Proof of Concept Issues

Internal Issues

External Issues

- Modular PKI meets most requirements of Law Enforcement.
- Nullifies industry objections of cost and viability.
- Modularity puts key escrow debate back into policy and takes it out of technology.
- Design uses accepted standards and protocols.
- PKI allows for arbitrary encryption algorithms.
- Only design for which an individual's secrets *never* come together in key recovery process -- this makes abuse of system much harder to accomplish.
- Data recovery and key recovery are accomplished through distinct mechanisms.
- Can be supported via hardware or software.
- Proof of concept demo marries in house development with commericially available products: a prototypical example of the best way to proceed.

ACTIONS:

- Prototype Modular PKI for internal security solution. Software first, hardware to follow. Q involvement essential. Make hard decision on FORTEZZA solution.
- Take PKI demo to government agencies to demonstrate ease of use and adherence to public key recovery guidelines and get feedback.
- Establish commercial awareness of solution; work together to build products (provided they are guaranteed a market).

A Modular Public Key Infrastructure for Security Management

Proof of Concept Proposal

(b)(1)
(b)(3)-P.L. 86-36

Abstract

A six month plan is outlined for developing and demonstrating a fully functional prototype software suite based on the [redacted] modular public key infrastructure (PKI). The prototype will support key escrow for law enforcement, a separate data recovery component for restoration of archived information, secure message encryption for electronic mail (e-mail), and strong authentication. Initially, two parallel approaches are advocated. One team will investigate the technical validity (and viability) of the design using in-house developed code leading to a prototype which will demonstrate the unique features of this PKI. The other team will determine the feasibility of using commercial off the shelf (COTS) products to implement the infrastructure. Time permitting, a fully interoperable prototype, using commercially available products, will be implemented and demonstrated.

The current Modular PKI description is similar to an Internet Engineering Task Force (IETF) draft. It provides a general blueprint of a PKI without the hardware/software implementations that demonstrate its viability. This project will determine that viability, and if successful, be sufficient evidence to consider pushing the PKI draft to the next natural stage: an IETF Request for Comment (RFC).

Introduction

The [redacted] Modular Public Key Infrastructure for Security Management, henceforth referred to as the PKI, is an exciting development in the attempt to achieve network-wide secure, authenticated communications while simultaneously addressing the needs of law enforcement and civil libertarians. There are several striking features of this design, not the least of which is its *modularity*: the ability of users to pick and choose the features that they need (or are required to have).

The PKI design is currently patent pending. Its release to a NIST technical advisory group, meeting to determine data recovery standards for the next Federal Information Processing Standard (FIPS), is likely. Other venues are being considered for its release, including EUROCRYPT and the Public-Key Solutions Conference.

The next logical step in the evolution of this PKI is the construction of a working prototype, programmed in software, to run on various platforms such as UNIX-based SUN workstations or Windows-based PCs. In preparation a one-week effort by a small technical group (intimately involved with either the design of NSA's ICARUS e-mail system or the [redacted] PKI) was convened to develop a set of specifications for both a prototype and a demonstration of the unique features of this PKI. The charge to the group was to lay the groundwork for demonstrating proof of concept in two areas:

- Validate, through implementation, the features and technical demands of the PKI.
- Determine the extent to which the PKI can be built - and maintained - with commercial off the shelf (COTS) products.

The group determined that a concentrated six-month effort involving approximately ten people would suffice to meet the stated goals. This effort is proposed to commence in June 1997 [redacted] drawing expertise and personnel from C, Q, R, X, [redacted] groups.

The following section outlines, in considerably more detail, the proof of concept proposal. It includes a timetable and names of individuals identified as potential team members. A companion draft outlining the *technical blueprint* of the proposal is also in final draft form and is available. The latter spells out specific implementation details that the technical team will follow in producing the prototypes (for example, X.509 certificate use, S/MIME, crypto-engines, signing protocols and parameters, etc.) While choices of some components were arbitrary, others were specifically driven by what we felt were likely to be offered in a COTS environment. Likewise, despite the fact that the PKI design is modular and will support multiple components, it was decided to limit the prototype and demonstration efforts so that a fully functional product could be produced quickly. Based on the level of success achieved, future expanded efforts may be warranted.

Proof of Concept Proposal

(b)(1)
(b)(3)-P.L. 86-36

Goals

The prototype and demonstration are designed to provide a proof of concept for

- the technical viability of the PKI design to meet the stated goals, and
- the ability to use commercial off the shelf (COTS) products to implement the design.

One of the unique features of the [redacted] PKI is the separation of the mechanisms which provide data recovery for the user from those needed to service warranted law enforcement access. This is a crucial feature that the group felt must be demonstrated.

Other general design criteria for the PKI were

- All components of the PKI will be public.
- The default protocols and algorithms will have been thoroughly vetted in the public domain.
- The infrastructure must be scalable to accommodate a large number of users.
- Secure communication must not *require* the recipient to play an active part in the key exchange (i.e., a common session key can be computed by the sender alone).
- Interoperability, at the cost of increased overhead, can be achieved with *key encryption key* (KEK) systems, such as *Royal Holloway.*

The group decided that the prototype needed to demonstrate an easy-to-use infrastructure supporting the normal functions of authentication and confidentiality while highlighting the key recovery feature. *The major service this prototype will demonstrate is secure e-mail.* The escrow functions will be implemented, and time permitting, demonstrated, but this will not be an overall goal. In addition, the prototype will initially serve only a small number of users. Issues of scalability will be addressed in terms of the network services that need to be in place to accommodate larger groups.

By exploring the use of COTS products, the requirements covering use of publicly known and vetted protocols and unregulated algorithms can be examined. Demonstrating use of such products might also help answer questions of scalability. Finally, noting any failures of the commercial market to meet the development of this PKI may help drive product redesigns to our benefit.

Major program components

Based on the above, the group determined that the following modules will be needed to implement the prototype and perform the demonstration specified.

1. A Client e-mail application which will perform:
   Standard e-mail functions,
   Authentication and verification through digital signatures of e-mail messages, and
   Confidentiality of message content through encryption.
2. A client level key-management module which will perform the following services:
   Enrollment of client for signature and confidentiality services,

Message key recovery, especially to uncover a users securely stored secret keys in the event of a forgotten pass phrase, and
Certificate management, including address book management and possibly caching of certificates.

3.A server module to implement Message Key Recovery Center Functions.
4.A server module to implement Certification Authority Functions, including mechanisms for
Authenticating users,
Providing directory services - public for users to obtain certificates, and private for holding sensitive enrollment information, and
Generating and signing users certificates.
5.A server module for the Escrow Agent which can
Verify signatures as a means of authenticating a request,
Form public parameters from the users secret parameters,
Sign the generated public parameter and return the signed message to the user,
Escrow the users private information into its database, and
Develop partial session key variables when confronted with a warranted request.

Strategy

To demonstrate the validity of the PKI design, a small group of individuals will be tasked to develop an in-house, home-grown prototype, probably developed on the NSA Classified Network, and leveraging, whenever possible, readily available packages for performing the required functions and services. The ultimate goal of this team is a working prototype meeting the demonstration specifications.

To determine if COTS products are capable of being used to build the system, another small team of individuals will study several readily available packages that could possibly be used to implement the PKI. This will involve purchasing these packages and attempting to use them to build some of the various modules. The main goal here is to determine the feasibility of using COTS, or, if not, what pieces of the PKI cannot be so supported. If time permits and a set of COTS products can be found to build a prototype, an effort will be made to do so.

If both efforts succeed in developing prototypes, and, if time permits, an attempt will be made to demonstrate interoperability. Once again, ***the ultimate goal is to realize the PKI in a COTS environment.***

Schedule

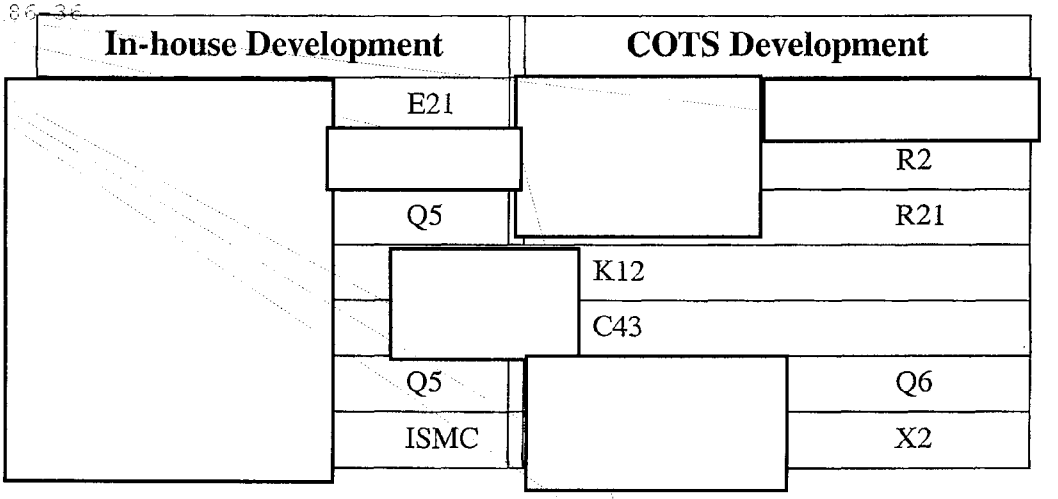
In the April/May time frame, it is expected that
1.The proposal will migrate from draft to finished document,
2.Team leaders will be determined for each effort,
3.Additional effort ("homework") will be performed to further specify the prototype and demonstration details,
4.A list will be generated of hardware/software requirements needed to support the effort, and
5.A list of team members will be formed.

It is expected the actual effort will start in June and probably last from 4 to 6 months, depending on the availability of the team participants.

Human Resources

The group cited the following individuals to be contacted for staffing the effort. It is expected that only a small number of these individuals will be available on a full time basis. Team leaders for the pre-start-up phase will be [redacted] for the in-house effort and [redacted] for the COTS development team.

(b)(3)-P.L. 86-36



In addition, a small number of junior personnel, interns and summer program participants will be asked to join in the effort, both to help with the programming and as an educational and training experience. The overall effort will be mentored by [redacted]

(b)(1)
(b)(3)-P.L. 86-36