Global Information Assurance Certification Paper

Consumer Labeling for Software Security

Abstract

Computer security is in a terrible state both in the corporate world and for home users. The foundation for many computer security problems is naiveté. While we can't totally solve this or any other security problem, there are steps we can take to improve computer security. For corporate computers, the answer is twofold: make security a priority for the organization and get security expertise either by hiring or training. But what can we do for home users? They cannot afford to hire consultants and cannot be expected to learn much about computer security before using their computers. What can we do to improve security for people who don't want to learn technical topics? I propose a security label inspired by the "Dolphin-Safe" tuna can label.

The early Internet culture

When the IP protocol was being invented, the researchers were mainly concerned with getting things to work. Any diagnostic information that could be given to another site attempting to connect to your machine was freely given and gratefully received. If you tried to connect to a port with no service running, you would get an ICMP port unreachable message (Braden 1) (Braden 2). This helped the people at the other site figure out what went wrong. There was general understanding that computers were vulnerable but most users were professionals and there was a collegial relationship of honor and trust among the early Internet sites. Many of the IP protocols assume that while you might not trust a user, the system administrator is a trusted, reliable person. This distinction is inappropriate now that most computers have a single user (Callas).

In 1988 the Morris Worm exploited 3 known vulnerabilities: a debug mode in sendmail, a buffer overflow in **fingerd**, and weak passwords through the r-commands. (Page) That such vulnerabilities would remain uncorrected in the dawn of the Internet is not surprising. That similar vulnerabilities remain in the face of multiple, credible threats is astonishing. We need to grow up.

The problem

The level of computer security risk is worse now than it has been before. This is due to both higher vulnerability and to increased threat. Vulnerability is weakness, the susceptibility to attack or failure. Threat is the likelihood of an attack or failure. For instance, leaving an extra port open is a vulnerability. The possibility of someone trying to break into the port is a threat.

Vulnerability

Computer security vulnerability takes many forms but can be broadly categorized into the following: confidentiality, integrity, and availability.

Confidentiality means protecting access to secret information. A poorly chosen password may allow unauthorized access. The browser may store lists of the search keywords that have been used. Unknown ports may be open, allowing an unexpected connection. The virtual memory system writes copies of conceptually ephemeral information to the hard drive. The overlooked floppy drive may allow a cracker to boot the computer to another operating system and steal files.

Integrity means maintaining assurance of the content of information. A computer crash may mangle file contents. Or, the computer may crash just before you were about to save your file. A user may inadvertently overwrite useful information or save it in a wrong format.

Availability means being able to use your computer. Loss of use is probably the most common vulnerability. The power fails while you are working on your computer. The computer may fail to boot when you need it. Your ISP may fail to connect you to the Internet. The eCommerce site you want to shop from may not respond.

Some vulnerabilities cross multiple categories. If you find out someone was using your computer, but you don't know what they did, then both confidentiality and integrity are at stake.

The increased vulnerability is mainly due to complexity. Our computers are far more complex than computers of twenty to forty years ago. Modern computers run software from disparate vendors on multitasking virtual memory operating systems. This software runs on a wide range of hardware, some of it dynamically reconfigurable. Does anyone still understand the whole system at a detailed level? A simple system where the user understands all the parts is much easier to secure. Adding to the complexity, few computers run in isolation any more. Computers must be understood in the context of the network they live on, including network hardware and interactions with other computers across the network.

Compared to a single-user PC, the network adds two whole new categories of vulnerability that previously were only of concern on multiple-user computers: authentication and accountability. The question of authentication is how do you establish who you are? The operating system on most home computers still doesn't care. Once you're on the network authentication becomes important. How do you know if that email is really from your boss? Accountability means keeping track of who did what. If several people share a password, one of them can make a change and deny that he did. There's no way to pin the action to the person. This issue doesn't come up on a single-user PC, but as soon as you connect to a network it's important.

There is some question of how much of this complexity is really needed (Callas), but basically, computers would not be as useful if they were less capable. This complexity makes them more vulnerable.

Threat

The increased threat is mainly due to connectivity. Back when someone had to have physical access to get to a computer, only local attacks were possible. Now a computer connected to the Internet may potentially be attacked from any other computer on the Internet. Worse, crackers now have more reason to want to break into every computer. Modern PCs, especially those with broadband Internet connectivity, are a resource for proxy attacks where a cracker uses 'captured' computers to attack a target computer. The use of captured computers ranges from simply providing the cracker anonymity to coordinating massive parallel attacks. Every computer connected to the Internet is now a target of crackers looking for dupes to use in these remote attacks.

In summary the increased risk is a direct result of the improved technology making computers both more useful and more accessible.

Chaos on the desktop

Home users have an even bigger problem. While IT professionals are used to thinking in abstract terms about software, most home users don't have this background. Probably all new users have a vague fear that the Internet is dangerous, but what to do about it? Even beautiful, easy-to-use tools like ZoneAlarm require a conceptual understanding that many people find difficult to learn. Anti-virus software has matured to the point where little technical competence is needed to use it. This helps, but is not sufficient to secure a desktop and may give some users a false sense of security.

When we first start using computers, we are focused on what the computer can do. When you look at a software product box, that's what you see. After all, we get computers for what they can do. The security implications of most software products are side effects to the main purpose. A user will pile on software to perform more and more functions without regard to security. After all, the software products don't come with warning labels like "This software opens two ports and you are depending on our software quality to protect those ports." No, the box touts the features, and that's what the user wants.

The current state of the art in operating system robustness is challenged to even run properly with the plethora of often-incompatible software the naïve user puts on it. Developers often don't check or don't understand security implications of their code so that security quality is often poorer than functional quality. Even setting that aside, the way the program is configured is unlikely to give weight to security concerns. Popular word processing and spreadsheet applications allow macros by default.

Even an experienced user might have trouble finding out the security implications of a product. How do you know what information is being sent back to the manufacturer? Few users have the know-how to find out on their own. ZoneAlarm can tell you the product is trying to send information, and Ethereal can tell you exactly what was sent.

But, few users are that sophisticated. And, if the product requires registration and makes an SSL connection from proprietary object code for which you don't have source code, even a security professional might not be able to figure out what information was sent.

For the present, such sophisticated concerns must hold a back seat to the more credible threats. There are enough gaping holes to be dammed that such unlikely leaks are a waste of time. The basics must be handled before asking about esoteric attacks.

Perception

Part of the problem is perception. We haven't learned to see computers through the wary eye of experience. If you build a wall around your house, you can look at it, compare it to other walls you've seen. Perhaps judge it against your experience breaking or scaling walls. But when you build defenses around a computer system there will be less correlation to physical experience. Worse yet, sometimes thinking from physical experience can be misleading. If I'm alone when I send an email, it feels private.

The comforting solidity of the door to the computer room can allay our concerns about security, but has no bearing on whether the computer system can be taken via its internet connection.

We hope that IT professionals won't need to be direct victims of cybercrime to wake up. But, it seems to be an uphill battle. In the economic pressure of a competitive industry, managers are constantly working the edge of the envelope. A trial system might be connected to the Internet directly, since, after all, no one knows about it. New software may be given cursory or no security testing. Crackers with specialized knowledge will attack the software that was built by programmers who either lack specialized security knowledge or were not given enough time to check their software for security vulnerabilities.

Naiveté

The weakest link in any computer security regime is the people implementing it. This problem is not unique to the computer security profession. As Gerald Weinberg says "It's always a people problem" (Weinberg). There are many reasons why people don't implement security properly, but one of the biggest is that we are naïve. By this I mean that we are trusting because we are uninformed.

All of these computer security issues have naiveté as a root cause:

- Lack of policy
- Conflicting demands on time
- Rush to incorporate new features
- Not knowing how to secure a computer
- "No one would care about my system" attitude
- That happens to other people

- Assuming the default configuration is good enough
- Lack of understanding of configuration tradeoffs

Managers are reluctant to spend money on security policy because their customers aren't willing to pay for the extra hardware needed for better security. People don't see the benefit of security, but the cost is clear. There are how-to guides on setting up computers for enhanced security, but they are still not delivered with the computer. Everyone is now a target of crackers looking for DDOS robots, safe places to cache data, and relays for obfuscating their identity.

How are these problems of naiveté? If people were more worldly, they would see these risks and protect against them. Managers would insist on having a security policy and on understanding the security implications of any system changes. Customers would see the cost of not securing computers. Users would get security how-to guides and only deviate from them after understanding the additional risk. Users would harden their computers to make them less vulnerable to network probing.

Unfortunately, as long as customers are unwilling to pay for security, the IT industry will not build it. Customers have to want it.

IT professionals vs. home users

We are not surprised when a novice home user makes an easy mistake like opening an attachment from an unknown source. But why do corporations continue to make mistakes like not keeping patches up to date, circumventing firewalls, and using weak passwords?

Again, the problem is that managers are naïve; they don't understand the problem. Managers tend to think of a computer as a box to be fit into a system diagram, not in terms of its often-subtle security implications. A manager rightly looks at the big picture, but needs to understand that any change to system configuration could have security implications and must be considered also from that point of view. A manager who understands the importance of security can hire or learn the expertise needed to strengthen security to a reasonable risk level. Even a computer professional who knows how to find security problems will not look for them without management support. If a manager does not value the time spent making sure patches are up to date, then his employees will be hard-pressed to continue spending time on that task.

Of course this is not the whole story. Even if the IT department understands a security problem, it will take a back seat to a business need.

Steps to improve commercial computer security

For corporate computers, the answer is twofold: get security on the organization's radar and get security expertise either by hiring or training.

Steps to improve home computer security

But, what can we do for home users? They cannot afford to hire consultants and cannot be expected to learn much about computer security before using their computers.

Any increase in user sophistication helps. There are automated web tools for probing PC security. Steve Gibson's "Shields Up" application (Gibson) will try various well-known ports to see if it can get into your computer. It gives a report of what ports it found and what the security implications are. Also, PC World (PC Pitstop) has a utility that will check security configuration of a PC's browser and email client. For some of their recommendations, PC World will display a link to click to change the setting to their recommendation.

There are security checklists for configuring PC's. The NSA has guidelines for improving security on Windows 2000, Windows NT , email, and downloading executables. Unfortunately these do not cover the most popular home computer operating systems, and the information they do have is quite technical (NSA).

We've still left the bulk of home users behind. What can we do to improve security for people who don't want to learn technical topics?

The label

Labeling on tuna fish cans is an example of a way that consumers can exercise power over a concern without having specific expertise in that area. Consumers don't have to go to sea or become experts in how dolphins are hurt by tuna fishing. All they have to do is understand that the "Dolphin-Safe" label is only allowed on cans of tuna that were caught in a way that did not threaten dolphins and avoid tuna cans lacking that label.

Since the 1950's tuna fishermen have killed 7 million dolphins. In the 1980's Congress changed the Marine Mammal Protection Act several times and in 1990 Congress created the "Dolphin-Safe" label for tuna cans (Defenders). In 1999 the Clinton administration weakened the dolphin protection (IATP), spawning a new "Flipper Seal of Approval" label (Earthtrust). But, no one doubts that this label saved many dolphins. Could a similar label work for the security of software?

What would the label mean?

This label would be a logo that guarantees a standard for software security. Software vendors would have to meet certain standards to place this logo on their products and on their advertising. Consumers would know that software with this logo adhered to basic security standards without having to know details of the standards.

The label would require disclosing security-related information including the following:

- When the product runs and what it does
- Where the product stores user information that will need to be backed up
- How to remove the product
- Warnings about security implications of configuration changes
- What ports are opened by their software and how those ports are used
- A product identifier to use on the label website to get up-to-date information about the product.

Also, the label would require compliance with software quality standards and independent security testing

Patches would be posted to the label's website so that even if the company failed, their latest patches would remain available. Earlier versions of patches would be maintained in the event that a patch introduces new problems.

Who would manage it?

The label would have to be held by a nonprofit organization. Otherwise, as the label became more successful, there would be pressure to increase the licensing fees to extortionate levels. This would cause resentment in the software industry, where cooperation is needed. The organization would walk the difficult balance between needing the support of software vendors and needing to keep a reputation of independence. This balance would be especially difficult at the start.

The label organization's first challenge would be to come up with software quality standards that are meaningful and achievable. These software quality standards would aim to reduce the occurrence of well-known problems like buffer overflows and reverse directory traversals. Any exploits against such problems would have to be corrected and a patch posted within a short time.

Ideally, the testing would be done by the label organization. But this might be too big of a challenge, so the security testing could be defined by the label organization and carried out by independent test labs. The work of the independent test labs would have to be subject to the label organization's overview.

Users could send bug reports to the label organization, which would track fixes. Software products could be rated based on the manufacturer's compliance and problems that users found (Callas).

Each software product manufacturer would also be rated on the label's website based on compliance with standards, timeliness of patches, and number of patches posted.

Conclusion

There is no magic bullet. Security for home computers will depend in some part on

everyone involved. The software security label, at best, would differentiate superior software vendors and reward their efforts with better sales. Meanwhile it would serve as a meaningful differentiator for all users and provide critical information to more savvy users.

Acknowledgements and Notes

My thanks to Jon Callas, who pointed out several problems with the draft of this paper. I have toned down my claim of naivete as a root cause and added business constraints in response to his comments. The ideas he added are referenced to him but have been reworded by me.

I found the article on the Morris worm through Larry Boettger's article on the Morris Worm (Boettger). The URL given in his article was no longer active, but I found Bob Page's article at Purdue (Page).

In April 1999 the Clinton administration weakened protection of dolphins to avoid a suit by Mexico in the World Trade Organization. This administrative action was reversed in federal court in April of 2000 (IMMP) and the Department of Justice agreed not to appeal in January of 2002 (Palmer). So the "Dolphin-Safe" label is once again a sign that the tuna was caught in a way that did not injure dolphins.

My link for PC Pitstop (PC Pitstop), works from my IE 6 browser but not from my MS Word 2000. If clicking the hyperlink does not work, please try pasting the URL into the browser address. All the other links work directly from MS Word 2000 on my computer. This link can be used without becoming a member. Click "New Members", download the utility and then choose "Test Anonymously".

This paper lumps together safety (failure and accident) with attack (Callas). People think of computer security in terms of attack. But realistically, most computers are in more danger of failure or accident than of attack. Software can mitigate all three. For instance, when you delete a file, the operating system may temporarily just move it to a cache it can be recovered from if you change your mind. This is an example of software reducing the risk of accident.

List of References

Boettger, Larry. "The Morris Worm: how it Affected Computer Security and Lessons Learned by it" SANS Information Security Reading Room. 24 December 2000. URL: http://rr.sans.org/malicious/morris.php (27 Jan 2002)

Braden, R. "4.1.3.1 Ports" RFC 1122. October 1989. URL: http://www.freesoft.org/CIE/RFC/1122/76.htm (27 Jan. 2002)

Braden, R. "4.2.3.9 ICMP Messages" RFC 1122. October 1989. URL: http://www.freesoft.org/CIE/RFC/1122/117.htm (27 Jan. 2002)

Callas, Jon. Private correspondence. 27 January 2002

Defenders. "Dolphins: Keeping America's Tuna Dolphin Safe" Defenders of Wildlife.

2001. URL: http://www.defenders.org/wildlife/new/dolphins.html

Earthtrust. "Flipper Seal of Approval". (no date). URL: http://www.earthtrust.org/fsa.html

Gibson, Steve. "New & Events" Gibson Research Corporation. 25 Jan 2002. URL: http://grc.com/default.htm From this page choose the "Shields Up" button and follow directions to test both shields and ports. This button assigns a unique id and then goes into SSL mode, so I have not directly linked the page.

IATP, Institute for Ag and Trade Policy. "'Dolphin-Safe' Tuna is No Longer Safe: Government Mandates False Labeling Regulations" April 1999. URL: http://www.organicconsumers.org/Corp/dolphinlabel.cfm

IMMP, International Marine Mammal Project. "Not so dolphin-friendly tuna from Mexico in US supermarkets?" San Diego Earth Times. Dec. 2000. URL: http://www.sdearthtimes.com/et1200/et1200s2.html (27 Jan 2002)

NSA. "Security Recommendation Guides". 27 Dec. 2001. URL: http://nsa1.www.conxion.com/index.html (27 Jan 2002)

Page, Bob. "A Report on the Internet Worm". 7 November 1988. URL: ftp://coast.cs.purdue.edu/pub/doc/morris_worm/worm.paper (27 Jan 2002)

Palmer, Mark J. "Victory at Sea: David Brower leaves a legacy for dolphins" Grist Magazine. 10 Jan. 2002. URL: http://www.gristmagazine.com/grist/imho/palmer011102.asp

PC Pitstop. "PC Pitstop Full Tests". 27 Jan. 2002. URL: http://www.pcpitstop.com/pcpitstop/ (27 Jan 2002)

Weinberg, Gerald M. The Secrets of Consulting: A Guide to Giving & Getting Advice Successfully. New York: Dorset House Publishing, 1985. 6.

Last Updated: October 17th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive