Please type a plus sign (+) inside this box → [+]

PTO/SB/016 (08-00)
Approved fro use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Thahn	Ta	Huntington Beach, California
Thomas	DeMartini	Culver City, Calilfornia
Joseph	Fung	Cerritos, California

☒ *Additional inventors are being named on the Page 2 separately numbered sheets attached hereto*

TITLE OF THE INVENTION (280 characters max)

DURING-CONDITION

Direct all correspondence to: **CORRESPONDENCE ADDRESS**

☐ Customer Number 22204 → *Place Customer Number Bar Code Label here*

OR *Type Customer Number here*

☒ Firm *or* Individual Name	Marc S. Kaufman				
Address	NIXON PEABODY LLP				
Address	8180 Greensboro Drive				
City	McLean	State	VA	ZIP	22102
Country	USA	Telephone	(703) 790-9110	Fax	(703) 883-0370

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages* 7 ☐ CD(s), Number

☐ Drawing(s) *Number of Sheets* ☐ Other (specify)

☐ Application Data Sheet. See 37 CFR 1.76

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. Se 37 CFR 1.27.

☒ A check or money order is enclosed to cover the filing fees

☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 19-2380

☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($) $160.00

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____

Respectfully submitted,

SIGNATURE _____ Date 11/20/2001

TYPED or PRINTED NAME Marc S. Kaufman

REGISTRATION NO. *(if appropriate)* 35,212

Docket Number: 111325-91

TELEPHONE 703-790-9110

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

Additional inventors:

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Guillermo	Lao	Torrance, California
Mai	Nguyen	Buena Park, California
Bijan	Tadayon	Germantown, Maryland
Vincent	Tieu	Torrance, California
Duc	Tran	Westminster, California
Xin	Wang	Los Angeles, California

Inventors: Thahn Ta; Thomas DeMartini; Joseph Fung; Guillermo Lao; Mai Nguyen; Bijan Tadayon; Vincent Tieu; Duc Tran; Xin Wang

During-Condition

Table of Contents

Introduction

The concept of conditional access is a foundation of both Access Control and DRM systems. A typical access condition defines a list of authorized users along with a set of access rights and their conditions to a given resource. Access conditions associated with a given resource can be predefined as simple as Access Control Lists, which define the access rights to the given resource for the list of users or user groups (role based). Access conditions can also be defined as lists of rules such as in Rule Based Access Control. Either access conditions are expressed as an access control list, a set of rules defined in some language or data structure, the conventional condition access as implemented by most systems is just an authorization process in which a subject (e.g., a user or a system process) can only access to a protected resources after a certain list of conditions have been verified.

This invention extends the concepts of our previous United States patents 5629980, 5634012, 5638443, 5715403 and 5715403 the specifications of which are incorporated by reference.

Summary of the invention

The invention in this proposal extends the conventional concept of prerequisite conditions for access to cover the entire lifecycle. The invention proposes a system design that could be used to verify and validate conditions either before or during usage of the protected resources. With the new concept, conditions are associated with both the protected resource as well as the state of the protected resource -- not just associated with the resource as in the conventional concept of prerequisite conditions. Attaching conditions to various states of the protected resource provide content owners or service providers a flexible way to protect different type of resources such as digital work (definition of digital work is defined in our previous patents), web services, entities, software systems, etc. The system also proposes a flexible way to represent each condition as a state so that the current status and history of each condition can be logged and later be used.

Conditions

Our framework presents a new model for authorization that integrates both authorization and protection for a wide range of resources. Like the conventional model, authorizing an authenticated principle the rights to access to a protected resource is based on a list of conditions. This type of conditions is called access condition or precondition. However, we extend the concept of conditions to protecting the resource during the time it is being accessed as well as the time the access has been committed. An example of use of this invention is the XrML rights language but this invention is not limited to use with XrML.

Our concept of conditions is associated with the whole lifetime of the protected resource and can be expressed by any data structures, rules or languages. To protect a resource, conditions can be imposed on both tangible and intangible resources such as conditions on the principle who is granted access and use the protected resource, conditions on the system from which the resource is consumed, conditions on the time interval from which the protected document is allowed to access, conditions on the geography (territory), conditions on the repository from which the protected resource is reside, conditions on the fee that the user has to pay – either pre-pay, per-use or meter, conditions on the approval notice that the principle who is granted the rights to use the protected resource must obtain before using the protected resources, conditions on the notification that must be notified before or after using the resource, or conditions on the previous rights either related to the target protected resource or other resources. However our concepts of conditions are not limited to those conditions mentioned above but can be applicable to any resources. Resources defined in our concept of conditions can be tangible or intangible but must be measurable. Examples of such resources are digital document, device, system, services, time, fee or even permission or rights. No matter how condition is expressed - data structures, rules or languages - the basic information contained in a condition must include at least the following information: the resource – implicitly or explicitly - from which the condition is applied, and a set of values associated with the conditions. Optional information in conditions may include the method to obtain the condition value, and the server from which the condition value is obtained. These optional information are conditions imposed on conditions that a certain method must be used in order to verify a condition.

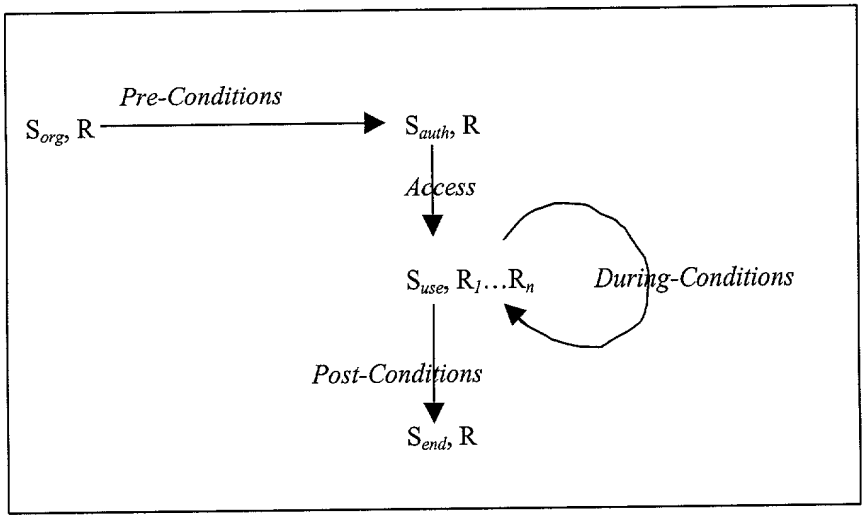
Current value of conditions can be represented by a data structure called state. State contains a reference to the condition from which it is associated to, the current value of the condition, the session id of the request and information needed to verify the value of the state such as method used to obtain the value of the conditions, the source from which the value is obtained, etc... Using state to represent condition has certain advantage that it will simplify the process of verify conditions. The state for each of conditions is constructed and then is used to verify against the associated condition. Each state contains all information needed by the verifier to verify the state value if the verifier decides to challenge the value stored in the state.

The state of a condition can either be fixed or changed over time and a collection of the states of conditions for a given rights/permission associated with an authenticated principle and a protected resource called "system state" for the principal and resource. Using the "system state" concept, condition for a given rights is defined as a set of required system states within which an authenticated principle is allowed to access to the protected resource. Thus, after a principal is authorized to access the resource, the system must be in one of these states; for convenience, we call them authorized states.

Access authorization: Origin System State -> Authorized System State

Once the system is in an authorized state, the authenticated principle is now able to access to the protected resource for an authorized operation. In many cases, it is not the authenticated principle itself that actually access the protected resource; rather the access is delegated to another authenticated principle (such as rendering application, service, etc.). While the protected resource is being accessed and consumed, the set of preconditions for granting the initial access

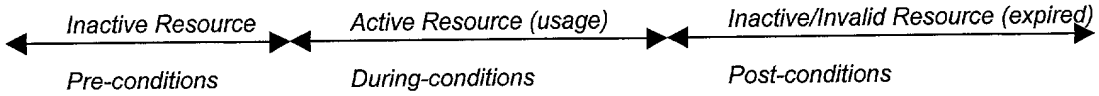
may no longer be applicable for authorizing the continuous access. Also, consuming the protected resource may transform the resource into a set of temporary resources (derived resources) from which the access conditions imposed on the original resources are also not applicable. In order to protect the protected resource and its derived resources while they are being accessed, our model introduces a new concept for authorization and protection, called during-conditions or protection conditions.



During-conditions are conditions that are transferred from the original resource to itself and any set of derived resources while they are being accessed and consumed by an authenticated principle. For example, if the protected resource is a document, which is displayed on the screen during the authorized operation view, then the derived resources may include the memory that contains the data from the document, the presentation format of the document, and the displayed windows. Those derived resources will all be protected by the set of during-conditions. Another example is that an application or user requests for a service and the requested service is a protected resource. Once the request is authorized, the application that executes the service may be considered as a derived resource and is subjected to the set of during-conditions while the service is being executed. During-conditions continuously change the system state until the derived resources are no longer used or the system state becomes unauthorized.

Once the requested operation is completed, either mandatory or voluntary, all the derived resources protected by during-conditions are deleted and the system state is then transferred to the final state by the set of post-conditions. State of conditions after the operation completed may or may not be changed. Those conditions with unchanged state are called stateless conditions, while others are called state conditions. Stateless conditions are usually pre-conditions used to control the access to the protected document. State conditions are usually during-conditions or post-conditions. They are used to control the lifetime of the protected resource. (For example, the protected resource becomes invalid once the number of copies is reached).

With different type of conditions associated with different stages of the protected resource, our framework does provide a complete mechanism to authorize the use of the protected resource and to protect that resource while it is being used.



DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.