

DETERRENCE BY DENIAL: A NEW THEORETICAL MODEL FOR A SAFE, DEFENSE-DOMINANT CYBERSPACE

Abstract

A new theoretical model is proposed to enable effective deterrence by denial, potentially providing for a cyberspace that is defense-dominant and thereby potentially ending the offense-dominant imbalance currently resulting in a highly unstable and dangerous disequilibrium. The theoretical model is based on a new computer hardware architecture that fixes an overlooked but fatal flaw in the ancient Von Neumann architecture used in current computers. That architecture is obsolete now because it has no inner hardware defense against Internet malware attacks and is therefore inherently vulnerable, literally inviting endless cyberattacks. The new architecture introduces a new inner impermeable hardware barrier or barriers with the capability denying with certainty any access from the Internet to a protected part or parts of the computer, including its central controller. The theoretical model is sufficiently straightforward and mature to enable commercial development now and widespread deployment in the relatively near future.

Introduction

Numerous assessments for the National Research Council (NRC) have concluded with good reason that relying primarily on the threat of retaliation to deter cyberattacks on the United States appears to be the “inevitable choice” because there is no alternative in a cyberspace that is so clearly offense-dominant now. Unfortunately, the same assessments recognize that such offensive cyber deterrence just as inevitably introduces an apparent host of extremely serious problems, including massive uncertainty of results and associated risks of unintended consequences, including uncontrollable escalation.

Moreover, the majority of these offensive cyberdeterrence problems have no realistic solution because they are inherent in any likely scenario. Consequently, despite seeming to be the only choice, offensive cyberdeterrence may in practice be ineffective and dangerous as well, particularly (and ironically) so because of the extraordinary weakness of cyber defense. The excessive imbalance is likely to amplify uncontrollably the effects of the dominant offense. As a result, securing cyberspace appears as a practical matter today to be impossibly complex, if not just plain impossible.

Fortunately, the assessment of the overwhelming superiority of offense over defense in cyberspace, while true today, is not in fact inevitable, either theoretically or practically. A new theoretical model has been created with surprising potential to actually invert the existing cyberspace asymmetry to defense-dominant, which is a far safer state, one that innately produces the most stable equilibrium to avoid cyber conflict.

The surprising potential is so usual because the new theoretical model is based on a single technological change so basic it touches nearly every component of cyberspace. The model replaces the original and now classic Von Neumann computer hardware architecture, over 65 years old, with a simple new architecture that fixes an inherent security defect in the Von Neumann architecture and does so at the most fundamental possible level, thereby finally enabling safe computer connection to the Internet.

Consequently, this paper elaborates on the alternative concept of deterrence by denial

instead of deterrence by threat of retaliation or punishment. That is, it focuses on the concept of deterring an adversary by creating a strong cyberdefense with a sufficiently high probability of thwarting any cyberattack or limiting any cyberattack damage to acceptably low levels that are both temporary and easily repairable.

The first part of the paper will elaborate on the inherent weakness of the Von Neumann computer architecture and on the simplest, quickest and most comprehensive possible fix to that obsolete architecture, which is to replace it with a new bilateral computer hardware architecture. The second part of the paper will discuss some of the potential policy implications of the new safe, defense-dominant computer architecture on cyberspace security and privacy.

Overview

Cyber security has become so bad that it now poses an extraordinarily grave threat to the U.S. economy and U.S. national defense. No comprehensive solution to this threat has been found, much less implemented. The existing architecture for computers was designed in 1945 and has no internal defense against Internet malware, which is software, except with other software, which inexorably cannot avoid potential defeated by the Internet malware.

Today Internet connection is absolutely mandatory and allowing such connection fundamentally requires that the external or perimeter defenses of any computer, such as conventional firewalls, be porous and therefore only filter incoming traffic. Since perfect filters are impossible, stopping all Internet malware is also impossible. Once into existing computers, any malware can then potentially go anywhere inside the computer and do anything. A simple new architecture for computers has been created to solve this basic problem. It can provide true security and privacy for computers when connected to the Internet. The new computer architecture has a bilateral hardware structure that provides a new internal hardware defense that is not porous and therefore with certainty can protect an essential part (or parts) of a computer from any access by Internet malware software.

The new bilateral hardware architecture provides an inner protected part that control the entire computer, but is disconnected by an impermeable hardware barrier from any access by the Internet and therefore is invulnerable to Internet malware. Today, the only known way to fully protect a computer or network from Internet malware is to disconnect it from the Internet, but that is impossible in an economic world in which Internet connection is absolutely mandatory to function. The new bilateral computer architecture manages the seeming impossibility of simultaneously being Internet connected and Internet disconnected, thereby with the potential for providing both fail-safe security and privacy in cyberspace for the first time.

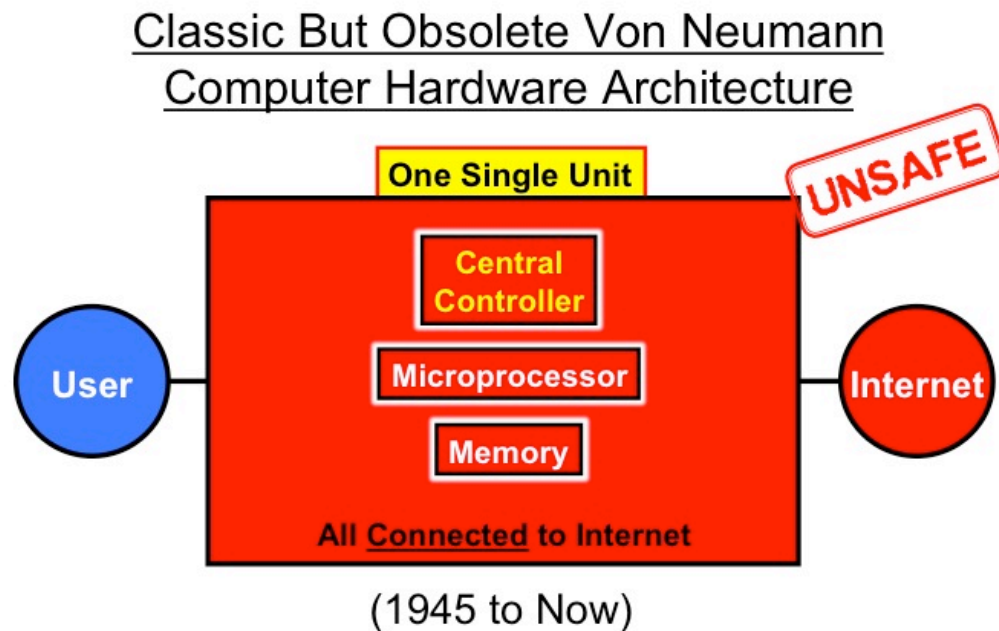
The Internet Malware Problem

The current architecture for computers is obsolete. Essentially unchanged since 1945, it was originally designed for a stand-alone computer. With the Internet providing connection to a billion other computers, it is inherently defective.

The modern computer's basic architectural defect has been overlooked in today's golden age of specialists because of its sheer generality and utter simplicity. The key problem is that existing computers have only a single, unitary hardware structure. Consequently, computers have no effective internal hardware defense to prevent even a single virus or any other software

malware from going absolutely anywhere inside the computer or doing anything, however destructive, without any fixed limit.

By its very hardware structure, then, existing computers are innately vulnerable to Internet attack by software malware and cannot be successfully defended internally by software alone. All that is required for successful attack is entry into the computer, which Internet connection to millions of malware sources now virtually ensures. Some malware inevitably gain entry and just one can be fatal. This potential vulnerability is shown schematically in Figure 1.



The Problem: Internet Malware has Potential Access to Entire Computer to Control Any Part or All of It

Figure 1

Consequently, however high tech they may be otherwise, existing Internet computers simply cannot be made reliably safe. In terms of basic structural architecture, they are not even as high tech as RMS Titanic (completed and sunk in 1912) and have a much more serious hardware structural defect.

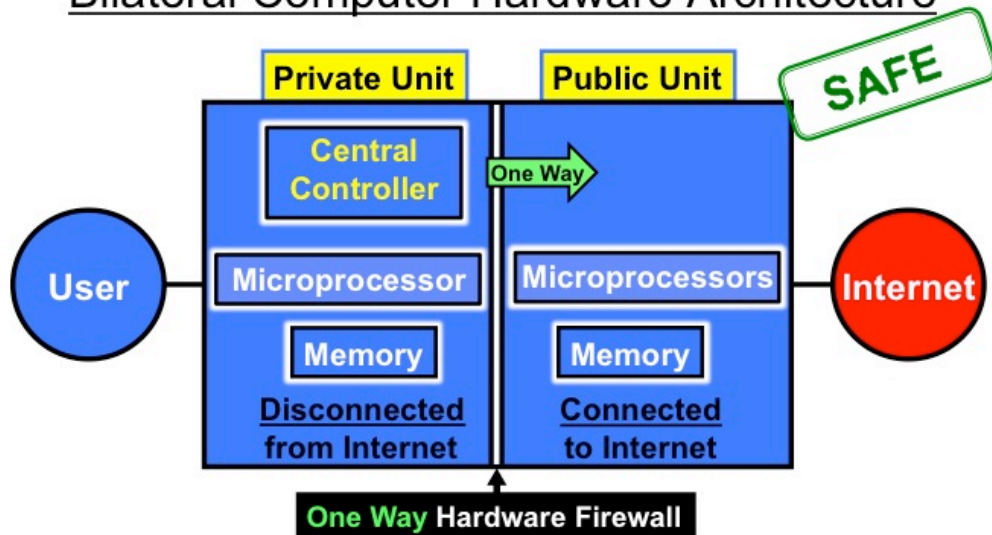
The Hardware Architectural Solution

The solution is a simple new computer architecture to solve an otherwise overwhelmingly complicated Internet security problem. A new, inner Private Unit is created by using an inner hardware barrier in the form of an uncomplicated firewall to protect the computer's Central Controller (with or without microprocessor and memory). The Central Controller is thereby made completely inaccessible from the rest of the computer and thereby also completely inaccessible from the Internet by this new impermeable hardware barrier. The remaining Public Unit includes one or more or many additional microprocessors (or cores) and memory, and is connected to the Internet, as illustrated in Figure 2b.

The computer's Internet-disconnected Private Unit controls the Internet-connected Public

Unit. Communication between Units is generally one way only, outbound from Private Unit to Public Unit, so the Central Controller functions generally like a TV remote controller (signals out only).

New Internet-Secure Bilateral Computer Hardware Architecture



The Solution: **Central Controller** Controls Entire Computer and is Hardware Protected to be Inaccessible from Internet

Figure 2b

In effect the new architecture subdivides the computer into two separate parts, creating a new bilateral structure. The bilateral structure is particularly useful now, when microprocessors are also evolving from a uni-processor into a multi-core structure using two or more processing cores, like the Intel Core 2 Duo, or its newer quad core models. The new bilateral structure is architectural change at the simplest, most fundamental possible level.

No other solution is available that can solve nearly all existing security problems of both computers and networks. Moreover, the new private unit can safely protect sensitive user files, thereby also providing a major improvement in user privacy. To summarize, making Internet computing safe is an urgent need requiring a new computer architecture specifically designed for the Internet..

A Potential Economic Crisis

President Obama declared in early 2009 that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity.” Nevertheless, the comprehensive White House Cyberspace Policy Review¹ of May 2009 has no clearly defined, comprehensive

¹ White House, *Cyberspace Policy Review*, 2009, available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review.pdf.

solution, just much more patchwork in reaction to specific attack outbreaks as they occur. One year later, we still cannot protect ourselves, as noted in the 2010 Annual Threat Assessment of the US Intelligence Community².

The lack of progress despite expenditures in the billions and nearly a decade of focused effort strongly suggests that some basic problem so simple it has been overlooked. It turns out the basic problem is not really a network issue, not the Internet itself. The Internet is, after all, just a relatively dumb network, with almost all the intelligence located at its edge in the hundreds of millions of computers connected to it. The main problem lies in all those computers themselves. Simply put, they were not originally designed to be networked. As a result, that design has an unforeseen, but fatal flaw that has remained unnoticed for almost half a century.

The Underlying Architectural Problem

The fundamental problem is the archaic underlying architecture of all those computers. First designed by John Mauchly and Pres Eckert³ and formalized by John von Neumann⁴ in 1945, the basic architecture of the computer today has since remained essentially unchanged since the very first computer in its most fundamental hardware structure. As decades passed and computer networks started to evolve in the mid 1960's, the simple basic architecture of computers was never reconsidered. Now, however, that architecture has been made functionally obsolete by the Internet.

The now relatively ancient Von Neumann architecture was designed for what was essentially a gigantic programmable calculator that filled an entire large room. The design predates even the most primitive of local networks, since there were no other computers in existence in 1945 with which to connect. Computer networking developed gradually in the 1960's. The exposure today of every Internet computer to the worst of millions of malicious hackers is an all too real nightmare now, but not even a daydream in 1945.

The fatal weakness of the Von Neumann architecture could not be more elemental: the computer's basic structure as a single unit. It follows directly from that archaic unitary structure that any malware, even a lone virus, having gained entry from anywhere in the vast Internet into any part of the computer, can potentially infect and destroy that part, or any other part, or even seize control of the entire computer.

Using the host computer's central controller (typically integrated into a microprocessor for the past several decades), the malware can potentially erase or alter or copy any or all data files, operating code, or both, or secretly join a rogue "botnet" to use the host computer to attack other computers. See Figure 1 again and note that all figures are schematic.

The only common internal computer defense today is built out of software, but unfortunately because of software's very impermanent nature, any defensive software is itself

² Blair, D.C. 2010. *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence*, available at http://www.dni.gov/testimonies/20100202_testimony.pdf.

³ McCartney, S. 1999. *ENIAC: The triumphs and Tragedies of the World's First Computer*. New York: Walker and Company.

⁴ von Neumann, J. 1945. *First Draft of a Report on the EDVAC*, available at <http://www.wps.com/J/EDVAC/index.html>.

inherently highly vulnerable to successful attack by Internet hackers, whose work can remain undetected. All that software internal defenses provide is the illusion of safety, just as did the watertight but topless inner compartments of the RMS Titanic.

The situation has become so bad that the only major alternative for the past few years to make computers or networks safe from Internet attack is to disconnect them completely from the Internet. But even that approach has failed and even at the highest level, since it still allowed an extremely serious security breach in the U.S. National Defense Command network in 2007, as reported in "Sabotaging the System" on CBS 60 Minutes⁵ on November 11, 2009.

If even the radical and drastic step of disconnecting computers from the Internet does not work, then fixing the fatal Internet security defect through any other existing technical means seems quite hopeless. But even if Internet disconnection did actually solve the huge current security problem, the equally huge benefit of Internet connection would be lost thereby, making Internet disconnection generally impractical today.

To sum up, the only apparent way to make computers safe today is by disconnecting them from the Internet, but even that approach can fail; and anyway, Internet disconnection is impossible due to the total dependence of the worldwide economy on the Internet connection.

Paradoxically, a safe Internet computer apparently needs to be connected to the Internet and also disconnected, simultaneously, which is seemingly both an impossibility and not entirely effective anyway, as noted above. It seems like the evolution of the computer and Internet has left us inexorably stranded in a technological dead end with no way out.

Surprisingly, there is in fact a relatively simple and practical solution to the basic Internet computer security problem. However, the answer does require a very basic change to the hardware architecture of all future computers to make them Internet safe.

The Simple Architectural Solution

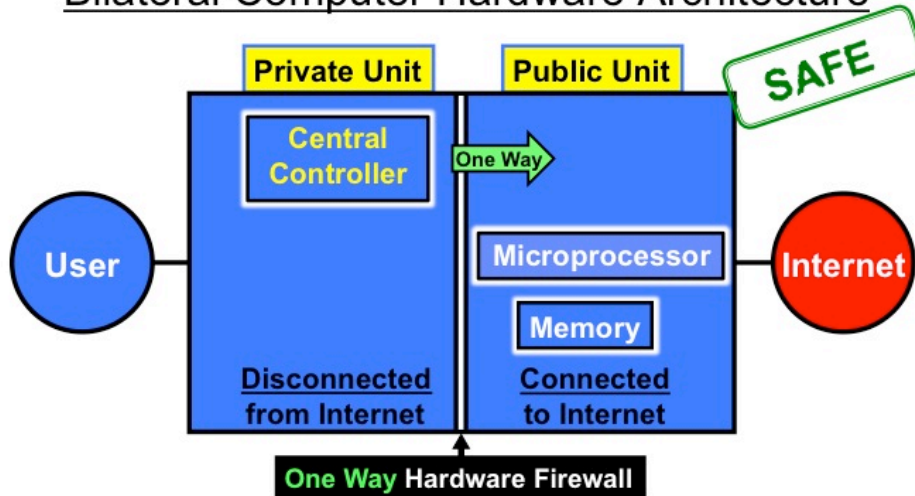
Apparently too simple to have been obvious, the radical but simple change needed in the new architecture is to make the hardware control of the computer totally inaccessible from the Internet or other networks. The new architecture subdivides the existing single unit computer into two separate units, roughly parallel but different. The simple new structure for computers is bilateral, like the human brain. Not essentially unitary, as the RMS Titanic proved to be, at least in effect.

The two different computer hardware units are, first, a private, Internet-disconnected unit, exclusively controlled by the computer owner, and second, a public, Internet-connected unit, with a range of potential users and shared operations, but always preemptively controlled by the owner.

The central controller of the computer is positioned in the private, Internet-disconnected unit, which is made completely inaccessible to the Internet by a simple inner hardware firewall barrier controlled by the central controller. The inner hardware firewall is an impermeable hardware barrier that operates on the uncomplicated general rule of totally denying access to the private unit from the public, Internet-connected unit. These new features are shown in Figure 2a.

⁵ CBS News, 1999. *Sabotaging the System*, available at <http://www.cbsnews.com/video/watch/?id=5578986n&tag=mncol;1st;1>.

New Internet-Secure Bilateral Computer Hardware Architecture



The Solution: **Central Controller** Controls Entire Computer and is Hardware Protected to be Inaccessible from Internet

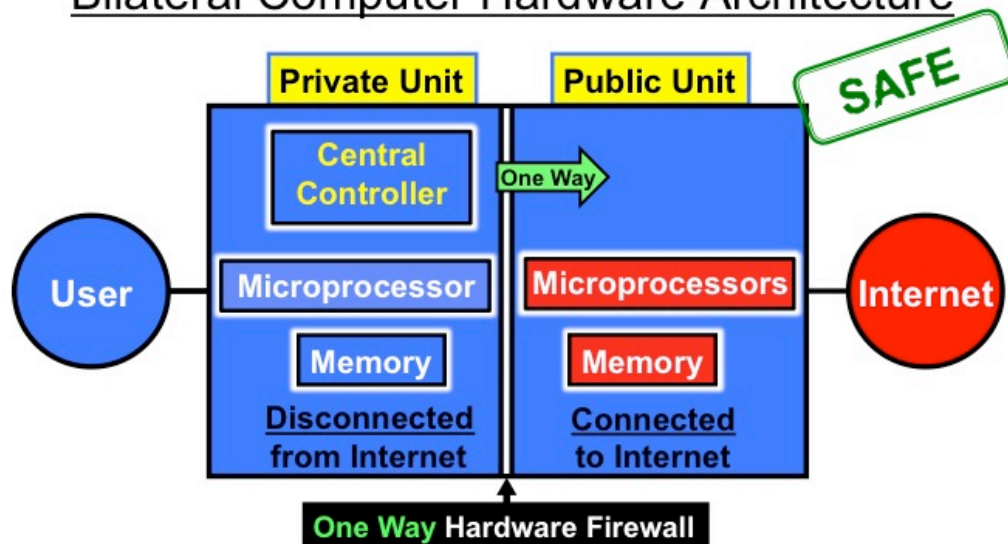
Figure 2a

The central controller can of course be conventionally integrated with a processing unit into a microprocessor and can have access to memory, particularly including non-volatile memory like Flash, also isolated on the private unit. The public unit can include one or more or even many microprocessor cores with access to memory, especially volatile memory like DRAM. Hard-drives can be used also, including a new dual control hard-drive with separate hardware-controlled partitions for private and public units. See Figure 2b again.

The computer's Internet-disconnected private unit always has preemptive control of the Internet-connected public unit. Communication between units is generally one way only, outbound from private unit to public unit. The central controller in the private unit acts sort of like a television remote controller sending control signals out to the television, but not receiving signals back (although viewing the television display).

To purge Internet malware on a routine basis, any part (or all) of the public unit volatile memory DRAM that is used for any operation involving direct connection or indirect exposure to the Internet can be erased by simply interrupting power after the operation ends and rebooting with software from the private unit. This can be done by default periodically or after every Internet operation or every Website connection, for example, as illustrated generally in Figure 2c.

New Internet-Secure Bilateral Computer Hardware Architecture



Internet Malware Flushed Away: Temporary **Malware** Infestation Limited to **Public Unit** & Erased by Controlled Power Interruption

Figure 2c

Amazingly, with the new Internet secure computer architecture, even the public, Internet-connected unit of the computer is far more secure than classic Von Neumann computers, because of both its Internet malware purging capability and its absolute protection of the computer's central control from the Internet.

From cell phones to personal computers to Webservers and blades, the exclusive use of only new bilateral computer architecture will enable - for the first time - a truly safe level of database privacy for existing network structures and for newer cloud computing, allowing far better protection for sensitive medical records, financial information and email stored in the cloud, including Google's.

It should be noted that Cloud Security Alliance's March, 2010, report on Top Threats To Cloud Computing V1.0⁶ lists seven top threats, all of which are computer-based issues and therefore addressed by the new bilateral computer architecture.

⁶ Cloud Security Alliance, 2010. *Top Threats to Cloud Computing V1.0*, available at <http://www.cloudsecurityalliance.org/topthreats/csathreats.v.0.pdf>.

Multiple Computer Inner Hardware Firewalls

Any or all operating code, data, and hardware components can potentially be separated into as many different levels of security as potentially required by a user for additional and differentiated security. A matrix of multiple inner hardware firewall barriers can create many separate compartments providing different levels of security for the central controller and processing units or cores and separate parts of the operating system, application systems, and user data, a schematic example of which is shown in Figure 3.

New Internet-Secure Computer Hardware Architecture

Matrix of Multiple Inner Firewalls Can Create Many Separate Compartments

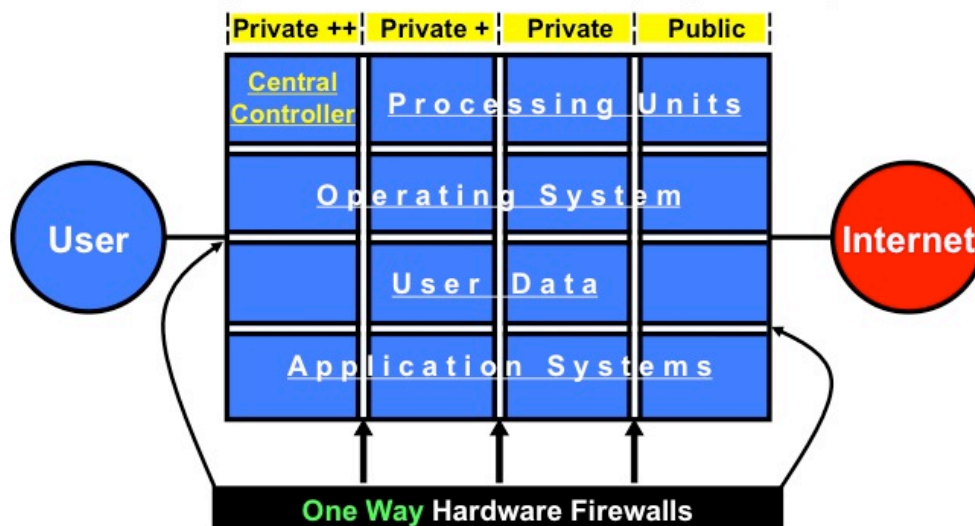


Figure 3

Successive Hardware Barriers Around A Kernel Or Other Subcomponent

The new safe Internet computers also require an upgrade of existing software to better match the new hardware architecture, especially the multiple inner firewall design of Figure 3 above. All existing software such as operating systems, Internet browsers, and application programs must be upgraded by separating their most essential, core functions into the private, Internet-inaccessible units of the computer. The levels together form a schematic structure like that of an onion, with the smallest, simplest and most essential software kernel in the center, as shown in Figure 4.

New Internet-Secure Computer Hardware Architecture

Any Computer Component can be Subdivided into Kernel and other
Subcomponents Protected by Successive Firewall Layers

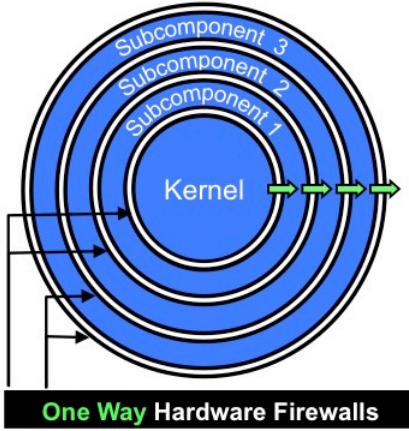


Figure 4

Any Computer Component Protected By Its Own Firewall Barrier

As a general rule, any hardware or software or firmware component (or group of components) of the safe Internet personal computer or smart cellphone or Webserver can advantageously have its own unique hardware firewall (or firewalls). The basic multi-compartment architecture is completely flexible and scalable, and can become ever more robust as it evolves to be ever more comprehensive over time, especially as more cores are added to microprocessor chips, as illustrated in Figure 5.

New Internet-Secure Computer Hardware Architecture

Any Computer Component Can Be
Protected By Its Own Inner Firewall (or Firewalls)

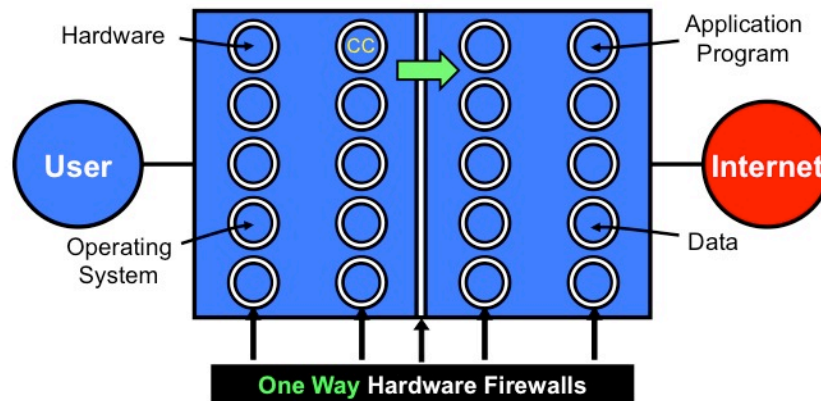


Figure 5

Faraday Cage Protection Is Necessary To Counter Serious EMP Threat

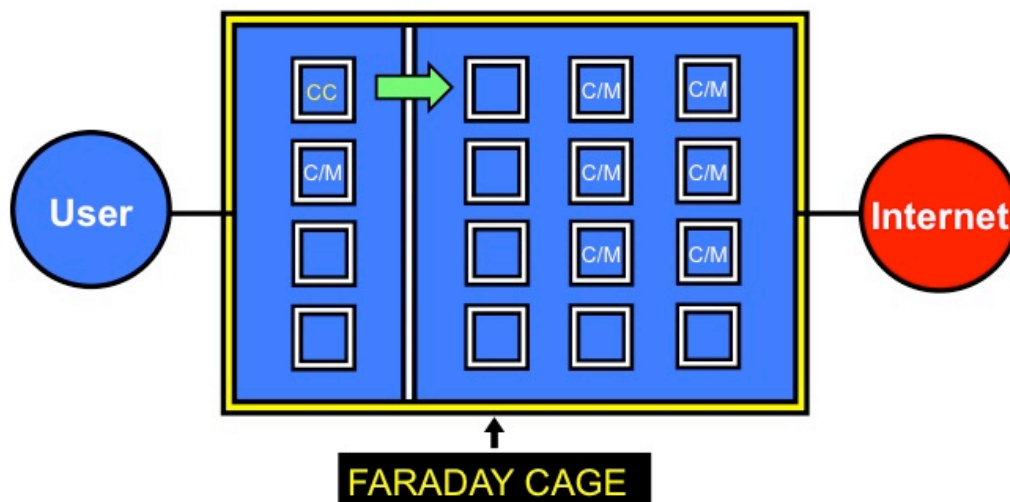
As technology evolves in the near future, many of these computer components will reside on a single microchip including the most essential components (or all components) of a personal computer on a system-on-a-chip (SOC) microchip. The SOC microchip will include many processors (cores), optimally with each having associated on-chip non-cache memory and/or shared non-cache memory.

Although the threat of electromagnetic pulse (EMP) is not formally considered in this NRC project⁷, it cannot be ignored in designing a basic new security architecture for computers because of its potentially devastating effects nationwide. Both critical vulnerabilities equally need to be fixed as soon as possible.

Computers, including especially the SOC microchip (and other microchips), should be fully surrounded by a Faraday Cage and related components to protect them against the growing EMP threat against entire geographic regions and of interference from other nearby electronic components or from outside sources, as well as surveillance threats. Figure 6 illustrates a Faraday Cage surrounding a computer or microchip.

New Internet-Secure Computer Hardware Architecture

Computer can be Personal Computer System on a Chip (SOC) Microchip
With Many Processing Cores (C) and Associated RAM (M), Each With Inner Firewall(s)



Surrounds Computer to Protect Against Electromagnetic Pulse (EMP),
Interference from Other Components & Surveillance

Figure 6

⁷ National Research Council, 2010. *Letter Report from the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, p. 2-3, available at <http://www.nap.edu/catalog/12886.html>.

Independent Preliminary Proof of Concept?

The new bilateral computer hardware architecture proposed in the preceding discussion is a unique approach that provides security and privacy capabilities beyond those of existing technologies. Various commercial hardware and software vendors large and small have taken some partial steps in the same general direction, such as creating protected partitions somewhat similar to those of the bilateral architecture. But almost all involve software partitions only, such as “sandboxes” in Java, introduced in the mid 1990’s, and more recently “trusted enclaves” by Blue Ridge Networks, Inc., for example. The ARM Holdings TrustZone technology seems to incorporate temporary cycle hardware protection of a single core microprocessor. However, none of these approaches nor any other known technology incorporate internal hardware partitioning, including partitioning of each of multiple individual microprocessor cores, or completely isolate the central controller of the computer from any access by the Internet, for example, as does the new bilateral computer hardware architecture.

A recent Bloomberg Business article titled “InZero: Closing the Gate on Cyber Crime”⁸ has described a relatively new and innovative computer security approach by InZero Systems that appears to have some important similarities to the bilateral computer architecture, although the InZero system is a proprietary add-on black box device for existing computers rather than a new general computer architecture. As reported in the article, InZero connects a separate second, custom external computer to a user's existing computer, with a “glass wall” barrier between the two computers. InZero’s proprietary add-on computer is a heavily protected area somewhat like the bilateral architecture private unit, but is directly connected to the Internet (instead of being disconnected from the Internet, as in the bilateral computer, so it is in the opposition position relative to the Internet connection). InZero’s add-on computer apparently is designed to be the exclusive proprietary interface located between the Internet and a user’s existing computer, the security status of which remains unchanged (meaning any existing security problems within the user’s computer remain unchanged by InZero’s add-on external computer, which just controls the existing computer’s interface with the Internet).

InZero claims, apparently with considerable support including testing by the Defense Advanced Research Projects Agency (DARPA), that its hardware-based system is hackproof, which if true would make it a truly major security improvement over other existing commercial systems. On the other hand, the Businessweek article reports a substantial number of unresolved questions remaining about the potential widespread utility of the InZero technology. The questions seem to be due primarily to some of the specifics of its heavily proprietary approach, such as its use of 60 million lines of proprietary software code and the source of that code.

It is difficult to compare two systems, in part because the InZero technology seems highly complex and only partially disclosed, but it appears reasonable to conclude that the new bilateral computer architecture would seem to be a far more basic approach than InZero's, since the bilateral architecture alone directly fixes the main problem in existing computers, which is the obsolete basic architecture. The new bilateral architecture is not an add-on product, but

⁸ Carey, J. 2010. *InZero: Closing the Gate on Cyber Crime*. Bloomberg Businessweek, February 25. Available at http://www.businessweek.com/magazine/content/10_10b4169052653415.html.

instead an integrated approach involving the entire computer. It therefore has potential to be the simplest and best available option for the next principal direction in the general evolution of the computer development, providing the capability to rapidly replace the insecure current national infrastructure of the U.S. with a future one that is secure. Significantly, in this evolution, all of the existing producers and suppliers of Internet hardware and software could continue to play the same roles in the future with the existing products upgraded for the new architecture. In contrast, InZero's proprietary approach seems to require that its own technology would replace that of a multitude of major industry vendors, which may not be likely.

Nonetheless, despite the apparent questions about the InZero Systems technology raised in the Businessweek article, the successful development of a hackproof hardware-based computer security system by InZero Systems possibly serves a very important role here as an independent preliminary proof of concept of the new bilateral computer hardware architecture. Its new basic architecture simply goes much farther in the same general direction of tight hardware partitioning as the InZero technology, but with major differences that appear to be better in what seem to be essential ways that make it potentially the best and perhaps only option for potentially making secure the entire computer and telecommunications infrastructure of both the United States and the rest of the world.

The apparent hackproof success of InZero's technology and the similarity of many important hardware features with that of the new bilateral computer architecture is at the very least a strong early indication that the general direction shared by both has enormous future potential for successful development well beyond that of any known competing approaches.

The New Bilateral Computer Architecture Can Prevent Denial-of-Service (DoS) Attacks

The above brief summary of the new bilateral computer architecture indicates clearly its exceptional theoretical potential for effective passive cyberdefense by the fail-safe containment of malware using new hardware partitioning barriers that can provide absolute denial of any Internet access, including use of a multitude of such barriers, as shown in Figure 3 through Figure 6. The new computer hardware barriers provide a critical and heretofore missing capability to strictly limit possible malware damage to a single, user-controlled area of the computer.

This reliable damage containment is in marked contrast to the classic Von Neumann architecture, shown in Figure 1, which provides no such reliable damage containment whatsoever, which is in fact the inherent and fatal security flaw of its unitary hardware structure. The new reliable containment capability inherent in the bilateral computer architecture renders obsolete the existing analysis on passive cyberdefense by the Committee on Deterring Cyberattacks provided below, which should be understood now to apply only to the classic Van Neumann unitary computer architecture:

... passive defensive measures must succeed every time an adversary conducts a hostile action, whereas the adversary's action need succeed only once. Put differently, attacks can be infinitely varied, whereas defenses are only as strong as their weakest links. This fact places a heavy and asymmetric burden on a defensive posture that employs only

passive defense.⁹

Indeed, the Committee's analysis summarizes well the principal security defect of the von Neumann unitary architecture, which is that the existing defect requires an impossibly perfect passive defense precisely because of the current architecture's inherent inability to contain malware damage in any reliable way.

In addition to the purely passive containment defense provided by the new bilateral computer architecture, it also provides a more active capability to eradicate malware by erasing it and rebooting securely with software from the computer's private, Internet-disconnected unit, as described previously with regard to Figure 2c above.

In discussing active defense, the Committee notes that active cyberdefense may be an option, but concludes that:

In practice, active defense is possible only for certain kinds of cyberattack (e.g., denial-of-service attacks) and even then only when the necessary intelligence information of the appropriate targets to hit is available to support a responsive operation.¹⁰

It is difficult to accept that such an active defense is practical at all or ever likely to succeed.

Their point is moot, however, because (and it is extremely important to note) that the structure of the new bilateral computer hardware architecture has the capability of preventing any such denial-of-service attacks, including distributed denial-of-service (DDoS) attacks employing "botnets". That is because the central controller of the new bilateral computer is located in the Internet-disconnected private unit, where it is not accessible to potential control from any Internet source but rather remains permanently and with certainty under the direct control of the computer's user.

What Kind of Development Program Is Appropriate?

Because of the urgent need to counter the cyberthreat to the U.S. and throughout the world, and since there are no other viable solution options, a crash program with the highest national priority to develop the new safe Internet computer may be overdue by at least a decade and could begin as soon as possible.

But it certainly should not be anything like a Manhattan Project, which has been suggested by some authorities, since the principal program goal now - beyond truly secure national defense systems - is billions of redesigned commercial computer products, not a few atomic bombs. A crash program may be warranted but would be best accomplished by natural competition focused in the U.S. private sector, with preliminary review by the National Research Council and the Defense Science Board (DSB), and R&D leadership by DARPA, with additional

⁹ National Research Council, 2010. *Letter Report from the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, p. 5, available at <http://www.nap.edu/catalog/12886.html>.

¹⁰ National Research Council, 2010. *Letter Report from the Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, p. 14, available at <http://www.nap.edu/catalog/12886.html>.

support from the National Science Foundation and the Institute of Electrical and Electronics Engineers.

A successful two year safe Internet computer crash program for design and development could potentially result in first commercial safe computers as early as in 2012. Starting in 2012, a safe Internet computer crash program could potentially ignite a world-wide boom in demand for U.S.-made safe microchips and computers, as well as related network products. The U.S. should have an inherently vast competitive advantage in terms of trusted computer security, particularly in the U.S. design and manufacturing of safe Internet system-on-a-chip (SOC) microchips, especially for vast and rapidly growing world-wide market for smart cellphones.

The Cost of New Infrastructure Based on the New Bilateral Computer Architecture

On one hand the cost of developing computer and network products with the new bilateral architecture is huge, in the probable range of as much as ten billion dollars over several years. Although much greater will be the cost over several years of replacing all the obsolete computers with safe Internet computers using the new bilateral architecture (since retrofitting most existing computers is either not feasible or cost effective or both), but of course such replacement occurs routinely anyway.

On the other hand, the actual increased development cost is probably very close to zero, since the cost will simply be the primary ongoing development cost of the industry for the next few years. In other words, existing development funding will be redirected to the new bilateral architecture from ongoing, lower priority development projects, such as for example developing the next 100,000 apps for the iPhone. The unquestionable reality is that the crucial unmet need in the high tech industry world-wide today is for trustworthy security and privacy, so that is where most existing development funding should flow for at least the next several years.

To the extent that increased development funding beyond existing levels is required to accelerate the speed of transition to the new bilateral architecture, that increase should be recaptured quickly by profits from increased market share for trusted U.S. products and from the temporary increase in the size of the overall market for the several years of transition.

The U.S. high tech industry has a unique advantage over its principal competitor, China. Without regime change, which is clearly not anticipated in the foreseeable future, China cannot be a trusted computer or microchip supplier outside of its controlled market in China.

Trusted computer security is likely to become a huge competitive advantage and therefore the one truly mandatory new feature of Internet computers as early as 2012 or 2013 (and remain so for at least five years), since earlier Internet computers are likely by then to become increasingly unsafe for use on the Internet, even though dependence on the Internet will be increasingly greater in the future. U.S. computer products like computers and microchips incorporating the new bilateral computer architecture would have a clear and sustained competitive market advantage world-wide outside of China.

The New Secure Technology Is Also Green

An important additional benefit of new safe Internet computers is that they are naturally clean and green. New system-on-a-chip (SOC) microchip-based personal computers will be naturally far more energy efficient than current computers with many microchips. And the new

safe computers will avert an Internet security meltdown, which would otherwise destroy the rapid growth in the Internet virtual world, economic and otherwise, that inherently and increasingly reduces real world fuel consumption and pollution through telecommuting for both work and play.

In conclusion, the new safe Internet bilateral computer architecture can neatly fix the dangerous Internet security situation which we currently face. In contrast, all other known potential computer and network security fixes, even taken together, are far less simple and direct, but also far less comprehensive and far less effective. And far less certain.

The new safe Internet computer architecture is the only solution that solves the basic underlying Internet security problem. All of the alternative solutions are severely limited because they all leave in place the underlying problem, the obsolete 1945 Von Neumann computer architecture.

The New Architecture May Become a Force for Individual Political Freedom

The preceding discussion leads directly to a surprising and profound political effect of the new security architecture. By developing and manufacturing the single most critical component of a secure and defensible Internet - which will likely be a huge competitive advantage and therefore a mandatory requirement in the competition for success in the future global economy - the U.S. may be creating an inexorable path to freedom and democracy in autocratic countries. The new bilateral computer architecture is designed to provide Internet security but also provides an unprecedented level of Internet privacy, which is fundamental to individual political and economic freedom.

Although this probably sounds quite politically naive, it may not be so. The reality may be that any country that opts out of this potentially mandatory technology will suffer the severe economic and military disadvantage of having to rely on a national Internet that is insecure and indefensible from cyber attack. A secret backdoor is unavoidably a potentially fatal security vulnerability, an access point for hostile intruders, if it becomes known. Therefore any computer security system with a secret backdoor is innately insecure. This potentially puts a country like China for example in a severe strategic bind. If it builds in secret backdoors in computers and microchips for use by Chinese citizens so that it can monitor and control their political activities in cyberspace, then China may thereby be creating a nation-wide Internet that is made inherently vulnerable and insecure by those same secret backdoors.

It may well be the case that to be competitive and safe in an Internet-dominated global economy, all nations will be forced to adopt the new totally secure bilateral computer technology. That technology allows its citizens the right to extreme cyberspace privacy and with it a very powerful freedom of private expression and secure communication in cyberspace, and thus powerfully the physical world as well.

Personal freedom of private expression and communication are perhaps the most fundamental of all freedoms, underlying all the other personal freedoms upon which political freedom is based and upon which the individual liberty of each of us depend. Seen in this light, Apple's famous and optimistic Big Brother television advertisement in 1984 may in fact have been prophetic, if somewhat premature. Little more than twenty-five years later, and now combined with the Internet, we may have arrived at a point where the new safe bilateral personal computer connected to the Internet (as well as the computer's smart cellphone and other

descendants) in only a few years more could possibly make political tyranny inherently much weaker in the developed and developing world, both economically and militarily.

Dominant Cyberdefense Can Reduce the Threat of “Big Brother” Surveillance

Besides increasing the certainty of ironclad cyberprivacy for U.S. citizens, the new bilateral computer architecture also reduces the need for “big brother” intrusive surveillance by the government that may be necessary now to protect those citizens from cyberattack. If cyberdefense can be made very strong, then the need for intrusive surveillance is potentially far less than currently appears to be necessary in the existing offense-dominant cyberspace.

This straightforward logic has potential implications, for example, regarding the recently announced new surveillance program called “Perfect Citizen” to be run by the National Security Agency (NSA). The “Perfect Citizen” program reportedly is to rely on sensors located in computer networks of critical infrastructure like the electrical grid and nuclear-power plants that would provide an alert to unusual cyber activity associated with an attack. In the current offense-dominant cyberspace, such surveillance needs to perfectly provide early warning of all potential cyberattacks to ensure that not even one is successful. This is just as unachievable a requirement as the assessment by the Committee on Detering Cyberattacks noted previously that passive cyberdefense needs to perfectly prevent all cyberattacks to ensure that no single one is successful. In short, the high level of surveillance that may now be necessary and justifiable in an offense-dominant cyberspace will not be necessary nor justifiable in a defense-dominant cyberspace, where a much lower level of cybersurveillance will likely suffice.

Future Protection from the Borg of Star Trek, the Matrix, and the Terminator

Although it might seem at least premature now, if not farfetched, it may prove later to have been crucial to have made the right basic decisions at this still very early stage in computer and network evolution in order to manage safely the cyber future of humans throughout the 21st Century and beyond. Medical device implants into humans have been occurring routinely for many years in the form of heart pacemakers and defibrillators, for example. In the near future, all implanted medical devices will likely be smart devices that incorporate computers with Internet connection. It will be critical for patient safety that the same kind of safe bilateral architecture outlined above is applied also to computers located in the human/machine interface.

Digital implants are now expanding in the direction of direct connection to parts of the human brain. It would therefore be prudent to adopt now a basic architecture that prevents the potential for human control by machine as seen, for example, in the “resistance is futile” Borg of Star Trek or in the Matrix. If, for example, some of the human race evolve in the future into some merged form of human and computer like a cyborg, it would also be prudent to act now to ensure that such cyborgs will be free and independent cyborgs, not slaves of the Borg. In the end, safely protecting the privacy and independence of the human brain from network control is roughly to the same as protecting the innermost control of consciousness of each human being, whether defined as self or soul.

In the next decade or two or more, something like an “Age of Spiritual Machines” as described by Ray Kurzweil, or more likely in some completely unanticipated form, could develop where the artificial intelligence of computers surpasses that of humans. If that comes to

pass, it may be fundamental to the continued free existence of humans that those "spiritual machines" be built on the safe bilateral computer architecture described above.

That basic bilateral architecture would support the continued human control of computers, no matter how immensely capable they are likely to become many decades in the future. By always providing the human user with preemptive control of an Internet-connected computer, the safe bilateral computer architecture has the potential to provide the fail-safe capability to prevent the possibility of a future defense system like the Terminator Skynet from launching a preemptive war against humans, for example. Clearly, building computer systems that are completely beyond human control or intervention presents unknowable risks. Similarly, robots or replicants or androids with potentially human or superhuman capabilities must be built on the same basic safe bilateral computer architecture. In that way it can be ensured that although they retain their own local version of self or soul, independent of control from the Internet, human user preemptive control can be retained.

An Open Standard for the New Bilateral Computer

The author is also the inventor of the new bilateral computer architecture described above and has developed an extensive and growing patent portfolio, currently consisting of about ten U.S. patents issued since 2000, with more applications currently pending. The author is a highly successful independent inventor and former member of the Board of Directors of Intellectual Property Owners Association (IPO), as well as runner-up for IPO's National Inventor of the Year in 1998. He is currently a member of the Intellectual Property Committee of the Institute of Electrical and Electronics Engineers (IEEE) and of its Research and Development Policy Committee. He also served as a commissioned officer in the United States Naval Reserve.

His issued U.S. Patents relating to the bilateral computer architecture provide additional information on the technology and are as follows: 6,167,428 issued 26 December 2000; 6,725,250 issued 20 April 2004; 6,732,141 issued 4 May 2004; 7,024,449 issued 4 April 2006; 7,035,906 issued 25 April 2006; 7,047,275 issued 16 May 2006; 7,506,020 issued 17 March 2009; 7,606,854 issued 30 September 2009; and 7,634,529 issued 15 December 2009.

Copies of the patents are most easily available at the author's company website: <http://www.glonetcomp.com>.

A nonexclusive licensing strategy for these patents is currently under development and is not yet completed, but will not include any licensing fees whatsoever on non-commercial open source software like Linux, Firefox, or Apache, for example, nor other than nominal nonexclusive licensing fees for any commercial use. The majority of the proceeds of the nominal commercial use licensing fees will be used to support and protect an open standard for the new bilateral computer architecture. The unity of ownership by the author of the pioneering patents covering the new bilateral computer architecture noted above should facilitate the rapid establishment of a new open standard for its general use, since potential ownership and proprietary technology disputes should thereby be minimized.

Conclusion

The new theoretical model proposed here needs to undergo careful, extensive review and potential modification in the immediate future by the NRC, DSB, and many others. Even so, due

to the extreme urgency of the cybersecurity problem, both nationally and worldwide, the main parameters of the simple new computer architecture are already sufficiently well defined and logically sound to provide a reasonable foundation for an almost immediate start to applied research and extensive prototyping. This initial effort should include the involvement of both hardware and software vendors for feedback and to beginning planning the earliest stages of product development. Learning by actually doing will provide the quickest route to successful and rapid development.

It is technically feasible to replace or upgrade most of the entire cyberspace infrastructure of the United States with safe, defense-dominant technology within roughly five years; this would include military, government, and private computers and telecommunications, including computers of individuals. Doing so would require redirecting the routine ongoing evolution of computers and networks to a focus on developing the new safe, defense-dominant technology. Although the total cost of doing so will be considerable, it should be almost entirely absorbed within the existing level of computer and telecommunications industry development costs. That is, costs associated with the development of the new infrastructure can be absorbed within existing vendor development budgets (although necessarily by being offset during the same period by reduced costs for far fewer nice-to-have but less urgent non-security enhancements and new apps, but also much less need for expensive patchwork security fixes). To accelerate the replacement process, consideration could be given to providing some start-up research and development costs allocated from the ongoing Comprehensive National Cybersecurity Initiative (CNCI).

Copyright 2010 by Frampton Ellis