone, Madrid, Canberra, DSN Test Facility (DTF-21) and Merritt Island (MIL-71), at Cape Canaveral will be protected by firewalls. Entrust (PKI) will be used for E-mail between and among the various NASA centers, JPL and other overseas facilities. DCE and Entrust can be integrated through connectivity of DCE and X.500 Global Directory Services, together worth X.509 Entrust (Certificate Authorization) and X.500

D. Conclusion and Recommendations

This report addresses two unique security infrastructures that may be considered in implementing JPL security architecture. These two infrastructures are the Distributed Computing Environment (DCE) and Entrust Public Key Infrastructure (PKI). At JPL at the present time, DCE infrastructure is in service at a small scale within the Telecommunications and Mission Operations Directorate (TMOD), The Network Control Project (NCP) and other sections. DCE equipment had also been purchased (but not yet commissioned) at various Deep Space Network (DSN) sites such as Goldstone, Madrid, Canberra, DSN Test Facility (DTF-21), and Cape Canaveral Merritt Island (MIL-17) at the other NASA Centers, Entrust (PKI) seems to be the favorable security architecture candidate for adoption.

Recommendations for security architecture adoption at JPL intra and inter-telecommunications with other NASA centers and overseas clients include the following:

1. At JPL, we should continue implementing the Open Software Infrastructure (OSF) Distributed Computing Environment since DCE supports authentication and authorization (Kerberos).
2. For DCE to support privacy and integrity, DCE should be integrated with SNARE software plug-ins, or other similar available plug-ins. Each workstation needs a plug-in unit.
3. DCE together with SNARE and utilizing DES-3 encryption would provide a security architecture that supports authentication, authorization, privacy and integrity. Thus we will have secure E-mail, data and full session encryption.
4. As far as inter-telecommunications between JPL and other NASA centers both parties should have DCE architecture and/or both belong to the same DCE cell.
5. If other NASA centers or other clients do not belong to DCE architecture or if they plan to implement Entrust (PKI), then JPL should plan to implement and utilize Entrust (PKI) to ensure secure E-mail between JPL and the other centers. At a later date, and after Entrust (PKI) is installed both DCE and Entrust can be interfaced through connectivity of DCE and the Global Directory Services (X.500), together with X.509 Entrust (Certificate authorization) and X.500.
6. Eudora E-mail may use PGP encryption for security.

References:

1. Transarc Publications, 1994-1997.
2. Entrust Publications, 1995 1997.
3. SNARE software Publications,1997.

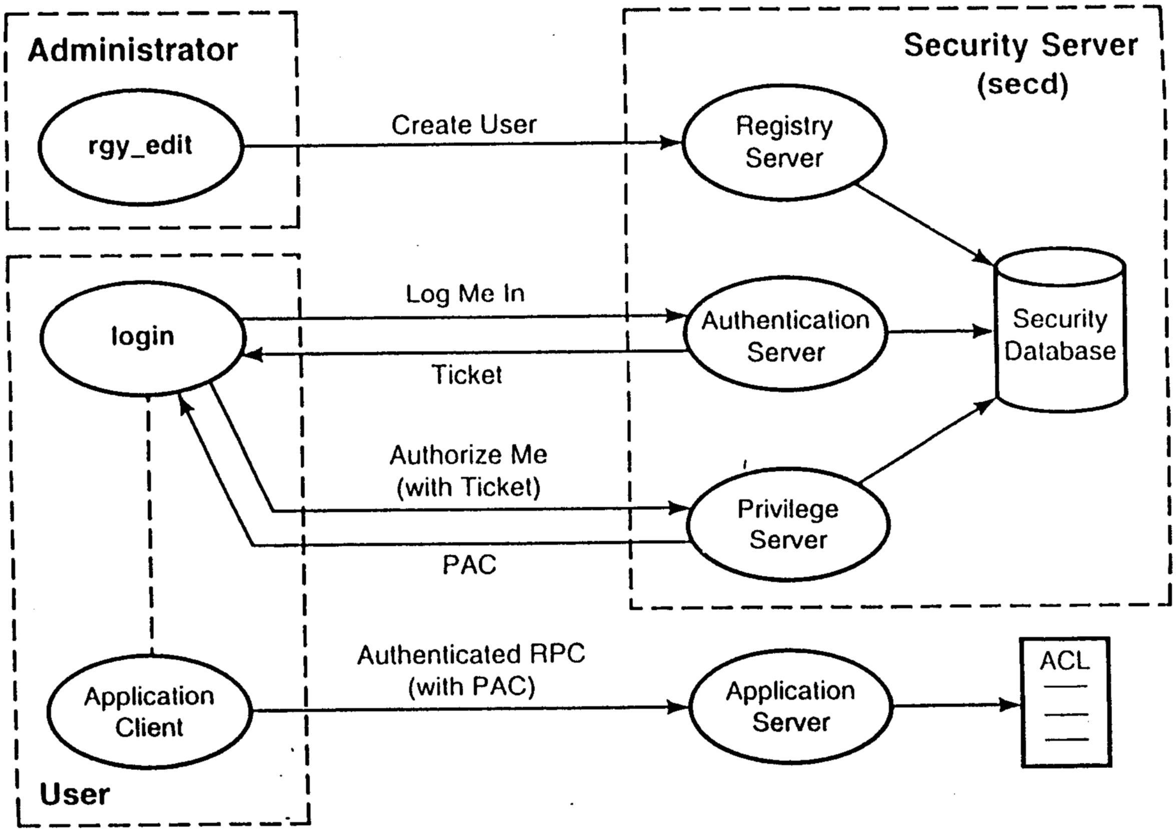

Figure 1. DCE Security Interactions [1]

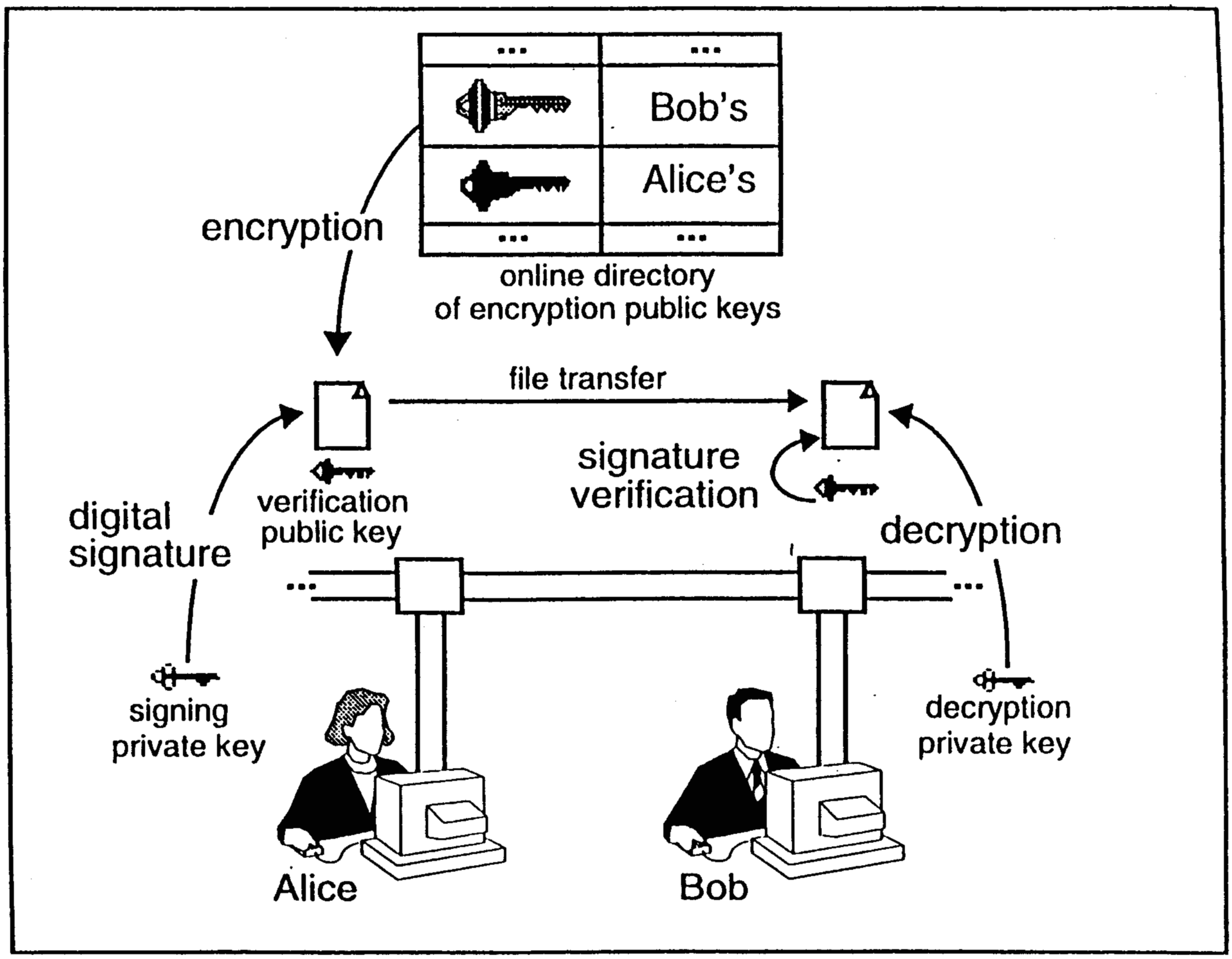

Figure 2. Entrust Public Key Cryptography [2]