Next Steps Towards Internet Security

Testimony Before the Joint Economic Committee of the U.S. Congress

23 Feb 2000

Mark Graff, Sun Microsystems

The Internet today is a sound platform for commerce, fueling an economic expansion unparalleled in our history. It reliably delivers billions of e-mail messages every day. It makes the miracle of the World Wide Web possible. To many, the Net is fast becoming essential to modern life. But substantial hard work remains before the Internet is as safe and stable as its older cousins, the telephone network and the electrical distribution system.

In this paper I will lay out what I see as the next steps towards Internet security[1]. There is work here for everyone. I have handed out assignments liberally. For government: provide a legislative and regulatory environment that encourages responsible behavior from all parties--but don't "kill the golden goose" with heavy-handed coercion. For the builders of the Internet ("my" industry): use the best techniques you know to make products of the highest possible security quality. For the media: learn and teach that Net vandalism is no cuter than drunk driving. For my fellow citizens: demand the best from those of us who, for now, are in the driver's seat. Oh, and a suggestion for Net vandals: grow up.

Security engineers usually begin a job with what we call a "threat analysis". We ask ourselves, what bad thing can happen?

Nature of the Threat to the U.S. Economy

What are the greatest cyber-threats to American commerce today? They are four; and all were illustrated by the distributed denial of service episodes of early February.
The most obvious threat is the current susceptibility of major World Wide Web sites to simple data flooding, and the weak security at thousands of other sites that enabled them to be used as attack amplifiers. These weaknesses result from out-of-date assumptions and trust models, created by the people who conceived the Net; from old and new engineering mistakes, shortcuts, and trade-offs, instituted as the Internet of today was built; and from the blithe inattention of many Net dwellers today to basic network hygiene.

The second threat is the widespread publishing of "vulnerabilities"—security flaws in the operating systems and servers that bring the Net to life. This activity is most dangerous when the disclosure is accompanied, as is often the case, by the release of free, ready-made software that exploits the bug. The practice is least defensible when the disclosure

[1] My views are based on my experiences at Sun Microsystems, but, unless other stated, do not necessarily reflect the policies or positions of the company.

is launched with no prior notice to the vendor involved, ensuring that the weaknesses will be exploited by Net predators until a patch can be devised, built, tested, and released.

The third threat is the common practice of dramatizing security incidents. The press and others routinely overstate potential losses, exaggerate the technical expertise required to disrupt the Net, and--perhaps most importantly--perpetuate and encourage the narcissistic element of the vandal mentality by accepting and repeating colorful "hacker handles" and "attack names".

The fourth and final key threat is the uncertainty and ignorance that obscure the world created by the other three. Uncertainty: How many networks are attacked each year, by what means, and with what degree of success? What do the losses to commerce total? How much is paid to extortionists, in response to what kinds of threats, enabled by which technical or procedural flaws? Which vulnerabilities have been fixed, but not patched; which discovered, but not fixed; which dormant, and not discovered? Now, ignorance: What do we mean when we say a system or network is "secure"? How can we meaningfully compare the relative security of two similar systems, or the same system after we have installed a patch? To the first set of questions, few who know will answer. On the second set, no one today can say. Yet, to keep the Net safe as it grows, we must measure in order to know.

Trends

I spent almost all of the last decade working for Sun. In working to secure networks, in my involvement with FIRST, in teaming with many other computer vendors and helping to beat the security bugs out of our products, I observed firsthand in the Nineties many of the challenges involved in building and securing the worldwide Internet. Let me tell you about some of the trends that have presented themselves along the way.

On the scary side of the equation:

- Attacks have increased in technical complexity
- Attack tools are increasingly simple to operate, and now are widely available
- Vulnerabilities are now usually routinely announced to the public before a fix is ready

But there’s good news, too:

- Vendor collaboration is increasing
- The public has become aware that security is an important “feature” of a system
- Government institutions are seeking to determine their appropriate roles in securing the Net

To close the discussion about trends, I must, on a personal note, point out another fact of Internet life: a trend, if you will, that never appeared. The security quality of networking software has not improved.

Functionality, what the software can do, has made tremendous advances, of course. So far as I am aware, however, the engineering techniques used by developers have changed

little in the past twenty years. Looking under the hood of all the major operating systems in use today, we find the same kinds of security flaws, coding errors, and faulty assumptions programmers like myself were turning out in the Seventies and Eighties. (To be clear: I made these mistakes in the Nineties, too.) I don't think the relative quantity of bugs has changed much, either. While groups such as the Software Engineering Institute were advancing the state of the programming art, industry, in day-to-day practice, did not advance with them.

The reasons for this stasis are, it seems to me, both economic and practical. Indeed, it may well be that the only way to achieve the rapid, world-transforming progress we have made in global networking was the path taken. Risk, I like to say, is a resource. It is like money: you invest it to get things done. And now that we have reached the point that the Net and the Web are significant (soon to be dominant) elements of our economy, now that we have become so quickly an essential part of the modern infrastructure, the network-building industry needs to step up to our new responsibilities and provide the best security quality in our products we know how. The widespread adoption of a higher standard of security quality must become one of the important trends of this new decade.

Likely Sources of Attack

Let me begin a discussion of "likely sources of attack" by discussing the kinds of attacks I find most threatening.

Most network users, and security experts, would probably list the following "attack types" as the ones to be feared most.

1. Denial-of-service attacks, particularly "distributed" attacks
2. Email "viruses", such as 1999's so-called "Melissa"
3. DNS spoofing, re-direction, and outages.

The first two threats on this list have received so much press lately that I am not going to explain them here.[2] The third, while it has received little public attention, may represent the most acute security weakness of the Internet today. Domain Name Service servers and such other software agents translate computer system names and World Wide Web URL's to the explicit Internet addresses ("IP numbers") needed for packet routing. Over the past three years we have experienced a few small-scale, accidental disruptions in these services. The result in each case was that a segment of the Internet was effectively unreachable for a few hours. An intentional, dedicated, coordinated attack could, I believe, isolate large sections of the Net, perhaps for days.

A question suggests itself here. If such an attack is possible, why hasn't it happened yet?

In general, why have we seen so few substantial attacks against the Net, and the Web it supports? Well, what would be the likely source of such an attack?

---

[2] I can't resist pointing out that since we at Sun run our enterprise largely on the hardware and software we make, our network was one of the largest in the country completely unaffected by the "Melissa" virus—unaffected, that is, except for one unfortunate woman in Marketing who had a terrible time for a few days getting her colleagues to respond to her e-mail. Her name, as it happens, was Melissa.

To answer that, ask another question. *Cui bono*? Who would benefit? The answer I accept is that to date, no sufficient economic or martial incentive has sufficed to motivate a large-scale action. The Net grows larger and more important to us every day, of course.

We should waste none of the time left to us in addressing such fundamental weaknesses as the IP-stack assumptions, mail protocol flaws, and DNS dependencies which make possible the three attacks I have singled out above.

Turning now to the experiences of Sun Microsystems with regard to attacks and losses, I am able to draw a much more positive picture. Both with regard to incidents referred to us by our customers, and those sustained in the operation of our own network, our experience tells us that:

1. Most threats, attacks, and losses come from inside the enterprise
2. Most attacks to date seem to be the work of individuals or very small groups, working alone.

For this reason, Sun has focused the majority of its internal security investment in recent years on the assessment and mitigation of internal risks. We have yet to experience a major loss or outage due to the malevolence of outsiders. (Of course, we have one of the oldest and strongest firewalls on the Net.)

Recommendations for Action

In light of the threats and opportunities I have explored above, I offer the following recommendations for action by the federal government and others. I must emphasize that I make these recommendations as an individual.[3]

To help reduce the susceptibility of the Net and the Web to attack:

1. Encourage site operators and ISP's to install security patches, and to practice the basic prophylactic measures suggested by CERT and many other such groups.
2. Encourage or require the adoption of "ingress filtering" by ISP's and other network routing agents. Encourage the adoption Net-wide of "IP v6" (a new, more secure version of the Internet Protocol) and Ipsec on IP v4. If funds are necessary to promote these efforts, consider the imposition of an "excise tax" on network routers to fund the effort
3. Establish and enforce uniform high standards of security quality in all government networks
4. Promote the use of sound, modern engineering practices in networks developed or managed by the government.
5. Encourage industry to practice the highest practicable standards for software development. Use the government's position as one of the largest computer customers in the world to advantage by setting procurement standards high in the area of security quality
6. Work with the computer and network industries to develop security metrics

[3] Sun Microsystems has not taken a position, so far as I know, with regard to any of these suggestions, and may in fact not support them--except the admonition to install security patches.

7. Work with the computer and network industries to develop standards for security quality. As one of my (non-Sun) colleagues remarked to me, "We already have to comply with UL electrical rules, RF emission rules, OSHA rules, and encryption export rules; why is software security any different?"
8. Facilitate collaboration between members of the industry by ensuring that meeting and working together for the purpose of improving network security is shielded from anti-trust and restraint-of-trade worries

To discourage the publishing and distribution of vulnerabilities and exploit scripts before patches or other preventive measures are in place:

1. Work with industry and academia to find sound alternative methods of spurring the development of security patches and improvement in security quality. Consider a "vulnerability escrow" arrangement[4] wherein the vulnerability would be held in confidence by a neutral third party while the vendor undertook to develop and release a fix within a short reasonable period of time.
2. Note: Punishment for releasing such information is in my opinion both undesirable and infeasible, both out of First Amendment concerns and because of the international and often anonymous nature of these releases. I suggest it *not* be considered.

To avoid encouraging Net vandalism:

1. Fund and/or encourage "security responsibility" educational campaigns in our primary and secondary schools, making sure especially that whenever we hook up another school to the Internet we also educate students, teachers, and administrators about responsible network use
2. Direct government agents and officials, and encourage other responsible figures, to avoid sensationalism in discussing security flaws and incidents. Specifically, do not adopt or repeat without qualification narcissistic "hacker handles" and dramatic "attack names"

To increase our understanding of the nature and scale of security incidents and vulnerabilities:

1. Require all networks managed by the federal government to report "sanitized" and canonical computer security incident statistics to a central collection point such as the FBI Computer Crimes Division. Report the aggregated statistics quarterly
2. Require publication of the same kind of reports from key industries, including the financial community and public utilities
3. Fund academic and industry research in basic security metrics and standards
4. Fund or facilitate the collection, sharing and analysis of security vulnerabilities among industry and government groups responsible for fixing them. If fear of liability is a barrier to the disclosure, sharing, and repair of security flaws, provide legislation to shield and spur the companies for a fixed period of time
5. Support cooperation between industry, academia, and the federal government by creating and funding industry and academic fellowships at the National

[4] First suggested to me by Dr. Eugene Spafford of Purdue.

Infrastructure Protection Center and similar institutions. Support similar "exchange programs" between groups, which we need to more effectively share information.

6. Strongly support the operation of Computer Incident Response teams such as CERT and CIAC
7. Encourage all sectors of American industry, particularly key elements of the infrastructure, to develop and support Computer Incident Response teams
8. Support independent associations such as FIRST, the Forum of Incident Response and Security Teams, to foster communication and coordination amongst security experts world-wide

Conclusion

Because security is the mother of liberty, those of us who love liberty must work to secure the Internet. The Net is the marketplace, the workshop, the printing press, and the town hall of the 21st century. If we fail to protect either its commerce or its communications, we are choosing to deprive future Americans of the societal sense of safety, surety, and stability that is one of the necessary conditions for freedom.