The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.

Paper No. 23

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte DONALD F. AULT, JOHN C. DAYKA,
ERIC C. FINKELSTEIN, and RICHARD H. GUSKI

Appeal No. 2000-1360
Application No. 08/632,251

ON BRIEF

Before KRASS, FLEMING, and DIXON, Administrative Patent Judges.

KRASS, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the final rejection of claims 1-12, all of the pending claims.

The invention is directed to a method and apparatus for controlling server access to a resource in a client/server system. More particularly, the invention is directed to the problem of “untrusted” servers which present a security risk since the host system cannot assume that they have not manipulated a client’s identity and are not accessing a resource on their own behalf while purporting to act on behalf of a client. Access rights of these servers acting as principals are specified by the instant invention by allowing such servers to access only those host resources that the servers themselves can access as principals, even when the servers purport to be acting on behalf of a client that has access to those resources. Since untrusted servers access rights are limited, untrusted servers are allowed to coexist on a host system together with trusted servers.

Representative independent claim 1 is reproduced as follows:

1. In a client/server system in which a server executing on a host system performs application services for a client that involve accessing a host resource, said client and said server each having independently specified access rights to said host resource, a method of controlling server access to said host resource comprising the steps of:

upon receiving a request from a client for a service from a server, creating a client security context for said client, said client security context indicating whether said client is an authenticated client that is authenticated to said host system or an unauthenticated client that is not authenticated to said host system;

upon receiving a request for a specified access to a host resource from a server purporting to act on behalf of a client:

determining whether said client is allowed said access to said resource;

determining whether said client is an authenticated client or an unauthenticated client;

if said client is an authenticated client, granting said access to said host resource if said client is allowed said access to said host resource; and

if said client is an unauthenticated client, determining whether said server is allowed said access to said resource independently of said client and granting said access to said host resource if both said client and said server are independently allowed said access to said host resource, otherwise, refusing said access to said host resource.

The examiner relies on the following references:

Baker et al. (Baker)	5,678,041	Oct. 14, 1997 [filed Aug. 25, 1995]
Teper et al. (Teper)	5,815,665	Sep. 29, 1998 [filed Apr. 03, 1996]

Claims 1-12 stand rejected under 35 U.S.C. 103 as unpatentable over Baker in view of Teper.

Reference is made to the brief and answer for the respective positions of appellants and the examiner.

OPINION

At the outset, we note that, in accordance with appellants' grouping of the claims, at page 4 of the brief, and lack of separate arguments directed to the patentability of separate claims, claims 1-12 will stand or fall together.

It is the examiner's position that Baker discloses the claimed subject matter but for the claimed "creating a client security context for said client" upon receiving a request from a client for a service from a server. The examiner relies on Teper for a teaching of creating this "client security context," pointing to various portions of Teper, including the abstract, Figures 1-3, column 3, lines 5-53, column 7, lines 30-65, column 9, line 25 through column 10, line 29, column 10, line 44 through column 11, line 33, and column 20, lines 6-48.

The examiner then concludes that it would have been obvious to incorporate the teachings of Teper for creating a client security context for each client with the method of Baker for controlling server access to the host resource because "it would decrease the client overhead and increase

the security in order to helps [sic] server system to verify that the user is valid user [sic] and helps user [sic] to verify that the service received from the server is valid service" [answer-page 6].

We reverse as the examiner has failed to establish a prima facie case of obviousness with regard to the instant claimed subject matter.

Each of the independent claims requires that the client and the server each has "independently specified access rights."

Thus, taking claim 1 as an example, a client is determined to be authenticated or unauthenticated when the client requests service from a server. When a server requests service on behalf of a client, it is determined whether that client is allowed access to the resource and it is determined whether that client is an authenticated or unauthenticated client. Based on the results, access is granted to the resource if the client is authenticated AND is allowed access to that resource. If the client is unauthenticated, a determination is made of whether the server is allowed access to the resource *independently* of the client. Access is granted to

the resource if both the client and the server are *independently* allowed the access to the resource. If not, access to the resource is denied.

Thus, access to a resource is granted only if both the client and the server are independently allowed access to the resource.

We do not find this limitation taught or suggested by the applied references. The examiner contends otherwise, stating that Baker's proxy server 112 has independently specified rights to the host resources 101-105. The examiner quotes, "...retrieves rating and rational information from resource categorization information listing 300, and provides a manager

with a page that facilitates editing of the rating," citing Figure 6 and column 7, lines 40-43, and concluding that this "implies that the server having independently specified access rights (user clearance and resource rating) to the host resource (network resource)" [answer-pages 10-11].

We are at a loss to understand how the examiner is interpreting Baker to arrive at the claimed limitation of the independently allowed access to the resource by the client and the server. Rather, we agree with appellants that Baker's

clients 107-109 and proxy server 112 do not have independently specified access rights to the host resources because Baker's network is a public network which presumes access rights. Therefore, Baker does not teach determining the access rights of a server to a host resource independently of a client for which it is acting, nor does it teach conditioning client access to that resource based upon the combined access rights of the client and server, depending on the authenticated status of the client.

Moreover, we agree with appellants that it is the untrustworthiness of the server that is at issue in appellants' invention. Therefore, it would be absurd, in the instant claimed invention, for the server to be performing the authenticating and access control steps, as it apparently does in Baker. As stated

by appellants, at page 9 of the brief, the better analogy would be if the internet sites 101-105 in Baker determined the authenticated status of the users 107-109 and granted access to unauthenticated users only if the proxy server 12 were also authorized to access the Internet resources. But, since Baker does not operate in this manner because the network therein is

public, there is no teaching of the instant claimed subject matter nor is there any suggestion in Baker that the proxy server in Baker presents any security problem. Rather, Baker is interested in restricting access to certain sites by particular users and the determination of whether those users are authenticated and able to gain access to the sites is made before forwarding any request from a client to a server. The determination is not made “upon receiving a request...from a server,” as claimed.

Teper clearly does not provide for this deficiency in Baker and the examiner does not rely on Teper for this feature. Since the combination of references does not reach the claimed limitation regarding the independently specified access rights of the client and the server, we do not reach the question of whether Teper provides a proper teaching of the creating of “a client security context” for combining with Baker.

The examiner’s decision rejecting claims 1-12 under 35 U.S.C. 103 is reversed.

REVERSED

ERROL A. KRASS Administrative Patent Judge	)	
MICHAEL R. FLEMING Administrative Patent Judge	)	BOARD OF PATENT APPEALS AND INTERFERENCES
JOSEPH L. DIXON Administrative Patent Judge	)	

EK/RWK

WILLIAM A. KINNAMAN, JR.
INTELLECTUAL PROPERTY LAW
2455 SOUTH ROAD, P386
POUGHKEEPSIE, NY 12601