

FILE HISTORY

60/030,639

INVENTORS: SHLOMO TOUBOUL KEFAR HAIM, (IL)

TITLE: SYSTEM AND METHOD FOR  
PROTECTING A COMPUTER FROM  
HOSTILE' DOWNLOADABLES

FILED: 08 NOV 1996

COMPILED: 11 MAR 2015

SOPHOS  
EXHIBIT 1005 - PAGE 0002

60/030,639

SYSTEM AND METHOD FOR PROTECTING A COMPUTER FROM  
HOSTILE DOWNLOADABLES

Transaction History

Date	Transaction Description
12/3/1996	Initial Exam Team nn
1/3/1997	Preexamination Location Change
4/12/2001	Official Search Conducted
4/12/2001	Case Reported Lost
5/7/2001	Termination of Official Search
5/23/2001	Termination of Official Search
5/23/2001	Case Found
9/21/2001	Set Application Status

PATENT APPLICATION

APPROVED FOR LICENSE ☐



60030639

INITIALS *DEA*

Entered  
for  
Counted

CONTENTS

Received  
or  
Mailed

1.	Application papers	
2.	Request for Access	10-2-01
3.	Request for Access	7-16-03
4.	Request for Access	9/24/05
5.	Request for Access	1-13-04
6.	Request for Access	3-25-05
7.	Request for Access	2-23-06
8.	Request for Access	6/12/06
9.	Request for Access	9/28/06
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		
31.		
32.		

(FRONT)

POSITION		ID NO.	DATE
CLASSIFIER			
EXAMINER		249	12/16/96
TYPIST		441	12/18/96
VERIFIER	4/12 12/19		
CORPS CORR.			
SPEC. HAND			
FILE MAINT			
DRAFTING			

(LEFT INSIDE)





PATENT APPLICATION SERIAL NO. 60/030639

U.S. DEPARTMENT OF COMMERCE  
PATENT AND TRADEMARK OFFICE  
FEE RECORD SHEET

PTO-1556  
(5/87)





60/030639

PTO/SB/16 (11-95)  
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

## PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (b)(2) &amp; 1.51(a)(2)(i).

Docket No. D-558		Type a plus sign (+) inside this box -->		+
INVENTOR(s) / APPLICANT(s)				
LAST NAME	FIRST NAME	MIDDLE INITIAL	RESIDENCE (CITY AND EITHER STATE OR FOREIGN COUNTRY)	
Touboul	Shlomo		Kefar Haim, Israel	
TITLE OF INVENTION (280 characters max)				
System and Method for Protecting a Computer from Hostile Downloadables				
CORRESPONDENCE ADDRESS				
Eppa Hite Carr, DeFilippo & Ferrell LLP 2225 East Bayshore Road, Suite 200 Palo Alto			Tel.: (415) 812-3428 Fax: (415) 812-3444	
STATE:	California	ZIP CODE:	94303	COUNTRY: U.S.A.
ENCLOSED APPLICATION PARTS (check all that apply)				
<input checked="" type="checkbox"/> Specification		Number of Pages [ 23 ]	<input type="checkbox"/> Small Entity Statement	
<input checked="" type="checkbox"/> Drawing(s)		Number of Sheets [ 7 ]	<input checked="" type="checkbox"/> Other (specify): 9 page "Appendix"	
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT				
<input checked="" type="checkbox"/> A check or money order is enclosed to cover the filing fees.				
<input type="checkbox"/> The Commissioner is hereby authorized to charge the filing fees and credit Deposit Account No. 06-0600.				
<input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge payment of the following fees associated with this communication or credit any overpayment to Deposit Account No. 06-0600. A duplicate copy of this sheet is attached.			Filing Fee Amount (\$):	\$150.00

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 member are: \_\_\_\_\_Respectfully submitted,  
Shlomo Touboul

*Eppa Hite*  
Eppa Hite, Reg. No. 30,266  
Carr, DeFilippo & Ferrell LLP  
2225 East Bayshore Road, Suite 200  
Palo Alto, CA 94303  
Tel.: (415) 812-3428  
Fax: (415) 812-3444

Date: 11-8-96

Send To: Box Provisional Application  
Assistant Commissioner for Patents  
Washington, D.C. 20231☐ Additional inventors are being named on separately numbered sheets attached hereto.

60/030689



IN THE  
UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT: Touboul, Shlomo  
SERIAL NO.: Unknown  
FILING DATE: On Even Date Herewith  
TITLE: System and Method fro protecting a Computer from  
Hostile Downloadables  
EXAMINER: Unknown  
GROUP ART UNIT: Unknown  
ATTY.DKT.NO.: PA-558

---

ASSISTANT COMMISSIONER FOR PATENTS  
WASHINGTON, D.C. 20231

CERTIFICATE OF EXPRESS MAIL

SIR:

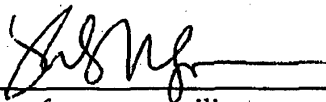
EM383068528US

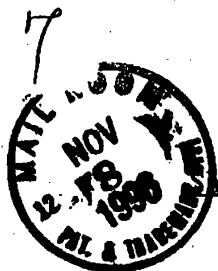
"Express Mail" mailing label number EM383068528US

Date of Deposit: NOVEMBER 8, 1996

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to Assistant Commissioner for Patents, Washington, D.C. 20231.

Deposited by: Theresa Sueoka

  
(Signature of person mailing paper or fee)



150.00

114 60 20/30/39  
PATENT

SYSTEM AND METHOD FOR PROTECTING A COMPUTER FROM HOSTILE  
DOWNLOADABLES

BACKGROUND OF THE INVENTION

5 1. Field of the Invention

This invention relates generally to computer networks, and more particularly to a system and method for protecting computers from hostile Downloadables.

10 2. Description of the Background Art

The Internet is a collection of currently over 100,000 individual computer networks owned by governments, universities, nonprofit groups and companies, and is expanding at an accelerating rate. Because the Internet is public, the Internet has become a major source of many system damaging and system fatal application programs, commonly referred to as "viruses."

Accordingly, programmers continue to design computer security systems for blocking these viruses from attacking both individual and network computers. On the most part, these security systems have been relatively successful. However, these security systems are not configured to recognize computer viruses which have been attached to Downloadable application programs,

## PATENT

commonly referred to as "applets" or "Downloadables." A  
Downloadable is an executable application program which is  
automatically downloaded from a source computer and run on the  
destination computer. Examples of Downloadables include applets  
5 designed for use in the Java™ distributing environment produced by  
Sun Microsystems or for use in the Active X distributing  
environment produced by Microsoft Corporation. Therefore, a  
system and method are needed to protect computers from viruses  
attached to these Downloadables.

PATENT

SUMMARY OF THE INVENTION

The present invention provides a system for protecting a computer from hostile Downloadables. The system comprises an interface for receiving a Downloadable, a first memory portion  
5 storing security policies and a second memory portion storing known hostile Downloadables. The system further comprises a first comparator, coupled to the interface and to the first memory portion, for discarding the received Downloadable when it matches one of the known hostile Downloadables. The system further comprises a  
10 second comparator, coupled to the first comparator and to the second memory portion, for discarding the received Downloadable if it violates one of security policies.

The present invention further provides a method for protecting a computer from hostile Downloadables. The method comprises the  
15 steps of receiving a Downloadable, discarding the received Downloadable when the received Downloadable matches a predetermined hostile Downloadable, obtaining Downloadable security profile data on the received Downloadable when the Downloadable does not match a predetermined hostile Downloadable  
20 and discarding the received Downloadable when the Downloadable security profile data violates a predetermined security policy.

## PATENT

The system and method of the present invention provide computer protection from potentially hostile computer viruses which have been attached to Downloadables. The system and method of the present invention advantageously identifies both known hostile

5 Downloadables and identifies potentially hostile commands by decomposing unknown Downloadables.

**BRIEF DESCRIPTION OF THE DRAWINGS**

FIG. 1 is a block diagram illustrating a network system in accordance with the present invention;

FIG. 2 is a block diagram illustrating the internal network security system of FIG. 1;

FIG. 3 is a block diagram illustrating the security program of FIG. 2;

FIG. 4 is a flow chart illustrating an example security policy of FIG. 2;

FIG. 5 is a block diagram illustrating the security management console of FIG. 1;

FIG. 6 is a flowchart illustrating a method for protecting an internal computer network from hostile Downloadables; and

FIG. 7 is a flowchart illustrating the FIG. 6 method for decomposing a Downloadable.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

FIG. 1 is a block diagram illustrating a network system 100 in accordance with the present invention. Network system 100 includes an external computer network 105, such as the Wide Area Network (WAN) commonly referred to as the Internet, coupled via a signal bus 125 to an internal network security system 110. Network system 100 further includes an internal computer network 115, such as a corporate Local Area Network (LAN), coupled via a signal bus 130 to internal network computer system 110 and coupled via a signal bus 135 to a security management console 120.

Internal network security system 110 examines Downloadables received from external computer network 105, and prevents all recognizably-hostile Downloadables from reaching internal computer network 115. A Downloadable is hostile if it threatens the integrity of an internal computer network 115 component. Security management console 120 enables modification of internal network security system 110.

FIG. 2 is a block diagram of a internal network security system 110 which includes a Central Processing Unit (CPU) 205, such as a Motorola Power PC® microprocessor or an Intel Pentium® microprocessor, coupled to a signal bus 220. Internal network



PATENT

security system 110 further includes an external communications interface 210 coupled between signal bus 125 and signal bus 220 for receiving the Downloadables from external computer network 105, and an internal communications interface 225 coupled between  
5 signal bus 220 and signal bus 130 for forwarding non-hostile Downloadables to internal computer network 115. Alternatively, external communications interface 210 and internal communications interface 225 may be functional components of an integral communications interface (not shown) for both receiving  
10 Downloadables from external computer network 105 and forwarding non-hostile Downloadables to internal computer network 115.

Internal network security system 110 further includes Input/Output (I/O) interfaces 215 such as a keyboard, mouse and Cathode Ray Tube (CRT) display, a data storage device 230 such as  
15 Read Only Memory (ROM) or magnetic disk, and a Random-Access Memory (RAM) 235, each being coupled to signal bus 220. Data storage device 230 stores a security database 240 which includes security policies and Downloadable data on for determining whether a received Downloadable is hostile, and stores an events log 245  
20 which includes the determination results for each Downloadable. An operating system 250 controls processing by CPU 205, and is typically stored data storage device 230 and loaded into RAM 235

PATENT

for execution. A security program 255 controls operations of internal network security system 110, and also may be stored in data storage device 230 and loaded into RAM 235 for execution by CPU 205.

5

FIG. 3 is a block diagram illustrating details of security program 255. Security program 255 includes an ID generator 315, a first comparator 320 coupled to ID generator 315, a code scanner coupled to first comparator 320, a second comparator 330 coupled to code scanner 325 and to first comparator 320, and a record-keeping engine 335 coupled to first comparator 320 and to second comparator 330.

Security program 255 operates in conjunction with security database 240 and events log 245. Security database 240 stores security policies 305 in a first data storage device 230 portion, known Downloadables 307 in a second data storage device 230 portion and Downloadable Security Profiles (DSPs) data corresponding to the known Downloadables 310 in a third data storage device 230 portion. Security policies 305 include a list of computer operations which are deemed to be potentially hostile to the integrity of internal computer network 115. Potentially hostile operations may include READ/WRITE operations on a system

20

PATENT

configuration file, READ/WRITE operations on a document containing trade secrets, or any other operation that a user deems potentially hostile. Known Downloadables 307 may include Downloadables which Original Equipment Manufacturers (OEMs) know to be hostile, 5 Downloadables which OEMs know to be non-hostile, Downloadables which second comparator 330 (described below) has previously determined to be hostile, and Downloadables which second comparator 330 (described below) has previously determined to be non-hostile. DSP data 310 includes the fundamental computer 10 operations included in each known Downloadable 307, and may include READs, WRITEs, file management operations, system management operations, memory management operations and CPU allocation operations.

ID generator 315 receives Downloadables from external 15 computer network 105 via external communications interface 210, and which generates a digital signature for each Downloadable. A digital signature may include a Downloadable identification number, the Downloadable type, the Downloadable source and the Downloadable destination.

20 First comparator 320 receives and bit-wise compares the Downloadables from ID generator 315 with known Downloadables 307 stored in security database 240. If first comparator 320

PATENT

determines a received Downloadable is identical to a known hostile Downloadable 307, then first comparator 320 discards the received Downloadable, and forwards a non-hostile Downloadable to the intended destination to inform the user that internal network security system 110 discarded the Downloadable. If first comparator 320 determines that the received Downloadable is identical to a known non-hostile Downloadable 307, then first comparator 320 forwards the received Downloadable and the corresponding DSP data 310 to second comparator 330. If first comparator 320 determines that the received Downloadable does not match a known Downloadable (i.e., an "unknown Downloadable"), then first comparator 320 forwards the received Downloadable to code scanner 325 (described below). In any case, first comparator 320 then sends a status report to record-keeping engine 335 (described below).

Code scanner 325 receives unknown Downloadables from first comparator 320 and uses conventional parsing techniques to decompose the byte code of the unknown Downloadable into DSP data. Code scanner 325 then sends the Downloadable and the corresponding DSP data to second comparator 330.

Second comparator 330 receives the Downloadable and the corresponding DSP data either from code scanner 325 or from first

PATENT

comparator 320, and compares the DSP data against security policies  
305 stored in security database 305. If, from the DSP data, second  
comparator 330 determines that the Downloadable includes a  
hostile operation, then second comparator 330 prevents the  
5 Downloadable from passing to internal computer network 115.  
Similarly to first comparator 320, second comparator 330 forwards a  
non-hostile Downloadable to the intended destination to inform the  
user that internal network security system 110 discarded the  
Downloadable. If second comparator 330 determines that the  
10 received Downloadable does not violate any security policy 305,  
then second comparator 330 forwards the received non-hostile  
Downloadable to internal computer network 115. Further, if second  
comparator 330 received the non-hostile Downloadable from code  
scanner 325, then the non-hostile Downloadable is stored in known  
15 Downloadables 307 and its corresponding DSP data is stored in DSP  
data 310. In any case, second comparator 330 sends a status report  
to record-keeping engine 335 (described below).

Record-keeping engine 335 receives status reports from first  
comparator 320 and from second comparator 330, and stores the  
20 reports in events log 245 in data storage device 230.

FIG. 4 is a block diagram illustrating an example security policy 305.

FIG. 5 is a block diagram illustrating details of security management console 120, which includes a security policy generator 505 coupled to signal bus 135, an event log analysis engine 510 coupled to signal bus 135, a user notification engine 515 coupled to event log analysis engine 510 and a Downloadable database review engine 520 coupled to signal bus 135. Security management console 120 further includes computer components similar to the computer components illustrated in FIG. 2.

Security policy generator 505 uses an I/O interface similar to I/O interface 215 for enabling user modification of security policies 305. Further, security policy generator 505 enables the user to provide multiple security levels, i.e., enables the storage of multiple sets of security policies 305 (wherein second comparator 330 can use only a particular set of security policies 305 based on the destination of a received Downloadable). For example, security policies 305 may enable a corporate manager to receive selected Downloadables but may prevent the corporate manager's secretary from receiving those Downloadables.

PATENT

Event log analysis engine 510 examines the status reports stored in events log 245 of data storage device 230. Event log analysis engine 510 determines if notification of the user (e.g., the security system manager) is warranted. For example, event log  
5 analysis engine 510 may warrant user notification whenever ten (10) hostile Downloadables have been discarded by internal network security system 110 within a thirty (30) minute period, thereby flagging a possible security threat. Accordingly, event log analysis engine 510 instructs user notification engine 515 to inform the user.  
10 For example, user notification engine 515 may send an e-mail via internal communications interface 220 or via external communications interface 210 to the user, or may display a message on the user's display device (not shown).

Downloadable database review engine 520 enables a user (e.g.,  
15 a network security manager) to examine and modify known Downloadables 307 and DSP data 310. Thus, if for example a user learns of new hostile Downloadables, the user can add them to known Downloadables 307 and the corresponding DSP data to DSP data 310. Similarly, the user can add new non-hostile  
20 Downloadables to known Downloadables 307 and corresponding DSP data to DSP data 310.

PATENT

FIG. 6 is a flowchart illustrating a method 600 for protecting an internal computer network 115 from hostile Downloadables.

Method 600 begins with step 605 by ID generator 315 receiving a  
5 Downloadable. ID generator 315 in step 610 generates a signature representing the received Downloadable. First comparator 320 in step 615 compares the received Downloadable with known Downloadables 307 previously-stored in security database 240. If first comparator 320 in step 620 determines that the received  
10 Downloadable is the same as a known hostile Downloadable 307, then first comparator 320 in step 625 discards the received Downloadable and in step 630 forwards a substitute non-hostile Downloadable to the intended destination to inform the user. First comparator 320 in step 635 instructs record-keeping engine 335 to  
15 record the findings, i.e., a status report, in events log 245. Method 600 then ends.

If first comparator 320 in step 620 did not recognize the received Downloadable as a hostile Downloadable 307, then first comparator 320 in step 640 determines whether the received  
20 Downloadable is a known non-hostile Downloadable 307. If so, then first comparator 320 in step 645 retrieves the DSP data 310 corresponding to the known non-hostile Downloadable and jumps to



PATENT

step 655. Otherwise, first comparator 320 forwards the received Downloadable to code scanner 325, which in step 650 decomposes the received Downloadable into DSP data and then jumps to step 655.

5 In step 655, second comparator 330 compares the DSP data, either retrieved by first comparator 320 from security database 240 or generated by code scanner 325, with security policies 310 stored in security database 240. If second comparator 330 in step 660 determines that the DSP data violates a security policy 310, then  
10 second comparator 330 proceeds to step 625. Otherwise, second comparator 330 in step 665 passes the received Downloadable to internal computer network 115 as a non-hostile Downloadable, and proceeds to step 635.

15 FIG. 7 is a flowchart illustrating details of method 650 for decomposing a Downloadable. Method 650 begins in step 705 with code scanner 325 disassembling the machine code of the Downloadable. Code scanner 325 in step 710 resolves a respective command in the machine code. Code scanner 325 in step 715  
20 determines whether the resolved command is a suspect command. Examples of suspect commands include a memory allocation

PATENT

command, a loop command such as "goto", "while", "if", "than" or the like. If not, then code scanner 325 returns to step 710.

Otherwise, code scanner 325 in step 720 decodes and registers the command and the command parameters as DSP data. Code  
5 scanner 325 in step 720 registers commands and command parameters into a format based on command class, e.g., file system class, network system class, memory system class and CPU system class). Code scanner 325 in step 725 determines whether the machine code includes another command. If so, then code scanner  
10 325 returns to step 710. Otherwise, method 650 ends.

PATENT

The foregoing description of the preferred embodiments of the invention is by way of example only, and other variations of the above-described embodiments and methods are provided by the present invention. For example, although the invention has been  
5 described in a system for protecting an internal computer network, the invention can be embodied in a system for protecting an individual computer. Components of this invention may be implemented using a programmed general purpose digital computer, using application specific integrated circuits, or using a network of  
10 interconnected conventional components and circuits. The embodiments described herein have been presented for purposes of illustration and are not intended to be exhaustive or limiting. Many variations and modifications are possible in light of the foregoing teaching. The system is limited only by the following claims.

PATENT

WHAT IS CLAIMED IS:

- 1 1. A computer-based method for determining whether a  
2 Downloadable is hostile, comprising the steps of:  
3 receiving a Downloadable;  
4 decomposing the Downloadable into Downloadable security  
5 profile data;  
6 comparing the Downloadable security profile data against  
7 predetermined security policies to determine if a security policy has  
8 been violated; and  
9 discarding the received Downloadable when a security policy  
10 has been violated.
  
- 1 2. A computer-based method for protecting a computer from  
2 hostile Downloadables, comprising the steps of:  
3 receiving a Downloadable;  
4 discarding the received Downloadable when the received  
5 Downloadable matches a predetermined hostile Downloadable;  
6 obtaining Downloadable security profile data on the received  
7 Downloadable when the Downloadable does not match a  
8 predetermined hostile Downloadable; and

PATENT

9       discarding the received Downloadable when the Downloadable  
10 security profile data violates a predetermined security policy.

1    3.    A system for determining whether a Downloadable is hostile,  
2    comprising:  
3       a security database storing security policies;  
4       an interface for receiving a current Downloadable;  
5       a code scanner, coupled to the interface, for decomposing the  
6    current Downloadable into Downloadable security profile data; and  
7       a comparator, coupled to the code scanner and to the security  
8    database, for comparing the security policies against the  
9    Downloadable security profile data to determine if a security policy  
10   has been violated.

1    4.    A system for protecting a computer from hostile  
2    Downloadables, comprising:  
3       an interface for receiving a Downloadable;  
4       a first memory portion storing security policies;  
5       a second memory portion storing known hostile Downloadables;  
6       a first comparator, coupled to the interface and to the first  
7    memory portion, for discarding the received Downloadable when it  
8    matches one of the known hostile Downloadables; and

PATENT

9 a second comparator, coupled to the first comparator and to the  
10 second memory portion, for discarding the received Downloadable if  
11 it violates one of security policies.

1 5. A system for determining whether a Downloadable is hostile,  
2 comprising:

3 means for receiving a Downloadable;

4 means for decomposing the Downloadable into Downloadable  
5 security profile data;

6 means for comparing the Downloadable security profile data  
7 against predetermined security policies to determine if a security  
8 policy has been violated; and

9 means for discarding the received Downloadable when a  
10 security policy has been violated.

1 6. A system for protecting a computer from hostile

2 Downloadables, comprising:

3 means for receiving a Downloadable;

4 means for discarding the received Downloadable when the  
5 received Downloadable matches a predetermined hostile

6 Downloadable;

PATENT

7 means for obtaining Downloadable security profile data on the  
8 received Downloadable when the Downloadable does not match a  
9 predetermined hostile Downloadable; and

10 means for discarding the received Downloadable when the  
11 Downloadable security profile data violates a predetermined security  
12 policy.

1 7. A computer-readable storage medium storing program code for  
2 causing a computer to perform the steps of:

3 receiving a Downloadable;

4 decomposing the Downloadable into Downloadable security  
5 profile data;

6 comparing the Downloadable security profile data against  
7 predetermined security policies to determine if a security policy has  
8 been violated; and

9 discarding the received Downloadable when a security policy  
10 has been violated.

1 8. A computer-readable storage medium storing program code for  
2 causing a computer to perform the steps of:

3 receiving a Downloadable;

PATENT

4       discarding the received Downloadable when the received  
5 Downloadable matches a predetermined hostile Downloadable;  
6       obtaining Downloadable security profile data on the received  
7 Downloadable when the Downloadable does not match a  
8 predetermined hostile Downloadable; and  
9       discarding the received Downloadable when the Downloadable  
10 security profile data violates a predetermined security policy.



## APPENDIX

### Gateway Level Corporate Security for the New World of Java™ and Downloadables

#### SurfinGate™ Means Business

New downloadable technologies including Java™ and ActiveX™ present today's enterprises with expanded Intranet capabilities, but they also expose corporate computer resources to new kinds of security attacks. SurfinGate™ addresses the new computing paradigm with corporate-level security at the gateway level for safe use of Java and other Internet downloadables. An intelligent security solution for companies with access to the Internet, SurfinGate functions at the corporate gateway, where it intelligently scans, digitally signs, and controls all downloadables before they access the network. SurfinGate's powerful enterprise-wide security is combined with efficient, centralized control of the company's Intranet computer users.

SurfinGate offers corporate security managers the ability to:

- Establish a security policy for use of Java applets and other Internet downloadables
- Prevent loading of suspicious Java applets or ActiveX entities at the gateway level
- Provide corporate users with safe Internet access without having to disable downloadable technology such as Java or ActiveX
- Protect the corporate resources from damage or unauthorized access by downloadables

SurfinGate addresses a new computing paradigm, where mini-applications called downloadables are automatically pushed into corporate Intranets unbeknownst to users. As Intranet users access the on-line resources they need, the business enterprise is exposed to downloadable-transmitted risks like corporate espionage, e-mail fraud, or resource attacks. For the corporate security manager, the new paradigm's Java applets and ActiveX technologies represent serious new security threats that are simply not addressed by built-in security systems like the Java Security Manager. SurfinGate offers sophisticated security at the outermost gateway level, keeping potentially problematic applets completely outside of the corporate environment.

SurfinGate functions:

- Intelligently scans, analyzes, and controls automatically downloaded Java applets or ActiveX entities
- Specifically executes corporate security policy as defined by the security manager via Security Management Console (SMC), including:
  - ◊ blocking out any applet that meets a suspicious applet profile
  - ◊ positively identifying applets before allowing them into the system
  - ◊ scanning applets for unauthorized actions and assigning appropriate applet security profile

31-OCT-1996 20:47 FROM FINJAN SOFTWARE

TO 0014158123444----- P.08

- ◊ intelligently deciding appropriate access based on security policy guidelines and on applet security profile
- ◊ digitally signing acceptable applets before entry

### *Control and Security from Three Different Perspectives*

The essence of SurfInGate's protective powers is a three-fold checks and balances process that includes the profile generator, database, and Security Management Console. Incoming applets or objects are first "x-rayed" to expose any potential problems and are assigned a security profile. That profile is then checked against known hostile applets in the database, and is evaluated yet again with information from the Security Management Console (SMC) to ensure that filtering precisely executes the company's security policy. An integral part of SurfInGate, the SMC allows corporate security managers specific control over business groups or departments, including what resources are available to which Intranet users at what times.

### **SurfInGate features and benefits:**

- easy customization and implementation of a corporate security policy for downloadables
- a layer of security several steps away from critical resources
- extensive built-in database of potentially hostile or problematic Java applets
- central control over Internet downloadable activity
- case-specific downloadable security policy instead of total exclusion of all downloadable technology
- protection against downloadables that is compatible with other security devices including firewalls
- simple set-up of corporate hierarchy to develop appropriate user access

SurfInGate is available from Finjan Software, the leading provider of multi-layer security solutions for the new world of Internet/Intranet downloadables. The Finjan suite of solutions protect enterprise and stand-alone computer resources from the potential risks of downloadables such as Java applets and ActiveX entities through a multi-layered approach. Finjan believes that no single security solution can eliminate all threats completely, and recommends customers choose degrees of security at various layers of the network according to their specific needs.

### **For more information contact:**

Sharon Hess, Marketing Director  
Telephone: +972-9-865-9440  
US phone: (415) 509-4836  
Fax: +972-9-865-9441  
E-mail: sharon@finjan.com

Ron Moritz, CISSP, Technical Director  
Telephone: +1.216.932.9775  
Toll-Free: +1 888.FINJAN.8  
Voice mail: +1.216.302.6873  
E-mail: ron@finjan.com

©1996 Finjan Software Ltd.

SurfInGate is a trademark of Finjan Software Ltd.; Java is a trademark of Sun Microsystems Inc.; ActiveX is a trademark of Microsoft Inc.

## Security Policy

A security policy is information that is stored in a database that includes the following:

A list of applets (identified with their ID signatures) and an ACL (access control list) for each applet vis-a-vis the file system, network system, memory system and process system. The following figure illustrates that user 1 of department A has a security policy BB. User 2 of the same department has security policy AA.

Security Policy BB includes:

Applet A with the following (sample) ACL:

File system ACL:

Applet A can write into file c:\data\mydata.dat  
can read from d:\info\general.doc  
cannot do anything else.

Applet B cannot read nor write from any file

Applet C can read file d:\bad\interest\info.doc

Network system:

Applet A cannot communicate with any other computer  
Applet B can communicate with mail.finjan.com for port 25 (mail protocol) only.  
Applet C cannot communicate with any other computer

Memory system

Applet A, B and C can allocate only 250Kbyte

Process system:

Applet A can run up to only 5 threads.  
Applet B and C can run up to only 8 threads.

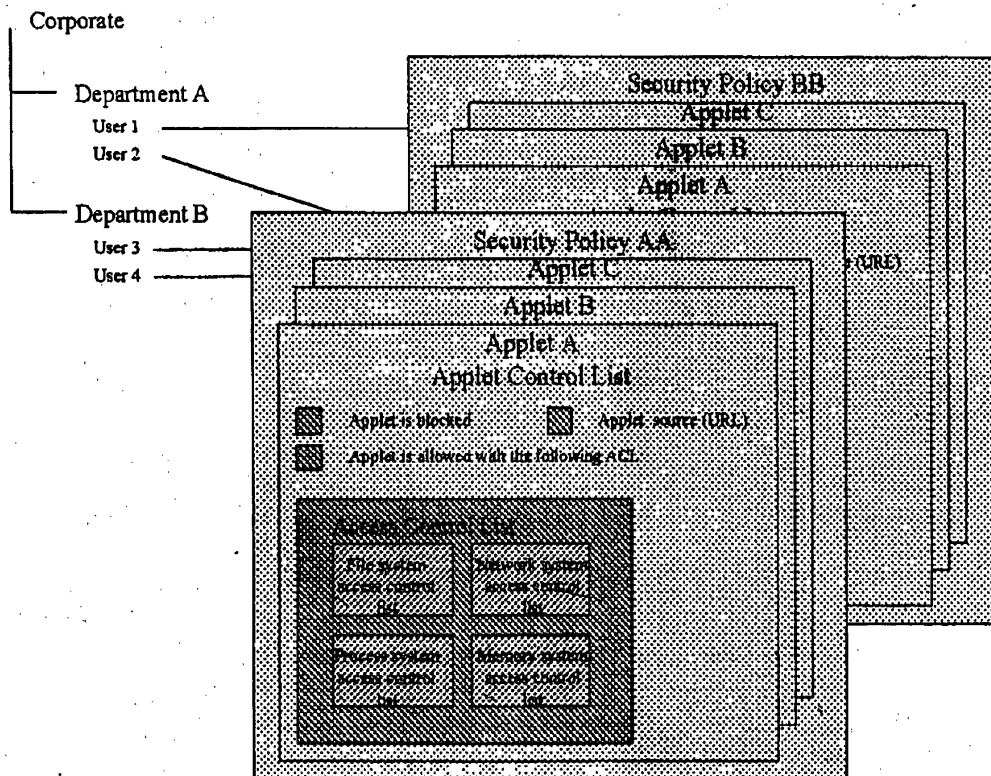
Security policy AA:

Similar as BB but:

Applet A can be loaded from source (URL) www.finjan.com only.

Applet B is completely blocked (unconditionally).

Applet C is hostile.



## ASP and Scanner

The following sample the process of scanning and the result - ASP:

1. An applet is getting as input into the scanner.
2. The scanner disassembly every machine code (for Java called "Bytecode") and decode its command.
3. Any command that is related to File System (for example - read or write file, list or delete directory, etc...) is decoded and is registered including its position (location) in the code, and all the input parameters for it. If the scanner can "resolve" the parameter ("understand its value") it will be registered too. For example a parameter to command read file will be the file name or descriptor. The scanner will go through the entire code to resolve such parameter that is not resolved. Only is case that it is impossible to be resolved (for example it is an input for run time from key board), it will be registered as "need to be resolved in run time. The scanner also track all the commands of network system (for example - connect to a computer, read socket etc..) and resolve their parameters too. Same for analyzing how much memory or elements or objects are allocated and registered this along with how many threads are allocated (process system).
4. Finding any "loop" command that may effect on any of the above command (from file system, network system etc...) or any conditional situation (if.. than... while... goto...).
5. All this traced command are registered in the ASP with the parameters, parameter status (resolved, yes/no).

6. Scanner can receive as parameters "rules" from a rule base that describe "logical" and heuristics and situations to be detected. Using this method the "behavior" of the scanner can be changed without changing its code. At any time after installing the scanner the user can add rules that may improve the scanning, for example: a rule of: if an applet try to connect to computer XXX at network location YYY and than it try to read file FFFF for reading - register this info in the ASP. Using this method any "suspicious" behavior may be traced and determine without recompiling the scanner.

ASP example:

ASP of Applet AAA

Applet ID (signature): xxx-xxxxxx-xxxx-xxxx  
 Applet source URL: www.gggg.xxx  
 Applet properties: xxx,ccc,vvv,bbbb  
 Applet originator: ERERERER corp. Inc.  
 Applet Version: yyyyyy  
 Applet date: mm-dd-yy

Applet list of operations:

File system:

operation	parameters	par status	par value	operation location in program
read file	c:\config.sys	resolved	c:\config.sys	class XX :method MM :line LL
write file	MY_File	not resolve	unknown	class XX :method MM :line L2

Network system:

operation	parameters	par status	par value	operation location in program
connect	www.finjan.com	resolved	www.finjan.com	class XX :method MM :line L3
connect	myserver	not resolved	unkown	class XX :method MM :line L5

Memory system:

operation	parameters	par status	par value	operation location in program
allocate	Object O	resolved	100bytes	class XX :method MM :line L6
allocate	Object R	in a loop	100 times 200 bytes	

Process System

operation	parameters	par status	par value	operation location in program
create thread	mythread	not resolved	unkown	class XX :method MM :line L1

## QUESTION LIST #2

### **Our understanding of the invention:**

- The first comparator bit-wise compares the received downloadable with known hostile and non-hostile Downloadables;
- If the received Downloadable is a known hostile Downloadable, then the first comparator replaces it with a safe substitute;
- If the received Downloadable is a known non-hostile Downloadable, then the first comparator passes the Downloadable and its previously-stored Downloadable Security Profile (DSP) data to the second comparator;
- If the received Downloadable is unknown, then the first comparator passes the Downloadable to the code scanner;
- The code scanner decomposes the Downloadable into DSP data, and passes the Downloadable and DSP data to the second comparator; and
- The second comparator compares the DSP data against security policies to determine if a security policy has been violated.

### **Questions:**

- Is the above understanding correct?
- If the understanding is correct, how is the example security policy consistent? That is,

----Shouldn't the public policies be subdivided only by command types and command restrictions? (For example, any Applet containing a command which allocates more than 250KB of RAM is deemed hostile, etc.).

----If the security policies examine commands of unknown Downloadables for security policy violations, then why does your example illustrate each security policy as subdivided by Applets (an Applet A, an Applet B and an Applet C).

1. Illustrate a "security policy" with a block diagram and a paragraph description.
2. An example applet or "downloadable" and a description of the decomposition of the applet into an ASP. Please be as detailed as possible in the description of the processing of the applet by the Scanner.



Answers to "Question List #2"

1. Yes, this is correct
2. Re your first example ("Shouldn't...").

---first example.

A public policy may be subdivided by command type and command restriction as in your example for memory and process system. But for File and Network system it may be subdivided by "rules" for example: Applet A can communicate with any server except server www.yoyo.com

Also, for the same example, you use the term "deemed hostile", but this is not necessary. Applet that is allocating more memory than defined, 250K, is not necessarily hostile. It is simply "not in accordance" with the security policy if the target user

---Second example

My example shows a situation in which the security policy "allow" to Applet A, B and C do different things as defined in the ACL of the specific Applet. These means that the permission for any other Applet is - cannot do anything. So, if unknown applet Y is getting on board, the ASP will specify what is attempt to do, and when it will be compared to the security Policy, it will be rejected since no mention exist that allow Applet Y do anything.

I hope this helps

Thx,  
Shlomo

60/030639

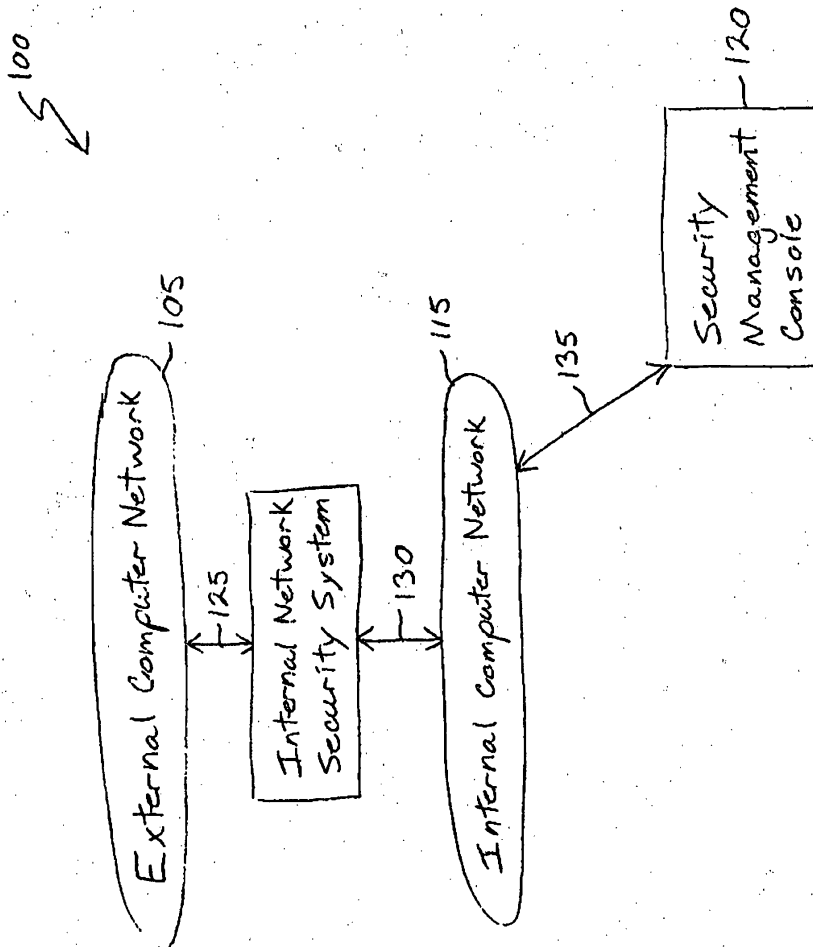
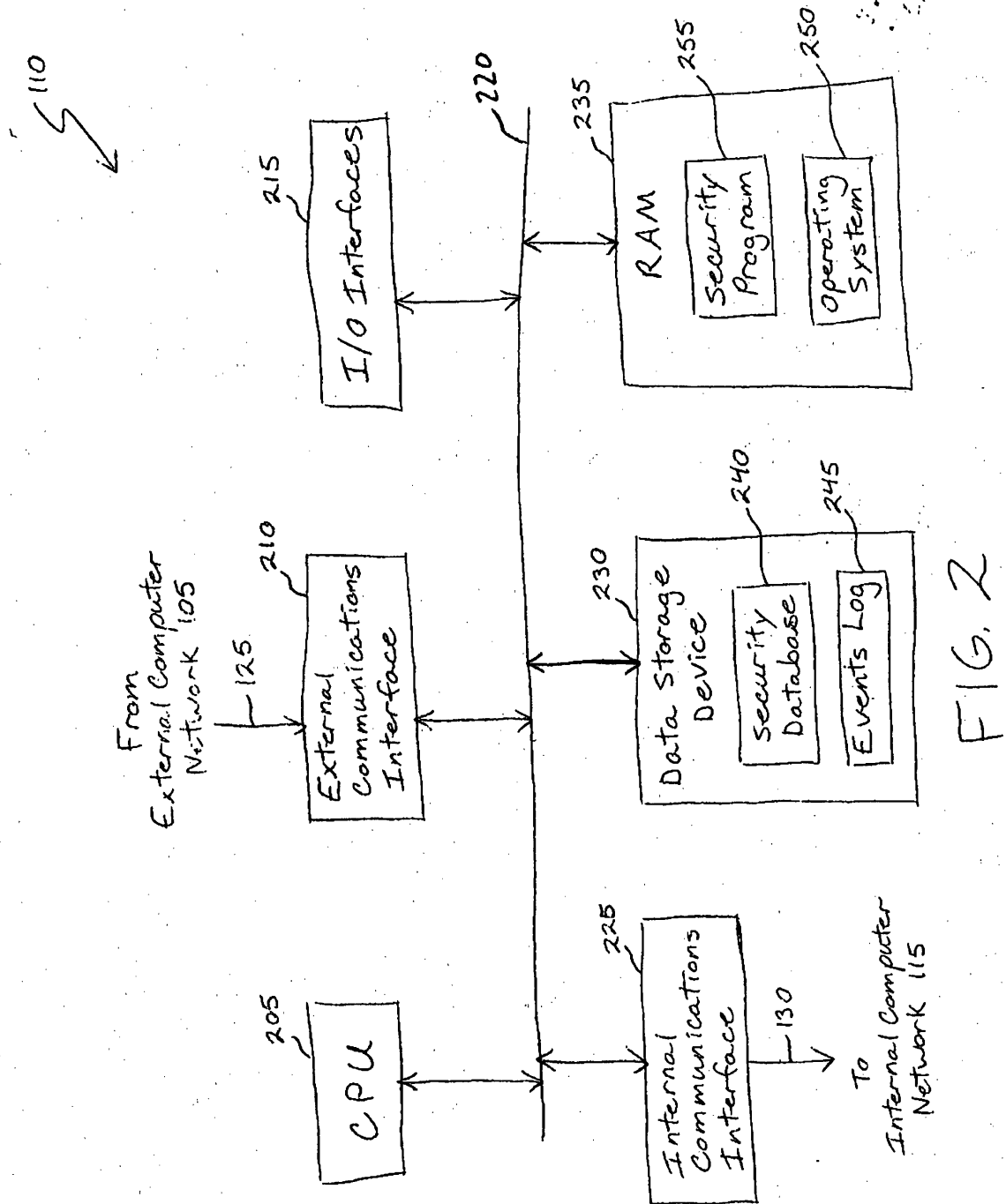


FIG. 1



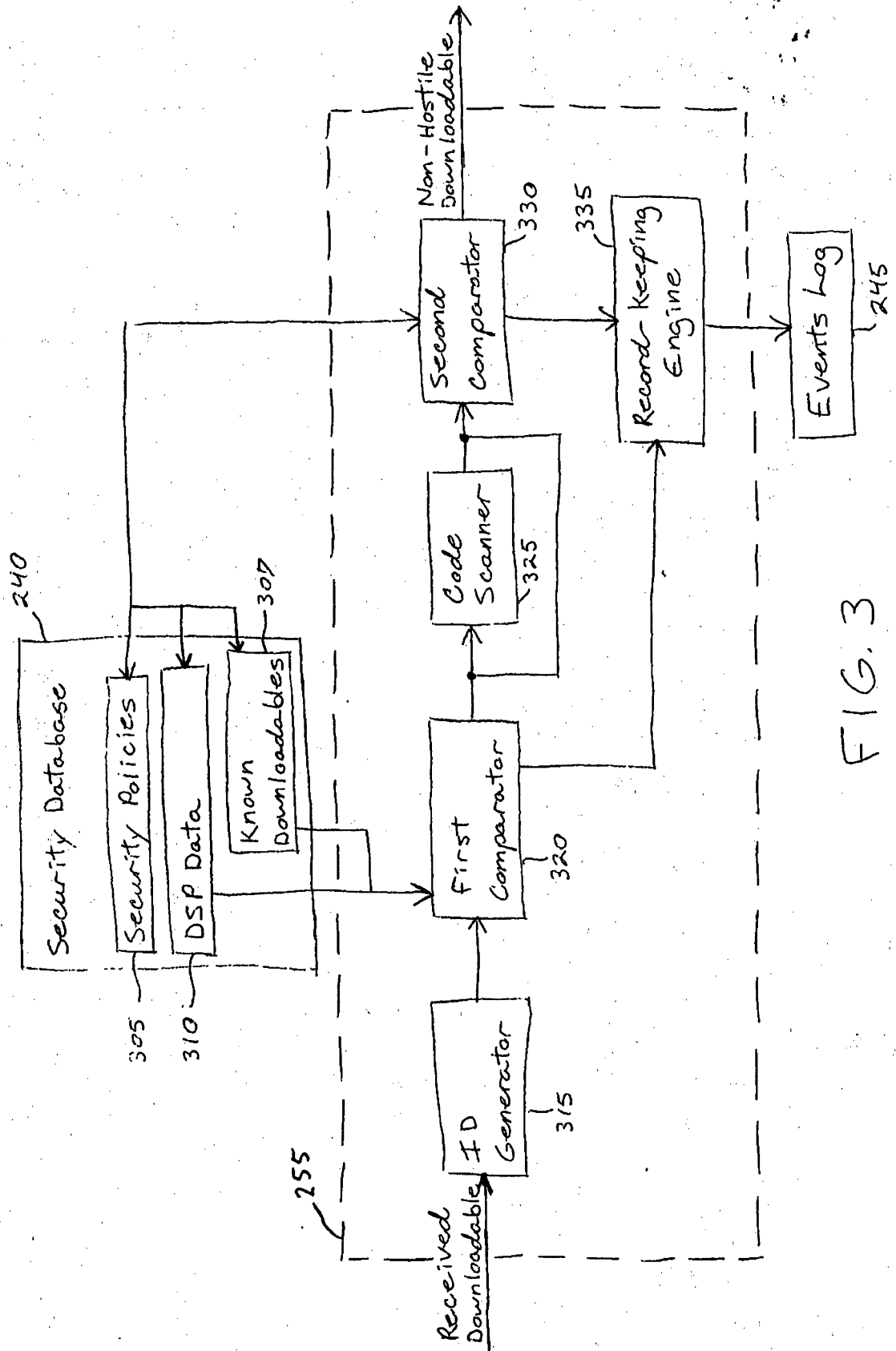


FIG. 3

60/030639

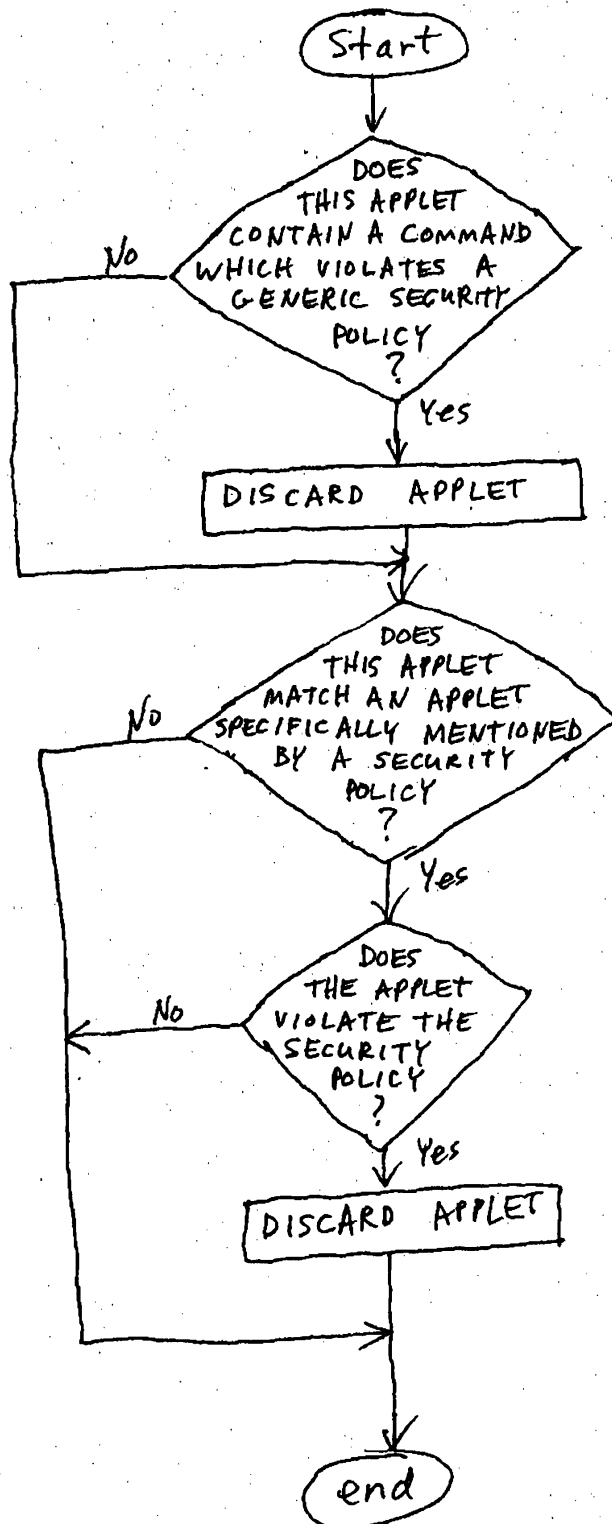


FIG. 4

60/030639



120

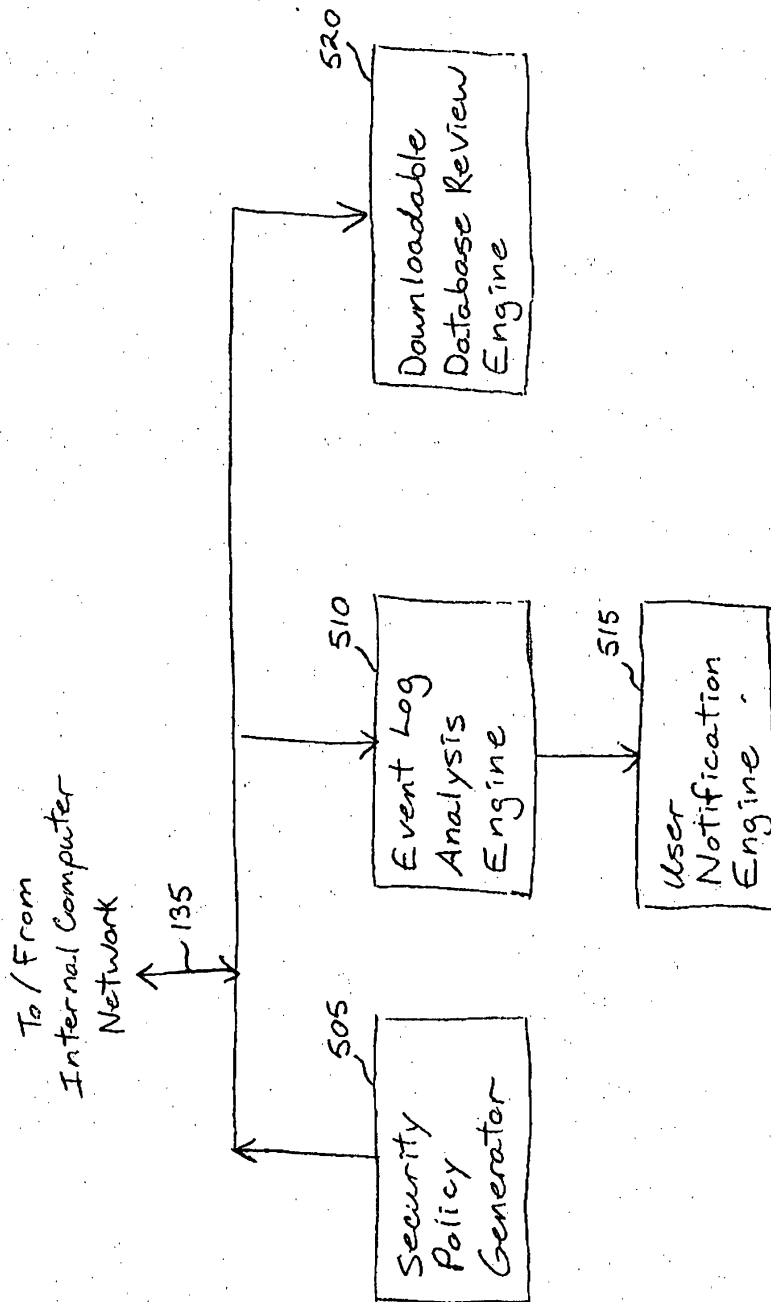


FIG. 5

60/030639

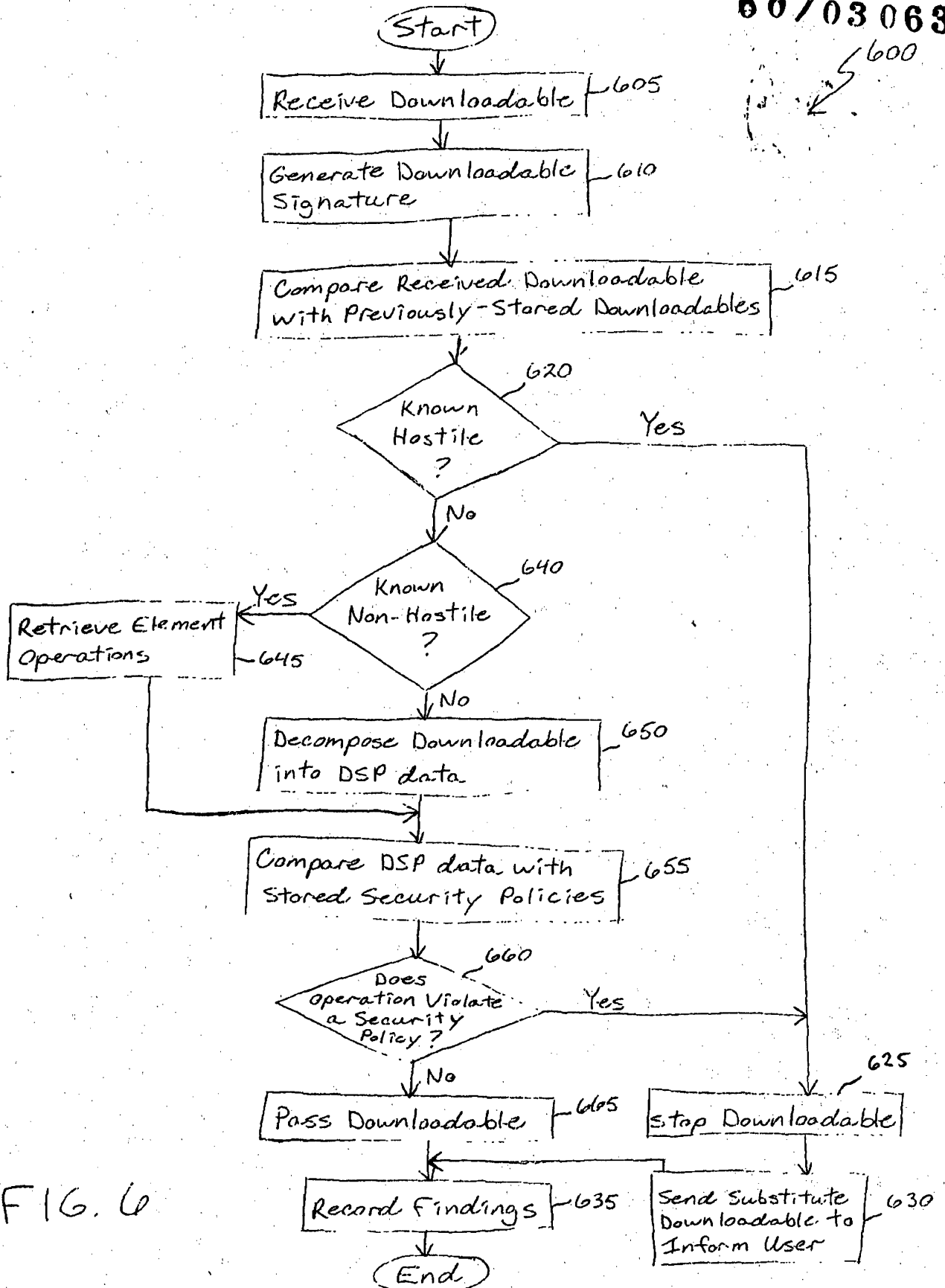


FIG. 6

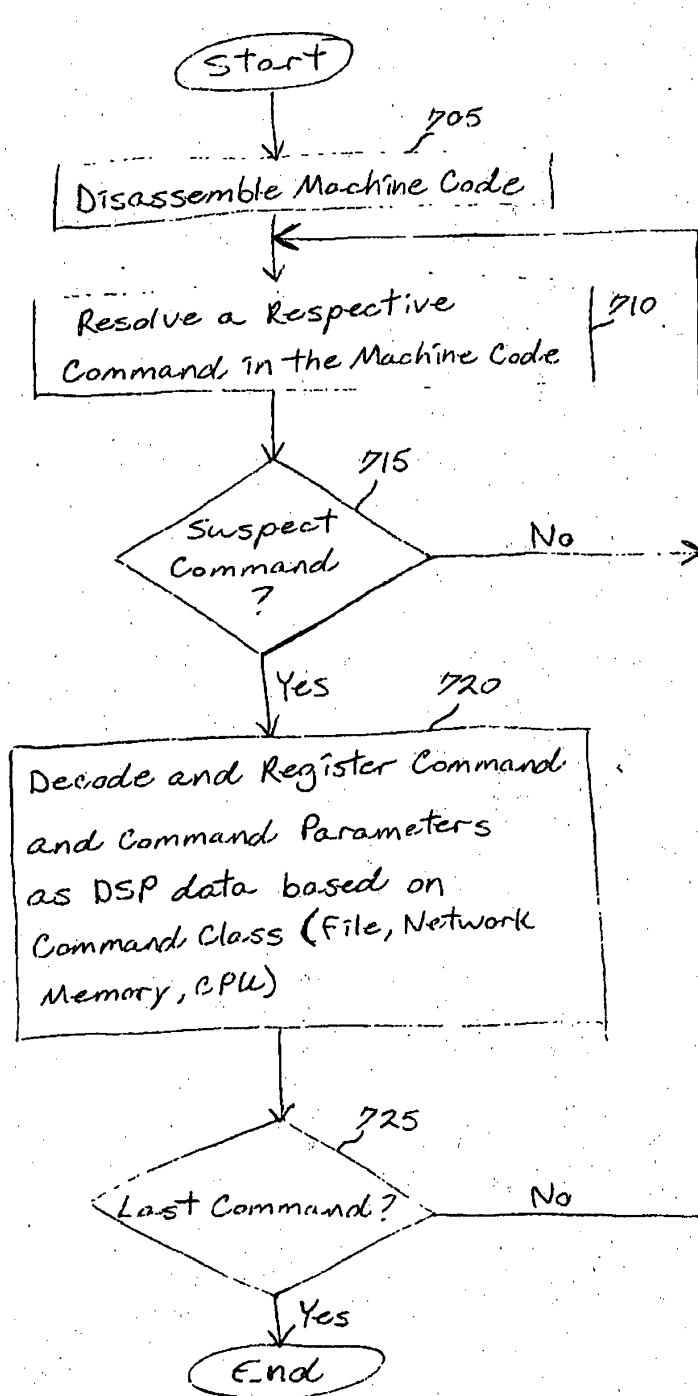


FIG. 7



REQUEST FOR ACCESS OF ABANDONED APPLICATION UNDER 37 CFR 1.14(a)

File Information Unit  
OCT 03 2001  
RECEIVED

In re Application of	
Application Number	Filed
601030439	NOV 8, 1996
Group Art Unit	Examiner

Paper No. 12

Assistant Commissioner for Patents  
Washington, DC 20231

I hereby request access under 37 CFR 1.14(a)(3)(iv) to the application file record of the above-identified ABANDONED application, which is: (CHECK ONE)

- ☐ (A) referred to in United States Patent Number 6016484 column \_\_\_\_\_
- ☐ (B) referred to in an application that is open to public inspection as set forth in 37 CFR 1.11, i.e., Application No. \_\_\_\_\_, filed \_\_\_\_\_, on page \_\_\_\_\_ of paper number \_\_\_\_\_
- ☐ (C) an application that claims the benefit of the filing date of an application that is open to public inspection, i.e., Application No. \_\_\_\_\_, filed \_\_\_\_\_, or
- ☐ (D) an application in which the applicant has filed an authorization to lay open the complete application to the public.

Please direct any correspondence concerning this request to the following address:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

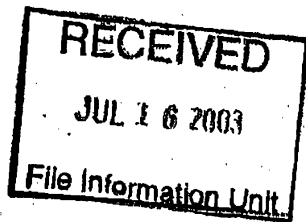
Darlene Jones  
Signature  
Darlene Jones  
Typed or printed name

10-3-01  
Date

FOR PTO USE ONLY	
Approved by: <u>FLY</u>	(Initials)
Unit: <u>F.I. 4</u>	

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. The time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Patent and Trademark Office, Washington, DC 20231.

REQUEST FOR ACCESS TO AN APPLICATION UNDER 37 CFR 1.14(e)



In re Application of	
Application Number <b>60/030,639</b>	Filed <b>11-8-96</b>
Art Unit	Examiner

Paper No. 3

Assistant Commissioner for Patents  
Washington, DC 20231

1. ☐ I hereby request access under 37 CFR 1.14(e)(2) to the application file record of the above-identified ABANDONED Application, which is not within the file jacket of a pending Continued Prosecution Application (CPA) (37 CFR 1.53(d)) and is: (CHECK ONE)

☐ (A) referred to in:

United States Patent Application Publication No. 6092,194, page \_\_\_\_\_, line \_\_\_\_\_,  
United States Patent Number \_\_\_\_\_, column \_\_\_\_\_, line \_\_\_\_\_, or  
an International Application which was filed on or after November 29, 2000 and which  
designates the United States, WIPO Pub. No. \_\_\_\_\_, page \_\_\_\_\_, line \_\_\_\_\_.

☐ (B) referred to in an application that is open to public inspection as set forth in 37 CFR 1.11(b) or  
1.14(e)(2)(i), i.e., Application No. \_\_\_\_\_, paper No. \_\_\_\_\_, page \_\_\_\_\_, line \_\_\_\_\_.

2. ☐ I hereby request access under 37 CFR 1.14(e)(1) to an application in which the applicant has filed an authorization to lay open the complete application to the public.

Selim McLaurin  
Signature  
Selim McLaurin  
Typed or printed name

7-16-03  
Date

FOR PTO USE ONLY	
Approved by	<u>[Signature]</u> (Initials)
Unit:	<u>FILE</u>

Burden Hour Statement: This form is estimated to take 0.1 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

REQUEST FOR ACCESS TO AN ABANDONED APPLICATION UNDER 37 CFR 1.14

Bring completed form to: File Information Unit Crystal Plaza Thres, Room 1D01 2021 South Clark Place Arlington, VA Telephone: (703) 308-2733	<b>RECEIVED</b>  SEP 24 2003  File Information Unit	In re Application of _____
		Application Number <u>60/030639</u> Filed <u>Nov 8, 1996</u>
		Paper No. <u>#4</u>

I hereby request access under 37 CFR 1.14(a)(1)(iv) to the application file record of the above-identified ABANDONED application, which is identified in, or to which a benefit is claimed, in the following document (as shown in the attachment):

United States Patent Application Publication No. \_\_\_\_\_, page, \_\_\_\_\_ line \_\_\_\_\_  
United States Patent Number 6167520 column \_\_\_\_\_, line, \_\_\_\_\_ or  
WIPO Pub. No. \_\_\_\_\_, page \_\_\_\_\_, line \_\_\_\_\_

**Related Information about Access to Pending Applications (37 CFR 1.14):**  
**Direct access to pending applications** is not available to the public but copies may be available and may be purchased from the Office of Public Records upon payment of the appropriate fee (37 CFR 1.19(b)), as follows:  
**For published applications that are still pending**, a member of the public may obtain a copy of:  
the file contents;  
the pending application as originally filed; or  
any document in the file of the pending application.  
**For unpublished applications that are still pending:**  
(1) If the benefit of the pending application is claimed under 35 U.S.C. 119(e), 120, 121, or 365 in another application that has: (a) issued as a U.S. patent, or (b) published as a statutory invention registration, a U.S. patent application publication, or an international patent application publication in accordance with PCT Article 21(2), a member of the public may obtain a copy of:  
the file contents;  
the pending application as originally filed; or  
any document in the file of the pending application.  
(2) If the application is incorporated by reference or otherwise identified in a U.S. patent, a statutory invention registration, a U.S. patent application publication, or an international patent application publication in accordance with PCT Article 21(2), a member of the public may obtain a copy of:  
the pending application as originally filed.

David Brown  
Signature  
DAVID BROWN  
Typed or printed name

9-24-03  
Date

Registration Number, if applicable  
7/418-2848  
Telephone Number

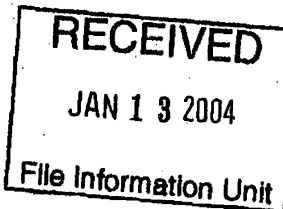
FOR PTO USE ONLY	
Approved by: <u>[Signature]</u> (initials)	Unit: <u>File Information Unit</u>

This collection of information is required by 37 CFR 1.14. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. BRING TO: File Information Unit, Crystal Plaza Thres, Room 1D01, 2021 South Clark Place, Arlington, VA.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

REQUEST FOR ACCESS TO AN ABANDONED APPLICATION UNDER 37 CFR 1.14

Bring completed form to:  
File Information Unit  
Crystal Plaza Three, Room 1D01  
2021 South Clark Place  
Arlington, VA  
Telephone: (703) 368-2733



App. Number: 60/030,639 11/08/96  
Page No. #5

I hereby request access under 37 CFR 1.14(a)(1)(iv) to the application file record of the above-identified ABANDONED application, which is identified in, or to which a benefit is claimed, in the following document (as shown in the attachment):

United States Patent Application Publication No. 6/67520 page \_\_\_\_\_ line \_\_\_\_\_

United States Patent Number \_\_\_\_\_ column \_\_\_\_\_ line \_\_\_\_\_ or

WIPO Pub. No. \_\_\_\_\_ page \_\_\_\_\_ line \_\_\_\_\_

Related Information about Access to Pending Applications (37 CFR 1.14):

Direct access to pending applications is not available to the public but copies may be available and may be purchased from the Office of Public Records upon payment of the appropriate fee (37 CFR 1.19(b)), as follows:

For published applications that are still pending, a member of the public may obtain a copy of:

- the file contents;
- the pending application as originally filed; or
- any document in the file of the pending application.

For unpublished applications that are still pending:

- (1) If the benefit of the pending application is claimed under 35 U.S.C. 119(e), 120, 121, or 365 in another application that has: (a) issued as a U.S. patent, or (b) published as a statutory invention registration, a U.S. patent application publication, or an international patent application publication in accordance with PCT Article 21(2), a member of the public may obtain a copy of:

- the file contents;
- the pending application as originally filed; or
- any document in the file of the pending application.

- (2) If the application is incorporated by reference or otherwise identified in a U.S. patent, a statutory invention registration, a U.S. patent application publication, or an international patent application publication in accordance with PCT Article 21(2), a member of the public may obtain a copy of:  
the pending application as originally filed.

Aziz Tesfay  
Signature  
Aziz Tesfay  
Typed or printed name

1/13/04  
Date

Registration Number, if applicable  
703-486-1150  
Telephone Number

FOR PTO USE ONLY	
Approved by:	<u>PAK</u>
Unit:	<u>File Information</u>

This collection of information is required by 37 CFR 1.14. The information is required to collect or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1480, Alexandria, VA 22313-1480. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. BRING TO: File Information Unit, Crystal Plaza Three, Room 1D01, 2021 South Clark Place, Arlington, VA.

If you need assistance in completing this form, call 1-800-PTO-9199 and select option 2

REQUEST FOR ACCESS TO AN ABANDONED APPLICATION UNDER 37 CFR 1.14

Bring completed form to:  
File Information Unit  
Crystal Plaza Three, Room 1D01  
2021 South Clark Place  
Arlington, VA  
Telephone: (703) 308-2733

In re Application of

Application Number

Filed

60/030,639 | 11/8/96

Paper No. 6

I hereby request access under 37 CFR 1.14(a)(1)(iv) to the application file record of the above-identified ABANDONED application, which is identified in, or to which a benefit is claimed, in the following document (as shown in the attachment):

United States Patent Application Publication No. \_\_\_\_\_, page, \_\_\_\_\_ line \_\_\_\_\_.

United States Patent Number 6092194, column Four, line, \_\_\_\_\_ or

WIPO Pub. No. \_\_\_\_\_, page \_\_\_\_\_, line \_\_\_\_\_.

Related Information about Access to Pending Applications (37 CFR 1.14):

Direct access to pending applications is not available to the public but copies may be available and may be purchased from the Office of Public Records upon payment of the appropriate fee (37 CFR 1.19(b)), as follows:

For published applications that are still pending, a member of the public may obtain a copy of:

- the file contents;
- the pending application as originally filed; or
- any document in the file of the pending application.

For unpublished applications that are still pending:

- (1) If the benefit of the pending application is claimed under 35 U.S.C. 119(e), 120, 121, or 365 in another application that has: (a) issued as a U.S. patent, or (b) published as a statutory invention registration, a U.S. patent application publication, or an international patent application publication in accordance with PCT Article 21(2), a member of the public may obtain a copy of:
  - the file contents;
  - the pending application as originally filed; or
  - any document in the file of the pending application.
- (2) If the application is incorporated by reference or otherwise identified in a U.S. patent, a statutory invention registration, a U.S. patent application publication, or an international patent application publication in accordance with PCT Article 21(2), a member of the public may obtain a copy of:
  - the pending application as originally filed.

Michael D. Winter  
Signature  
Michael D. Winter  
Typed or printed name

Registration Number, if applicable

205-625 3312

Telephone Number

3/25/05

Date

RECEIVED

FOR PTO USE ONLY

MAR 25 2005

Approved by:

File Information Unit

Unit:

This collection of information is required by 37 CFR 1.14. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. BRING TO: File Information Unit, Crystal Plaza Three, Room 1D01, 2021 South Clark Place, Arlington, VA.

REQUEST FOR ACCESS TO AN ABANDONED APPLICATION UNDER 37 CFR 1.14

Bring completed form to:  
File Information Unit  
Crystal Plaza Three, Room 1001  
2021 South Clark Place  
Arlington, VA  
Telephone: (703) 303-2733

**RECEIVED**  
JUN 12 2006  
File Information Unit

In re Application of \_\_\_\_\_  
Application Number: 60/030639 File # 11/8/96  
Paper No. 118

I hereby request access under 37 CFR 1.14(a)(1)(iv) to the application file record of the above-identified ABANDONED application, which is identified in, or to which a benefit is claimed, in the following document (as shown in the attachment):

United States Patent Application Publication No. \_\_\_\_\_, page, \_\_\_\_\_ line \_\_\_\_\_  
United States Patent Number 6167520, column \_\_\_\_\_, line, \_\_\_\_\_ or  
WIPO Pub. No. \_\_\_\_\_, page \_\_\_\_\_, line \_\_\_\_\_

**Related Information about Access to Pending Applications (37 CFR 1.14):**  
Direct access to pending applications is not available to the public but copies may be available and may be purchased from the Office of Public Records upon payment of the appropriate fee (37 CFR 1.19(b)), as follows:  
For published applications that are still pending, a member of the public may obtain a copy of:  
the file contents;  
the pending application as originally filed; or  
any document in the file of the pending application.  
For unpublished applications that are still pending:  
(1) If the benefit of the pending application is claimed under 35 U.S.C. 119(e), 120, 121, or 365 in another application that has: (a) issued as a U.S. patent, or (b) published as a statutory invention registration, a U.S. patent application publication, or an international patent application publication in accordance with PCT Article 21(2), a member of the public may obtain a copy of:  
the file contents;  
the pending application as originally filed; or  
any document in the file of the pending application.  
(2) If the application is incorporated by reference or otherwise identified in a U.S. patent, a statutory invention registration, a U.S. patent application publication, or an international patent application publication in accordance with PCT Article 21(2), a member of the public may obtain a copy of:  
the pending application as originally filed.

Donna L. Wyatt  
Signature  
DONNA WYATT  
Typed or printed name  
\_\_\_\_\_  
Registration Number, if applicable  
\_\_\_\_\_  
Telephone Number

6/12/06  
Date

FOR PTO USE ONLY  
**RECEIVED**  
(initials)  
JUN 12 2006  
File Information Unit

This collection of information is required by 37 CFR 1.14. The information is required to obtain or retain a benefit by the public who wish to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. BRING TO: File Information Unit, Crystal Plaza Three, Room 1001, 2021 South Clark Place, Arlington, VA.

# REQUEST FOR ACCESS TO AN ABANDONED APPLICATION UNDER 37 CFR 1.14

Bring completed form to:

File Information Unit, Room 2E04,  
 2900 Crystal Drive  
 Arlington, VA 22202-3514

Telephone: (703) 952-2338

In re Application of \_\_\_\_\_

Application Number

60/050639

Filed

11/08/96

Paper No. 29

I hereby request access under 37 CFR 1.14(a)(1)(iv) to the application file record of the above-identified ABANDONED application, which is not within the file jacket of a pending Continued Prosecution Application (CPA) (37 CFR 1.53(d)) and which is identified in, or to which a benefit is claimed, in the following document (as shown in the attachment):

United States Patent Application Publication No. \_\_\_\_\_, page, \_\_\_\_\_ line \_\_\_\_\_

United States Patent Number 6804700, column \_\_\_\_\_, line, \_\_\_\_\_ or

WIPO Pub. No. \_\_\_\_\_, page \_\_\_\_\_, line \_\_\_\_\_

## Related Information About Access to Applications Maintained in the Image File Wrapper System (IFW) and Access to Pending Applications in General

A member of the public, acting without a power to inspect, cannot order applications maintained in the IFW system through the FIU. If the member of the public is entitled to a copy of the application file, then the file is made available through the Public Patent Application Information Retrieval system (Public PAIR) on the USPTO Internet web site (www.uspto.gov). Terminals that allow access to Public PAIR are available in the Public Search Room. The member of the public may also be entitled to obtain a copy of all or part of the application file upon payment of the appropriate fee. Such copies must be purchased through the Office of Public Records upon payment of the appropriate fee (37 CFR 1.19(b)).

For published applications that are still pending, a member of the public may obtain a copy of: the file contents; the pending application as originally filed; or any document in the file of the pending application.

For unpublished applications that are still pending:

- (1) If the benefit of the pending application is claimed under 35 U.S.C. 119(e), 120, 121, or 365 in another application that has: (a) issued as a U.S. patent, or (b) published as a statutory invention registration, a U.S. patent application publication, or an international patent application publication in accordance with PCT Article 21(2), a member of the public may obtain a copy of: the file contents; the pending application as originally filed; or any document in the file of the pending application.
- (2) If the application is incorporated by reference or otherwise identified in a U.S. patent, a statutory invention registration, a U.S. patent application publication, or an international patent application publication in accordance with PCT Article 21(2), a member of the public may obtain a copy of the pending application as originally filed.

Nguyen Ngyam

Signature

Nguyen Ngyam

Typed or printed name

Registration Number, if applicable

(703) 916-1500

Telephone Number

09/20/06

Date

FOR PTO USE ONLY

Approved by:

SEP 28 2006

Unit:

File Information Unit

This collection of information is required by 37 CFR 1.11 and 1.14. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS BRING TO: File Information Unit, Room 2E04, 2900 Crystal Drive, Arlington, Virginia.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2

PAGE DATA ENTRY CODING SHEET

U.S. DEPARTMENT OF COMMERCE  
Patent and Trademark Office

1ST EXAMINER *J. H. [Signature]* DATE *12/16/96*  
2ND EXAMINER \_\_\_\_\_ DATE \_\_\_\_\_

APPLICATION NUMBER

60/030639

TYPE APPL

9

FILING DATE  
MONTH DAY YEAR

11 08 96

SPECIAL HANDLING

0

GROUP ART UNIT

\_\_\_\_

CLASS

\_\_\_\_

SHEETS OF DRAWING

- 17

TOTAL CLAIMS

\_\_\_\_

INDEPENDENT CLAIMS

\_\_\_\_

SMALL ENTITY?

0

FILING FEE

150

FOREIGN LICENSE

Y

ATTORNEY DOCKET NUMBER

0-558

CONTINUITY DATA

CONT STATUS CODE

\_\_\_\_

PARENT APPLICATION SERIAL NUMBER

\_\_\_\_

PCT APPLICATION SERIAL NUMBER

P C T / / /  
P C T / / /  
P C T / / /  
P C T / / /  
P C T / / /

PARENT PATENT NUMBER

\_\_\_\_

PARENT FILING DATE

\_\_\_\_

PCT/FOREIGN APPLICATION DATA

FOREIGN PRIORITY CLAIMED

\_\_\_\_

COUNTRY CODE

\_\_\_\_

PCT/FOREIGN APPLICATION SERIAL NUMBER

\_\_\_\_

FOREIGN FILING DATE  
MONTH DAY YEAR

\_\_\_\_