



Devon Richards

Power and Persuasion in Relation to Computer Security

5/19/11



Computer security in its current form is a nearly unneeded industry causing the waste of millions if not billions of dollars a year. It would be much less so except for the inadequate programming ability of modern software designers in big companies with corporate monopolies on the software and hardware industries. The designers only care about how good their programs look and leave out many important functions and open up an excessive amount of security holes. A security hole is a vulnerability that allows attacking parties to interfere with the operation of a computer and/or read all documents on said computer. These security holes are very dangerous to anyone who might use their computer for confidential documents like tax papers, business papers, or work. These holes can allow others to completely take over your computer. They can also allow people with malicious intent to destroy all functionality of your computer, wiping out all files on it. This can be easily prevented though and should not require the usage of software costing hundreds of dollars or more per license.

What most people are not aware of is that there is as good if not better free software developed by people who want to prevent malicious software from being able to harm anyone's computers. The reason most people do not use this is that it does not look good and is not advertised so people do not see it or want it. It has actually been shown that most large free or open source software is better at its task than the comparable commercial software. Open source is software that has had its source code released to the public on a variety of licenses. The most popular of these licenses is the General Public License or the GPL. This license basically says you can use the software and change it as much as you want as long as you do not sell it or take credit away from the original developer or developers. This source code gives developers the ability to change anything about the program to their needs if they know how to do it.

The most basic point of a computer's security suite is the operating system. The operating system is what decides how the computer runs and what it can do. It

is a vital backbone to any security setup. It does not matter how well your computer's other software is at security if you have an operating system with bad security. All requests for changes to security setup and access to files have to go through the operating system. Modern operating systems are very alike, but very different in a few key categories like security. The most common operating system there is for people to use is Windows XP. This might be the most common, but it has been proven many times that it is not the safest in terms of security. This operating system holds great power over the computer market. When it has a discovered problem about seventy-four percent of all working computers have to be updated or leave a gaping hole open in their security. These gaping holes should be unacceptable to most modern companies, but it isn't. Companies instead of upgrading their operating system just dish out millions of dollars to anti-virus corporations to protect themselves. This anti-virus software will prevent most viruses that have been experienced by multiple people and work as an adaptive network of webs to trap malicious software. Malicious software is software that exploits or uses security holes on a computer network or system. The anti-virus software like any other web will have its own exploitable holes. Most security risks you end up hearing about are the ones that have exploited these common holes that are common to most of the anti-virus software.

The most common kind of operating system in the world is collectively known as Windows. Windows is actually a group of operating systems made by Microsoft. Microsoft holds an extremely powerful corporate monopoly on computer operating systems and office software. They effectively control how the computer software industry works. If Microsoft adds certain software by default most their operating systems will also add it or a proprietary version of it by default. The exception to this is open source operating systems like Linux, BSD, and Solaris most of which are based off of Unix. Unix is the most popular base in existence for open source operating systems. You might think that being open source would make an

operating system easier to break into, but it doesn't. Open source operating systems are actually proven to be on average more secure than their closed source proprietary counterparts. Open source operating systems are more secure because of the simple fact that they are based off of what the group of people working on it and using it suggest and find bugs with. For this reason new versions of open source operating systems are released every six to eighteen months. The only really bad thing about open source operating system's security is that unless it is an extremely serious problem like easy, anyone can do it from anywhere, complete takeover of computers or networks the fixes for it will not be released till the next development cycle is over.

Software security is the most lucrative specialized industry within the computer security industry. It earns millions if not billions of dollars every year out of people. These people should not have had to pay anywhere near that amount. If you look at the earnings from the software security industry almost all of them end up back at the same people who develop the software that needs protection. Does it seem amoral to anyone else to create a bad software sell it as good, and then release more software that costs extra money to fix it? This does not seem to faze most developers though. They still produce the same kind of software with the same bugs as they always have. Once they finish making the software they go to work on helping other developers make more expensive software to protect your computer against the errors in their own code. If developers acted responsibly the software security industry would only be an efficient million dollar industry instead of the billion dollar behemoth it has become.

If all else fails, you do not want intruders into your computer to be able to read your confidential documents like bank records, tax records, and work files. For many people this would be a complete and other catastrophes. Can you imagine what it would be like to have all of your personal documents were forcibly shoved into the public domain. The public domain is places like WikiLeaks that show information to

anyone and anything that asks. Anything means anything from autonomous programs collecting information on where you shop to programs looking for credit card information that then run it against banks and steal thousands of dollars. You may be asking, "how do I prevent this?" To tell you the truth there is no method that will work more than ninety-eight percent of the time, but the way most informed people protect themselves, their work, their friend's, and their familie's information is that they use cryptography. Cryptography is the making and breaking of codes, use of codes, and exchange of ways to use those codes. Cryptography is probably the only part of the computer security industry that will never be able to die. It is too vital to have a working powerful way to protect your information to leave it to someone you aren't paying, but some might argue its too important to not be able to check the code for secret ways to decrypt it that only the developers would know about. Some of the most common seen uses of cryptography are in communication. You might not realize it but almost all electronic traffic like email, phone calls, private chat rooms, and video calls were encrypted while being transferred to protect you and whoever you are communicating with. If you want to be really safe you will encrypt all the information on your hard drive with some form of modern algorithm. Your hard drive is the place where all of your computers information like personal files, operating system, and programs are stored. Modern algorithms are nearly impossible to break even with a supercomputer like the ones the National Security Agency which is also known as the NSA have. If even the United States government can't break it you have absolutely nothing to worry about for a couple of years at the least. After a couple of years though computers might get up to the level to break it. This is why modern algorithms are constantly getting better and new ones are being developed.

You have now seen how great of a behemoth the computer security industry has become. It sucks the money out of ordinary people and enrages both amateur and professional programmers with their stupidity. A truly efficient computer security

industry would only cost the common consumer about twenty to fifty dollars per development cycle. This software would provide all of the security essentials like anti-virus, firewall, and a cryptographic suite. These would be as close to military grade as international law allows. Professional developers and amateur programmers might need to pay a little more because the nature of what they are doing can endanger the computer. Free operating systems would be used much more because they have greater security applications than the operating systems made by the bloated, behemoth corporation with monopolies like Microsoft. If all of this was applied there would be no more kids who could just easily break into computers. You would need a professional software developer to even stand a chance of breaking into the computers with lower level security.

Bibliography

Works Cited

Geek, Mad. "Command Prompt Tricks And Hacks." *Logic Club | iPhone, iPad, IOS, Gadgets, Mobiles and Apple*. Logic Club, 19 May 2011. Web. 6 May 2011.
<<http://www.logicclub.com/command-prompt-tricks-hacks>>.

Gunn, Angela. "USATODAY.com - Three New Windows Security Holes Come at a Bad Time." *News, Travel, Weather, Entertainment, Sports, Technology, U.S. & World - USATODAY.com*. USA Today, 24 Dec. 2004. Web. 3 May 2011.
<http://www.usatoday.com/tech/news/computersecurity/hacking/2004-12-24-we-three-winholes_x.htm>.

"How PGP Works." *The International PGP Home Page*. Network Associates, 19 May 2011. Web. 9 May 2011. <<http://www.pgpi.org/doc/pgpintro/>>.

"How to Change a Computer Password Using Command Prompt - WikiHow." *WikiHow - The How-to Manual That You Can Edit*. WikiHow, 19 May 2011. Web. 6 May 2011.
<<http://www.wikihow.com/Change-a-Computer-Password-Using-Command-Prompt>>.

"IT Law Wiki." *The IT Law Wiki*. IT Law Wiki, 21 Apr. 2011. Web. 19 May 2011.
<http://itlaw.wikia.com/wiki/The_IT_Law_Wiki>.

"Modern Cryptography." *Stony Brook Mathematics*. 8 Aug. 2002. Web. 5 May 2011.

<http://www.math.sunysb.edu/~scott/Book331/Modern_cryptography.html>.

Queen, Nat. "Introduction to PGP." *Nat Queen's Home Page*. Nat Queen, 4 May 2010. Web. 5

May 2011. <<http://www.queen.clara.net/pgp/pgp.html>>.

"US-CERT Cyber Security Tip ST04-020 -- Protecting Portable Devices: Data Security." *US-CERT: United States Computer Emergency Readiness Team*. US Government, 27 Jan. 2010. Web. 19 May 2011. <<http://www.us-cert.gov/cas/tips/ST04-020.html>>.