

VERSATILE ACCESS CONTROL SYSTEM

CROSS-REFERENCE TO RELATED APPLICATIONS

5 Cross-reference is hereby made to U.S. Application No. ____, entitled
“HYBRID COMPUTER SECURITY CLOCK” and U.S. Application No. ____,
entitled “VERSATILE SECURE AND NON-SECURE MESSAGING, which were
filed on even date herewith and are hereby incorporated by reference.

Cross-reference is also made to copending U.S. Patent Applications:

09/912,931, filed July 25, 2001 and entitled "METHODS AND SYSTEMS FOR PROMOTING SECURITY IN A COMPUTER SYSTEM EMPLOYING ATTACHED STORAGE DEVICES"; 10/963,373, filed October 12, 2004 and entitled "SYSTEM AND METHOD FOR DELIVERING VERSATILE SECURITY, DIGITAL RIGHTS MANAGEMENT, AND PRIVACY SERVICES FROM STORAGE CONTROLLERS"; 10/984,368, filed November 9, 2004 and entitled "SYSTEM AND METHOD FOR DELIVERING VERSATILE SECURITY, DIGITAL RIGHTS MANAGEMENT, AND PRIVACY SERVICES"; 11/178,908, filed July 11, 2005 and entitled "METHODS AND SYSTEMS FOR PROMOTING SECURITY IN A COMPUTER SYSTEM EMPLOYING ATTACHED STORAGE DEVICES"; 11/343,338, filed January 31, 2006 and entitled "METHOD AND APPARATUS FOR PROVIDING VERSATILE SERVICES ON STORAGE DEVICES"; and 11/346,118, filed February 2, 2006 and entitled "METHODS AND SYSTEMS FOR PROMOTING SECURITY IN A COMPUTER SYSTEM EMPLOYING ATTACHED STORAGE DEVICES".

25 FIELD OF THE DISCLOSURE

The present disclosure generally relates to access control systems and methods such as those used for securing computer systems.

BACKGROUND OF THE DISCLOSURE

Generally, access control systems limit who or what can execute methods on objects. Permission to execute a method on an object is governed by which secrets or information a host application has proven that it knows. For example, 5 in normal log on systems, the host application acts as an interface between the user and the client application that the user desires to access (such as reading a file). Typical access control systems are limited to particular types of authentication protocols, such as a password, a public key challenge/response, a symmetric key challenge/response, or a keyed-hash message authentication code 10 (HMAC).

These protocols are often fixed to a single type of authentication by the operating system or the firmware of the device being accessed. As a result, access control systems are typically limited to a single or limited number of authentication protocols and have limited flexibility.

15 Improved access control systems and methods are therefore desired, which could provide increased versatility and extensibility to many different authentication protocols.

Various embodiments of the present invention address these problems, and offer other advantages over the prior art.

20 SUMMARY

One embodiment of the present invention is directed to an access control system, which includes a plurality of authorities, a plurality of access control elements and an access control list. Each authority associates at least one of a plurality of proof of knowledge operations with at least one of a plurality of proof 25 of knowledge credentials. Each access control element identifies a Boolean combination of at least one of the authorities. The access control list identifies one or more of the access control elements by which a method to be executed can be authenticated.

Another embodiment of the present invention is directed to an access control system, which includes a credential table, an authority table and an access control element table. The credential table includes a plurality of proof of knowledge credentials that can be proven by at least one of a plurality of proof of knowledge operations. The authority table identifies a plurality of authorities and for each authority, associates at least one of the proof of knowledge operations with at least one of the proof of knowledge credentials. The access control element table identifies a plurality of access control elements and for each access control element, identifies a Boolean combination of at least one of the authorities.

Another embodiment of the present invention is directed to a method, which includes: maintaining a plurality of authorities, each authority associating at least one of a plurality of proof of knowledge operations with at least one of a plurality of proof of knowledge credentials; and maintaining a plurality of access control elements, each access control element identifying a Boolean combination of at least one of the authorities, the plurality of authorities and the plurality of access control elements being maintained at least in part within a memory associated with a device for which access is controlled.

Another embodiment of the present invention is directed to a computer readable medium having a tangible component with instructions. When the instructions are executed by a computing device, the instructions cause the computing device to perform steps including: maintaining a plurality of authorities, each authority associating at least one of a plurality of proof of knowledge operations with at least one of a plurality of proof of knowledge credentials; and maintaining a plurality of access control elements, each access control element identifying a Boolean combination of at least one of the authorities, the plurality of authorities and the plurality of access control elements being maintained at least in part within a memory associated with a device for which access is controlled.

Other features and benefits of one or more embodiments of the present invention will be apparent upon reading the following detailed description and review of the associated drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

5 FIG. 1 is a block diagram of a peripheral controller having an access control system according to an embodiment of the present invention.

FIG. 2 is a diagram illustrating an example use of access control lists (ACLs) for methods operating on a peripheral device.

10 FIG. 3 is a block diagram of a multicomponent trusted platform having a trusted peripheral device with an access control subsystem according to an embodiment of the present invention.

FIG. 4 illustrates a simplified visual example of a method table having the format shown in Table 1, according to an embodiment of the present invention.

15 FIG. 5 is a diagram illustrating an example of a session implementing pass code authentication between a host and a peripheral device.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

The present disclosure provides a description of a compact but versatile access control system and method for embedded applications, for example, and which are highly extensible. The system and method are more flexible than
20 simple username/password logons, and can incorporated an indefinitely large number of other proof of knowledge methods within a single access control framework.

In one or more embodiments, the access control system and method are embedded within the firmware of a peripheral device being accessed, such as
25 within a graphics controller or a storage device controller. The access control system and method allow a set of policies to be defined for features and resources in dedicated controllers, for example. The system and method are embedded as a feature or resource inside the peripheral device controller. The system and method provide a mechanism that allows a user to flexibly define authentication

using many different kinds of authorities by implementing the authentication process through a series of simple access control tables that can be easily defined for a particular application.

For example, the access control system can include a set of Credential
5 tables, an Authority table and an Access Control Element (ACL) table. The
Credential tables each include a plurality of proof of knowledge credentials that
can be proven by at least one of a plurality of proof of knowledge operations,
known as Authentication Methods, Authentication Operations or Protocol
Operations. The Authority table identifies a plurality of Authorities and for each
10 Authority, associates at least one of the proof of knowledge operations
(Authentication Operations) with at least one of the proof of knowledge
Credentials. The ACE table identifies a plurality of ACEs and for each ACE,
identifies a Boolean combination of at least one of the Authorities.

Each "method" that makes use of any resource or feature on or associated
15 with a peripheral device can have an associated Access Control List (ACL), which
identifies one or more of the ACEs by which the method to be executed can be
authenticated. Once authenticated, the method is permitted to execute.

The access control system can be implemented for any peripheral of a
computing device, for example. As used herein, "computing device" includes,
20 but is not limited to, desk top computer systems, laptop computer system,
networked computer systems, wireless systems such as cellular phones and
PDA's, digital cameras including self-contained web-cams, storage devices,
and/or any reasonable combination of these or other systems and devices.

FIG. 1 is a block diagram illustrating a general risk model for a peripheral
25 device in which an access control subsystem 102 according to an embodiment of
the present invention can be used. The peripheral device has peripheral controller
electronics block 100, including loadable firmware 102 with firmware functions
104, a data sync/source 106 and special hardware functions 108. The general risk
model for a peripheral device typically has four major channels of attack on the

device. These channels include a primary host interface 110, a power interface 112, diagnostics ports 114 and probe points 116. As described in more detail below, access control subsystem 120 can be embedded into the loadable firmware 102 of peripheral controller electronics 100 to provide versatile access control over these points of vulnerability and over the features and resources of the peripheral device.

1. ACCESS CONTROL

At least one Security Provider (SP) is generated for each peripheral device for which access to the SP may be controlled, for example as described in U.S. Patent Application Publication US2003/0023867, published January 30, 2003. An SP includes, for example, an atomic collection of access control Tables and Methods that can be issued in a peripheral device on behalf of a host software provider. A host software provider includes any device or process, such as a software application, that is directly or indirectly coupled to the peripheral device and desires access to make use of a resource or feature on or associated with the peripheral device.

Access Control limits who or what can execute methods on a Security Provider, an access control table, or even on specific rows and columns of a table. The term "Method" is used herein to refer to the actions that the host application desires to perform that makes use of a resource or feature of the peripheral device and to which one or more authorities are attached. For example, Method calls to an SP can include a Get (get a value), a Set (set a value), Unlock (e.g. unlock a serial port), etc. These Methods can be directed to actions on an access control table maintained by the SP and actions on other peripheral resources governed by the SP, such as actions on data storage media.

Permission to execute a Method is governed by which secrets the invoker has proven that it knows. The secrets and their public parts are called Credentials. As mentioned above, the operation for proving knowledge of a secret is called an

Authentication Method or Authentication Operation. The actual proving of knowledge of a secret is called Authentication.

In one embodiment, the access control system is implemented in simple tables of three types, a table of Access Control Elements (ACEs), a table of
5 Authorities, and a set of tables of Credentials. The “secrets” or information of which knowledge is to be proven are stored in the Credential tables.

1.1 Access Control Lists (ACLs)

Access Control is specified in layers. The top layer of the mechanism is Access Control Lists (ACLs). ACLs are lists of Access Control Elements (ACEs).
10 This layering gives the host a way in which it can delegate control of an ACL, via control of its ACEs, to various independent entities. In one embodiment, an ACL is implemented as a token list of a predetermined number of bytes. It represents an ACE expression in postfix notation, wherein the logical operators AND, OR, and NOT are encoded as the integers -1, -2, and -3.

15 With ACEs as the building blocks of ACLs, each ACE can have separate managerial control. For example, one Authority might create a Table and give another Authority control of some of the ACEs on it. This allows flexible, fine-grained management of access.

The simplest ACL is one ACE of one Authority. The minimum and
20 maximum number of ACEs in an ACL and the minimum and maximum number of Authorities in an ACE is device specific.

1.2 Access Control Elements (ACEs)

ACEs are Boolean combinations of Authorities. This permits the ACE to express cross-certification or other forms of restriction. When an Authority is
25 authenticated, it is true in the Boolean expression, and false otherwise. If any ACE in an ACL is true, then the ACL is true.

FIG. 2 is a diagram illustrating an example use of ACLs. At the top level, 130, a Table or Object in the SP identifies the Authentication Operations by which two Method Calls (Method 1 and Method 2) can be authenticated by the SP. For

example, "Method 1" may have an ACL that lists ACE1 and ACE2. Thus, Method 1 may be authenticated by satisfying ACE1 or ACE2. As mentioned above, each ACE is a Boolean expression of one or more Authorities. In this example, ACE1 may be satisfied by "AUTH1 and (AUTH2 or AUTH3)", whereas ACE2 may be satisfied by "AUTH4 or AUTH5". Similarly, "Method 2" may have an ACL that lists ACE3 and ACE4, where ACE3 is satisfied by "AUTH1 and AUTH3", and ACE4 is satisfied by "AUTH2 and NOT AUTH4".

1.3 Authorities

The Authority Table on an SP associates specific Credential-Operation pairs together in Authority objects. For example, one Authority may include a credential that contains the secret password and the stipulated proof-of-knowledge Operation of password authentication. A host application Authenticates to the Authority. The Authority is the base level building block of access control system 120.

An Authority can be used by the host application to represent a person, a role, a program agent, etc. These are distinctions of meaning to the application, not to the SP.

Authorities come in two types: Individual and Class. An Individual Authority specifies one Credential (secret) and one Authentication Method (how to prove knowledge of that secret) for that Credential. Each Individual Authority may be a member of a Class Authority. A Class may also be a member of a Class. A Class Authority is identified only by its Class Name and Authority UID, for example. A Class Authority does not refer directly to a Credential.

A Class Authority is authenticated when an Individual Authority that is a member of that Class Authority is authenticated. Class Authorities cannot be directly authenticated. Class Authorities are a convenient way to allow an ACE to be set on a method without enumerating all the individual Authorities that may authorize that method. This means that the Individual Authorities that belong to

that Class can be changed without having to change any of the ACEs that refer to the Class Authority.

1.4 Credentials

A Credential is an object in a Credential Table, noted by a name C_*, where

5 “*” is a variable indicating a particular Authentication Operation. Each Credential Table is associated with a corresponding Authentication Operation and includes one or more of the proof of knowledge Credentials (such as a plurality of unique passwords or public-private key pairs) that can be proven by that Authentication Operation. It may have private parts and public parts, such
10 as public keys and certificates. A particular Credential need not have all its columns filled in. For example, if only a public key and certificates validating that public key is known, then the private key may be absent. A Credential Table also has internal functions for using the secrets and the public parts of each credential and handles all optional parts.

15 1.5 Authentication Operation Types

The Authentication Operation is selected, as appropriate for the Credential. Examples of possible Authentication Operations include:

- Password or PIN or Passcode;

- Signing:

- 20 Public Key Challenge/Response Sign/Verify
 Symmetric Key Challenge/Response Sign/Verify
 Hash MAC, or HMAC Challenge/Response Sign/Verify;
- Key Exchange (Certificates or other methods provide implicit Authentication):

- 25 Public Key Encrypt/Decrypt
 Symmetric Key Encrypt/Decrypt; and

- None or “” This operation will always Succeed and therefore the Authority will always Authenticate.

Access control is permitted in that ACEs can apply to Methods on an SP, on a particular Table in an SP, or on arbitrary parts of a particular Table in an SP, down to the granularity of a single Table cell.

5 In an embodiment, Authentication to an Authority occurs within a session initiated between the host application and the peripheral device and applies only to that session, for example. During a session the host may make any number of Authenticate method calls.

2. IMPLEMENTATION OF ACCESS CONTROL FOR A PERIPHERAL DEVICE

10 FIG. 3 is a block diagram of a core architecture 200 for implementing an Access Control System as discussed above over a trusted peripheral device according to one embodiment of the present invention. FIG. 3 shows a single platform host 202 or Multicomponent Trusted Platform (MCTP). Host 202 keeps track of the peripherals through a Component Authentication Administrator (CAA) 208. Various host software applications, such as APP1 (labeled 210), APP2
15 212 (labeled), and CAA (labeled 208), may interact with a trusted peripheral 204 through a driver 214 and a peripheral interface 216. Trusted peripheral 204 includes a security provider (SP) 220, which includes an issued set of tables and methods that control a persistent trust state of the peripheral device.

20 In one embodiment, each row of a table is a security association, such as an association between a login name and a password, while each column names the parts of the association, such as "login_name" and "password". An Authority object is one such row in an Authority object table. A table that establishes a security association may have many different associations recorded as rows
25 within it. Depending on the set of various tables, or personalization, specific authorities may have to Authenticate to perform specific methods on specific rows and columns of specific tables. Security provider SP 220 is a completely self-contained and stand-alone security domain of such tables. Peripheral device 204

may have more than one issued service provider, such as 220 and 222 dedicated to specific applications of host 202.

A security provider contains objects that are each composed of persistent data and methods (or remote procedure calls). In one embodiment, the methods,
5 not the data, are bound to access control lists (ACLs). In the simplest case, there are two types of objects in an SP:

- a. Table Objects, which establish methods and ACLs for arbitrary tables,
- b. Authority Objects, that specify passwords or cryptographic proofs
10 that are required to prove knowledge prior to executing the methods in the SP or the associated objects.

In one embodiment, all trusted peripherals have at most one locking SP that allows manipulation security characteristics of the trust peripheral through its set of tables and access-control methods on the tables. In trusted peripherals
15 that can issue new SPs, an Administrator SP can be used to manage multiple SPs.

Applications on host 202, including CAA 208 can query or change a persistent state by establishing sessions with an SP that execute one or more object methods (connectors 230 in FIG. 3).

Host 202 communicates with SP 220 by opening a session using the
20 interface commands of the particular interface 216. In the simplest case, host 202 is the platform host to which the trusted peripheral is directly attached. In a more general case, host 202 could be some other platform host that communicates with an intermediate platform host, which relays the session stream to trusted peripheral 204 over a network.

25 Trusted peripheral devices that are capable of issuing new SPs may have SP templates from which the new SPs are created. SP templates define the initial tables and the methods that SPs that are based on them will have when issued. SP templates can combine to extend the functionality of the base SP template.

3. TABLES

3.1 General Description of Tables

In one embodiment, for example, the access control tables are the only persistent state for an SP. That is, the only data for an SP that persists past the end of a session is the data that is stored in the tables. The tables survive peripheral
5 device reboots and operations on the non-secure areas of the device.

The access control tables can be stored (in whole or in part) in any physical memory device that is associated with the peripheral device 204. For example, the tables can be stored in SP-specific parts of a secure storage area of the device.

A table includes a grid with named columns and addressable rows. At each
10 column and row intersection there is a cell. All the cells in a column have the same type. A table's size is determined when it is created, as the types of the columns and the maximum number of rows can be fully specified. However, the term "table" as used in the specification and claims can include any data structure or arrangement that can be used to associate two or more fields of data in memory.
15 The "rows" and "columns" of the table refer to the manner in which the fields are associated with one another, not necessarily the physical arrangement of memory cells in which the fields are stored.

A table or table column name may be up to 18 bytes in length. By way of example only, the names used herein consist of ASCII characters, the first of
20 which is be a letter and others being a letter, digit or underscore.

SPs may be issued and deleted. Within an SP, tables may be created and deleted. For each table, rows may be created and deleted (except within a Byte table – see below), but columns are created only when the table is created.

Each SP can have a set of metadata tables that completely describes all the
25 tables of the SP including the metadata tables themselves.

Access control provides a means to limit what methods can be executed on tables or particular rows of tables.

3.2 Kinds of Tables

In one exemplary embodiment, there are four kinds of tables:

A Byte Table has one unnamed column of type `uinteger{1}`. This provides a raw storage abstraction. In one embodiment, the rows of this table cannot be allocated or freed.

5 An Array Table has rows that are addressed by an unsigned integer. The first row is 1, etc.

An Indexed Table has one or more columns designated as the index. Each row of the table has a unique and distinct index (has unique and distinct values in all indexed columns). The index is the only way to address a row.

10 An Object Table is a kind of Indexed Table. An Object Table always has a Name column. Its index is a single column with name "Name" and type `bytes{max=18}`. This is the name of the object and provides a fast way to find an object with a specified object type and name. An Object Table has columns for storing row (object)-specific ACLs. Each row (object) has its own ACLs based on who created the row (object) with an implicit row-restriction for the row
15 containing the ACL.

Except for Byte tables:

a newly created table is initially empty and rows must be created before it can be used;

20 there is always an ID column of type `uinteger{4}`. Each row has a unique value in this column that is never shared with another row, and is never reused. New values are assigned when rows are created and old values are discarded when rows are deleted. The ID column may be an index column in an indexed (or object) table. The ID column is present to provide anti-spoofing capability.

4. ACCESS CONTROL TABLES

25 The following sections define the access control tables used in one embodiment of the present invention for implementing an embedded Access Control System. Additional tables and other table formats can be used in alternative embodiments. These tables are provided as examples only. In the

following tables, new ID references (UIDREF) are used in all table-to-table links in order to prevent one object from being mistaken for another.

4.1 Method Tables (Indexed Table)

As mentioned above, Methods are bound to access control lists (ACLs), which list access control elements (ACEs) that define Boolean combinations of Authorities that are required to be proven before the Security Provider allows the Method to be executed.

Table 1 describes the columns of a Method Table, which can be used to associate a method with an ACL according to one embodiment of the present invention. The Method Table contains one row for each table and method.

TABLE 1: METHOD Table Description

Column	Index	Type	Description
Type	Yes	uidref{Table}	Will be 0 for SP methods. For object methods this refers to the object table.
Name	Yes	name	The method name, in UTF-8 characters.
ID		uid	Autoindex row identifier.
CommonName		name	A convenient name that may be shared by several methods. May be null.
Program		ref{Program}	Pointer to the encoding of the program to be executed for this method. Will be 0 for built-in methods.
ACL		access_control_list	The ACL for the method.
Log		bytes{1} {none = 0, LogSuccess = 1, LogFail = 2}	Log to SP log whether this method succeeds for fails or both. This is a bit mask.

As shown in Table 1, each row of the Method table identifies a method by a unique method identifier “UID” and associates that method with an access control list. The Method Table can also include a pointer to a Program to be executed for that method.

FIG. 4 illustrates a simplified visual example of a method table 260 having the format shown in Table 1. Header 261 defines the columns for table 260. Method table 260 includes a plurality of rows 262 and 263. Each row identifies a particular method and an ACL for that method. In this example, row 261 defines that the Get method having ID=GET1 has an access control list with a single ACE,

ACE1. Thus, the Credential and Authentication Operation defined by ACE1 must be Authenticated by the host in order to perform a GET method.

4.2 ACE Table (object table)

Table 2 defines the columns of an Access Control Element (ACE) table,
5 according to one embodiment of the present invention.

TABLE 2: ACE Table Description

Column	Type	Description
ID	uid	Unique autoindex ACE identifier.
Name	name	Name of ACE.
BooleanExpr	access_control_element	The expression of Authorities and/or Authority Classes that authorizes the ACE if true.
RowStart	uinteger{2}	The first row restricting this ACE, if 0, the first row of the table.
RowEnd	uinteger{2}	The last row restricting this ACE, if 0, the last row of the table.
ColStart	name	The first column restricting this ACE, if null, the first column of the table.
ColEnd	name	The last column restricting this ACE, if null, the last column of the table.

The ACE table has one row with each ACL element that may be Authenticated by the host. As mentioned above, the ACE table includes a column
10 named "BooleanExpression", which provides an expression of the Authorities and/or Authority Classes that authorize the ACE, if true.

The default for rows and columns is all rows and all columns unless otherwise restricted.

4.3 Authority Table (Object Table)

Table 3 provides a description of the columns in each row of the Authority
15 table, according to one embodiment of the present invention.

TABLE 3: AUTHORITY Table Description

Column	Type	Description
ID	uid	Unique identifier of authority object.
Name	name	Name of the authority.
CommonName	name	Name common to several authorities
IsClass	boolean	If True, this is a Class Authority.

Column	Type	Description
		If False, this an Individual Authority.
Class	uidref{Authority}	Optional. Designates the Class Authority this Authority participates in.
Enabled	boolean	If False, Authority is Disabled and Authentication automatically Fails.
Secure	boolean	True if authority requires secure messaging. This field is only used in establishing a secure session.
HashAndSign	hash_protocl	If not NONE, a signed hashes are to be used either during session creation or with session messaging.
PresentCertificate	boolean	If the Authority is a public key authority and if the credential contains a certificate chain, then present the certificate chain along with the authority.
Operation	authentication_method	What Operation to perform with the Credential (e.g., Exchange, Signing, SymK, HMAC, PIN, None)
CredentialTable	Credential	Which type of Credentials – a C_* table name, like C_RSA1024 selected from the publicly readable CryptoSuite Table in Admin.
Credential	uidref{credential}	Which specific Credential to use.
ResponseSign	uidref{Authority}	If present (non-zero), a required bilateral condition with another Authority
ResponseExch	uidref{Authority}	If present (non-zero), a required bilateral condition with another Authority
ClockStart	date	Authority is enabled starting on this date if the Peripheral device has a trusted date. No date signifies no start limit.
ClockEnd	date	Authority is disabled on this date if the Peripheral device has a trusted date. No date signifies no end limit.
Log	bytes{1} {LogSuccess = 1, LogFail = 2}	These flags enable logging of different events that occur when this authority is authenticated. Log = 0 is no logging. This logging is only applicable when authentications are done in establishing a session or in augmenting the authorities on it, not when authentication is tested on a method.

Each row of the Authority table is an Authority. An Authority is a specific use of a Credential, and possibly other Authorities. A class Authority is a reference to multiple individual Authorities and cannot use a Credential.

5 Thus, each row (Authority) of the Authority table has a column named “Credential”, which identifies a specific Credential to use for Authenticating proof of knowledge for this particular Authority and identifies a particular Authentication Operation by which the Credential is authorized.

The “Credential Table” column identifies the table name of the particular type of Credentials being used, and the “Credential” column identifies the specific row of the Credential Table that is being used. For example, if the Credential type is C_RSA1024, the Credential column of the Authority table specifies the particular row (particular key) of the C_RSA Credential table.

4.4 Certificate Data Tables (Byte Table)

Table 4 provides a description of the columns of a Certificate Data table, according to one embodiment of the present invention.

TABLE 4: CERTIFICATE DATA Table Description

Column	Type	Description
Code	certificate	Bytes of a certificate or trusted certificate chain. May use more than one contiguous row. X.509 as defined by the certificates requirements.

The Certificate data table stores data that is used for data validating a public key, for example.

Certificates (Object table)

Table 5 defines the columns of each row of a Certificates table. Each row has a Certificate name and a pointer to the Certificate’s byte code.

TABLE 5: CERTIFICATES Table Description

Column	Type	Description
ID	uid	ID of Program
Name	name	Name of Certificate
Code	ref{CertificateData}	Pointer to the certificate’s byte code.
CodeCount	uinteger{4}	Number of bytes actually used in the certificate.

4.5 Credential Tables (Object Tables)

The following tables provide examples of different types of Credential tables that can be used in one or more embodiments of the present invention. These tables are not exclusive, and additional tables can be included to implement addition types of Credentials. In one embodiment, each Credential table is associated with a corresponding one of a plurality of proof of knowledge operations, called Authentication Operations.

The Credential tables represent an extensible basis for providing the public and private parts of Authentication mechanisms. Each Credential table represents a different mechanism and each row a different Authentication using the mechanism represented by the table.

5 The Credential tables contain secrets that might never need to leave the trusted peripheral. Normal ACEs can prevent disclosure of a secret from an attack that comes over the interface. To help protect against an attack in which the trusted peripheral electronics are changed, the Credential tables can have a Hide column to tell the trusted peripheral to hide the columns that contain secrets on the storage media. For example, the secrets can be Cryptographically hidden on the storage media when possible.

4.5.1 C_PIN (Object Table)

Table 6 defines the columns of a PIN Credential table according to one embodiment of the present invention.

TABLE 6: C_PIN Table Description

Column	Type	Description
ID	uid	Unique identifier of the password.
Name	name	Name of the password.
PIN	password	Password string.
Hide	boolean	Cryptographically hide value on media when possible
TryLimit	uinteger{1}	Maximum number of failed tries before always failing.
Tries	uinteger{1} = 0	Current number of failed tries.

The Credential table PIN, C_PIN, contains one row for each Authority that requires a password. Table 6 provides a definition for each column of the C_PIN table. Each row of the C_PIN table contains a column named “PIN” that stores a password string for a particular Authority. The “HIDE” column can be used to cryptographically hide the password string on the storage media when possible.

The “Tries” column is updated by the peripheral device on every failed Authentication attempt, including the implicit Authentication attempt if the Authority is a Signing Authority invoked during a session startup. The “Tries”

column is set to zero by the peripheral device when the Authenticate succeeds. Also, the tries column can be reset from the host by establishing an ACE for the Set method on that cell.

4.5.2 C_RSA_1024 (Object Table)

5 Table 7 defines the columns of a CRSA_1024 Credential table according to one embodiment of the present invention.

TABLE 7: C_RSA_1024 Table description

Column	Type	Description
ID	uid	Unique identifier.
Name	name	Name.
CryptoCall	name = RSA	Crypto Type
CryptoLen	uinteger{2} = 1024	Length of Key
Pu_Exp	uinteger{10}	RSA Public Exponent
Pr_Exp	uinteger{10}	RSA Private Exponent
Mod	uinteger{10}	Modulus
P	uinteger{10}	p and q, the primes from the key generation,
Q	uinteger{10}	
Dmp1	uinteger{10}	d mod (p-1) and d mod (q-1) (often known as dmp1 and dmq1)
Dmq1	uinteger{10}	(1/q) mod p (often known as iqmp)
Hide	boolean	Cryptographically hide value on media when possible
ChainLimit	uinteger{1}	The chaining Limit for using a chained down key from this one. -1 indicates no limit. 0, no chain, is the default.
Certificate	uidref{Certificate}	Certificate(s) - provides a chained set of unencoded X.509 certificates if needed to prove an ancestor authority

10 Table 7 implements an RSA Laboratories public-key cryptosystem having a key length of 1024 bytes. The public exponent and the private exponent columns of the RSA table represent a public-private key pair for each row of the table. Again, the column containing secrets such as the RSA private exponent, modulus, P and Q primes, DMP1 and DMQ1 and IQMP can be hidden on the medium.

4.5.3 C_RSA_1048 (Object Table)

15 Table 8 defines the columns of a C_RSA_2048 Credential table according to one embodiment of the present invention.

TABLE 8: C_RSA_2048 Table Description

Column	Type	Description
--------	------	-------------

Column	Type	Description
ID	uid	Unique ID.
Name	Name	Name.
CryptoCall	name = RSA	Crypto Type
CryptoLen	uinteger{2} = 2048	Key Length
Pu_Exp	uinteger{20}	Public Key
Pr_Exp	uinteger{20}	Private Key
Mod	uinteger{20}	Modulus
p	uinteger{10}	p and q, the primes from the key generation,
q	uinteger{10}	
Dmp1	uinteger{10}	d mod (p-1) and d mod (q-1) (often known as dmp1 and dmq1)
Dmq1	uinteger{10}	(1/q) mod p (often known as iqmp)
Hide	boolean	Cryptographically hide value on media when possible
ChainLimit	uinteger{1}	The chaining Limit for using a chained down key from this one. -1 indicates no limit. 0, no chain, is the default.
Certificate	uidref{Certificate}	Certificate(s) – provides a (possibly chained) set of unencoded X.509 certificates if needed to prove signing from an ancestor authority

Table 8 implements an RSA public-key cryptosystem having a key length of 2048 bytes.

4.5.4 C_ES_160 (Object Table)

5 Table 9 defines the columns of a C_EC_160 Credential table according to one embodiment of the present invention.

TABLE 9: C_EC_160 TABLE DESCRIPTION

Column	Type	Description
ID	uid	Unique identifier.
Name	name	Name.
CryptoCall	name = EC	Crypto Type
CryptoLen	uinteger{2} = 160	Key Length
Hide	boolean	Cryptographically hide value on media when possible
p	uinteger{20}	Modulus
r	uinteger{20}	Order of the curve
b	uinteger{20}	Curve coefficient ($y^2 = x^3 - 3x + b \pmod p$)
x	uinteger{20}	Base point coordinate
y	uinteger{20}	Base point coordinate
alpha	uinteger{20}	Private key
u	uinteger{20}	Public key x-coord: $(x,y) \propto x$
v	uinteger{20}	Public key y-coord: $(x,y) \propto y$

Column	Type	Description
ECDSAs	uinteger{20}	Hash Initialization Vector
ECDSAc	uinteger{32}	Hash Message Block (PseudoRNG)
ECDSHash	enum{Plus-1x, SHA-1, SHA-256}	Hash for ECDSA
MQVHash1	enum{Plus-1x, SHA-1, SHA-256}	
MQVHash2	enum{Plus-1x, SHA-1, SHA-256}	
ChainLimit	uinteger{1}	The chaining Limit for using a chained down key from this one. -1 indicates no limit. 0, no chain, is the default.
Certificate	uidref{Certificate}	Certificate(s) – provides a (possibly chained) set of unencoded X.509 certificates if needed to prove signing from an ancestor authority

Table 9 is an example of a Credential Table for implementing an elliptical curve cryptography.

4.5.5 C_AES_128 (Object Table)

5 Table 10 defines the columns of a C_AES_128 Credential table according to one embodiment of the present invention.

TABLE 10: C_AES_128 Table Description

Column	Type	Description
ID	uid	Unique identifier.
Name	name	Name
CryptoCall	name = AES	Crypto Type
CryptoLen	uinteger{2} = 128	Key Length
Key	uinteger{16}	Key
Hash	hash_protocol	When hashing is required, this selects the hashing algorithm.
Hide	boolean	Cryptographically hide value on media when possible

10 Table 10 implements an advanced encryption standard having a 128-byte symmetric key. Again, the key can be cryptographically hidden on the media when possible.

As mentioned above, the access control tables, such as the Method Table, Ace Table, Authority Table, the set of Credential Tables, and other related tables, of each SP of a peripheral device are stored (in whole or in part) in a physical
15 memory device that is associated with or accessible by the peripheral device. The

host will include a similar set of Authority and Credential Tables for the SP's it wishes to access. These tables can be stored in whole or in part in any memory that is associated with or accessible by the host. The information stored in the host's Authority Table and Credential Tables, however, might contain only part of the information stored in the SP's Tables. For example the host Credential Table might include only a public part of a public-private key pair. This allows the host to request the correct Authority Operation and provide a corresponding Credential for review by the SP in the peripheral.

5. SESSION

In one embodiment of the present invention, all communications with an SP occur during a session. A session is always started by a host, for example. Normally the host application will end a session when it has finished its communication, but either the SP or the host can abort a session at any time for any reason. For a specific SP there can be any number of read sessions active simultaneously, but only one write session, for example. Read and write sessions are mutually exclusive. The implementation may limit the number of simultaneous read sessions to any SP and/or limit the total number of open sessions available to a peripheral device.

Methods are procedures that operate on tables or SPs, and are called within a session to an SP. The caller passes a list of parameter values to the method and the method returns a list of result values followed by a uinteger status code. Within a given session at most one method can be active at a time. Each session to an SP has at least two streams of bytes onto which data is encoded. One stream goes from the host to the SP, and the other comes from the SP to the host.

Method calls, their parameters, and their results are sent and received over session streams. Each stream operates asynchronously from all other streams. Typical host method calls will send all their parameters/data to the SP before trying to read any of the results, but the SP is free to generate results incrementally as it consumes its parameters. The host is similarly free to try to

read SP results while sending parameters. The SP implementation decides how synchronous or asynchronous to be, so long as the semantics of the method call(s) are not compromised.

Transactions are used to provide a clean model for how changes to an SP are to take effect. They also provide an easy way for host applications to handle error recovery. All changes to an SP take place within the scope of a transaction. When a session is opened to the SP a transaction is automatically started. When the session is closed, that transaction is closed. If the session is aborted, the transaction is aborted. If the session is closed successfully, the transaction is committed to persistent storage. Only when a session is closed and committed are its changes made persistent (to the media, made visible to subsequent sessions on the same SP, etc.). Any effects on other aspects of the peripheral device (i.e. hardware settings) do not happen until and unless the session is successfully committed. If a session is ended before nested transactions are closed (committed or aborted), then all the transactions are aborted and the session is aborted.

A method call includes of the following steps:

- a. The host tells the SP the method it wants to call;
- b. The host sends a list of parameters to the SP;
- c. The body of the method is executed in the SP; and
- d. The method results are returned from the SP to the host.

Steps 2-4 may be repeated when input and output are incrementally streamed.

Starting a session depends upon three independent requirements, for example:

- a. The peripheral device and the requested SP having sufficient resources;
- b. Negotiating symmetric keys if secure messaging is required; and
- c. Authenticating requirements (one of the following, for example):
 - Host must authenticate to SP;
 - SP must authenticate to Host;

Both of the above; and

None of the above (No authentication).

The first requirement, sufficient resources, is often time-dependent, so if a session fails to start for this reason a short delay may be necessary before retrying.

- 5 The host sets the second and third requirements when it attempts to start the session, as described below.

The Host application starting the session determines the secure messaging and authentication requirements to be satisfied by specifying up to four authorities, for example:

- 10 HostExchangeAuthority: Host's Exchange Key – and implicit authentication
HostSigningAuthority : Host's Signing Key – used for authenticating the host to the SP
SPExchangeAuthority SP's Exchange Key – and implicit authentication
SPSigningAuthority: SP's Signing Key – used for authenticating the SP to the
15 host.

Note: These authorities are already known to the SP.

- Host authorities, if used, are passed in the StartSession method call. SP authorities are bilateral authorities called out in the Host authorities' Authority table rows. The ability to specify authorities in the StartSession method call,
20 coupled with the linking of authorities in the Authority table, provides a large and diverse set of possible session protocols, including secure messaging. It is the initial selection of authorities by the host that determines which protocol is to be followed.

- When the host makes a StartSession method call it knows which
25 SPExchangeAuthority and SPSigningAuthority (if any) the SP will use. Those may be the root authorities in a certificate chain whose ultimate effective authority the host does not know. This is why the SP may return certificates to the host as part of a SyncSession.

If a HostSigningAuthority or SPSigningAuthority requires a Challenge-Response, as is the case for PuK, SymK, and HMAC authorities, or if secure messaging is to be used (or both), then the StartSession and SyncSession methods are followed by StartTrustedSession and SyncTrustedSession methods.

5 An authority (HostExchangeAuthority, SPExchangeAuthority, HostSigningAuthority, or SPSigningAuthority) that is also a Public Key Authority (an Authority with public key credentials--PuK) may have additional information supplied for it in the form of a Certificate or Certificate chain. In this case the Effective Authority (the one responding to the challenge) will be the tail PuK of
10 that chain. The effective authority is transient to the session. An effective authority transmitted to the SP, the full contents of its certificate chain, will be available only during the session. In one embodiment, it is necessary to create a new authority on the SP (in a write session) if the host wants that authority to persist past on the SP.

15 Seven examples from among the many possible ways to start a session include:

- a. None. No Authorities are used. This is a non-authenticated, non-secure messaging session.
- b. Host-PIN. This is the rudimentary case of passcode authentication that is
20 passed in the clear. Secure messaging is not an option in this case.
- c. SP-SymK-Exch. The simplest case that provides for full Host & SP session key encryption. The SP needs to perform only symmetric encryption.
- d. Full-PuK. This uses public keys for signing and key exchange, for both the Host application and the SP. With a proper certificate chain or other validation
25 proof for the exchange key, this is also authenticated. SP Issuance is an example where Full-PuK is used.
- e. Full-SymK. This uses SymK keys for signing and key exchange, for both the Host application and the SP.

f. Host-PuK-Authentication. This is a simple strong enabler that does not start up secure messaging. An example use case might be a TCG TPM that authenticates a session in order to unlock the Read/Write functions of a disk drive and, because of the nonce and the private key, does not need a secure channel.

g. Host-PuK-SP-SymK. This is a case where it is desired that the SP sign, but that public key signing, and indeed all the private key operations of public key cryptography, are deemed too computationally expensive for the SP. The Host application is allowed to PuK sign and the SP to PuK verify and PuK encrypt a session key. But the SP only SymK signs, and does SymK session key receipt.

6. EXAMPLE

FIG. 5 is a diagram illustrating an example of a session implementing pass code authentication between host 202 and peripheral device 204. For clarity only the security related parameters are shown in FIG. 5. The host begins communication with peripheral device 202 by calling a StartSession method and passing parameters, including an SPName, a HostChallenge and a HostSigningAuthority. In this case, the HostChallenge includes the host PIN.

The peripheral device receives the method call, looks in the Method Table (e.g., Table 1 above) of the named SP (SPName) to identify the ACL for that method and identifies the resulting ACE and its Boolean expression of Authorities from the ACE Table (Table 2 above). If the HostSigningAuthority is not valid (i.e., not satisfying the Boolean combination of Authorities in the identified ACE Table), the peripheral device aborts the session.

If valid, the peripheral device identifies the associated Credential of the invoked HostSigningAuthority from the Authority Table (e.g., Table 3 above) and retrieves the identified Credential from the associated Credential Table (e.g., Table 6 above). The peripheral device verifies that the HostChallenge (e.g., PIN) is equivalent to the Credential PIN of the invoked HostSigningAuthority. If not, the

peripheral device aborts the session. If so, the peripheral device authorizes the called method, such as by calling a SyncSession method.

7. CONCLUSION

The access control system can be implemented wholly or partly on any
5 computer-readable media and can comprise one or more instructions or databases that are resident at various times in various memory and storage devices associated with the peripheral device and/or the host. When read and executed by the host or peripheral device the instructions cause the host or device to perform the instructions and/or process the databases or tables embodying the
10 various aspects of the invention. Examples of computer readable media on which such instructions, tables, objects and/or modules can be stored include but are not limited to recordable type media such as volatile and nonvolatile memory devices, floppy and other removable discs, hard disc drives, optical discs, e.g., CD-ROMs, DVDs, etc., among others, and transmission type media such as digital
15 and analog communication links.

It is to be understood that even though numerous characteristics and advantages of various embodiments of the invention have been set forth in the foregoing description, together with details of the structure and function of various embodiments of the invention, this disclosure is illustrative only, and
20 changes may be made in detail, especially in matters of structure and arrangement of parts within the principles of the present invention to the full extent indicated by the broad general meaning of the terms in which the appended claims are expressed. For example, the particular elements may vary depending on the particular application for the access control system while
25 maintaining substantially the same or similar functionality without departing from the scope and spirit of the present invention. In addition, although the embodiments described herein are directed to an access control system for a peripheral device, it will be appreciated by those skilled in the art that the teachings of the present invention can be applied to any device for which access to

a resource or feature of the device is controlled, without departing from the scope and spirit of the present invention.

WHAT IS CLAIMED IS:

1. An access control system, comprising:
a plurality of authorities, each authority associating at least one of a plurality of proof of knowledge operations with at least one of a plurality of proof of knowledge credentials;
a plurality of access control elements, each access control element identifying a Boolean combination of at least one of the authorities;
and
at least one access control list, which identifies one or more of the access control elements by which a method to be executed can be authenticated.
2. The access control system of claim 1, wherein the plurality of authorities, the plurality of access control elements and the access control list are maintained by firmware embedded within a peripheral device for which access is controlled by the system.
3. The access control system of claim 1 and further comprising:
a credential table, which identifies a set of the proof of knowledge credentials that can be proven by the associated proof of knowledge operation.
4. The access control system of claim 3 and further comprising a plurality of credential tables, where each credential table is associated with a corresponding one of the plurality of proof of knowledge operations.
5. The access control system of claim 1 and further comprising:

- an authority table, which identifies each of the plurality of authorities and for each authority associates one of the proof of knowledge operations with one of the proof of knowledge credentials.
6. The access control system of claim 1 and further comprising:
an access control element table, which identifies each of the plurality of access control elements and for each element, identifies the Boolean combination of the authorities for that access control element.
 7. The access control system of claim 1 and further comprising:
a method table, which identifies the method among a plurality of methods and for each method, identifies the access control list for that method.
 8. The access control system of claim 7 wherein for each method, the method table further comprises a pointer to a program to be executed for that method.
 9. An access control system comprising:
a credential table, which comprises a plurality of proof of knowledge credentials that can be proven by at least one of a plurality of proof of knowledge operations;
an authority table, which identifies a plurality of authorities and for each authority, associates at least one of the proof of knowledge operations with at least one of the proof of knowledge credentials;
and
an access control element table, which identifies a plurality of access control elements and for each access control element, identifies a Boolean combination of at least one of the authorities.

10. The access control system of claim 9 and further comprising:
a plurality of credential tables, where each credential table is associated with a corresponding one of the plurality of proof of knowledge operations and comprises the plurality of proof of knowledge credentials that can be proven by that proof of knowledge operation.
11. The access control system of claim 9 and further comprising:
a method table, which identifies a plurality of methods that can be executed, and for each method identifies a list of a subset of the access control elements by which that method can be authenticated.
12. The access control system of claim 9, wherein the credential table, the authority table and the access control element table are maintained by firmware embedded within a peripheral device for which access is controlled by the system.
13. A method comprising:
maintaining a plurality of authorities, each authority associating at least one of a plurality of proof of knowledge operations with at least one of a plurality of proof of knowledge credentials; and
maintaining a plurality of access control elements, each access control element identifying a Boolean combination of at least one of the authorities, the plurality of authorities and the plurality of access control elements being maintained at least in part within a memory associated with a device for which access is controlled.
14. The method of claim 13 wherein the plurality of authorities and the plurality of access control elements are embedded at least in part within firmware of the device.

15. The method of claim 13 and further comprising:
maintaining a credential table, which comprises a plurality of the proof of
knowledge credentials that can be proven by at least one of the
plurality of proof of knowledge operations.
16. The method of claim 15, wherein maintaining a credential table comprises:
maintaining a plurality of credential tables, where each credential table is
associated with a corresponding one of the plurality of proof of
knowledge operations and comprises the plurality of the proof of
knowledge credentials that can be proven by that proof of
knowledge operation.
17. The method of claim 13, wherein maintaining a plurality of authorities
comprises:
maintaining an authority table, which identifies the plurality of authorities
and for each authority, associates one of the proof of knowledge
operations with one of the proof of knowledge credentials.
18. The method of claim 13, wherein maintaining a plurality of access control
elements comprises:
maintaining an access control element table, which identifies the plurality
of access control elements and for each access control element
identifies the Boolean combination of at least one of the authorities.
19. The method of claim 13 and further comprising:
maintaining a method table, which identifies a plurality of methods that
can be executed, and for each method identifies a list of a subset of
the access control elements by which that method can be
authenticated.

20. A computer readable medium having a tangible component comprising instructions, which when executed by a computing device cause the computing device to perform steps comprising:

maintaining a plurality of authorities, each authority associating at least one of a plurality of proof of knowledge operations with at least one of a plurality of proof of knowledge credentials; and

maintaining a plurality of access control elements, each access control element identifying a Boolean combination of at least one of the authorities, the plurality of authorities and the plurality of access control elements being maintained at least in part within a memory associated with a device for which access is controlled.