Continued from page 1

Expert Predictions for Security Trends In 2001

Alan Paller, Director of Research, and Stephen Northcutt, Director of the Global Incident Analysis Center, The SANS Institute

1. Very large businesses will require their e-business partners to comply with a set of operating regulations that ensure that minimum levels of security are maintained. (VISA has already begun for its 21,000 partners). *(Tied for most likely)*

2. The specifications developed by leading businesses will be integrated and codified into standards that all organizations can follow. Auditors will begin using the common operational security standards as a basis. ISPs will offer auditing compliance with these standards as a value-added service.

3. Many more insurance companies will offer cyber insurance once the standards are in place and company compliance can be measured.

4. Organizations will begin to move from a single firewall to a network of distributed firewalls and substantially expand outsourcing firewall management to organizations (often ISPs) that can offer 24 x 7 management.

5. Organizations will outsource more of their intrusion detection monitoring and response because of the need for 24 x 7 management and the extreme global shortage of certified intrusion analysts.

6. Security training will be required for all system administrators in many large organizations. Certification will be optional but preferred for employees and consultants.

7. System vendors will begin (very slowly) to take more responsibility for informing users of important security patches and for automating their safe installation. Microsoft will lead SUN in providing this service.

8. Very large companies will experiment with allowing the information security function to move out of the IT organization. *(Least likely)*

9. Several universities will establish information security training programs for undergraduate and graduate students.

10. Despite the new training programs, the shortage of security people will worsen as nearly three million new computers are added to the Internet every month.*(Tied for most likely)*

Bruce Moulton, Vice President - Infrastructure Risk Management, Fidelity Investments

(Mr. Moulton's comments reflect his own professional opinion and do not represent the opinion of or recommendation by Fidelity Investments.)

1. New privacy legislation in the US (GLB) will significantly raise the profile of information security programs in US financial institutions. HIPAA will have a similar impact for health care organizations. InfoSec programs in general will become less "closeted" and will be more business-connected. Medium-sized enterprises will seek to set up infosec programs.

2. Email-borne virus/trojan payloads will become much more damaging and probably targeted. Other mal-ware vectors (such as Java applets and ActiveX controls) will emerge and perhaps rival email as a concern.

3. Hactivism and other cyber attacks emanating from countries with weak or non-existent legal sanctions and investigative capabilities will escalate. This is likely to be the root of at least one headline-grabbing cyber incident (much bigger than DDOS or LoveBug) that will send a loud wake-up call to the commercial sector.

4. W2K/NT2000 will be rapidly adopted by commercial organizations and a variety of significant security benefits will result (e.g., stronger and reduced sign-on). We might begin to feel better about Microsoft as a security-conscious vendor.

5. PKI will continue to steadily but not explosively evolve and improve. It will not (must not) die. Throughout 2001, the world will still rely primarily on passwords/PINs for online authentication.

6. Wireless will continue to explode as a communication medium. End-user devices will prove vulnerable but transmissions will get solid protection through encryption (ECC).

7. Intrusion detection will remain a hot topic, but the "killer" tools will not arrive in 2001.

8. We will keep ahead of the bad guys. For sure, they have been and continue to be an annoyance, but significant operational impacts are few and far between. Industry groups, vendors, government and professional/specialist groups (like SANS, CERT) have collaborated effectively to keep the intruders at bay. The good guys will continue to win.

9. Significantly more infosec programs will be outsourced.

10. The shortage of qualified and experienced information security professionals will continue.

Marcus Ranum
Chief Technology Officer, Network Flight Recorder, Inc.

I predict that over the next year we will see a pair of intersecting trends. One trend will be an increase in the number of applications that are self-patching; enabling vendors to distribute security-critical bug fixes quickly and automatically. The other trend, which is interdependent with the first, will be a reduction in the number of vulnerability disclosures made for personal or commercial marketing purposes before a correction is available. I believe that the user community is getting sick of people trying to make a reputation by releasing damaging information, and that will further tend to reduce the rate of such disclosures.

Eric Cole
Eric headed a group at the CIA responsible for advanced penetration testing and teaches SANS programs on how to stop the most common hacker exploits.

Most companies have built and implemented a very robust network to meet their specific needs. However, when it comes to security, in most cases it was an afterthought. My prediction for the year 2001 is that we are going to start to see more and more companies that are going to redesign their networks from the ground up and incorporate security into the design from the beginning. Unless companies incorporate proper security into their networks, so that it is ingrained with the network infrastructure and not an afterthought, companies will continue to have major security problems.

Marcus H. Sachs
Joint Task Force - Computer Network Defense, US Department of Defense

The year 2001 will see a marked increase in small computer security companies. Like the mom-and-pop ISPs of the mid-90s that later consolidated into the major ISPs we have today, these companies will flourish by filling a void generated by businesses looking to outsource the security of their computer networks and e-commerce systems. Eventually, these companies will consolidate into larger e-security businesses: the 21st Century equivalents of Pinkerton and Brinks. 2001 will also see continued development of distributed denial of service attack networks. These attack networks will no longer rely on manual establishment by the attacker, but will automatically establish themselves through the use of mobile code and html scripting.

Chris Brenton
Senior Research Engineer, Dartmouth Institute for Security Technology Studies (ISTS)

One trend in 2001 will be a dramatic class separation between the skilled and unskilled attacker communities. The unskilled will continue using automated attacks for Web page defacement and DDoS attacks. The skilled attackers will start focusing greater effort on more esoteric types of attacks in order to prove their level of expertise. These sophisticated attacks will include payload-based attacks at the perimeter, since most firewalls on the Internet today only react to IP header information. They will also include greater development of system back doors that do not show up in process or task lists as this makes them far more difficult to locate during an audit.

Bruce Schneier
CTO, Counterpane Internet Security, Inc.
Author of the new book, "Secrets and Lies"

The Coming Third Wave of Internet Attacks
The first wave of attacks targeted the physical electronics. The second wave – syntactic attacks – targets the network's operating logic. The coming third wave of attacks – semantic attacks – will target data and its meaning. This includes fake press releases, false rumors, manipulated databases. The most severe semantic attacks will be against automatic systems, such as intelligent agents, remote-control devices, etc., that rigidly accept input and have limited ability to evaluate. Semantic attacks are much harder to defend against because they target meaning rather than software flaws. They play on security flaws in people, not in systems. Always remember: amateurs hack systems, professionals hack people.

John N. Stewart
Director Systems Engineering and Security, Digital Island, Inc.

The year 2001 promises to further pit the good guys against the bad guys, as the next generation of computer viruses, distributed attacks, and new operating system vulnerabilities will rear their ugly heads. The first distributed penetration attacks will arrive. The method for attack delivery will change from email/web to instant messaging and wireless, and we'll see the first "electronic protection borders" appear in countries around the world.

Jesper M. Johansson
Assistant Professor of Information Systems, Boston University
Editor, SANS Windows Security Digest

In the year 2001, computer security will continue on its current path. Bugs and sub-standard programming practices will continue to cause holes. Some clever deviants continue to discover how to defeat the protections in Microsoft's e-mail programs and send out "ILY The Next Generation." Netscape Mail will be hit with its first e-mail virus, and viruses on handheld platforms, both Palm and Windows CE, will come on strong. Organizations will finally realize that Windows 9x is not an industrial-strength OS and start moving to Windows 2000. Microsoft will ship NT 6.0 (Whistler) and, right before it hits the shelves, AOL and/or Novell will publicize a major security flaw in it.

A. Padgett Peterson
Corporate Information Security, Lockheed Martin Corporation

The churning I predicted last year is starting as new security "experts," complete with pointy hats, are coming out of the trees. Many are repaints of Y2K "experts" seeking new homes while others are simply doing a Willie Sutton as the "B" in B2B turns into Billion$.

Companies that learned from Melissa can be easily identified since they were not a LoveLetter statistic. Part of this mitigation is a new discipline: Crisis

Manager. Not a Disaster Recovery function since the job description is management of a dynamic and evolving event. Crisis Management requires the ability to separate true information from the false and to be able to make the correct decision immediately. Preplanning helps. Often the most important (and hardest) job is to be able to say, "no worries, it's already covered" in the midst of panic.

Crispin Cowan
Chief Research Scientist, WireX

1. Variations on the "Love Bug" active content transmission vector that exploit Microsoft's wide-open desktop architecture will be used to deliver much more damaging payloads. Dangerous payloads may include stealthy payloads that infect the machine and then lay dormant, waiting for some particular time or condition to occur. Worse, the payload may be coded to look for a particular person, steal particular secrets or keys, and mail them home to effect industrial or military espionage.

2. "Format" bugs as prototyped by the WU-FTPD bug in June, will grow to rival buffer overflow bugs in 2001, in all kinds of networked systems. However, because format bugs are much easier to detect and control than buffer overflows, the problem will fade, and by 2002 buffer overflows will again be the dominant problem.

And the last word on 2001 from …

Peter G. Neumann
Principal Scientist, Computer Science Lab,
SRI International

Compared to what could happen, computer security misuses have been mostly ankle-biters – with denials of service, penetrations, and insider misuse relatively limited in scope, and some extrinsic misuse such as privacy violations. Consequently, there have been relatively few incentives to dramatically improve our security. We are likely to see some organized, possibly collaborative, attacks that do some real damage, perhaps to our critical infrastructures, perhaps to our financial systems, perhaps to government systems—all of which have significant vulnerabilities. Unfortunately, such misuses may be needed to inspire fundamental improvements in system and operational security.

2001 Planning Calendar for SANS Educational Program:

SANS Security New Orleans 2001

January 28-February 2, 2001
New Orleans Marriott, The French Quarter
New Orleans, Louisiana

Here you will find all seven of the SANS GIAC immersion tracks:
- **Kick Start**
- **Security Essentials**
- **Firewalls and Perimeter Protection**
- **Intrusion Detection**
- **Hacker Exploits and Incident Handling**
- **UNIX and Linux Security**
- **Windows Security**

Plus a dozen one-day courses on a variety of current security topics.

SANS 2001 (The largest security training conference in the world)

May 21-28, 2001
The Baltimore Convention Center and Hyatt Inner Harbor
Baltimore Inner Harbor, Maryland

At SANS 2001, you can take any of the immersion tracks listed above or choose from among 40 other full-day courses, a management conference and a five-track technical conference. You'll also find one of the largest security tools expositions at in the world.

SANS Network Security 2001

October 15-22, 2001
Town & Country Conference Center
San Diego, California

All of what you'll find at SANS'01, plus more advanced security briefings.

Regional conferences with smaller selections:

- **February 12-15, 2001 – Sydney, Australia**
- **April, 2001, – Chicago, Illinois**
- **June 20-23, 2001 – London, England**
- **July, 2001 – Washington, DC**
- **August, 2001 – Ottawa, Ontario, Canada**
- **November, 2001 – Seattle, Washington**

For updates on all these programs, see the Events section at www.sans.org

You don't have to travel to a SANS conference to master the materials! You can take many of SANS' most popular programs online. See www.sans.or/giactc.htm

Certification Update

1. New book on Intrusion Detection from the certification process and participants

Six weeks ago, Stephen Northcutt put out a call for authors on the GIAC Daily Incidents Report (www.sans.org/giac.htm) for volunteers to develop an advanced book on intrusion detection signatures and analysis. Several recent GCIA (GIAC Certified Intrusion Analyst) graduates banded together under the leadership of Matt Fearnow and the respected New Riders Publishing has agreed to publish it. Working together, the team has already delivered the first four chapters, and the book "Intrusion Signatures and Analysis" is expected to be in print January 2001. The book is based on the best GCIA student practicals (http://www.sans.org/y2k/analysts.htm) and will be the most comprehensive technical book on intrusion detection ever written. This is another example of the power of the community working together to improve the defensive state of practice.

2. Sample Practicals that are also tutorials for every intrusion detection analyst

To earn GIAC certifications, students must pass a test and complete a practical exercise demonstrating real mastery of the material. More than a two hundred of these practicals on Intrusion detection alone are posted at http://www.sans.org/y2k/analysts.htm, and hundreds more are posted at http://www.sans.org/giactc/cert.htm in five other categories of security mastery, providing a rich teaching and research resource for the entire security community—and it grows every week.

If you are involved in advanced security and/or intrusion detection, and/or in correcting the Top Ten Internet Security Threats, take a look at the following examples of practicals completed by two Certified Intrusion Detection Analysts students and one Firewall and Perimeter Protection Analyst. They are not only great analyses of issues; they are also valuable tutorials. The first two cover the top two threats on SANS Top Ten Internet Security Threats list.

Lenny Zeltzer: http://www.sans.org/y2k/practical/Lenny_Zeltser.htm
Dustin Childs: http://www.sans.org/y2k/practical/Dustin_Childs.doc

The third shows how to block the ports on Cisco routers that are most commonly attacked and scanned and how to test your settings.

Donald J Kuntz: http://www.sans.org/y2k/practical/Donald_Kuntz.doc

You can use the search engine (http://www.sans.org/search_query) at any time to find unique papers and the other resources at the SANS Institute site.

Hardening Scripts

One of the most important tasks for a system administrator is setting up new servers safely. Fail to do that and your machine can be compromised in minutes.

More than 40 experts in the SANS community worked together over a full year to created two elegant and effective scripts. They are available now. There is no cost.

For Solaris:
http://yassp.parc.xerox.com/

For Red Hat Linux:
http://www.sans.org/newlook/projects/bastille_linux.htm

SANS

The SANS Security Alert is published as a service for SANS students, certification candidates, and alumni. Order additional copies at http://www.sansstore.org.

There is no cost for up to 10 copies for SANS alumni; Others: $12 for a single copy; $7 per copy up to 50. $4 per copy up to 200. $3 per copy over 200. Plus shipping.

Security Self Assessment

Do you know the fundamental concepts and technologies of information security? At least well enough to pass over the Kick Start Level of your security education and certification program? Try this self assessment, and if all eight answers are obvious to you, skip Kick Start and go right to Security Essentials. If you answer six or more questions correctly, you may skip Kick Start, but a score of five or fewer means you will benefit from mastering Kick Start before attempting some of the more advanced materials.

1. Which of the following best describes the three pillars of Information Security?

(a) Firewalls, Patches, and Incident Handling
(b) Encryption, Certification, and Training
(c) Confidentiality, Integrity and Availability
(d) Policy, Prevention and Protection

2. Which of the following best describes Two Factor Authentication?

(a) A Logon and a Password
(b) Something You Have and Something You Know
(c) Challenge and Response
(d) Diffie-Hellman Two-way key exchange

3. Which of the following best describes the three main IP protocols?

(a) SMTP, FTP, HTTP
(b) IGMP, TCP, UDP
(c) X.509, X.400, X.15
(d) TCP, UDP, ICMP

4. Which of the following best describes the number of bytes in a Megabyte?

(a) 2^{10}
(b) 2^{20}
(c) 2^{30}
(d) 2^{40}

5. Which of the following best describes the ATTRIB bits in the FAT32 File System?

(a) Read-only, Archive, Hidden, System
(b) Read-only, In-Use, Hidden, System
(c) Read-only, Archive, Master, System
(d) Read-only, Archive, Hidden, Temporary

6. Which of the following best describes how to view a hidden file in Unix?

(a) Start -> Programs -> Unix Explorer -> View -> All Files
(b) list –all (list – all in linux)
(c) ls -a
(d) dir /a

7. Which of the following best describe the three methods of risk assessment?

(a) Accept, Mitigate or Transfer the risk
(b) Quantitative, Qualitative, Knowledge Based
(c) Government, Contractor, Wing it
(d) Dynamic, Static, Adaptive

8. Which of the following best describes RAID technology?

(a) It is a process to kill software errors or bugs dead.
(b) Redundant Array of Inexpensive Disks approach to mass storage.
(c) RAID is a Hacker Conference held in Las Vegas yearly.
(d) Real time Access of Information and Data, high-end data storage.

Answers are posted with explanations at www.sans.org/giactc/quiz1299.htm

DECEMBER 2000

SANS SECURITY

ALERT...ALERT...ALERT.

Expert Predictions for Security Trends In 2001

Here's a chance to peek inside the crystal balls of several of the nation's thought leaders in information security. We begin with predictions by the SANS folks and by Bruce Moulton, the dean of the chief information security officers, and follow them with targeted predictions from ten of the most respected security consultants, vendors, users, and researchers.

continued on page 3

TABLE OF CONTENTS

Security Awareness UPDATE

On September 4, 2000, SANS invited the security community to help build a world-class security awareness course for general computer users that had significant, relevant content and included comprehension tests. The course will help anyone who serves as a system, network or security administrator for three reasons:

- An education program developed by over hundreds of security professionals is comprehensive and credible—one that users will be inclined to accept.
- A security-aware user is more likely to make the right choices.
- Users who pass the test would be accountable for knowing what they should do.

In the first three weeks, we received over 350 submissions, many showing impressive insight. Some overlap; about half are related to password management and email issues. Stephen Northcutt has been working late each night assessing and categorizing each submission. The current draft of the outline is available at: http://www.sans.org/newlook/projects/cap_outline.htm

Everyone who participated in the project will have access to the entire collection to help select the best papers. We will also post awareness-related projects written by students in the Information Security KickStart program (http://www.sans.org/giactc/kickstart_info.htm) so we can all access and evaluate multiple styles and ideas on the best way to present the material. Watch the progress of the project through statistics posted at http://www.sans.org/newlook/projects/cap_welcome.htm

If you want to help make the project successful, please write us at awareness@sans.org. Our goal is for the final product to reflect the combined wisdom of over 500 security professionals.

SANS INSTITUTE

5401 Westbard Avenue
Suite 1501
Bethesda, MD 20816