

The opinion in support of the decision being entered today was not written for publication and is not binding precedent of the Board.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. 34

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS  
AND INTERFERENCES

---

Ex parte CARY A. JARDIN

---

Appeal No. 2002-2126  
Application 08/931,187<sup>1</sup>

---

HEARD: April 8, 2003

---

Before BARRETT, DIXON, and GROSS, Administrative Patent Judges.  
BARRETT, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 from the final rejection of claims 1-34.

We affirm.

---

<sup>1</sup> Application for patent filed September 18, 1997, entitled (as amended) "Method and System for Establishing Secure Communications Over Computer Networks."



substitute appeal brief (Paper No. 26) (pages referred to as "Br\_\_") and the reply brief (Paper No. 29) (pages referred to as "RBr\_\_") for a statement of appellant's arguments thereagainst.

OPINION

Claims 1, 3-5, 10, 12, 13, and 15-34

The independent claims define an apparatus, system, or method for secure communications between a server and a remote client, in which the server selects a security algorithm from a plurality of security algorithms and communicates the selected security algorithm to the client (Br10-12). Independent claims 17, 28, 29, and 31 recite that the selection is random. Independent claims 17, 29, and 31-34 recite linking or potential linking of the selected security algorithm to the client application program and/or the server process.

Borza discloses that prior art solutions to secure communications on the Internet include a known encryption algorithm such as a public key/private key system (col. 1, lines 31-46) as described in connection with Fig. 2 (col. 4, line 51 to col. 5, line 12). Borza notes (col. 5, lines 13-20):

It is evident to those of skill in the art that implementation of security according to the prior art requires standardisation of encryption algorithms and processes, either through the use of software from the same vendor or through the use of a standard encryption algorithm. There are disadvantages to each of these approaches in that using a common vendor reduces flexibility and maintainability, while using a standard encryption algorithm reduces security.

Borza describes that "it is an object of this invention to provide a method for securely transmitting data across a network that is not confined to a single encryption algorithm" (col. 1, line 67 to col. 2 line 3). Thus, an object of Borza's invention is directed to overcoming the same problem as appellant's invention, that security upon a single algorithm is vulnerable.

Borza discloses a method of enhancing network security using two kinds of "process": a "security process" for securing information to be transferred and a "characterisation [Canadian/British spelling] process" to characterize biometric identification data. For purposes of this appeal, we consider only the "security process." However, we note that the claimed "security algorithm" is a broader term than "encryption algorithm," as indicated by dependent claims 3 and 12, and could also encompass the "characterisation process." Borza discloses that the "security process" could comprise "an encryption algorithm" (col. 5, lines 65-66; col. 8, lines 57-59), that the "server 51 is provided with a plurality of security processes (or characterisation processes for use with biometric identification systems) implemented using the JAVA programming language" (emphasis added) (col. 8, lines 47-50), the "server 51 transmits an encrypted security process ... to the client computer 52 where it is deciphered and executed" (col. 8, lines 52-55), and states that "[a]lternatively, the security process is determined

randomly" (emphasis added) (col. 8, lines 66-62). Thus, Borza discloses randomly selecting a security algorithm (the security process which may be an encryption algorithm) from a plurality of security algorithms. As shown in Fig. 4, the secure communication is initiated by the client. The security process is linked to the client application because "[a] client computer 52 provided with a JAVA interpreter is capable of executing the security processes" (col. 8, lines 50-51), which appears to be the disclosed method in the specification, page 8. It is inherent that if Borza sends an encryption algorithm as a security process to the client, it must have a decryption algorithm on the server to be able to decode the data. For these reasons, we find the independent claims to be anticipated.

Appellant argues that column 5 to column 6 of Borza cited by the examiner do not disclose the limitations of the independent claims (Br14), that no selection of a security algorithm at the server is required, nor is there any transmission of the selected security algorithm from the server to the client computer (Br16), and that "there is **no** disclosure anywhere from Borza [of the limitations of the independent claims]" (Br19).

These arguments are not persuasive based on the findings above. The rejection is based on anticipation and appellant is responsible for reading the entire reference, not just the portions expressly referred to by the examiner.

Appellant argues that Borza relies on private key/public key algorithms incorporated in both the server and the client (Br13) and that only after the exchange of public encryption keys can the server prepare an enhanced security process (Br17), whereas in appellant's independent claims, the selection of a security algorithm is made in direct response to the client's request, not after an exchange of public keys as in Borza and there is no exchange of public keys in the claims (Br18). See also RBr5-6.

These arguments are totally unpersuasive. The claims are open ended and, therefore, do not preclude the existence of other structure or steps, such as the additional encryption in Borza.

Appellant argues that Borza does not randomly select from one of a plurality of security algorithms (RBr4: RBr7; RBr8).

As previously discussed, Borza discloses selection from a plurality of security processes stored on the server, the security process can be an encryption algorithm, and the security process can be randomly selected. Appellant has not dealt with any of these teachings of Borza.

Appellant argues that "[t]he security process as suggested by Borza '167 is a biometric characterization process" (RBr5; see also RBr6-7).

This is an erroneous argument. Borza distinguishes between "security process" and a "characterization process" (e.g., col. 8, lines 47-49), although it discloses that the security

Appeal No. 2002-2126  
Application 08/931,187

process can be in the form of a characterization process (col. 10, lines 49-50) as well as an encryption algorithm (col. 5, lines 65-67; col. 10, lines 64-66).

Arguments not made have not been addressed. See 37 CFR § 1.192(c)8)(iv) (1990) (arguments must be made in the brief).

Appellant has not shown error in the finding of anticipation. The rejection of claims 1, 3-5, 10, 12, 13, and 15-34 is sustained.

Dependent claim 2

Appellant argues that Borza does not disclose that "the selected security algorithm encodes and decodes information communicated between the server and client" in claim 2 and "[t]here is **no** disclosure anywhere from Borza '167 of any selected security algorithm" (Br21).

Borza discloses that a "security process" transmitted to the client can be an encryption algorithm (col. 5, lines 65-67), which necessarily encodes information. Inherently, the server must contain a complementary decryption algorithm to decode the encrypted information. Appellant has not shown error in the rejection. The rejection of claim 2 is sustained.

Appeal No. 2002-2126  
Application 08/931,187

Dependent claim 6

Appellant argues that the limitations that "the server communicates the selected security algorithm to the client as a data stream, and wherein the the application program is configured to transform the data stream into at least one accessible routine" in claim 6 are "not disclosed anywhere in Borza '167" (Br21). It is argued that column 8, line 65 to column 9, line 48, cited by the examiner, is a pseudo-code listing of a JAVA applet for performing biometric characterization (Br21) and (Br21): "There is **no** disclosure anywhere from Borza '167 of any selected security algorithm as alleged by the Examiner. As a result, no selected security algorithm can be communicated to [a] client in any form as incorrectly alleged by the Examiner."

Borza discloses that a "security process" transmitted to the client can be an encryption algorithm (col. 5, lines 65-67). Borza discloses transmitting the security process, implemented in the JAVA programming language, to the client where it is deciphered and executed. Since the client computer is capable of executing the transmitted security process in JAVA form, it is necessarily configured to transform the data stream from the network into an executable routine. Appellant has not shown error in the rejection. The rejection of claim 6 is sustained.

Appeal No. 2002-2126  
Application 08/931,187

Dependent claims 7, 8, and 11

Appellant argues that the virtual machine configured to transform the security algorithm into program code or a routine accessible by the client application program in claims 7, 8, and 11 is not taught by Borza (Br21-22).

Borza discloses that the method of transmitting security processes "relies on the cross platform compatibility built into the JAVA programming language" (col. 8, lines 45-46) and that the client "provided with a JAVA interpreter is capable of executing the security process" (col. 8, lines 50-51). It was well known that a JAVA interpreter is a JAVA Virtual Machine. The interpreter transforms the data stream into an executable program. Appellant has not shown error in the rejection. The rejection of claims 7, 8, and 11 is sustained.

Dependent claim 14

Appellant argues that Borza does not disclose "selecting the security algorithm based on at least one of: the geographic location, IP address, and security level of the client" in claim 14. It is argued that since there is no disclosure of any selected security algorithm anywhere in Borza, no selection of security algorithm can be based on the three criteria (Br22-23).

Borza discloses that a "security process" transmitted to the client can be an encryption algorithm (col. 5, lines 65-67).

Appeal No. 2002-2126  
Application 08/931,187

Borza discloses that "the location of the client--in a secure environment, in a university computer lab, mobile computer, etc.--is also a factor" (col. 13, lines 30-32) in determining a minimum set of requirements for security. Appellant has not shown that the minimum set of requirements do not apply to the security process. For the examiner's benefit in any continued prosecution, we note that determination of the security algorithm based on location was well known, the best example being the use of different encryption standards for U.S. and export (international) use. Appellant has not shown any error in the rejection. The rejection of claim 14 is sustained.



Appeal No. 2002-2126  
Application 08/931,187

ANTONELLI TERRY STOUT AND KRAUS  
SUITE 1800  
1300 NORTH SEVENTEENTH STREET  
ARLINGTON, VA 22209