the Future of Information Security

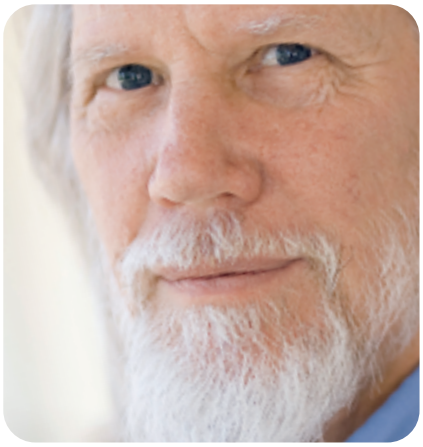
WHAT WILL INFORMATION SECURITY look like 10 years from now? Will it evolve or be radically different from today? We posed these questions to information security's leading thinkers and industry luminaries. Read on for their predictions and a peek into what the future may hold.

INSIDE

INFORMATION SECURITY®

The View from Visionaries

IN 10 YEARS, information security as we know it may not exist. Rather than a separate product, it may simply be embedded into everything. Or Web services may upend traditional enterprise security. We asked some of the best and brightest minds in the business what they see ahead and the answers were far ranging: everything from from attacks masked heavily with encryption to zombification of corporate networks. Some predict radical changes while others foresee more of the same. Read on for a peek into what the future may hold. COMPILED BY MARCIA SAVAGE



1 WHITFIELD DIFFIE

Vice president, Sun fellow and chief security officer, Sun Microsystems

Today, when we say that a company is doing its computing securely, we usually mean that it is doing the computing on its own computers and that it has taken whatever means are appropriate to protect those computations. In 10 years, no major business computation will be secure in this sense. Today, every developer, manager and marketer uses Google a dozen times a day. In 10 years there will be thousands of Web services that, like Google, do things that you cannot realistically do for yourself. When this happens, what we call security today will have vanished forever.

2 MARCUS RANUM

CSO, Tenable Network Security

Vulnerability pimps—excuse me, "security researchers"—will continue to publish flaws in critical software, saying that it's a crucial part of the process of making it better. Since this process has been going on for the last 10 years, and software hasn't gotten better, it will likely not get better in the next 10 years either. Meanwhile, the vulnerability pimps will keep buying and selling vulnerabilities and using them as marketing vehicles for their consulting services.

3 MIKKO HYPPÖNEN

Chief research officer, F-Secure

Within the next 10 years, the main focus of the Internet will shift from West to East: Asian Internet users will outnumber American and European users 10-to-1. As a result, English-language [websites] will become a small and insignificant part of the big picture; most of the action will be elsewhere. This also means that over the next years, hundreds of millions of new computers will get online in China, India and elsewhere in Asia. How well will these computers be protected?

Internet access becomes ubiquitous, like electricity. People won't notice it any more. Everybody assumes that all devices have connectivity. This includes phones, MP3 players, cars, fridges, watches…and this of course brings us an entirely new set of security problems.

Wireless attacks could become a major headache. Imagine Wi-Fi Windows viruses, jumping from one laptop to another just because they are too close. Such Wi-Fi worms could spread between office buildings because of proximity, bypassing corporate firewalls and other safeguards. And they would be spreading globally like biological viruses: when people travel with their laptops.

4 ALAN PALLER

Director of research, SANS Institute

The next three years will see a cascading transformation from soft security skills (policy/writing/awareness training) to hard security skills (attack exploits, intrusion detection, isolation and segmentation). The director of one of the largest security consulting firms in Washington painted the picture most starkly, saying, "Eighty percent of our employees have soft skills and only 20 percent have hard skills. If we don't reverse that ratio within the next two years, we'll be out of business." The reason for the change is that the attackers have identified ways of beating the current defenses, creating push-back from executives who ask, "What do we need to do to stop these penetrations?" The answer increasingly is, "Replace soft skills with hard skills so your people can actually find the attacks, clean them up, and stop them from recurring."

5 PETER G. NEUMANN

Principal scientist, computer science lab, SRI International

Big security problems [ahead]: First, pervasively imbuing system developments with good software engineering practices and trustworthy system architectures (encompassing security, reliability, human safety, survivability in the face of many realistic adversities, networking, interoperability, evolvability, operationally aware, and so on).

Second, having small, proven operating system and application components that can be predictably composed into bare-minimum subsystems and used to develop trustworthy systems tailored to specific needs. Examples: trustworthy special-purpose servers such as file servers and network servers that might otherwise be looked at as stark subsets of general-purpose systems.

Third, securely and predictably embedding good cryptography into trustworthy systems, and fourth, pervasive education on how to build trustworthy systems.

6 BRUCE SCHNEIER

CTO, BT Counterpane and author of Beyond Fear: Thinking Sensibly About Security in an Uncertain World

Computer security is poised for a major transformation: from a consumer product to an industry product. As computers and networks become infrastructure, users—both individual and organizational—will care less about how security works and more that it simply does work. Security will cease to be a separate product, and instead will be embedded into everything. This isn't to say that security will lose its importance—far from it—only that the security marketplace will more resemble other industry marketplaces: new automobile technologies, for example.

7 MARK LOVELESS

Vernier Networks, senior security architect and white-hat hacker known as "Simple Nomad"

While the main short-term security threat still appears to be compromised home systems as a part of a botnet sending spam, spreading malware, and DDoS, these issues will begin to surface more and more in a corporate environment. This can be symbolized in the case [earlier this year] of Viagra spam being sent from zombified desktop computers in the Pfizer corporate network (ironically the makers of Viagra) to systems on the Internet. With the dynamic nature of networks, systems that are not protected by sophisticated networks that regulate access will find themselves targeted more frequently as potential unwilling botnet participants. I would expect with the recent trend of sales of zero-day security flaws in modern software to criminal elements that the overall zombification process will make greater gains in corporate networks than ever before.

8 HOWARD SCHMIDT

Former White House cybersecurity adviser, president and CEO of R&H Security Consulting

The trend in the next five to 10 years will be to significantly increase security professional certifications…in the various disciplines—for example, secure application development and governance. We'll [also] see IT professionals who aren't necessarily security people getting the same sort of certifications that have traditionally been reserved for security folks.

Data lifecycle is a problem we'll have to struggle with—that's how to create data that has a specific life term where

it's good, for example, long enough to get a credit card issued then it self destructs. …The whole data management issue—how to find and keep data, the encryption issues—is something we'll be dealing with for the next five to 10 years.

Lastly, we're struggling with the whole concept of identity management. This is truly a global issue. …We need to develop a new world system that basically allows us to control our identity and thereby gives us the ability to protect it and ensure that if it is compromised, we can recover it in a relatively short amount of time without depending on everybody else in the world to protect us after something bad has happened.

9 MARTIN ROESCH

CTO and founder of Sourcefire and creator of Snort

The threat community will continue to accelerate and become more sophisticated. As the rate of release and sophistication of threats increases, it will become increasingly difficult to characterize those threats ahead of time.

Attackers will concentrate on end hosts more than ever as a way to leverage access to critical servers in ways that are difficult to detect. Encryption will also be used more heavily to mask any overt attack methods as well.

Defenders will have to rely much more heavily on awareness technologies to understand the operational environment that they're protecting and change in that environment that heralds security events. They will also need much heavier automation to perform analysis of data coming out of the environment and to take action when security events happen in order to have response in relevant timeframes.

Host-based defenses will become critically important as the trends of rapid exploit development, client-side attacks and near-pervasive encryption combine to limit the effectiveness of intrusion prevention systems, firewalls and content-analysis systems.

10 MARCUS SACHS

Director of SANS Internet Storm Center

The virtual world certainly has come of age this year—Second Life, World of Warcraft, EverQuest…. The criminals have just started to take notice of this, and the Chinese [cybercriminals] in particular have begun to figure out you can make money in that world. …Zero-day attacks have kind of fallen off, but I don't think they'll go away. There's a lot of interest in being the first one on the scene, not just with the vulnerability but the exploit that goes with it.

Hacking new devices [like the iPhone] will be a growing threat. In a lot of cases, it's proprietary [technology], so there's the thrill of the hunt to be the first one to say, "I've cracked this closed product." Young kids who want to make their mark on the world by defacing a Web site or breaking a Microsoft application—that's so last year. …Teens and preteens, as they come of age and the adolescent disruptive mindset starts to grip them, they'll want to break the things that they've been using, and they've been using texting, instant messaging and hand-held devices. Microsoft has gotten pretty good at the patch cycles, but can you imagine how hard it would be to get updates to cell phones, iPods, iPhones, and Bluetooth [devices]—the gadgets that will rule the coming years?

High-end cars are coming [equipped] with Bluetooth and it will continue to penetrate more common cars. …With Bluetooth, you get a lot of nice conveniences but you also get the introduction of insecurity. …BlackBerry service was out for a day [in April]. We can see how disruptive that can be to our society should someone find a common vulnerability in Bluetooth or in BlackBerries that causes a denial of service, not just theft or fraud.

Photograph by EMILY NATHAN

Warning Signs

Today's online games illustrate tomorrow's security problems. BY DENNIS FISHER

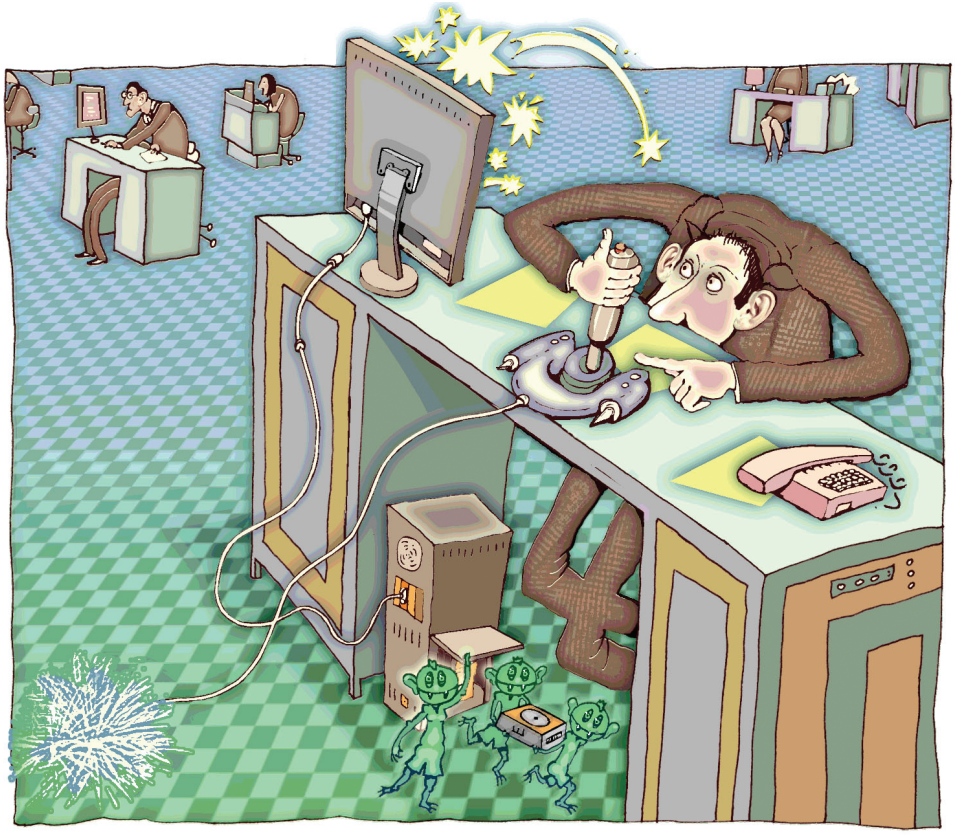


Illustration by VICTOR GAD

IF YOU WANT A PEEK at the future of software threats and security, look no further than the alternate universe that is online gaming.

Once the exclusive domain of erstwhile Dungeons & Dragons enthusiasts with too much time on their hands, online games such as World of Warcraft, EVE Online and The Lord of the Rings Online attract players from across the demographic spectrum and are generating hundreds of millions of dollars in revenue for their creators. World of Warcraft has more than 9 million registered players, and even casual players readily drop hundreds or thousands of dollars on monthly access charges, transaction fees and in-game purchases.

Inevitably, all of the real dollars, euros and yen flying through the air in these fantasy worlds are attracting the attention of skilled online criminals looking to make an easy score. Hackers have begun writing custom Trojans and keyloggers designed to steal players' account information, which they use to make fraudulent withdrawals from bank accounts or to sell characters and goods in online games. This new reality has raised some serious security concerns among players and game developers. And those concerns are beginning to make their way into the enterprise as well, as security staffs are forced to confront the risks associated with employees using company machines to play these games.

But it's not just the security of the games that is so worrisome. The larger issue, experts say, is what these problems say about the future of enterprise security in an environment in which applications are increasingly hosted remotely and built on technologies such as Ajax, JavaScript and XML. If the present is any indication, the future is bleak, experts say.

"Our software systems are moving to new architectures that are massively distributed. As people adopt service-oriented architectures, the new generation of applications will look just like the massively multiplayer online role-playing games [MMORPGs] we see today," says Gary McGraw, CTO of software security firm Cigital and co-author of *Exploiting Online Games*, a book about game security published last year. "Most people who build software don't think the way that security people think. It was always about network security before, but now it's about making software work better. Warcraft has like 9 million users and 400,000 are online at any given time. That sounds an awful lot like an SOA design."

PROBLEMATIC ARCHITECTURE

Most MMORPGs such as World of Warcraft install large pieces of client software on users' machines that communicate with one of the game's remote

servers. It's a straightforward architecture, except there are hundreds of thousands of players in the game at one time, all needing to see the same game action at the same time.

"The security model has to involve trying to control the state of the game," McGraw says. "But the only way to do that is to crack off a piece of the state of the game and give it to each user. If you don't think about security, that sounds like a great idea. But if you realize that users might try to manipulate the program, it's a really bad idea."

That architecture is similar to the way companies such as Google and others are building their applications. Many of Google's offerings, such as Gmail and Google Docs, are Web-based, but others, like Google Desktop, sit on the user's PC gathering large amounts of data and communicating constantly with Google's servers. This model requires a high level of trust between the application server and the user's PC, something that can be problematic if the user has some malicious tendencies.

"The average security guy can talk about trust in a very clear way, but in the case of putting a fat client on an attacker's PC, there's a big trust model problem," McGraw says. "This piece of software you're running on the attacker's PC is outside the trust boundaries."

WEB SERVICES

Meanwhile, following the lead of vendors like Salesforce.com and NetSuite, Microsoft and other major software providers are making many of their applications available as Web services. Microsoft Office is available for use online, for example. This shifting architecture makes security a challenge for application developers and enterprise security staffs, most of which are more accustomed to dealing with network security challenges and patching desktop applications than dealing with distributed applications.

"The likelihood is that the exploits that are successful against these gaming environments will be successful against Web applications too," says Avi Rubin, a professor of computer science at Johns Hopkins University and founder of Independent Security Evaluators. "Authentication becomes much more important in this environment because the data is now stored in the network, and if someone is able to get your credentials and break into the application that stores all of your data, it's a much bigger problem. The application becomes a huge target." ›

Web of Worry

Security researchers say attackers will exploit Web 2.0, VoIP and virtualization vulnerabilities. BY BILL BRENNER

WITH WEB 2.0 TOOLS LIKE Ajax all the rage and companies snapping up VoIP and virtualization technologies, security researchers are worried about what's ahead in the next decade on the security horizon.

Businesses are so eager to acquire the capabilities of these technologies that developers are churning out programs with little thought to security. As a result, the corporate world is basing huge chunks of the business on programs riddled with vulnerabilities. The underground realizes this, and is quickly coming up with ways to exploit the technology, mostly with the goal of stealing sensitive data that can be monetized.

For security researchers who have been piecing together a picture of future threats from their labs, there's little doubt that enterprises will pay a price for throwing security to the wind as they satisfy their craving for Web 2.0 technology.

"There's a big rush today to take advantage of Web 2.0 applications, VoIP and virtualization," says Iván Arce, CTO of Core Security Technologies. "Because security is not a high priority in the rush to deploy, it will probably end up hurting enterprises tomorrow."

In the next two years, experts agree, companies will start to suffer the consequences of all this insecurity.

WEB 2.0 ATTACKS ABOUND

In the research lab at SecureWorks, the consensus is that exploits targeting Web 2.0 technology will be the dominant threat in the next couple of years, says senior researcher Joe Stewart.

"What I see in development are more Web-based exploits. More people are putting out these turnkey attacker kits like WebAttacker, Mpack and IcePack *(see "Attack Toolkits," p. 7)*, he says. "A commodity market has sprung up around these tools, and its authors are making more money as they add new features."

Also worrisome is that more third-party ActiveX controls are being worked into business applications. With third-party ActiveX controls, it's up to the user to find the necessary fixes, whereas ActiveX controls built into Windows can be fixed via a Microsoft security update, Stewart says. More Trojans are taking advantage of third-party ActiveX controls since

updates are less frequent.

"Average users are sitting ducks," he says. "The more of these they install on their machines, the more vulnerable they are."

Ed Skoudis, a SANS instructor and founder and senior consultant with consulting firm Intelguardians, shares Stewart's concerns.

"Browser scripting attacks are something that concerns me a lot," he says. "With Web 2.0, we have millions of people surfing to Web sites to view content posted by hundreds of thousands of people. Google, eBay, MySpace and YouTube are all based on this model. If someone posts evil browser scripts along with their content, the bad guy can gain complete access to the browsers, and worse yet, the network infrastructure on which the browsing machine resides."

The threat is especially dire in the enterprise, Skoudis says, because companies have Web enabled most major applications and use browsers to manage critical IT infrastructure.

"Consider this scenario: we have an enterprise application, perhaps an e-commerce application, an enterprise security tool, or the cash management system of a bank," he says. "Suppose that the application logs various aspects of given transactions, such as transaction variables, date, time, etc. Also, it will likely log the user agent string presented by the browser of an application user. I've seen attacks in which the bad guy puts a malicious browser script in their user-agent string of the browser. They then engage in a transaction, leaving that malicious browser script in the application's logs."

Then, Skoudis explains, when an administrator uses a browser to access a Web-based application to view the logs, the attacker's script is delivered to the admin's browser, where it runs. It can then do anything in that application that an administrator can do, such as transferring money or shutting off security. "As we move more of our applications to Web services, the threat grows even bigger," he adds.

VoIP AND VIRTUALIZATION DANGERS

When looking at threats surrounding VoIP and virtualization, researchers see the potential for everything from VoIP-based spam to server attacks accomplished via vulnerabilities in virtualization programs.

One might expect VoIP security is better today than it was three years ago, when experts started sounding alarm bells. But according to several industry experts, VoIP security hasn't improved much *(see "VoIP Vulnerable," p. 8).*

Himanshu Dwivedi and Zane Lackey of security firm iSEC Partners warn that VoIP protocols such as IAX and H.323 remain open to easy exploits. The latter, they say, is particularly vulnerable to attack but that most users assume it's secure because there has been little evidence to the contrary.

Dwivedi says it's important to shed light on the threat because VoIP use has exploded in the last three years without much consideration of the security risks. Lackey agrees, saying, "While companies are in the same mindset with VoIP as they were a couple years ago, there are more and more tools out there that can be used to both attack and defend it."

While the security implications of virtualization are cloudier, Core's Arce is convinced of a gathering threat there.

"I see big implications for virtualization, though the impact isn't yet clear," Arce says. "Flaws in the technology could be used to disrupt virtual environments, and if you run a bunch of virtual machines on a server and that server

Malware

ATTACK TOOLKITS

CYBERCRIMINALS ARE CHURNING OUT TURNKEY TOOLS TO EXPLOIT WEB 2.0 VULNERABILITIES. HERE ARE THREE EXAMPLES:

WebAttacker This malware creation kit was reportedly developed by a group of Russian programmers and requires minimal technical sophistication to use. Its scripts are designed to make computer infections easy and include spamming techniques to trick users into visiting specially rigged Web sites.

Mpack Russian programmers are also believed to have created this PHP-based malware kit, which was released in December 2006. A new version is released about once a month, and it has reportedly been used to infect up to 160,000 machines with keyloggers. It's sold as commercial software on the black market for anywhere from $500 to $1,000.

IcePack This tool is similar to Mpack and is regularly tweaked to target the latest vulnerabilities, but at $400 is cheaper to acquire.

–BILL BRENNER

is compromised, there could be a lot of damage. The flip side of using virtualization to reduce your number of servers is that you can do more damage by hitting fewer servers."

Some of the dangers associated with the technology surfaced earlier this year, when virtualization giant VMware was forced to fix 20 security holes. The flaws plagued all supported versions of VMware ESX Server, VMware Server, VMware Workstation, VMware ACE and VMware Player. The company quietly acquired host intrusion prevention vendor Determina to help bolster its defenses from within, but has offered little by way of a clear security vision.

WORDS OF ADVICE

So what's an IT professional to do given these threats? SecureWorks' Stewart says IT shops need good policies for the interactive content that people are allowed to use. The safest measure, though unpopular he admits, is to forbid Internet Explorer from using ActiveX controls. "Don't let users arbitrarily decide which ActiveX controls to use," he says.

Matasano Security researcher Thomas Ptacek's advice is something IT pros have heard time and again in the wake of high-profile data breaches: "Stop thinking about flashy, blinking-light security and focus more on segmenting—carving up the network to block people from sections they shouldn't be able to access."

Those who heed that advice will be better positioned to minimize the damage from Web 2.0-based attacks because the crown jewels will remain out of the bad guys' reach, he says.

Skoudis advises approaching browser scripts with extreme care.

"You may want to use a different browser and a different computer for managing infrastructure apps versus the browser you use to surf the Internet," he says. "For example, you might use Firefox to surf the Internet, and Internet Explorer for managing internal applications."

He also suggests deploying an HTTP proxy or even a network-based IPS tool that can filter out malicious browser scripts. Not all of the tools can detect or block malicious browser scripts, but some can, he notes.

Finally, Skoudis says, IT pros must look at the script-filtering features of their Web-enabled applications.

"They should filter all scripts that come in as part of user input, and filter what goes out as well, removing scripts," he says.

Threats

VoIP VULNERABLE

SECURITY RESEARCHERS SAY VoIP PROTOCOLS ARE SUSCEPTIBLE TO EAVESDROPPING AND OTHER ATTACKS.

Security experts have repeatedly warned that companies are rolling out VoIP with insufficient attention to security. At the Black Hat USA 2007 conference in Las Vegas earlier this year, Himanshu Dwivedi and Zane Lackey of digital security firm iSEC Partners demonstrated various ways attackers can exploit three VoIP protocols: SIP, IAX and H.323. Attackers can exploit weaknesses in the protocols to:

- *Listen in on VoIP conversations*
- *Steal sensitive information*
- *Create havoc through denial-of-service attacks*
- *Impersonate certain people on a call*
- *Sniff out IDs, timestamps and certain hashing functions*

—BILL BRENNER

Illustration by HARRY CAMPBELL