

Patently Obvious™

...powered by



Intellectual Property Analysis of Symantec's Virus Definition Update Technology U.S. Patents Nos. 6,052,531 & 6,167,407 May 25, 2001

Background

On February 7, 2001, Symantec Corporation (Nasdaq: SYMC) announced that it had secured two United States Patents for its automated virus definition update technology. This technology is a key component of Symantec's Norton AntiVirus™ software suite.

According to market research by IDC, sales of anti-virus and other computer security software are expected to reach \$5 billion annually by the year 2003.¹ This rise in demand for these products can be attributed to the increased amount and sophistication of newly released computer viruses. As more businesses rely on computer systems for mission critical operations, such protection continues to increase in importance.

Symantec enjoys a large share of the anti-virus and computer security software market. Its chief competitors include Computer Associates, F-Secure, Network Associates, Parsons Technology, and Trend Micro. Symantec's U.S. Patents Nos. 6,052,531 and 6,167,407 (hereinafter '531 and '407, respectively) claim important innovations used to automatically update an anti-virus program's virus definition files. This functionality is a vital component of most modern releases of anti-virus software, including Network Associate's McAfee VirusScan, as it provides a mechanism to protect computers soon after a new virus is discovered.

M-CAM has conducted an intellectual property analysis of Symantec's '531 and '407 patents to determine their strength and defensibility in the face of prior and concurrent art innovations. Using M-CAM DOORS™, the innovation space surrounding the '531 and '407 patents was examined to identify patent claims that may show weaknesses in Symantec's patents.

Patents Under Consideration (in order of filing)

Assignee	U.S. Patent	Title	Filed	Issued	Expires
General Electric	3,396,723	On-line modification of computer programs	7/3/74	7/13/76	1993
Xerox	4,558,413	Software version management system	11/21/83	12/10/85	2003
IBM	4,714,992	Communication for version management in a distributed information service	11/26/85	12/22/87	2005
Network Associates	6,151,643	Automatic updating of diverse software products on multiple client computer systems by downloading scanning application to client computer and generating software list on client computer	6/7/96	11/21/00	2016
Neuromedical Systems	5,948,104	System and method for automated anti-viral file update	5/23/97	9/7/99	2017
Trend Micro	6,119,165	Controlled distribution of application programs in a computer network	11/17/97	9/12/00	2017
Network Associates	6,035,423	Method and system for providing automated updating and upgrading of antivirus applications using a computer network	12/31/97	3/7/00	2017
Symantec	6,052,531	Multi-tiered incremental software updating	3/25/98	4/18/00	2018
Symantec	6,167,407	Backtracked incremental updating	6/3/98	12/26/00	2018

¹ Symantec's 2000 Annual Report.

Intellectual Property Analysis

Technology in '531 and '407

The two Symantec patents, '531 and '407, claim (among other things) a software system on a computer to query a centralized source (i.e., a server) to check for any updates to the software package. If an update is located, the software system then retrieves any necessary files and updates the software system accordingly. These updates can be scheduled to run automatically by the client machine (personal computer, workstation, or server). The language of the claims is deliberately broad, as to include as much "landscape" as possible. However, the intended use for these patents, as shown in Symantec's Norton AntiVirus™ products, is for the automatic updates of virus definition files and related system files in an anti-virus software system.

A look at the important independent claims in the '531 and '407 patents will help illustrate the primary innovation(s) asserted by Symantec. Some of the more integral claims language is shown in **bold**.

<i>Excerpts of claims 1 and 15 from Symantec's '531 patent</i>	<i>Excerpts of claims 1 and 8 from Symantec's '407 patent</i>
<p>1. A system for transforming a computer readable file of a beginning state to a computer readable file of an ending state, where the beginning state and the ending state are both states within a sequence of states associated with the computer readable file, the system comprising:...</p> <p>at least one update data source, each update data source having access to at least one of the update patches, each update data source being disposed to receive a request which is associated with one of the update patches, for transmitting the update patch associated with the request; and</p> <p>a client coupled to each update data source and having access to the computer readable file, disposed to receive transmitted update patches from each update data source, for determining a sequential set of update patches which specify information for transforming the computer readable file from the beginning state to the ending state.</p> <p>15. A computer implemented method for transforming a computer readable file of a beginning state to a computer readable file of an ending state using available update patches, the beginning state and the ending state both being states within a sequence of states associated with the computer readable file, each update patch having a first state and a second state associated therewith, the first state of each update patch preceding in the sequence of states the second state of that update patch, and each update patch specifying information about differences between the first state and the second state associated with that update patch, the computer implemented method comprising the steps of:</p> <p>determining a sequential set of update patches from those available such that the first state associated with the initial update patch in the sequential set of update patches ...</p> <p>requesting each update patch in the sequential set of update patches from at least one update data source, wherein each update data source has access to at least one of the available update patches, and is disposed to receive the request and transmit the requested update patch;</p> <p>receiving each requested update patch in the sequential set of update patches from at least one update data source; and</p> <p>producing a computer readable file of the ending state by using each update patch in the sequential set of update patches to transform the computer readable file from the first state associated with the update patch to the second state associated with the update patch.</p>	<p>1. A method for facilitating updating of a computer readable file to a final state, the final state being a state within an ordered sequence of states associated with the file, the sequence including at least one hub state, the method comprising the steps of:</p> <p>determining as a final hub state a hub state which is at least as early in the sequence as the final state; for each hub state which is earlier in the sequence than the final hub state, making available a hub incremental update containing information about differences between that hub state and the final hub state; and responsive to the final hub state not being the final state, making available a final incremental update containing information about differences between the final hub state and the final state.</p> <p>8. A method for updating a computer readable file of an original state to a final state, the file of the original state residing on a local computer system, the original state and the final state being states within an ordered sequence of states associated with the file, the final state being later in the sequence than the original state, and the sequence including a final hub state which is not preceded in the sequence by the final state, the method comprising the steps of:</p> <p>accessing from a local storage location a file of an original hub state, the original hub state being a hub state in the sequence which is not preceded in the sequence by the original state;</p> <p>responsive to the original hub state not being the final hub state:</p> <p>accessing a hub incremental update containing information about differences between the original hub state and the final hub state;</p> <p>using the hub incremental update and the file of the original hub state to produce a file of the final hub state; and</p> <p>storing the file of the final hub state; and</p> <p>responsive to the final hub state not being the final state:</p> <p>accessing a final incremental update containing information about differences between the final hub state and the final state;</p> <p>using the final incremental update and the file of the final hub state to produce a file of the final state; and storing the file of the final state.</p>

A Look at Uncited Prior Art

Using M-CAM DOORS™, several examples of uncited prior art were identified that may limit the strength and breadth of the '531 and '407 patent claims. Excerpts from patents held by General Electric, Xerox and IBM are provided to illustrate the similarities in innovation in this technology space. Interestingly, the '407 patent only cited four patents from the hundreds of patents involving automated software updates. Key similarities are shown in **bold**.

<p><i>Excerpt of claims from General Electric's U.S. Patent No. 3,969,723</i></p>	<p><i>Excerpt of claims from Xerox's U.S. Patent No. 4,558,413,</i></p>	<p><i>Excerpt of claims from IBM's U.S. Patent No. 4,714,992</i></p>
<p>1. In a controlled equipment system of the type operable in response to signals resulting from logical operations based upon operating parameters of the controlled equipment, a control system comprising:</p> <p>a. a programmable controller including a store having stored therein an executive program serving to,</p> <p>1. direct on-line communication between said controller and equipment external thereto, and</p> <p>2. simulate an equipment control circuit having a format comprised of a plurality of logic strings, each logic string comprised of a conductor including at least one switch element disposed in a designated position and a continuity status means controlled by the condition of the switch elements of its associated logic string, said continuity status means serving to effect output signals from said controller to the equipment external thereto; and,</p> <p>b. a programming console in communication with said controller comprising:</p> <p>1. means for specifying to said controller a one of the simulated logic strings to be modified,</p> <p>2. means for directing said controller to copy the simulated specified logic string into a predetermined region in said store while retaining the specified logic string in the executive program,</p> <p>3. means for specifying to said controller a position in the conductor of the logic string copied,</p> <p>4. means for modifying the copied logic string by specifying to said controller a type of switch element,</p> <p>5. means for directing said controller to test the modified logic string on-line as a part of the executive program in place of the retained specified logic string, and</p> <p>6. means for directing said controller to replace the retained specified logic string with the modified logic string while maintaining the modified logic string on-line whereby the modified logic string becomes an integral part of the executive program to control the external equipment in accordance with the logic now defined by the modified logic string.</p>	<p>1. A software version management system for automatically collecting and recompiling updated versions of component software objects comprising a software program for operation on a plurality of personal computers coupled together in a distributed software environment via a local area network and wherein said objects include the source and binary files for various of said software program and are stored in various different local and remote storage means through said environment, said component software objects being periodically updated via environment editing means by various users at said personal computers and stored in designated storage means, said system including:</p> <p>models comprising system objects, each of said models representative of the source versions of a particular component software object, each of said models containing object pointers including a unique name of the object, a unique identifier descriptive of the chronological updating of its current version, information as to an object's dependencies on other objects and a pathname representative of the residence storage means of the object,</p> <p>means in said editing means to notify said management system when any one of said objects is being edited by a user,</p> <p>means in said management system in response to notification of object editing to track said edited objects and alter their respective models to the current version thereof,</p> <p>said management system upon command adapted to retrieve and recompile said source files corresponding to said altered models and load the binary files of said altered component software objects and their dependent objects into said computers.</p>	<p>1. A method for managing obsolescence of replicas of data objects, the objects being utilized in multiple nodes of a distributed processing system in which at least one node operates as an object source location having access to a source database containing source data objects and a least one other node operates as an object replica location having means for storing replicas of requested objects received from a source location, each source data object being alterable whereby replicas of altered objects stored at replica locations may become obsolete, comprising the steps of:</p> <p>responsive to a request from a first replica location to ascertain obsolescence of data objects, extracting at the source location identifiers of a set of obsolete objects;</p> <p>communicating said identifiers, if any, as an atomic demand/response transaction to said first replica location;</p> <p>rendering inaccessible at said first replica location any replicas corresponding to those identifiers received from the source location; and</p> <p>removing from the source location those identifiers communicated to said first replica location.</p> <p>3. A method for locating and rendering inaccessible obsolete versions of data objects, the objects being utilized in multiple nodes of a distributed processing system in which at least one node operates as an object source location having access to a source database containing source data objects and at least one other node operates as an object replica location having means for storing versions of requested objects received from a source location, each source data object being alterable whereby a plurality of versions are created and versions stored at replica locations may become obsolete, the relative obsolescence of each version at any time t being identifiable by a version number corresponding to its position in a temporal sequence, including an oldest version and a most recent version, among versions of source data objects comprising the steps at each source location of..</p>

Intellectual Property Analysis (contd.)

Technology Competitors

In addition to the aforementioned patents, a total of 660 other patents were identified by M-CAM DOORS™ to be closely related to the '531 and '407 patents. As shown in Figure 1, IBM Corporation is an important player in the field of anti-virus and computer security software, holding nearly fourteen percent of all patents in this innovation space.

While Network Associates holds over 15 U.S. Patents, these patents generally occupy a different innovation space as compared to the '531 and '407 patents. Regardless, Network Associates is clearly a competitor in the industry. Another of Symantec competitors, Micro Trend, holds 8 U.S. Patents.

Of particular interest are Network Associates' U.S. Patents Nos. 6,035,423 ('423) and 6,151,643 ('643) and Trend Micro's U.S. Patent No. 6,119,165 ('165). These related patents were being examined in the USPTO at the same time as '531 and '407.

Figure 1- Companies and their Patent Holdings in the Innovation Space of Symantec's U.S. Patents 6,052,531 and 6,167,407

Company	Related Patents Assigned	Percent of Total
IBM	92	13.9
Sun Microsystems	26	3.9
Microsoft	21	3.2
Hewlett-Packard	20	3.0
Hitachi	20	3.0
Digital Equipment Corp	19	2.9
Motorola	17	2.6
Kabushiki Kaisha Toshiba	11	1.6
LSI Logic Corporation	11	1.6
Advanced Micro Devices	8	1.2
All Others	415	62.9
TOTAL	660	

Financial Information Through March 2000

Symantec (Nasdaq: SYMC), www.symantec.com			
	2000	1999	1998
Revenue	\$745.7 Million	\$633.9 Million	\$578.4 Million
Net Income (loss)	\$170.1 Million	\$50.2 Million	\$85.1 Million
EPS (diluted)	2.73	0.86	1.42

Intellectual Property Analysis (contd.)

Concurrent Art

Another important consideration of the innovation space is the quality and thoroughness of the original patent examination. Figure 3 lists the USPTO Classification Codes and the corresponding number of patents included in the '531 and '407 innovation space.

A total of 660 patents in the innovation space were filed before the '531 and '407 patents. The '531 patent's original field of search included USPTO Classifications 707, 395, and 712. The '407 patent's original field of search included USPTO classifications 707, 710, 345, and 360. These six classifications account for nearly 50 percent of all patents in this innovation space – a good indicator of patent examination strength. However, the field of search failed to capture other important classifications such as *Class 364 – Electrical Computers and Data Processing*, that are closely related to the technology in the '531 and '407 patents.

Figure 3- Top USPTO Classification Codes Represented in the M•CAM DOORS™ Innovation Space of Symantec's '531 and '407 Patents

Code	Description	Number of Patents	Percent of Total
395	INFORMATION PROCESSING SYSTEM ORGANIZATION	271	41.1
364	ELECTRICAL COMPUTERS AND DATA PROCESSING	112	17.0
709	ELECTRICAL COMPUTERS AND DIGITAL PROCESSING SYSTEMS: MULTIPLE COMPUTER OR PROCESS COORDINATING	35	5.3
379	TELEPHONIC COMMUNICATIONS	33	5.0
707	DATA PROCESSING: DATABASE AND FILE MANAGEMENT, DATA STRUCTURES, OR DOCUMENT PROCESSING	32	4.8
342	COMMUNICATIONS: DIRECTIVE RADIO WAVE SYSTEMS AND DEVICES (E.G., RADAR, RADIO NAVIGATION)	22	3.3
455	TELECOMMUNICATIONS	17	2.6
	All Others	138	20.9
	TOTAL	660	

(Note: Original U.S. Class codes are used.)

M•CAM's intellectual property analysis has identified four examples of concurrent art that may limit the strength and defensibility of '531 and '407. In addition to Network Associate's '643 and '423 and Trend Micros' '165 patents, Neuromedical System's U.S. Patent 5,948,104 (System and method for automated anti-viral file update) is an important consideration. Excerpts of the claims of these four patents are provided below. Key claim language is indicated in **bold**.

<i>Excerpt of claims from Neuromedical System's U.S. Patent No. 5,948,104</i>	<i>Excerpt of claims from Network Associates' U.S. Patent No. 6,151,643</i>	<i>Excerpt of claims from Network Associate's U.S. Patent No.6,035,423</i>	<i>Excerpt of claims from Trend Micro's U.S. Patent No. 6,119,165</i>
<p>1. A method for updating virus signature files of a computer system comprising the steps of: storing first and second update data on a portable storage medium to be installed to the computer system, the first update data including virus signature updating data, the second data including data that is regularly delivered to the computer system; installing the second update data to the computer system; and prompting a user of the computer system to decide whether or not to update the virus signature files with the first data.</p> <p>11. A method for updating virus signature files of a computer system comprising the steps of: storing first and second update data on a portable storage medium to be installed to the computer system, the first update data including virus signature updating data, the second data including data that is regularly delivered to the computer system; installing the second update data to the computer system; and displaying to the user a first target drive and directory where the virus signature files are stored.</p>	<p>1. A computer-implemented method of providing information for software residing on a client computer, comprising: maintaining a service provider computer on a network, the client computer accessible over the network by the service provider computer; maintaining on the service provider computer a database, the database containing references to network locations where information relating to software from a plurality of software vendors can be obtained; maintaining on the service provider computer a downloadable application, the application being capable of performing a scan of the client computer to identify one or more software products residing on the client computer; establishing a communication link between client computer and the service provider computer over the network; downloading the application to the client computer over the communication link; scanning the client computer with the application; as a result of the scan, generating a list of software residing on the client computer for which the service provider has information; and for at least one product on the list, downloading to the client computer at least a portion of the information for that product that is available to the service provider.</p>	<p>1. A method for providing updated antivirus files to a plurality of client computers on a local area network, the client computers being supported by a common service computer on the local area network, the common service computer being operated by a system administrator, the method for providing allowing for minimal affirmative involvement by the system administrator in updating antivirus files on the plurality of client computers, the method for providing comprising the steps of: installing the updated antivirus files on a central antivirus server, said central antivirus server comprising: an antivirus database, said antivirus database comprising... a second field for storing the identity of the last updated antivirus file received by each of said plurality of computers on the local area network; transmitting the updated antivirus files from said central antivirus server to a push administration computer connected to the Internet... executing an automatic installation script at said service computer for automatically installing updated antivirus information on said plurality of client computers across the local area network; wherein said transmitting steps include... transmitting a first query from said push administration computer to said central antivirus server, said first query requesting an identity of updated antivirus files appropriate for the service computer; transmitting a first response from said central antivirus computer to said push administration computer identifying said appropriate updated antivirus files; and transmitting said appropriate updated antivirus files from said push administration computer to said service computer.</p>	<p>1. In a computer network including a remote server, an agent, and a client, a method comprising the steps of: the client attempting to connect to the remote server through the agent; the agent determining a characteristic of the client and providing a code module in response to the determined characteristic; the agent downloading the code module to the client, resulting in the code module residing at the client; the client executing the code module; the agent forming a connection to the remote server on behalf of the client; and the code module reporting to the client a status of an operation performed by the agent, the operation relating to the connection formed between the agent and the remote server.</p>

Armed with greater detail on the innovation space surrounding the '531 and '407 patents, M•CAM focused on those patents most likely to present claims that would limit the strength and defensibility of these patents. Only after comparing the '531 and '407 patent claims with those of several closely related prior art documents, including but not limited to patents, can one make an informed opinion of the '531 and '407 patents. The results of this analysis have identified a group of patents that effectively “crowd” the innovation space of the '531 and '407 patents with closely related innovations in software version management and updating. This fact, coupled with the shortness of the innovation cycle in this industry, may limit Symantec’s ability to effectively extract licensing revenue for these technologies over the long term.

Conclusion

M•CAM's intellectual property analysis has identified several examples of uncited prior and concurrent art that may limit the strength and defensibility of Symantec's U.S. Patents 6,052,531 and 6,167,407. Excerpts of claims from patents assigned to General Electric, Xerox, IBM, Trend Micro, Neuromedical Systems, and Network Associates were provided in this report to illustrate the similarities. In addition to these patents, the analysis included examination of prior and concurrent art patent claims from over 660 closely related U.S. patents.

In Symantec's February 7, 2001 press release announcing the issuance of '531 and '407, it states, "[T]he technology may also be used to update general computer readable files, which may include data files, program files, database files, graphics files, or audio files. As the patent holder, Symantec is the only company authorized to incorporate this sophisticated technology into its best-of-breed products."

Clearly, from the statement above, Symantec is looking to claim the broadest claim interpretation possible. The technology developed by Symantec has helped the company create market-leading products, such as Norton AntiVirus. However, from an intellectual property licensing perspective, the abundance of uncited prior and concurrent art may strongly limit Symantec's ability to license this technology in the long term.



M•CAM DOORS™ is an on-line intellectual property diagnostic tool that puts comprehensive, often-missed prior art and unintended-use data into clear view with outstanding data visualization. Powered by the award-winning M•CAM analysis process and running on any standard Internet browser, M•CAM DOORS™ provides relevant data to relevant people making relevant decisions in seconds.

**For a free demonstration of
M•CAM DOORS[®]
call toll free 877.636.M•CAM
or email us at doors@m-cam.com**

The information in this report was prepared by M•CAM, Inc. ("M•CAM"). M•CAM has used reasonable efforts in collecting, preparing and providing quality information and material, but does not warrant or guarantee the accuracy, completeness, adequacy or currency of the information contained in this report. Users of the information do so at their own risk and should independently corroborate said information prior to any use of it. M•CAM is not responsible for the results of any defects that may be found to exist in this material, or any lost profits or other consequential damages that may result from such defects. The information contained in this report is not to be construed as advice and should not be confused as any sort of advice. M•CAM does not undertake to advise the recipient or any other reader of this report of changes in its opinions or information. This information is provided "as is." M•CAM or its employees have or may have a long or short position or holding in the securities, options on securities, or other related investments of companies mentioned herein. This report is based on information available to the public.

M•CAM's Patent Glossary

<u>Aligned Sector:</u>	The business sector in which the product(s) resulting from the patent(s) is currently or intended to be sold.
<u>Applicant:</u>	The person or corporation that applies for a patent with the intent to use, manufacture or license the technology of the invention; under U.S. law, except in special situations, the applicant(s) must be the inventor(s).
<u>Application:</u>	Complete papers submitted to the U. S. Patent and Trademark Office seeking a patent including oath, specification, claims, and drawings. This usually does not signify a Provisional Patent Application, but only a regular patent application.
<u>Art:</u>	The established practice and public knowledge within a given field of technology. This also identifies a process or method used to produce a useful result. A term used in consideration of the problem of patentable novelty encompassing all that is known prior to the filing date of the application in the particular field of the invention.
<u>Assignee:</u>	The person(s) or corporate body to whom the law grants or vests a patent right. This refers to the person or corporate entity that is identified as the receiver of an assignment.
<u>Business Method Patent:</u>	A patent that controls the way a business process is undertaken. The issuance of these patents by the United States Patent and Trademark Office (USPTO) is new and controversial, since many allege that it is unfair to allow a patent on a way of doing business.
<u>Citation:</u>	This may include patents or journal articles that the applicant or examiner deems relevant to a current application. A reference to legal authorities or a prior art documentation are examples of a citation.
<u>Claim:</u>	The language in a patent application that defines the legal scope of the patent. Most patents have numerous claims. This is typically the single most important section in the application.
<u>Concurrent Art:</u>	Concurrent art occurs when related patent applications are being examined by the USPTO at the same time. It is difficult for any company or inventor to know, at the time they file for a patent, whether a "related" patent application exists.
<u>Filing Date:</u>	The date when a properly prepared application reaches the patent office in complete form.
<u>Innovation Cycle:</u>	A description of the commercialization timeframe for the intellectual property.
<u>Innovation Space:</u>	M•CAM's representation of the innovation(s) that occur before, during, and after the pending period of the subject patent. The innovation space is the first place to look for patents that are closely related to the subject patent and that may impact the defensibility of the subject patent or create opportunities for patent licensing.
<u>Issue Date:</u>	Not to be confused with the filing date, which is the date the patent application was physically received by the U.S. Patent and Trademark Office. This is the date on which the patent actually issues.
<u>Non-Aligned Sector:</u>	Any sector in which the patent can be used or sold, other than the sector for which the patent or resultant product was invented or intended.
<u>Pod:</u>	A group of patents owned by a company that should be treated as a single unit of innovation (e.g., a certain group of patents that comprise a single product or multiple related products).
<u>Prior Art:</u>	Any relevant patent that was issued before the patent being analyzed. If this previous patent was specifically mentioned in the new patent's application, the previous patent is referred to as "cited prior art". If it was NOT mentioned, then that previous patent is referred to as "uncited prior art".
<u>Subsequent Art:</u>	Any patent that has a filing date with the USPTO that is after the issuance date of the subject patent. This subsequent art patent may or may not have cited (see "Citation" above) the subject patent. As subsequent art represents more recent innovation than the subject patent, it has great potential to shrink the market opportunity for the subject patent.