Metering: A Pre-pay Technique

Russell Housley

SPYRUS, Incorporated
P.O. Box 1198, Herndon, Virginia 20172

Jan Dolphin

SPYRUS, Incorporated
2460 N. First Street, Suite 100, San Jose, California 95131

ABSTRACT

The SPYRUS Metering System allows intellectual property suppliers to control access to electronic information with content-based meters. Information is distributed to users in encrypted form, and each user has a hardware token that contains the cryptographic keys necessary to decrypt the information as well as the meters that control the use of each key. The hardware token will not grant access to the information by decrypting it unless the supplier provided meter constraints are met. Since the hardware token includes a built-in real time clock, time-based meters can be enforced without relying on the easily modified computer system clock.

Keywords: metering, key management, encryption, hardware token

1. INTRODUCTION

Intellectual property suppliers want to distribute information to users in electronic form, either on physical media or over popular networks like the Internet. At the same time, the suppliers require protection so that the electronic information is not misused. Protection may prevent copying, alteration, or prevent access altogether. Today's on-line Internet environment has generated new requirements. Many parents want to prohibit "X rated" World Wide Web (WWW) pages from being downloaded by their children. Employers are concerned about the amount of time that their employees spend "browsing" the WWW during work hours. In the first example, access must be limited based on the content itself, and in the second example, access must be limited based on time of day without keeping people from doing their job. Technical solutions to protect intellectual property in this networked, multimedia environment must be available before business can use electronic distribution effectively.

The SPYRUS Metering System allows suppliers to protect the information, then distribute it via any media. The information is distributed in encrypted form, thus only authorized users are able to decrypt the information.

Hardware tokens are used. The high assurance hardware tokens implement the cryptographic algorithms, store the keys, and enforce the meters. Use of the hardware token ensures that the user cannot bypass the meter checks and decrypt the information. Since the hardware token includes a battery-operated real time clock, time-based meters can be enforced without relying on the easily modified computer system clock. Additionally, since each user will have their own token, the token can provide the user with other services as well. For example, the cryptographic algorithms on the card can be used to provide the user with a digital signature capability for electronic mail or fax services; the hardware token can provide authentication to WWW sites or firewalls; and the hardware token can be used to provide end-to-end network security services beyond those provided by firewalls.

Within the last year, user acceptance of PCMCIA PC Card and Smart Card tokens has significantly increased. One significant event in this area is the definition of the Microsoft Internet Security Framework which provides a standardized cryptographic interface for user tokens on all Windows 95 and Windows NT platforms. The Microsoft architecture includes a Cryptographic Service Provider (CSP) under the standardized interface. The CSP provides a "Plug and Play" solution to seamlessly integrate applications with hardware tokens. Standardization at this level, on these platforms, opens the floodgates to technical solutions to protect electronic intellectual properties.

2. METERS

Like the gas or electric meter attached to a house, the user maintains possession of the metering token. The hardware token will not grant the user access to the information by decrypting it unless the meter constraints established by the publisher are met. Conversely, the token may not grant a user access to particular content, based on the user identification. Depending on

the complexity of the system, meters may take on many different forms, and meters may be coupled with different communications or storage functions. Meter can be contained in PCMCIA PC Cards, Smart Cards, or computer boards to meet higher input/output performance requirements. For example, a meter combined with a modem allows the application to invoke the modem functions when billing or audit information needs to be transferred. For environments requiring large amount of meter use information, they can be coupled with multi-megabytes of flash storage. Looking into the future, as smart card processors evolve, the use of downloadable meters to maintain user functions such as customer loyalty programs is easily achievable.

As described earlier, meters may be based on many different attributes. Attributes are built into and monitored by the hardware token. The meters can be associated with any symmetric or asymmetric key on the hardware token. Symmetric keys can be used to encrypt intellectual property prior to distribution, and asymmetric signature keys can be used for remote authentication. Attributes that a meter can monitor include:

- The name or alias of the key holder;
- Description of the key;
- Activation date of the key;
- Expiration date of the key;
- Number of uses of the key;
- Data usage;
- Subscription Counter;
- Access time of day; and
- Access calendar date.

In addition, arbitrary attributes can be supported by the application. In this case, the application tells the hardware token when to increment the meter. In this way, LYNKS *aware applications* tell the hardware token when meter relevant events occur, and the meters are tracked inside the protected memory of the hardware token. The user has no way to decrement the meter, thus the hardware token will refuse to decrypt additional information once the meter threshold is reached. This functions is particularly useful for implementing a "30 day free trial use" function. In one system, this function was used to provide a thirty day free sample period for a word processing program. This was implemented with a key that expired in thirty days. Once the key expired, the word processing application disabled certain functions such as copy and print. When the user purchased the application key, these functions were re-enabled.

The hardware token associates some user information with the data. As examples, this feature may be used to track user accesses to certain types of data and track the amount of information accessed during a session. The hardware token contains a limited amount of audit information. This audit information is periodically downloaded from the hardware token to the publisher's Billing/Audit Center. This audit information allows the publisher to understand how and when their information is used. This audit information is readily available, and extensively used, by publishers with on-line systems; however, obtaining this audit information from off-line systems is quite difficult. Alternate hardware token packaging could provide large amounts of audit information to the publisher if the system includes a convenient way to transfer the audit information from the user to the publisher.

3. METERING SYSTEM COMPONENTS

The SPYRUS metering system has four components: the Personalization Workstation, the Billing/Audit Center, the Publisher, and the Authenticator. Figure 1 illustrates the relationships between these four components. The Personalization Workstation is responsible for hardware token initialization and enrollment of users. The Billing/Audit Center is responsible for hardware token registration and meter distribution. The Publisher creates meters, assigns access controls, and encrypts the information. Lastly, the Authenticator requests meters and decrypts the protected information for the user. In many cases, the Authenticator is embedded in another application.

Together, these components support electronic publication and payment, yet user misuse of the information is prevented.

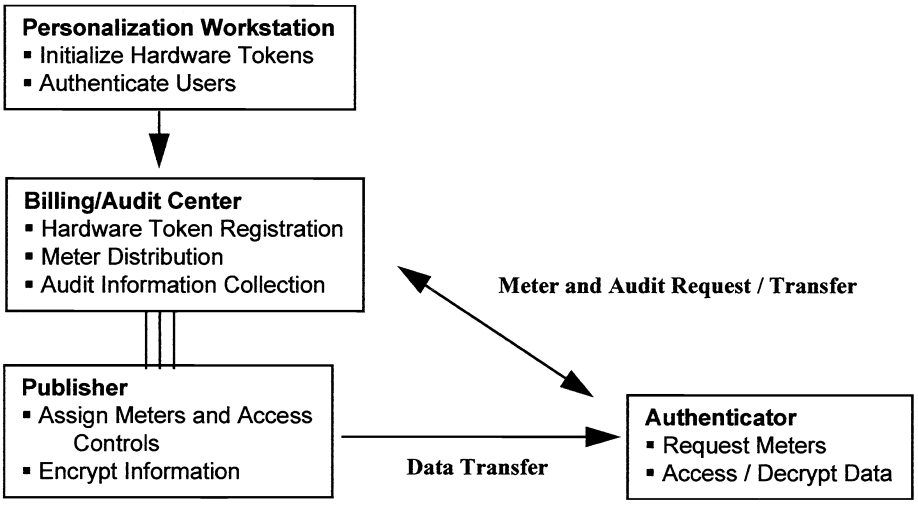

Figure 1. SPYRUS Metering System Components.

4. PUBLISHING

Prior to publication of the information, the Publisher must decide on the attributes of the meter. Theses attributes are determined by the publisher's payment model. Does the publisher want to charge for information access based on time, quantity, or events? If the publisher wants to charge for WWW page access based on time, then the publisher may allow a user access to their WWW pages for thirty days or access it in the month of February. If the publisher wants to charge for access to a image repository based on quantity, a user may be granted access to 10,000,000 bytes of photographic information. If the publisher wants to charge for database access based on events, the publisher may allow 250 database queries. The key point is that the Publisher determines how much data is protected with each key and establishes the metering parameters prior to publication. The Publisher could protect a single file, a whole directory, an arbitrary collection of files, an entire CD-ROM, or a WWW page. The metering system does not impose any limitations on the creativeness of the publisher. Further, when publishers use LYNKS *aware applications* there are no limit on the publisher's creativeness to define the billable event.

For example, the metering system can use keys to implement a magazine subscription service. Each magazine issue is encrypted in a different key. The key from the previous magazine issue is used to derive the key for the subsequent issue by applying a one-way update function. The one-way update function is applied to the first issue key to obtain the second issue key; the one-way update function is applied to the second issue key to obtain the third issue key; and so on. The meter contains the number of updates that are permitted. In this way, the meter determines which magazine issues that a particular user may read. Renewals may be implemented by distributing the key for the first magazine issue in the renewal period and permitting the number of updates that are permitted. This approach allows a user to joint the subscription at any point.

The meters are tightly coupled with the cryptographic keys, and the distribution of the keys and the meters to the user is all that is necessary for the user to access the information. Therefore, if payment is required for the information, payment must be received before the key and associated meter is provided to the user.

5. PAYMENT

Payment is tightly coupled with key management. That is, keys and associated meter are distributed after payment is received. For example, the Publisher may put many products on a single CD-ROM, and associate a separate key and meter attributes with each product. When a user purchases one product, the CD-ROM containing all of the products is sent to the user, but the user is sent only one key and the associated meter. When the user purchases a second product, the user is sent the key and associated meter for the second product. There is no reason to send the CD-ROM again, so the second delivery may be accomplished electronically with a small message.

During the life of the subscription service, the Billing/Audit Center communicates with the hardware token and securely updates the meter status. The cryptography contained within the hardware token is used to provide secure communications, and audit information as well as the meter state is received by the Billing/Audit Center. This information is distributed to the associated information publishers to plot histograms associated with information usage. Also, the secure communications can be used in the evolution of new services or promotions. A publisher can change the meter or give away a "free month" to any information user. The hardware token audit information can contain access thresholds that support brand loyalty programs. After a fixed amount of access to a particular WWW site or use of a particular software package, the publisher can provide free upgrades or other promotional information to foster customer loyalty.

Even though pre-payment is most easily supported by this scheme, "try before you buy" is still accommodated. A "try before you buy" meter might limit on-line access to non-prime time, limit access to a subset of the available data, limit the number of bytes that can be decrypted, or limit the number of database queries.

The Billing/Audit Center can be maintained by the publisher, or the payment center can be provided by a third party.

6. USER APPLICATIONS

Current meter information on the hardware token must be accessible to the user. This capability is provided by the meter reader application. All keys and information maintained by the hardware token have an associated alias name that is human readable, and this alias name allows the user to determine time or events remaining on a particular meter. Bundled with this application is the electronic order form to purchase new services and sign the purchase request prior to sending it to the Publisher or Billing/Audit Center.

Another application, Authenticator, is a transparent application responsible for decrypting the information in accordance with the meter, transparently to the user.

7. WORKED EXAMPLES

SPYRUS has used the metering technology described in several projects. Two projects are briefly described in the following sections.

7.1 CD-ROM Distribution and Access Control

For the Navy, SPYRUS developed a system that protects CD-ROM images. The ISO 9660 CD-ROM image encryption standard is used. The SPYRUS Authenticator is implemented as an interposing device driver, so the user can continue to use CD-ROMs with any software application. The SPYRUS Authenticator verifies the Publisher's signature on the CD-ROM, providing authentication of the source of the information. The system allows the users to query the CD-ROM jukebox to obtain the table of contents and list of required keys, and, if authorized, to download the appropriate keys from a key distribution system. The SPYRUS system provides access control to critical information and also provides authenticates information sources and dates of information for critical functions.

Figure 2 illustrates the Graphical User Interface used to associates meters with CD-ROM files.

7.2 Copyright Initiative

The National Research and Education Network (NREN) copyright initiative is using this type of technology to limit redistribution of electronic documents, assure that copies remain unmodified, and to identify the attributes of alternate data distribution modes. Using a "sealed envelope" and digital signature based on public key cryptography, meters provide:

- Authentication - source of the information;
- Limit redistribution - meters restrict the number of copies that may be printed to the number purchased;
- Protection against plagiarism and change - mechanism to ensure that the materials are used with jeopardizing authenticity; and
- Remuneration - metering for subscription fee, license fee, contract fees, or fee for services.

8. FREQUENTLY ASKED QUESTIONS

One important question that is frequently asked by system developers is: "How do I recover the cost of the hardware token?" One can look at the pay per view television market for one solution. In that environment, the decryption box in the user's home is provided as part of the service. Likewise, a software distribution company can provide hardware tokens as part of the subscription to their service. Every month, instead of sending out a set of floppies or a CD-ROM, they can post the encrypted application on their WWW page. Alternatively, physical distribution of a CD-ROM could be used more efficiently by sending out a single CD-ROM with all of the distributions managed by the company. Each subscriber would be limited to the software that is part of their subscription or subscriptions. In either case, the meters stored on the hardware token permit access to their subscription, and they can also contain their individual maintenance subscription keys for the maintenance releases to software which has already been purchased. In the future, several companies might collaborate and share the cost of the hardware token. For example, one hardware token could serve as a bank card, rental car company card, airline frequent flyer card, and computer software store card. In this case, the user's bank card is the hardware token, and it can be used to purchase software products while encouraging brand loyalty.

Another important question is: "How do I connect the hardware token to my computer?" Most laptop computers come with slots for PCMCIA PC Cards. Recently, Microsoft has announced support for a Smart Card reader embedded in keyboards. So, many computers have or will have easy access to hardware tokens. Also, low cost readers are available that connect to serial ports, parallel ports, or the SCSI bus.

An interesting question is: "How will the use of digital signatures effect this technology?" Digital signatures are being used to provide authentication and non-repudiation services. The use of hardware tokens to protect the private key needed to digitally sign information is strongly recommended to reduce the possibility of masquerade. As digital signatures become more prolific, the binding of meters to signature private keys and signature values is an exciting possibility. For example, threshold meters can ensure that two people are needed to sign purchase orders over a particular value.

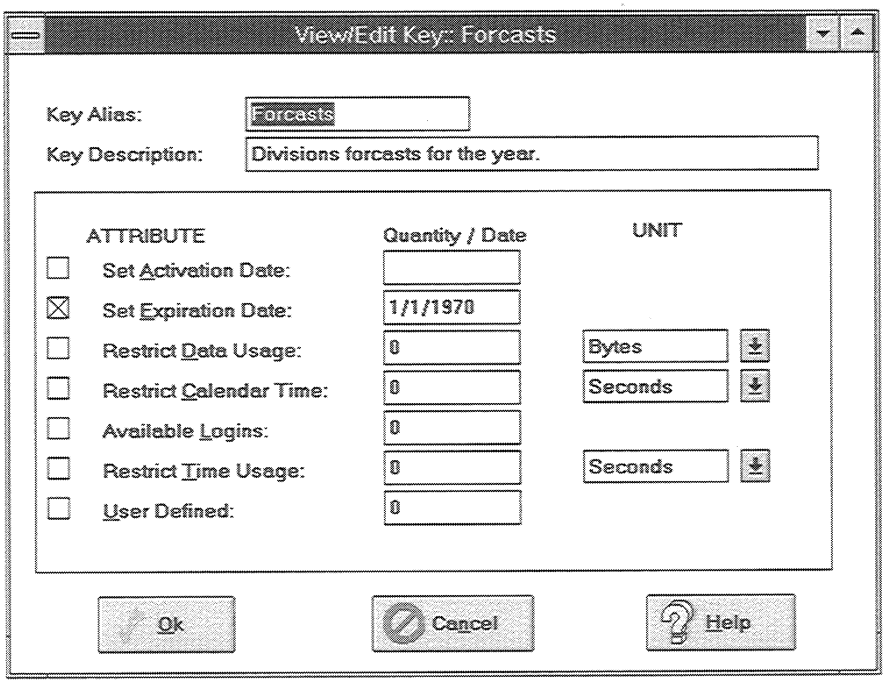

Figure 2. CD-ROM File Meter Attributes.