Given the virtually instantaneous and worldwide dissemination widely available via the Internet, the only rational assumption is that once a computer program capable of bypassing such an access control system is disseminated, it will be used.¹ (emphasis added)

Three can keep a secret if two are dead. (Benjamin Franklin)

Responsible developers work hard to produce secure, reliable, and efficient software packages. No company wants its integrity compromised by hackers, employees, or legitimate users. Negative publicity damages a firm’s reputation. Legal proceedings can cost an organization millions and destroy any chance of long-term success.

Realistically, few products are released without security flaws. Programmers and system designers strive to find security bugs during the development cycle or at worse during beta testing, when bugs can be fixed easily. Careful testing will allow internal programmers to debug the software without publicity or industry notice.

The outcome may differ if outsiders discover a security breach. Malicious hackers may exploit the breach to obtain classified information, to destroy the integrity of the information, or simply for the challenge. Even self-described “ethical hackers” may share this information with no discretion. Given the speed of the Internet, security breaches can be transmitted worldwide in hours.

This article deals with vulnerability disclosure, where the details of a security breach are freely available. It also deals with the bizarre case of Bret McDanel, a young computer expert who spent 16 months in federal prison after he exposed a security breach in his former employer’s software package.

VULNERABILITY DISCLOSURE

A vulnerability is a set of conditions that may compromise the confidentiality, integrity, or availability of an information system. It is often a simple oversight or weakness in a computer’s software that lets a hacker manipulate computer data.² Vulnerability disclosure is the publication of confidential

Address correspondence to Edward H. Freeman, JD. E-mail: edfreeman@hotmail.com.
information that describes such problems. Due to the nature of computers and networked systems, and our reliance on their integrity, the release of this information has the potential to do great harm or great good.³

Some security experts feel that vulnerabilities should be publicized as soon as they are discovered. Once the information is released, developers can write appropriate patches to fix the flaws. Under the threat of negative publicity, “vendors are pressured into providing security fixes quickly. Users can identify similar vulnerabilities on systems other than the original.” Public notification may prevent widespread exploitation of the error.

Other authorities maintain that this information should not be released until developers have had an opportunity to diagnose the problems and release appropriate patches. The release of this information does not improve overall security. If there is no patch to fix the vulnerability, hackers may attack vulnerable systems. It also punishes well-intentioned organizations by not providing them a reasonable amount of time to address the vulnerability.⁵

Restrictions on the release of this information reduce exposure until a fix can be developed. “There is some validity to the industry argument that it is the publication of information on holes that is responsible for them being so widely exploited. Studies have shown that there is an upswing in intrusions using a given security weakness once it has been publicly disclosed.”⁶

Both sides agree that the ultimate goal is to reduce the risk to information systems, to stop security breaches, and to prosecute the responsible parties. To achieve this goal and to determine whether a particular vulnerability should be disclosed, security experts have developed complex mathematical formulas to determine when or if a specific vulnerability should be made public.⁷ Factors in making this decision include:

- Time before a suitable patch can be released
- Time before the “evil hackers” learn of the vulnerability
- Actual loss to users if they are exposed to the vulnerability for a specific amount of time
- Extent of the vendor’s loss, in future sales or reputation loss, if news of the vulnerability is made public.

Microsoft recently disclosed it does not automatically disclose the existence of software vulnerabilities that are discovered internally, in the belief that full disclosure of every security-related product change only serves to aid attackers. Mike Reavey, operations manager of the Microsoft Security Response Center (MSRC), said the company’s policy is to document flaws but that full details on the fixes are withheld. “We want to make sure we don’t give attackers any [additional] information that could be used against our customers. There is a balance between providing information to assess risk and giving out information that aids attackers,” Reavey said.

When Microsoft receives a report of a security flaw from external researchers, Reavey said, the MSRC conducts an extensive investigation. Security experts and developers evaluate the code to make sure a comprehensive fix is released in a timely manner. If a related bug is found internally, it will be fixed in the eventual patch, he said, but the details will be kept private.⁸

---

THE DIGITAL MILLENNIUM COPYRIGHT ACT

In October 1998, Congress passed the Digital Millennium Copyright Act (DMCA).⁹ President Clinton signed the bill later that month. The DMCA made major changes in U.S. copyright law to address new issues created by the Internet and other new technologies. The Act also amended U.S. copyright law to comply with the World Intellectual Property Organization (WIPO) Copyright Treaty adopted in December 1996.

American companies have attempted to use the provisions of DMCA to control publication of information about security vulnerabilities. In 2002, Hewlett-Packard threatened to sue a team of researchers who publicized a security bug they discovered in HP’s Tru64 Unix operating system. The bug might have allowed an intruder to take over the system. An HP vice president warned SnoSoft (now Netragard), a loosely organized research collective, that it “could be fined up to $500,000 and imprisoned for up to five years (sic)” for its role in publishing the information.¹⁰ After receiving pressure from the industry, Hewlett-Packard backed down from his threatened use of DMCA against SnoSoft.¹¹
DMCA was also used to threaten the free exchange of ideas in the area of academic research on computer security. The Recording Industry Association of America (RIAA) threatened civil and criminal prosecution against Professor Edward Felten of Princeton University if he did not withdraw a paper scheduled for delivery at a computer conference. The paper discussed his success in breaking the Secure Digital Music Initiative (SDMI) encryption code in response to an RIAA publicly announced challenge to security researchers. The RIAA letter to Felten stated that:

public disclosure of your research would be outside the limited authorization of the Agreement [concerning an RIAA Public Challenge to “break” the SDMI code], you could be subject to enforcement actions under federal law, including the DMCA. The Agreement specifically reserves any rights that proponents of the technology being attacked may have ‘under any applicable law, including, without limitation, the U.S. Digital Millennium Copyright Act, for any acts not expressly authorized by their Agreement.’ The Agreement simply does not ‘expressly authorize’ participants to disclose information and research developed through participating in the Public challenge and such disclosure could be the subject of a DMCA action. (emphasis added)

Felten withdrew his paper from the conference and posted a response that stated in part that “the Recording Industry Association of America . . . threatened to bring a lawsuit if we proceeded with our presentation or the publication of our paper. Threats were made against the authors, against the conference organizers, and against their respective employers.” Felten’s organization, the International Information Hiding Workshop Conference, has chosen to hold all of its future conferences outside of the United States.12

**BRET MCDANIEL**

Bret McDanel worked for Tornado Development, Inc., a Los Angeles firm that provided Web-based email and voice mail services. At his job, he discovered a serious security flaw in the company’s email system that might have allowed outsiders to read customers’ private messages. McDanel notified his supervisors, but the bug was never fixed.13 McDanel soon left Tornado and went to work for another organization.

About six months later, McDanel learned that Tornado had never fixed the vulnerability. Using a fictitious email name, he sent an email to about 5,600 Tornado customers. The email told Tornado’s customers about the vulnerability and directed them to his own Web site for information about it. His goal was to minimize the effect on Tornado’s email servers.

When Tornado learned of the email, they scrambled to delete their own customers’ emails (without their permission) to prevent them from learning about the vulnerability. Then they took other steps to conceal the hole. Ultimately, they fixed the vulnerability and upgraded their general security.

In 2002, McDanel was convicted and sentenced to 16 months in federal prison.14 There was no evidence that McDanel or anyone else ever exploited the vulnerability. To put McDanel in jail, the government adopted a rather unique interpretation of the federal computer crime statute. The applicable language in the Computer Fraud and Abuse Act (CFAA) makes it a crime to “knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer.”15 This statute was designed to go after people who were responsible for denial of service attacks, the sending of so many emails to a server that its computers crash, an act that actually shut down or affect the computer system itself.

After McDanel served his sentence, the government decided that his prosecution had been a mistake and moved to vacate the conviction. In the brief, Justice Department lawyers wrote they first believed prosecuting McDanel involved a “proper, good-faith construction” of the CFAA.16 “The government concedes that the evidence did not establish an intent to ‘damage’ within the meaning of the statute and requests that this Court reverse the defendant’s conviction,” Ronald Cheng, assistant U.S. attorney for the Central District of California, stated in the filing. Jennifer Granick, McDanel’s attorney, added:

This prosecution rode on the government’s contention that McDanel was a ‘hacker’ with a criminal mind and a bone to pick against
his former employer. That bone was Tornado’s refusal to fix identified security problems, and McDanel dealt with it by telling customers so that they could help themselves. This is not a crime.17

Tornado went out of business soon after McDanel publicized the flaw. The most recent information about McDanel is that he is living in Ireland.

**VULNERABILITY DISCLOSURE POLICIES**

The 3Com Corporation is located in Marlborough, Mass., with annual sales over $1 billion. It is a “leading provider of secure, converged voice and data networking solutions for enterprises of all sizes.”18

3Com has a vulnerability publication policy that is typical of the industry. The policy outlines how 3Com handles responsible vulnerability disclosure to product vendors, 3Com customers, security vendors and the general public.19 If a vendor’s product is discovered to contain flaws, 3Com will follow these steps:

- 3Com will email the vendor notifying it of a flaw with its product or service. At the same time, 3Com may distribute vulnerability protection filters to its customers.
- If 3Com does not receive a response within five business days, it will call a representative of the vendor. If there is still no response, 3Com may rely on an intermediary to establish contact with the vendor. After 15 business days, 3Com may issue a public advisory disclosing its findings.
- If the vendor responds in a timely fashion, 3Com will allow it a reasonable period of time to develop a fix. 3Com will use its discretion to determine what constitutes a “reasonable period of time” for a vendor fix to be developed. 3Com will make every effort to work with vendors to ensure they understand the technical details and severity of a reported security flaw. If a product vendor is unable to, or chooses not to, patch a particular security flaw, 3Com will offer to work with that vendor to publicly disclose the flaw with some effective workarounds. In no cases will an acquired vulnerability be “kept quiet” because a product vendor does not wish to address it.
- Before public disclosure of a vulnerability, 3Com may share technical details of the vulnerability with other security vendors who are in a position to provide a protective response to a broader user base. Such a security vendor must show they are able to provide security protection for vulnerabilities, while at the same time not revealing the technical vulnerability details in their product updates.
- 3Com will formally and publicly release its security advisories on its Web site and on selected security mailing list outlets.

**RECOMMENDATIONS**

Obviously, an organization’s best strategy is to find and repair potential security bugs before the product is released, either during development or beta testing. What, then, should an organization do if a software flaw is publicized by outsiders before an appropriate fix can be made?

The developer’s absolute first priority, of course, is to fix the problem. This will minimize potential damage to clients and the company’s reputation. All communications should be kept and recorded for future reference. This is not the appropriate time to evaluate the status of the organization’s security or to fire the guilty parties. Code is written by humans. It is inevitable that errors will be found occasionally no matter how much we try to avoid it.

Once the problem has been resolved, then you can deal with the person releasing the information. A corporate attorney specializing in computer forensics may be required. The communications that you documented will be handy for legal proceedings.

Organizations should perform a thorough analysis of existing code to minimize subsequent problems. All code should include thorough documentation to make further modifications quicker and easier. You won’t find every hole, but if you test properly, in addition to regular Q&A testing, you’ll likely eliminate the more basic and obvious ones.20

**CONCLUSION**

Analysts from X-Force, the research and development team at Internet Security Systems (ISS), evaluated 4,472 vulnerabilities in both hardware and
software during 2005. From the public announcement of the vulnerability on the Internet, the report highlights that 3.13 percent of threats discovered had malicious code that surfaced within 24 hours, whereas 9.38 percent had code that surfaced within 48 hours.\textsuperscript{21}

Vulnerability publication is a threat for any organization that develops or maintains software for sensitive industries. Such companies must develop and enforce policies that will protect it from malicious hackers and from the damage that can result for their actions. Legal assistance in developing these policies and investigating breaches will go a long way to minimize these concerns.

\section*{BIOGRAPHY}

\textbf{Edward H. Freeman, JD} is an attorney and educational consultant in West Hartford, Connecticut. He has written over 50 articles on computer technology, privacy, security and legal issues. He is also an adjunct faculty member at Central Connecticut State University, St. Joseph College in West Hartford, Connecticut and the University of Connecticut.

\section*{REFERENCES}

4. Id.
15. 18 U.S.C. 1030.
18. Full information about 3COM is available at www.3com.com (Visited October 1, 2006).
21. LINK to \textit{INTERNET SECURITY SYSTEMS: ‘Patching window’ is getting shorter and shorter, says ISS’ X-Force; The number of vulnerabilities discovered in hardware and software has increased by 33 per cent in 2005}, M2 Presswire, March 7, 2006.