symantec

Virus and Vulnerability Classification Schemes: Standards and Integration

by Sarah Gordon

Senior Research Fellow
Symantec Security Response

INSIDE

INSIDE

Contents

Introduction

Created and implemented by various groups with diverse goals, standards are everywhere. For example, the World Wide Web Consortium (W3C) works developing specifications, guidelines, software and tools to facilitate interoperability on the World Wide Web. Another standard, the Metric standard, allows us to agree on all kinds of physical measures, such as weight or length throughout the world. Without this standard, it would be difficult to collaborate on a building project, as one meter may mean a different thing to one builder than to another! Thus, from the World Wide Web Consortium to the weights and measures we use in our everyday lives, and many other places in between, standards help people work together.

Standards are not just of interest to scientists or technicians – they are very important to the consumer as well. Consumers are so familiar with standards, even indirectly, that they may not even realize how much they rely on them: standards are a part of everyday life. For example, people expect that when they plug in a 50-watt light bulb, it will draw the appropriate amount of current. They expect when they buy organic foods that these foods will contain no pesticides.

Standards mean that a nut built to a particular specification in England will fit a bolt made to similar specifications in America: that is, standards provide *interoperability,* allowing information to be exchanged easily and accurately. One only needs to consider the $250 million Mars Climate Observer crash – reportedly attributed to confusion over imperial versus metric measurements – to see that the lack of standards (or in this case, confusion over standards) can lead to disaster. Consumers use these standards to order their lives, and testers ensure that given standards are adhered to.

The situation is no different with information technology. Administrators and computer users alike make use of standards every single day. From the PCI bus inside most computers to the CD-ROMs and DVDs we load software from, standards make the computer industry scalable and allow interoperability. Even in the computer security world there are standards – albeit new or developing ones – that help people assure that the information they receive is accurate. Adherence to these standards is aided by a variety of testing organizations that measure the compliance of security products to a given standard.

By participating in testing processes initiated by governmental organizations like *NIAP* (the *National Information Assurance Partnership),* and by working to ensure unbiased, scientific tests from commercial, vendor-supported groups like West Coast Laboratories, *NSTL (National Software Testing Labs)* and *ICSA Labs (International Computer Security Association),* developers can monitor the various standards implementations – as well as see how security products perform when measured to criteria set by the various testing bodies.

However, despite the security industry's high (and continually evolving) standards, the fact remains that the industry is lacking standards in certain critical areas, making it difficult to measure "correct" and "complete" performance. In this paper, the history of antivirus and security related standards is examined, in order to facilitate optimal use of those standards that are extant, as well as warn a buyer of those areas that are still to be adequately covered by a standards group. Finally, suggestions for improving the current situation are given.

Standards in the real world

Standards evolve when communities need to find a way to share resources – information, or, more frequently, physical things. For example, the development of standards to help promote quality assurance and control is an integral part of the global effort to strengthen norms for pharmaceuticals [WHO, 2002]. In this initiative, the community of health professionals working with the *World Health Organization* strives to assess quality, safety and efficacy of drugs, enhancing norms and standards for pharmaceutical legislation and promoting the development of drug nomenclature and classification efforts.

Similarly, the community of scientists working in the field of chemistry needs to be able to communicate with each other regarding chemicals and chemical reactions. Thus, their communities have developed standards for how the chemicals and their reactions are described. These standards follow certain rules. For example, naming of compounds requires first the identification and naming of a parent structure; the name is then sometimes modified by including prefixes, infixes and, in the case of parent structures, suffixes that convey the structural changes required to create the actual compound from the parent structure. Using these guidelines, a researcher can create a name that identifies to other chemists exactly what the organic compound is [IUPAC, 1993]. There are even tools that can help chemists generate names according to these guidelines [Williams & Erin, 2002].

Working according to agreed upon standards allows people within different groups to work collaboratively both inter and intra organizationally, for the benefit of all. With this in mind, some of the existing standards efforts have made a crossover from work within a local community to work within the global community [Bergner, Deifel, et al. 2002; Global 2002; ITCG, 2003; NIEH, 1996].

Today, the antivirus and security industries are approaching a similar nexus of collaboration, and facing many of the same obstacles previously encountered by other developing organizations and disciplines. Before these hurdles can be overcome, it is important to examine the historical precedents that complicate these efforts, so as to avoid isolationism and premature consensus thinking (groupthink) that has hampered antivirus industry maturation [Gordon & Ford, 1999].

Different worlds

While the security world developed primarily out of the networked UNIX community, the antivirus professionals for the most part worked in the single user, DOS environment. For many years, those skilled in virus research were comparatively unaware of the nuances of more general computer security research, and vice versa. Thus, the worlds have developed very differently, utilizing different standards, organizations and information sharing paradigms [Gordon, 1994].

In many ways the security industry has matured faster than the antivirus world. One example of this maturity is the opportunity for qualified individuals to take part in well-organized and open professional organizations and societies (ISC2, ACM, IEEE). There are peer organizations within the antivirus world, however, these tend to be casually organized, relationship based, and with no formally documented or recognized entry requirements. Three formally organized research oriented organizations, AAVAR, WLO and EICAR, offer the opportunities for antivirus professionals to exchange information. However, even these organizations within the antivirus world are not well-known within the security world. This is probably due in part to the historically virus-centric nature of these organizations.

The antivirus and security communities developed in parallel to the respective threat communities – but whereas the antivirus work initially developed as a response to viruses, the security industry developed not only as a response to security threats, but as part of the process of software and system development. This has created different mindsets and skillsets for the researchers working within each community.

These differences in the ways in which the industries developed have influenced the way the people involved share information. In the early days of computer viruses, while there was cooperation amongst some antivirus professionals, little information about the viruses was provided to users. Antivirus products found viruses and removed them – end of story. However, as time went on, users began to want, and need, information about the viruses that were infecting their systems. Today, this trend for information acquisition continues, with vendor web sites providing extensive information regarding new viral threats and countermeasures. However, while public sharing of information concerning viruses is commonplace, the widespread sharing of explicit technical details and viral code samples to end users is *verboten* within the industry.

Discussion and dissemination of vulnerabilities and example exploits have followed a somewhat different path. Security issues have always been openly discussed and vulnerabilities have been examined in detail on public mailing lists since the early days of the Internet. Today, lists like Bugtraq, Full-Disclosure and NT-Bugtraq offer a variety of disclosure models.

The most open of the disclosure models, full disclosure, is controversial. In a full disclosure model, vulnerabilities and complete working exploits of these vulnerabilities are made available publicly to anyone that wants them. The equivalent of this behavior in the antivirus world would be the public distribution of live viruses – something that is anathema to industry "best practices". However, even outside this full disclosure model, detailed technical information is usually shared much more openly in the security world than in the antivirus world. This difference in disclosure positions between virus and security researchers has probably been the number one factor in hindering information exchange both within the virus world, and between virus and security researchers.

The current state of affairs

One obvious area in which to push for standards in the antivirus and security world is that of virus and exploit naming, as these areas are critical for accurate information sharing. However, the virus naming scheme is radically different from the exploit naming scheme.

Historically, viruses were given "common names" like Ping Pong, MTE or Spanish Telecom. Common names of viruses, just like common names of plants, are useful because they are descriptive, easy to remember, and easy to pronounce. However, there are some disadvantages to using this common name system as a formal naming scheme. This is well illustrated by considering the way plants are named.

Common names for plants have no rhyme or reason, and can be vague. They also may be botanically incorrect; for example, the Jerusalem artichoke is neither from Israel nor is it an artichoke. Common names may also lead to dangerous confusion: the Chinese star anise *(Illicium verum)* is edible, but the Japanese star anise *(Illicium anisatum)* is poisonous [Saupe, 2002].

Botanists deal with this by assigning a more descriptive scientific name to the plant. This name is tied to a specific sample in question, and groups plants into families. Thus, scientific names provide a stable way of referencing samples. When sharing information, scientists use these specific names when dealing with plants, because these names are exact, and globally accepted. While the common name for a plant varies from location to location, the scientific name is universal and, most importantly, *sample based* – that is, there exists a reference sample of the plant with that particular name that can be referred to and compared against.

Formal virus naming

Even a cursory investigation of virus naming shows that there is a relation between the common name for a virus and its "scientific" name. For example, Ping-Pong's "proper" name is Ping-Pong.A or Ping-Pong.B, depending upon the variant of the virus. However, as the names indicate, both these viruses are part of the Ping-Pong virus family.

The "scientific" naming of viruses stems from a standard proposed by some individuals who are affiliated with Computer Antivirus Research Organization (CARO[1]) several years ago. The standard is mutable in that it has been changed several times as different needs have been encountered within the antivirus community. The current version of the naming standard is described in Virus Bulletin [Fitzgerald, 2003], but in summary the idea is as follows (see page 7):

1. CARO is an informal AV industry group; one of several such groups, most noteworthy among achievements of CARO members was a formation of virus naming rules in the early days of computer viruses.

THE GENERAL FORM OF MALWARE NAMES UNDER THE NEW GUIDELINES IS:

<malware_type>://<platform>/<family_name>.<group_name>.<infective_length>.<sub_variant><devolution><modifiers>

Thus, the "full" name of a virus looks suspiciously like a Universal Resource Locator (URL – see RFC 2396 for a good discussion of URL's and how they relate to their parent structure, URI's), where the modifiers represent different attributes of virus behavior. An example of such a modifier is "@MM" for viruses that are Mass Mailers.

While there are several issues with this naming scheme (see [Gordon, 2003] for a full discussion) from a purely technical perspective, from an ease of use perspective this scheme is not ideal for the following reasons:

- Names using the new scheme are very long and somewhat complex, making them unwieldy for general users
- Having a naming standard is only a small part of the problem – the issue of reconciling names with standards is not addressed. This is especially true for viruses that are newly discovered in the wild, and that must be addressed in a time-critical nature by antivirus product developers
- The issue of how these names should be shortened by products that cannot display such a long name is paramount, as this is the usual way that the name will be displayed and used
- If the name is not supposed to be a URL, it should be modified so that it does not appear to be a URL – this is confusing to those that understand the URL standard. Similarly, if it is a URL, or follows the same format as a URL, the appropriate RFCs that fully specify the form should be quoted and followed

For several of these reasons, there is not total consistency of naming between different vendors. Despite this, there is often partial information about a virus and some of its attributes in the names displayed by products. Vendor web sites elaborate on this information, providing useful data for users and administrators, and, in a limited way, allow information from different sources to be cross-referenced. For example, vendors may provide cross-references to names used by other products; however, even the best of these are limited.

This scheme is very different from those used for vulnerabilities, that are usually classified by number. There are three standards developing in the security industry: The *Microsoft* Bulletin Vulnerability ID number[2], the *Bugtraq* ID number[3], and the CVE vulnerability and candidate IDs (CVE and CAN) numbers[4]. These identifiers provide information about specific vulnerabilities; ideally, they can be cross-referenced. For example, the *Bugtraq* ID provided by *SecurityFocus* can be correlated by vendor, title, keyword, or cross-referenced with its corresponding CVE ID.

2. www.microsoft.com/security/
3. http://online.securityfocus.com/bid/bugtraqid/)
4. http://www.cve.mitre.org

VGREP, Aliases and the WildList™

Given the importance of standards for information sharing, it would be logical to use vulnerability and virus naming as a basis for creating a global model for general computer security related information sharing. However, there are many unresolved issues in this area.

Although the virus industry is moving towards a single standard for the format of virus names, there are still many examples where different vendors call viruses by different names. This has arisen partly because there is no *universally* recognized sample-based naming standard for computer viruses.

One challenge in creating such a standard is that the rapid response required to new threats makes the process of virus naming (and therefore, by extension, sharing of information about a particular virus) problematic, as detection is often implemented before a name has been "correctly" established.

Furthermore, many products flawlessly prevent and remove entire classes of viruses without exactly identifying the virus variant – this pragmatic approach (sufficient, within certain guidelines, for user protection) poses problems for those interested in tracking virus prevalence.

Whereas new species of plants are not discovered on a daily basis, many viruses are discovered every day, and in some cases information about these viruses needs to be distributed to the user community (and other researchers) very quickly. This requires that the virus be called something in the interim. Additionally, viruses may be discovered at different times by different vendors, and until the samples can be compared, there is no way to coordinate the names.

NAME OF VIRUS	ALIAS(ES)	DATE	# OF REPORTS	BY:*
AntiCMOS.A	Lenart	1/95	5	OzSmSoWsZz
AntiEXE.A	D3, New Bug	9/94	4	FpSoWsZz
BAT/HitOut.A-mm	Without	9/02	2	RzTa
Bleah	Bleah.D, Bleah.	2/02	4	AlFpSkSo
Dodgy		4/02	3	SgSkSo
Empire.Monkey.B	Monkey 2	6/94	3	SoWsZz
Form.A	Form 18	7/94	3	SmWsZz

Figure 1: Excerpt from the WildList.™ Note the Aliases known for each virus, listed in the center column.

**Letters indicate first and last initials of the Reporters*

As seen [in Gordon, 2002], some of the issues related to virus naming have been resolved by the WildList. For example, the user can consult the alias function to help translate between virus names used by different companies (see Figure 1). Additionally, the *WildList Organization* has addressed the lack of a non-commercial, vendor-neutral, scientifically established and maintained, acceptable (and accessible) central reference virus sample collection with the creation of "Wildcore". This sample set is created by the *WildList Organization* and made available to vendors, developers and testers who have developed collaborative relationships with their peers, allowing them access to a sample-based system for virus identification.

Hopefully, the *WildList* naming methodology will continue to provide a cross referencing system for the names chosen by vendors and a comprehensive and accessible collection of reference samples for those viruses in the wild. Ideally, this should be part of an overall move toward cross-referencing and categorization of all known computer viruses. This is obviously a gargantuan task, and one that is of limited benefit, given the comparatively small percentage of viruses that end up in the wild. However, if the industry is to truly address the information-sharing problems it faces, such a system is a necessity, at least on a "go forward" basis.

Another useful tool for researchers and users is VGREP (ref: http://www.virusbtn.com/resources/vgrep/index.xml), a powerful tool created by virus researcher Ian Whalley, and currently maintained by Dmitry Gryaznov. This tool is a full cross-reference utility that can be used to compare the names products use for different viruses. While this is excellent for remedial action, it does not help solve the cause of the problem, as it is focused on alleviating the symptoms.

Aside from the rapid action required by researchers when a new virus is discovered, the sheer numbers of viruses pose a problem for those involved in virus naming. A numeric database model proposed by Pearson [Pearson, H. 2001; Genbank, 2002] offers some interesting possibilities for dealing with such large tasks. These efforts depend on submissions from scientists, and facilitate cross-disciplinary data exchange. For example, exchange occurs daily between the GenBank, European Molecular Biology Lab (EMBL) and the DataBank of Japan (DDBJ) on a daily basis.

Blended threats

Earlier we discussed the ways in which viruses are named with their longer or "more scientific" names: Ping-Pong.A, Ping-Pong.B, _1963 (Necropolis.1963.c; 1963.overwrite), Tequila.A, , MtE_Pogue, W95/CIH.1003, W32/KRIZ.A, WM/Concept.A, W32/Nimda.A@mm etc. While these names provide information about the viruses, they do not indicate if there exist any vulnerabilities associated with the virus, and if there are, what these vulnerabilities are. Until recently, this was not an issue: viruses exploited only regular system functionality. However, this is no longer the case, as many new viruses make use of vulnerabilities in order to spread more effectively. Such a program is an example of a class of threats known as "Blended Threats" – a combination of different threat types. Furthermore, such viruses have the ability to spread extremely quickly within a population of vulnerable machines, as many are capable of spreading without any user interaction whatsoever.

Blended threats are defined as malware that combines the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. By utilizing multiple methods and techniques, blended threats can spread rapidly and cause widespread damage. Characteristics of blended threats include the following:

- CAUSES HARM: Launches a denial of service attack at a target IP address, defaces Web servers, or plants Trojan horse programs for later execution.
- PROPAGATES BY MULTIPLE METHODS: Scans for vulnerabilities to compromise a system such as embedding code in html files on a server, infecting visitors to a compromised Web site, or sending unauthorized email from compromised servers with a malicious attachment.
- ATTACKS FROM MULTIPLE POINTS: Injects malicious code into .exe files on a system, raises the privilege level of the guest account, creates world readable network shares, makes numerous registry changes, and adds script code into html files.
- SPREADS WITHOUT HUMAN INTERVENTION: Continuously scans the Internet for vulnerable machines to attack.
- EXPLOITS VULNERABILITIES: Takes advantage of known vulnerabilities such as buffer overflows, http input validation vulnerabilities, and known default passwords to gain unauthorized administrative access.

Consider the virus W32/Nimda.A@mm. It is a virus (or worm) named Nimda. The current name, W32/Nimda.A@mm tells us it is the A variant, and that it is a mass mailer – that is, one of the way it spreads is to email itself to many different recipients. Testers wanting to test whether or not a product detects this virus can refer to the *WildList* WildCore sample set to be sure they have the correct variant for testing a product's detection and/or disinfection capabilities.

However, a closer look reveals that there is more to Nimda than meets the eye… it also exploits a vulnerability; several of them in fact. This makes it a Blended Threat. In particular, Nimda makes use of two different vulnerabilities to spread – one in IIS, and one in some implementations of MIME, both listed in the *Microsoft* vulnerability database. It sends itself out by email and searches for open network shares. It attempts to copy itself to vulnerable *Microsoft* IIS Web Servers, and uses the Unicode Web Traversal exploit to infect the machine (MS00-078). Additionally, emails sent by Nimda utilize a MIME exploit in order to execute malicious content upon preview of an infected email (MS01-020).

Consider now an administrator who discovers that one or more of his machines are infected with this virus. Antivirus software identifies the sample as W32/Nimda.A@mm. Being an informed user, they know that this means they have a Windows 32 virus, called Nimda, and that it is a mass mailer. They consult the *WildList,* checking for aliases, and the antivirus software removes the infection. However, this is not sufficient. They need to know if there was any damage done, what remedial actions, if any, are needed. Most importantly, they need to know that this virus uses *exploits* to spread. Removing the virus is not sufficient to secure the network – the vulnerabilities also need to be indicated and repaired.

Tests of antivirus software may certify that the software is 100% compliant in virus detection and repair; however, issues concerning vulnerabities are not addressed. In practical terms, this means that although your product may be certified *VB 100, ICSA Certified,* or *Checkmark compliant* with any one of several levels, a vulnerability could remain on your system that would allow future or further exploit.

One possible extension here is to add the CVE vulnerability ID to the name of a virus that also exploits a vulnerability. In the case of Nimda, the virus name would become W32/Nimda.A@mm_CVE00-078,00-120. The problem with such a scheme is that it is clumsy – the names produced are far from intuitive. Thus, another possibility is simply appending the letters VULN to all viruses that utilize exploits, and require the vendor to provide the details of which vulnerabilities used in the virus description. Finally, it has been argued [Gordon, 2003] that virus names should be simplified, as the current scheme confuses *attributes* with *identifiers.*

Such a discussion is beyond the scope of this paper, but the argument can clearly be made that upon discovering any virus on a system, more information than that contained in the name *must* be referenced during cleanup. Thus, given that authoritative information always needs to be consulted, the information in the name needs only to serve as a unique identifier pointing to the complete information.

Perhaps pursuing a scheme (as suggested in [Gordon, 2003]) based upon a simple unique identifier, supported by an XML schema for attribute information is of more practical use: such a scheme would seem to meet the needs of users and the needs of researchers. The WildList Organization could easily implement and assign identifiers similar to those used by CVE, Microsoft and Security Focus. This would have the added benefit of aiding the user in reconciling systems after virus attacks.

Impractical solutions?

Information on viruses and vulnerabilities can be found on most product vendors' WWW sites. However, partly due to the fact that there is no testing by third parties on this information, it is sometimes incomplete, or wrong. An analysis of antivirus and security product vendor WWW sites was performed to assess vendor current performance in comprehension of information provision.

The information for the W32/Aliz.A@mm, a blended threat, was examined on three major vendor sites. Aliz is a simple mass mailing worm that exploits a vulnerability in Internet Explorer 5.5, allowing attackers to execute attachments by setting an unusual MIME type for the attachment.

- "Vendor A" described the virus, and made reference to the appropriate *Microsoft* Bulletin (MS01-020) and the CVE identity (CAN-2001-0154). The information provided was complete and comprehensive, providing the user with information about both the virus, and the vulnerabilities that needed to be patched.
- "Vendor B" described the virus, and made reference to a *Microsoft* Security Bulletin – but it was the wrong *Microsoft* Bulletin (MS01-027). This vulnerability is related to flaws in web server certificate validations. The user relying on this information would patch the wrong vulnerability.
- "Vendor C" described the virus but initially made no reference to any bulletins or vulnerabilities. Subsequent to the presentation of these findings at a security conference in November, 2002, the vendor supplemented the virus description with a link to the *Microsoft* Security Bulletin.

Combined with the fact that tests of antivirus software do not address the issue of the vulnerabilities that may be exploited, this is a potentially dangerous scenario.

Testing and future research

One question raised by some has been "should compliance to standards naming be a part of tests and certifications?" Ultimately, the answer to this question is yes… but not in the foreseeable future, and not without considerable groundwork first. There are several reasons why.

First, there is no universal naming standard administered by any central and catholic standards authority within the industry capable of coordinating names quickly enough to dispense identifiers to vendors; speed of response dictates that things be called something before loose (and informal) industry collaboration produces a formal name. Second, to insist on adherence to a *specific* name for a virus would be counterproductive: any standard for naming would be using compliance with the format, not the form. Thus, any tests involving a "naming" criteria would need to recognize the formats used by vendors, which could include not only specific, but generic identifiers. This would not achieve naming consistency between vendors, nor should we expect it to. However, it may well serve to eventually achieve consistency via the identifier. Finally, whether or not these identifiers should be present as part of a product, or are better suited for distribution on a vendors WWW site is an issue that warrants serious consideration.

Another question concerns the set of samples of ItW viruses maintained by the WildList Organization. Should this be the foundation of an overall virus sample reference system. If not, where/who would create and manage such a sample-based system? Such a collection would need to be vendor neutral and scientific, at the same time recognizing there is no real user requirement for "standard names" of viruses as long as reliable cross referencing is available. This is a topic for future research.

Conclusion

The way in which viruses and security exploits have traditionally been categorized has worked, in a limited fashion, until now. However, with the advent of blended threats, the case for integrating the way in which both the antivirus and security industry classifies threats is becoming highly compelling.

Self-replication of exploits means that threats are moving too fast now for the vertical, compartmentalized approaches to work, as blended threats require integrated responses. Thus, we need to strive for enhanced information sharing amongst the communities, helping all involved achieve a more balanced, holistic approach. This can be achieved by developing standards for information exchange, beginning with synergistic naming schemes.

While such standards are already the norm within some segments of the industry, it will take time and leadership for widespread adoption. Just as biochemical nomenclature bodies encourage close relations with colleagues and peers in order to help avoid conflicting names, there are opportunities for multi-disciplinary approaches to threat analysis and mitigation within the antivirus industry. By participating in these initiatives, vendors can learn from others' experiences.

The current approach to virus naming encourages the medical model of antivirus response: users continue to be concerned by symptoms, rather than disease. The problem of treating the symptom rather than the underlying cause is illustrated in the anti-virus industry's response to Nimda: removing the virus is of limited effect, as the underlying (and enabling) security problem remains. This world view is often perpetuated by the AV industry, which in the case of blended threats focuses almost exclusively on effect rather than cause.

The primary area in which collaborative efforts could achieve maximum benefit is that of virus naming, and synthesis with security exploits used by particular viruses. However, it is not the only area; Testing issues also arise here. Tests should tell us not only are our symptoms (fevers/payloads) being dealt with, and is the infection removed (virus gone), but are the vulnerabilities addressed (provide a better diet to eliminate scurvy, for example).

Ultimately, two different forces will drive the move towards standards. The first, information sharing within the industry, is driven by the increasing number of blended threats, which are capable of spreading extremely quickly. The second, and more powerful force, however, is the user base. Standardization resulting in uniformity of names may well be unachievable. However if there is sufficient understanding of the issues faced by the buying population, standardization regarding how information is provided and how viruses are uniquely referenced amongst vendors may well be inevitable.

Resources

Bergner, K., Deifel, B., Jacobi, C. Keller, W., Rausch, A., Sabbah, A., Schatz, B., Sihling, M., Vilbig A. & Vogel, S. 2002. *The Future of Information Technology: an interdisciplinary, scenario-based approach.* From Bayerischer Forshungverbund Software Engineering. Technical University of Munich. Munich. Germany.

Fitzgerald, N. 2003. *A Virus By Any Other Name: Virus Naming Revisited.* Virus Bulletin – pp. 7-9. January 2003.

GenBank, 2002. *GenBank NIH Genetic Sequence Database.* National Institute of Health. Retrieved from the WWW on December 10, 2002. http://www.ncbi.nlm.nih.govGenbank/GenbankOverview.html

Global, 2002. *Standards Action in the Global Marketplace.* International Standards Organization.

Gordon, 1994. *Technologically Enabled Crime: Shifting Paradigms for the Year 2000.* From the Proceedings of the 1994 IFIP Conference, Curacao, Netherlands, Antilles.

Gordon, S. & Ford, R. 1999. *When Worlds Collide: Information Sharing for the Security and Antivirus Communities.* From the Proceedings of the annual Virus Bulletin Conference. Vancouver, British Columbia. September 1999.

Gordon, S. 2002. *What is in a Name.* Secure Computing. June 2002.

Gordon, 2003. *That Which We Call a Rose.A.* Virus Bulletin. March 2003.

ITCG, 2003. *ITGC Industry Technical Guidelines Committee. IPC/WHMA-A-620.* From the proceedings of the Third Annual Wire Processing Technology Expo. Arlington Heights, Illinois. May 2003.

IUPAC, 1993. *A Guide to IUPAC Nomenclature of Organic Compounds.* Recommendations 1003. Commission on Nomenclature of Organic Chemistry. Blackwell Scientific Publications. 1993.

NIEH, 1996. *On the Trail of Mutations at MIT.* NIEH News.Volume 104, Number 2. Environmental Health Perspective. February 1996.

Pearson, H. 2001. *Biology's Name Game.* Nature. 7 June 2001.

Saupe, S. 2002. *Naming.* Biology Department. College of St. Benedict. St. John's University. Collegeville, MN.

WHO, 2002. *Norms, Standards and Guidance for Pharmaceuticals.* World Health Organization.

Williams, A. & Erin, A. 2002. *Quality First in Systematic Naming.* Advanced Chemistry Development European User Meeting. October 2002. Obernai France.

About the Author

Sarah Gordon is Senior Research Fellow at Symantec Security Response. Her research areas include testing and standards for antivirus and security software, privacy issues, cyberterrorism, and psychological aspects of human/computer interaction.

She has been featured in IEEE Monitor, The Wall Street Journal, and Time Digital, and profiled by PBS, ITN, and CNN International. Her work, for which she has won several awards, has appeared in publications such as Information Security News and Virus Bulletin. She is a highly sought-after speaker, having presented at conferences ranging from DEFCON to Govsec.

Sarah was recently appointed to the Editorial Board for Elsevier Science Computers and Security Journal. She is on the Advisory Board of Virus Bulletin and is co-founder and board member of The WildList Organization International. She is also Technical Director of The European Institute for Computer Antivirus Research where she serves on the Board of Directors and Conference Program Committee, and is a member of SRI's cyber-adversary working group.

Sarah was previously responsible for security testing and recommendation for The United Nations, and has participated in various initiatives for Homeland Security and Infrastructure Protection. Her work in ethics, technology, and profiling computer criminals is required coursework in various academic information security programs.

Sarah graduated from Indiana University with special projects in UNIX system security and ethical issues in technology. She is a member of the American Association for the Advancement of Science, The American Counseling Association, and the Association for Family Therapy and Systemic Practice in the UK. Prior to joining Symantec, she worked with the Massively Distributed Systems Group's Antivirus Research and Development Team at IBM's Thomas J. Watson Research Laboratory in New York.

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
408.517.8000
800.721.3934

www.symantec.com

For Product information
In the U.S. call toll-free
800.745.6054

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.