Best Practices in the use of Bloodletting Technology and Information Security Technology

by **Wes Kussmaul**

Introduction

While bloodletting technology and information security technology may appear to be two of the most unrelated subjects of study imaginable, upon examination it may be seen that they have two things in common.

First, the methods and procedures and technologies of both bloodletting and information security were considered for years to be the the very essence of "best practices."

The second thing that bloodletting and information security technology share is the fact that they do not work.

We juxtapose the two "best practices" in this paper to show that "best practices" that are widely accepted by practitioners of a profession may in fact be *bad practices*.

We will then argue that since information security problems are a byproduct of *inauthenticity*, that the solution to security problems is to solve the underlying inauthenticity problem by means of the methods and procedures of *authenticity*.

We will then introduce a means of establishing authenticity in information facilities.

Phlebotomy / Venesection

The most common form of bloodletting was phlebotomy / venesection, which refers to the withdrawal of blood from the median cubital vein at the inner crease of the elbow. This vein is preferred for a number of reasons. It is close to the skin, causing minimal trauma and bruising, and the surrounding area lacks an abundance of nerve endings.

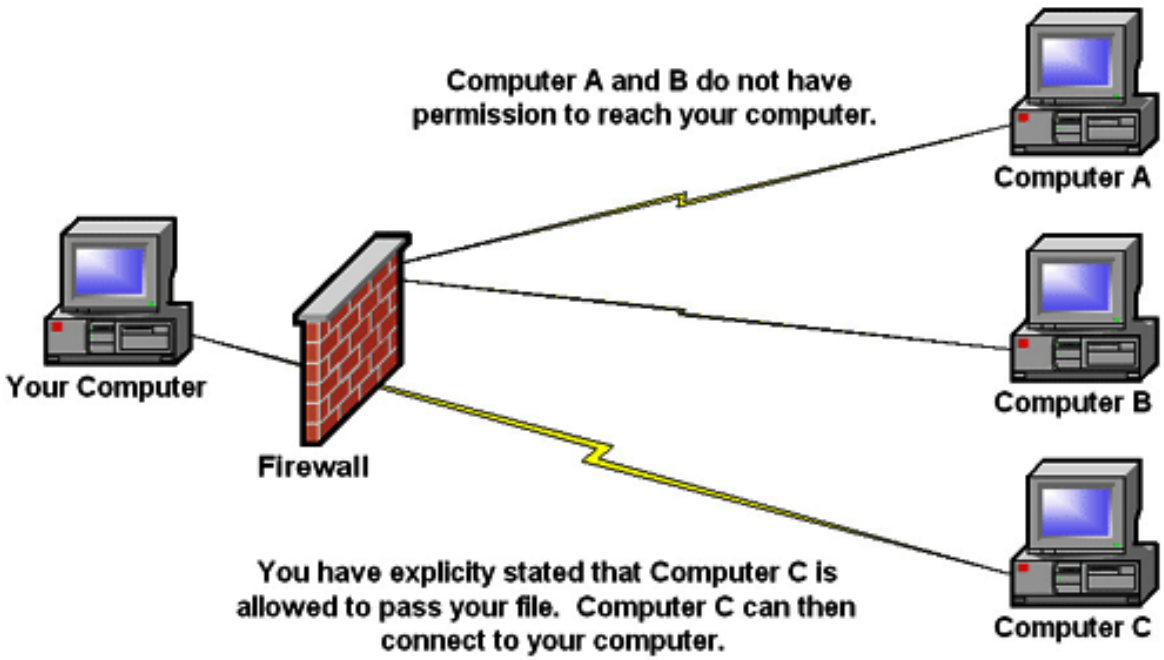
Phlebotomy (not to be confused with the modern practice of (unfortunately) the same name) involved the direct and manual cutting of the vein with a knife to release blood. In most cases, many shallow cuts were made. Venesection (quite similar to the practice of phlebotomy) was introduced when new tools were developed, specifically lancets and fleams. Spring loaded lancets (or thumb lancets) were small instruments with sharp points and two edges. After they were cocked, a trigger fired the spring loaded blade into the vein of the patient. Lancets were often carried in ivory or tortoise shell cases. Fleams (also used by veterinarians) were devices with multiple, variably sized blades that folded into a case much like that of a pocketknife. They were often aimed and hammered with a wooden fleam stick to be driven into the vein of interest.

Firewalls

First generation packet filter firewalls acted by inspecting the packets that transfer between and among computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will silently discard the packet or quarantine it, sometimes sending an error message to the source. This type of packet filtering stores no information on connection state, but filters each packet based only on information contained in the packet under examination.

Transmission control protocols (TCP) and user datagram protocols (UDP) are used in the majority of communication over the Internet. Since TCP and UDP traffic both use well known ports for certain types of traffic, a 'stateless' packet filter can distinguish between and control those types of traffic (like web browsing, emailing, file transfers and remote printing), unless the machines on either side of the packet filter are both using the same non-standard ports. With packet filtering firewalls, most of the work is done between the network and physical layers, with a small amount in the transport layer to figure out source and destination port numbers. When a packet originates from the sender and filters through a firewall, the device checks for matches to any of its filtering rules configured in the firewall and rejects the packet accordingly. When the packet passes through the firewall, it filters the packet on a port number basis.

Second-generation (stateful filter) firewalls perform the work of first-generation packet filters, but operate up to layer 4 of the open systems interconnection (OSI) model. This happens by means of stateful packet inspection; retaining a packet until enough information is available to make a judgment about its state. Second-generation firewalls record all connections passing through them, and determine whether a packet is the start of a new connection, part of an existing connection, or not part of any connection at all. Only packets matching a known active connection are allowed by the firewall. All others are rejected.



Arteriotomy

Arteriotomy is defined as the abstraction of blood by cutting the wall of an artery. In the practice of bloodletting, this process involved the direct puncturing and bleeding of the arteries in the temples and behind the ears. Surgeons of the time believed that different types of headaches called for incisions in different arteries of the head. For example, patients who experienced headaches with pain centering around or behind the eyes were often cut in the arteries of the temples to alleviate collection of 'excess' blood. Patients who experienced headaches or pain in the back of the head were drained behind the ears, to relieve excess pressure caused by a perceived abundance of blood in that region of the head.

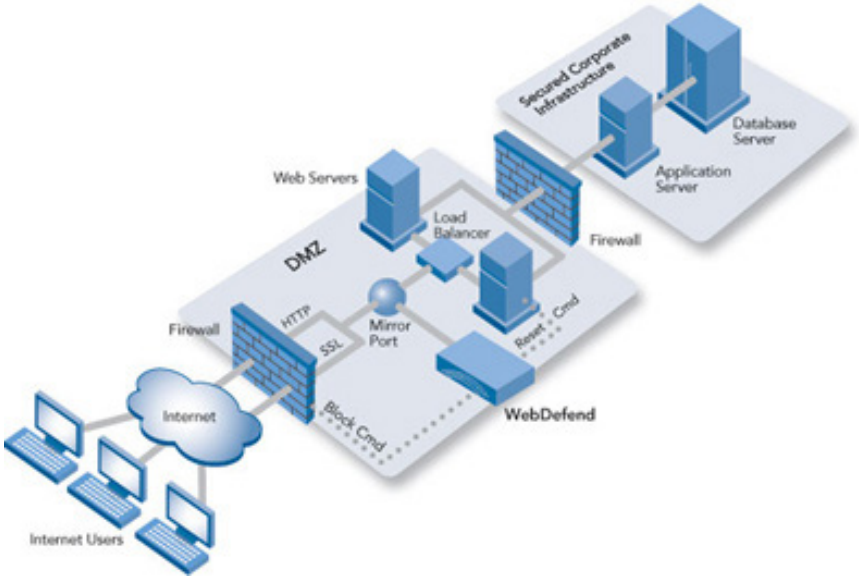
Arteriotomy posed some material possibility of complication because the arteries of the head are often difficult to clot after incisions are made. The slip of a hand could severely wound an artery, thus resulting severe hemorrhaging and/or aneurism.

Application Firewalls

Application firewalls, whether network-based or host-based, control input, output and access from, to or by an application or service. They operate by monitoring and blocking any input, output, or system service calls that do not meet its configured policy. Application firewalls are most often built to control network traffic on any OSI layer, up to the application layer. Unlike stateful network firewalls, application firewalls are able to control distinct applications or services.

Cupping

In the practice of cupping, the cup receptacle was placed over the wound to catch and suck the blood of humans or animals. Cups were made of tin, brass, rubber, horn and, most commonly, glass. Suction materials were commonly attached to cups to allow for quicker and more efficient blood removal. In 'wet cupping', rubber bulbs, brass syringes and even human lips were used as sources to create suction, drawing the blood out. In 'dry cupping', a suction cup was heated, sometimes with a wad of burning material or a heat lamp. The hot cup was then placed over un-punctured skin and allowed to cool, creating intense suction. As a result, the skin became engorged with surfacing 'humours'. The resulting boil or blister was then punctured for bloodletting. Cupping was considered beneficial because more blood could be drawn from a superficial wound.



Intrusion Detection Systems

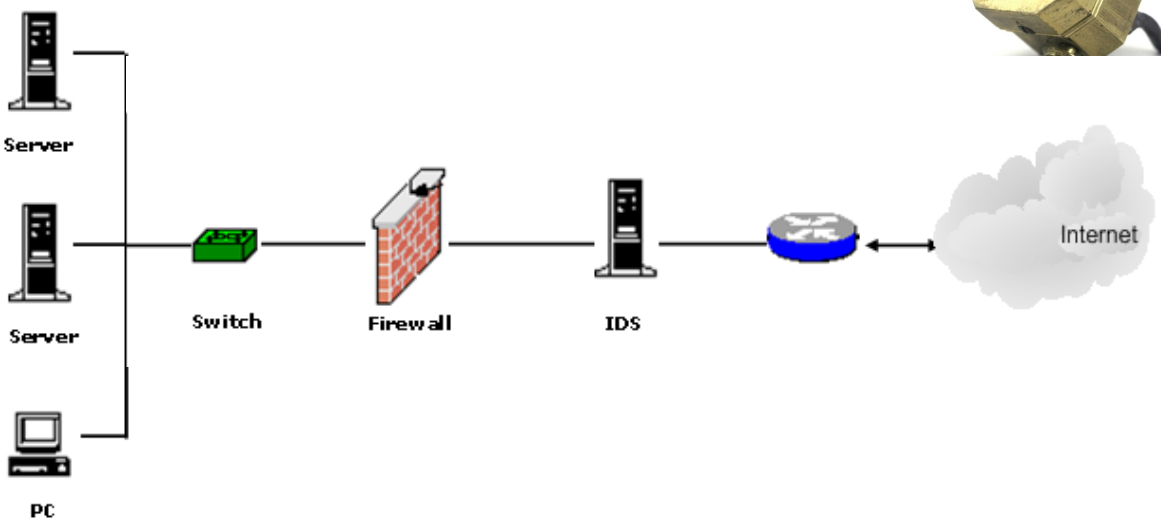
Intrusion detection systems (IDS) are devices or software applications that are primarily focused on identifying malicious activities or policy violations, logging information about them, and reporting attempts to management stations. They watch for attacks that originate from within a system by examining network communications and identifying signatures of common computer attacks.

Intrusion Detection Systems use one of two detection techniques; statistical anomaly-based or signature-based. A statistical anomaly-based IDS determines normal network activity (like bandwidth use, protocol use, and what ports and devices generally connect to each other). Both types alert the administrator or user when they detect abnormal traffic. Signature based IDS monitors packets in the network and compares them with signatures. A disadvantage is that this can cause a lag between threat discovery and signature application in IDS. During this lag time your IDS will be unable to identify threats.

Many limitations have historically been characteristic of IDS systems, although the limitations have been gradually reduced. For example, noise can potentially limit effectiveness and create a high false-alarm rate. It is not uncommon for the number of actual attacks to be significantly below the false-alarm rate. As a consequence, real attacks are often dismissed or ignored by the user. Furthermore, many attacks are geared for specific versions of software. Therefore, a constantly changing library of signatures is needed to keep up with new threats. Outdated databases leave IDS vulnerable to new strategies of attack.

Scarification

In scarification, 'superficial' blood vessels were drained by scraping the skin. A variety of tools could be used for the technique. Syringes, lancets and glass cups were popularly used. However, one specific tool, the scarificator was primarily used in 19th century medicine. This tool was less invasive than other popular bloodletting instruments of the time. It consisted of a cube-shaped brass box containing a series of small knives. It was powered by a spring-loaded mechanism with gears that propelled the blades out through openings in the front cover, and pulled them back in, in a circular motion. The multiple blades on the mechanism were mechanically turned in opposite directions for optimal bloodletting.



Intrusion Prevention Systems

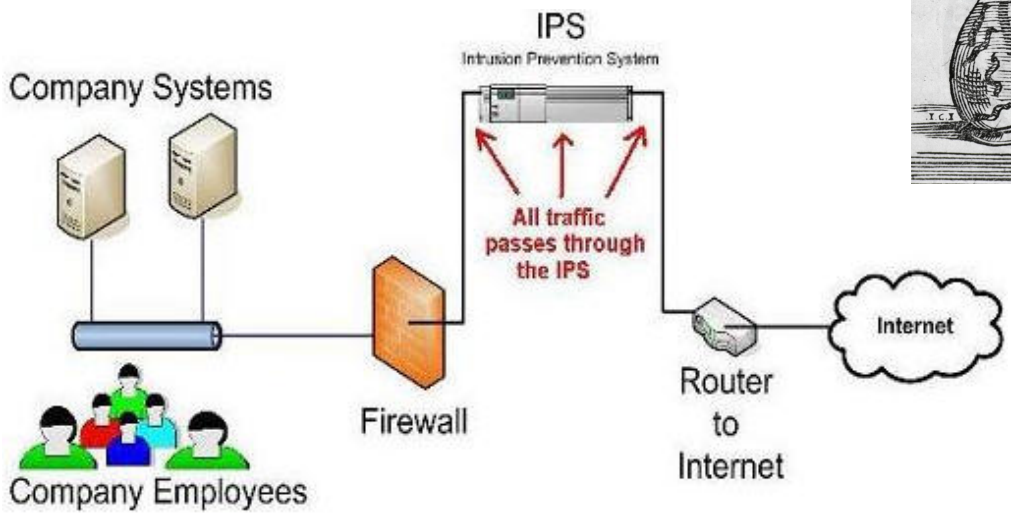
Considered extensions of IDS's, the term intrusion prevention system (IPS) is commonly used to refer to IDS's that have the ability to both detect and prevent potential threats. Several response techniques can be employed. IPS's can correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options. They can also send alarms, drop malicious packets, reset connections and block traffic from the offending IP address. Organizations commonly use IDPS's to deter individuals from violating security policies.

IDPS technologies are primarily differentiated by the types of events that they monitor and the ways in which they are deployed. Network-based IDPS's monitor traffic for specific segments or devices, and analyze the network and application protocol to identify threats. Wireless IDPS's monitor wireless network traffic and analyzes it to identify suspicious activity involving the wireless networking protocols themselves. Network behavior analysis examines network traffic to identify threats that generate unusual traffic flows, like distributed denial of service (DDoS) attacks, types of malware, and policy violations. Lastly, host-based IDPS's monitor the characteristics of a single host and the events occurring within that host for suspicious activity.

The majority of intrusion prevention systems utilize one of three detection methods: signature-based, statistical anomaly-based and stateful protocol analysis. Recall that signature-based monitors packets in the network and compares them with signatures. Statistical anomaly-based determines normal network activity (like bandwidth use, protocol use, and what ports and devices generally connect to each other). In addition to the aforementioned techniques, stateful protocol analysis identifies deviations of protocol states by comparing observed events with predetermined profiles of generally accepted definitions of benign activity.

Leeches

The use of medicinal leeches in the practice of bloodletting became especially popular in the early nineteenth century. Leeches were used to draw out 'bad' blood believed to cause physical ailments. When applied to the skin, this type of water-dwelling worm could suck 5 to 10 mL of blood, nearly 10



times its bodyweight. One 'advantage' of this method was that blood could be removed in predictable quantities and easily measured. However, doctors would often allow leeches to withdraw blood until a patient began to lose consciousness (at the time, referred to as syncope). Leeching also required little skill and could be done at home, since leeches were ready to suck blood at any time.

Through the early nineteenth century, hundreds of millions of leeches were used in European medicine. The rise in the use of medicinal leeches was due to new proposed theories that suggested excessive leeching and starvation would cure all forms of disease. A French physician, Francois Broussais, claimed that all fevers were a result of organ inflammation, and could be cured by the direct placement of leeches above the organ at fault.

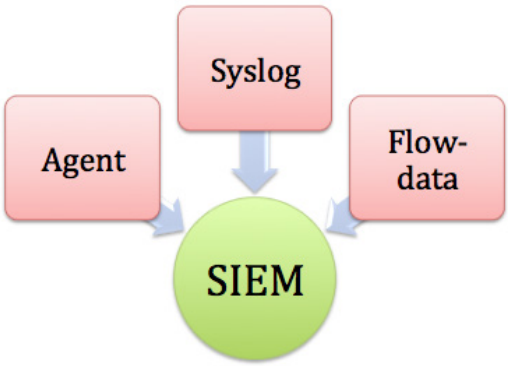
SIEM

Security Information and Event Management (SIEM) solutions are a combination of Security Information Management (SIM) and Security Event Manager (SEM) technologies. SIEM provides real-time analysis of security alerts produced by network hardware and applications. These solutions come as software, appliances or managed services. Its key focus is to monitor and manage user and service privileges, directory services, and system configuration changes. SIEM's also provide log auditing, review and incident responses.

SIEM technology offers various capabilities. Data aggregation (SIEM log management solutions) compiles data from many sources (including network, security, servers, databases and applications. This provides the ability to consolidate monitored data, thus avoiding the overlook of crucial events. Correlation looks for common attributes, and links events together, turning data into useful information. Alerting allows for the automated analysis of such correlated events, thus, producing alerts to notify users of necessary issues often on a dashboard or via e-mail. Dashboards take event data and turn it into informative charts to assist in the detection of patterns, or rather, the identification of activity that does not form a standard pattern. Compliance allows for the automation of gathering compliance data and producing reports that adapt to existing security, governance and auditing processes. The final feature, retention, facilitates the long-term storage of historical data over time, providing the retention necessary for compliance requirements.

Veterinary Bloodletting

Animals were treated with the same bloodletting practices that were applied to humans. House animals like dogs and cats were routinely bled to maintain a balance of humours and good health. Horses, cows, sheep and



pigs were also bled to prevent the spread of disease among farm animals.

Considerable force was needed to bleed a horse or cow. These animals were frequently bled directly from the jugular in the neck, veins in the thigh, breast, forelegs, palate or the toe. Large lancets and fleams were utilized to open the deep veins of such animals. The blade was held against the vein of the animal and hammered with a stick to draw blood. The steady stream of blood was then caught and measured in a container. Once enough blood was collected, a needle was inserted in the vein to stop the flow of blood.

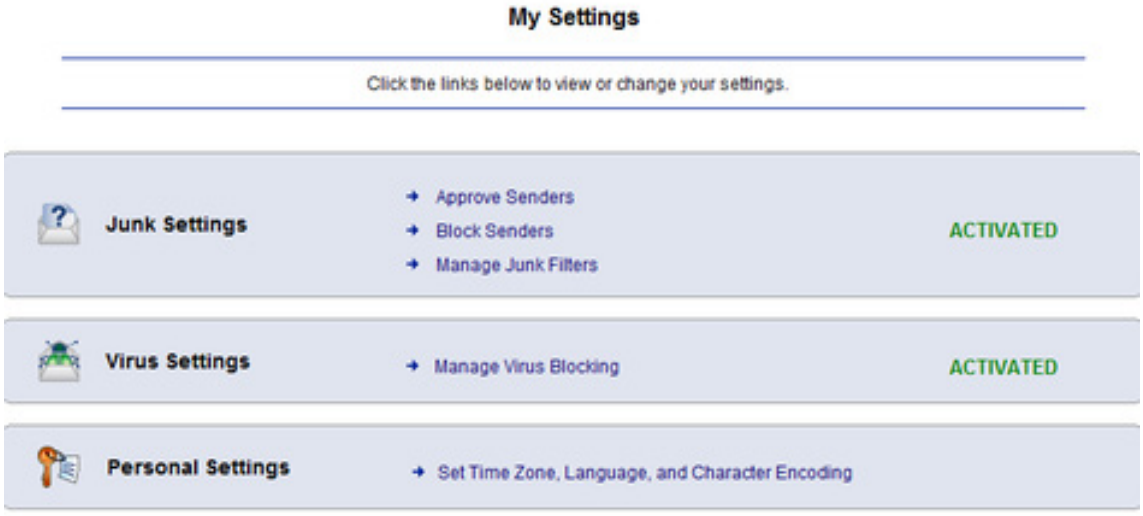
Whitelisting

A whitelist is a list of entities that are provided a particular privilege, service, mobility, access or recognition. Only entities that appear on this list will be accepted, approved or recognized.

For example, a commonly used type of whitelist is an email whitelist. This refers to a user's list of contacts that are deemed acceptable to receive email from. Spam filters utilized by email clients or internet service providers have whitelists (and blacklists) of senders and keywords to identify in emails. Mail on the spam filter's whitelist, of email addresses, domains, and/or IP address will always be allowed. Although whitelists can assist in allowing wanted messages to get through, they are not flawless. Email whitelists operate based on the assumption that most legitimate male will come from a limited list of senders. To effectively reduce spam, email filters must be updated as consistently as email spam senders create new email addresses, allowing their messages to slip through the whitelist.

Another use for whitelists is local area network (LAN) security. Often times, network administrators set up MAC address whitelists to control who is allowed access to their networks. This method is utilized when encryption is not a practical solution. MAC address whitelists are sometimes ineffective because MAC addresses can be copied or faked.

Program whitelists are records of software deemed acceptable for use. This allows organizations to ensure that users will not be able to download and use programs that have been deemed inappropriate. Application whitelists combat viruses and malware by allowing the operation of software that is considered safe to run, blocking all others. Program and application whitelists are common in schools, libraries and places of employment.



Lancet/Spring Lancet

Lancets were developed in the 19th century and manufactured by the millions in England, France, the United States of America and elsewhere. Some lancets were marked with the name of the owner, while others were marked with stamps or other insignia. Lancets were not disposed of after use. Rather, they were used again from patient to patient. Lancets were considered to be standard equipment for doctors and barbers alike. They were carried in valuable cases, made of ivory, mother of pearl, tortoise shell or even gold. Prized possessions of the time, lancets were necessary instruments in the tool kit of any physician.

Unified Threat Management

Unified Threat Management (UTM) is the comprehensive evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single appliance. UTM facilitates network firewalling, network intrusion prevention and gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data leak prevention and on-appliance reporting. The claimed advantages of UTM come from the facilitation of anti-virus, content filtering, intrusion prevention and spam filtering functions deployment in a single appliance. The UTM approach claimed cost-effectiveness both in terms of purchase price and in cost of operation compared to other information security technology solutions.

Traditional point solutions, commonly installed to solve major threat and productivity issues, are more difficult to deploy, manage and update than UTM solutions. A single UTM appliance simplifies security strategy by reducing the number of components that must be made to work together and permitting configuration and monitoring of all security solutions from one console.

UTM appliances assist with compliance with the increasingly regulatory global environment including compliancewith HIPAA, GLBA, PCI-DSS, FISMA, CIPA, SOX, NERC

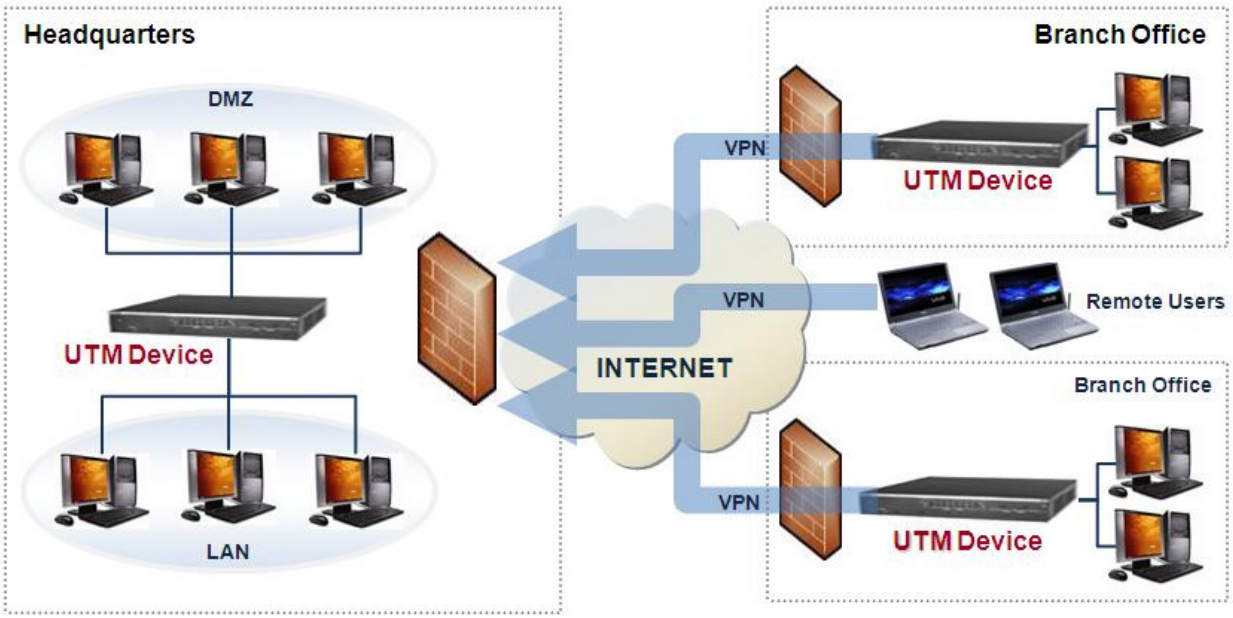
and FFIEC, which specify access controls and auditing capabilities. Some UTM's make a step toward authenticity-based solutions by enabling policy creation based on the user identity, in order to comply with some regulations.

Although UTM's provide many advantages, they bring a few key disadvantages such as: the potential of a single point of failure for network traffic, single point of compromise if the UTM has vulnerabilities and the potential impact on latency and bandwidth when the cannot keep up with traffic.

Fleam and Bloodstick

The fleam and bloodstick were used in both human and veterinary bloodletting. Fleams are instruments with beveled blades set at right angles to the handle. A fleam kit typically housed blades of varying sized to offer a wide selection for the preference of the practicing physician. Smaller blades were typically used for humans, and larger blades were used to penetrate deeper tissues on animals.

Bloodsticks were heavy wooden clubs used to quickly drive the fleam into the flesh of the animal or human patient. For animal bloodletting, sheets were often placed over the heads of the victims so they did not know what to expect. In most cases, humans were not treated in such a way.



The Epistemology of Best Practices

While we are tempted to begin this section with parables involving naked emperors, we will stay with our more objective and less allegorical explanation of how large numbers of intelligent people come to believe that which is not true. Epistemology is the study of the way people come to know things – or to "know" - things.

The Epistemology of Bloodletting Best Practices

Ancient physicians Hippocrates (400 B.C.E., Greece) and Galen (2nd century A.D. Rome) accepted the common belief that the universe was comprised of four basic elements: earth, wind, fire and water. A belief in a mysterious symmetry between the makeup of the universe and that of the human body led to Hippocrates' hypothesis of the existence of four basic substances in the overall makeup of the human body. Those substances, referred to as humours, were blood, phlegm, yellow bile and black bile. From this notion, the philosophers suggested that optimal health depended upon the perfect balance of the humours within the body. Conversely, disease was seen as an effect of the imbalance of the humours.

The practice of bloodletting was conceived as a means to effect the balancing of bodily humours. Bloodletting is the surgical removal of quantities of a patient's blood so as to heal sickness and disease. Galen believed that blood was the vital force of the body, the dominant humour, and thus in need of the most control. Bloodletting was thought to regulate the balance of this humour by releasing excess fluid and impurities. Galen created a formula that specified how much blood was to be removed from a patient based upon age, location, constitution, the season and the weather. The nature of the blood let was determined by the type of disease; certain blood vessels were associated with particular organs. The more severe the disease, the more blood to be released. Fevers, considered to be among the most fatal of illnesses, were thought to be cured by the letting of copious amounts of blood.

While Hippocrates and Galen deserve the recognition they have received over millennia for practically originating the field of medical care, their attempts at effective medical practice were undermined by erroneous assumptions leading to ill-advised procedures. Bloodletting was only one such misguided practice borne of bad assumptions. Galen's writings on human anatomy were full of errors; Hippocrates believed that sneezing was caused by an overabundance of heat surrounding the brain, or the head being filled with excess humours.

A common thesis about the shortcomings of ancient medical care puts the blame on lack of diagnostic tools and technologies, and certainly that is part of it. Also responsible, however, is the simple lack of development of effective thought processes and observational methods.

Epistemology is the study of the ways in which we come to know things. Where did Hippocrates and Galen come up with their "balance of humours" hypothesis? It seems that the best answer is that somehow Hippocrates developed a hunch about the symmetry between the way the universe was constructed and the makeup of the human body; and in the absence of other hunches, especially observationally sound hunches, the four humours hunch became the basis for "Best Practices" in medical care for nearly two thousand years.

It wasn't until the middle of the nineteenth century that the notable French physician and researcher Pierre Charles Alexander Louis decided to test the effectiveness of bloodletting practices through statistical analysis. Just how many lives were bloodletters saving? Physicians believed that daily application of the therapy, followed by perceived patient recoveries provided all the 'proof' they needed to see that bloodletting was effective. However, when Louis completed his statistical analysis, he found that bloodletting actually increased mortality! At first, Louis considered his find-

To his dismay, Louis's statistical analyses showed that bloodletting increased, rather than decreased, mortality

TABLE 1. Age, number of bleedings, duration of illness, and risk of death according to day of first bleeding in Pierre-Charles-Alexandre Louis's "Researches on the effects of bloodletting . . ."

Day of first bleeding	No. of subjects	Mean age (years)	No. of bleedings	Duration of disease (days)	Mortality (%)	Relative risk[a] (95% CI[b])
1–4	41	41	2.8	17.8	44	1.8 (0.9–3.5)
5–9	36	38	2.3	20.8	25	1.0 (reference)
Total	77	40	2.6	19.2	35	—

Sources: [16, 17].
[a]Not computed by Louis.
[b]CI = confidence interval.

P.C.A. Louis, French physician
1787-1872

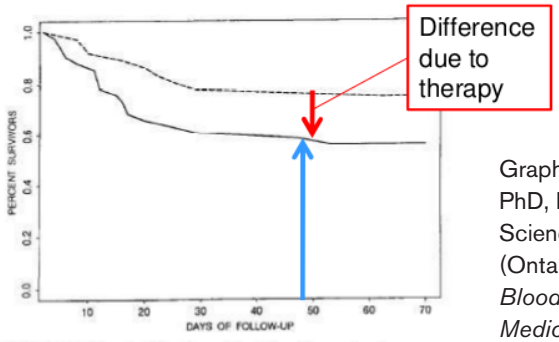


FIGURE 4. Survival by day of first bleeding, using data presented in Figures 2 and 3. Bled Days 1–4 (*solid line*), bled Days 5–9 (*dashed line*), log rank $p = 0.07$.

Graphic by Brad Hanna, DVM, PhD, Department of Biomedical Sciences, University of Guelph (Ontario) from his lead talk *From Bloodletting to Evidence-Based Medicine* at Equine Guelph's first *Integrative Therapies Night*, May 19, 2011. By permission of Dr. Hanna.

ings to be absurd, but further examination led him to believe that they were accurate.

When the news of Louis's analysis reached medical research facilities in the United States, his conclusions were met with skepticism and even ridicule. After all, how could such long-accepted and constantly relied-upon best practices be based upon unsound assumptions?

Among those doubting Louis's findings was J.J. Jackson, a renowned Massachusetts General Hospital physician. Jackson decided to repeat the procedures used by Louis in research of his own, using his own data sets. Much to his surprise, he found similar results with his own patient histories.

Thousands of years of direct clinical experience with bloodletting proved two things: (a) bloodletting leads to increased mortality rates in patients suffering from systemic diseases, and (b) bloodletting convinced millions of physicians and patients alike that it somehow saved lives.

Despite the numerical evidence presented by Louis and Jackson, physicians continued to use bloodletting techniques in the treatment of their patients because they felt that anecdotal observations based upon their clinical experience was all they needed to prove that the techniques were effective.

The Event That Raised Popular Doubt

Among the general population there existed a "they're the experts, they must know what they're doing" attitude toward the practice of bloodletting. After all, we must trust the experts.

But occasionally an event such as the death of George Washington evokes questions; or perhaps it provides the catalyst for private doubts to be expressed openly.

In 1798 the recently retired George Washington developed a severe throat ailment while performing work on his home in the rain. After many rounds of bloodletting in quick succession, General Washington died two days later.

As Dr. White McKenzie Wallenborn of the University of Virginia School of Medicine notes, "It would be improper for today's medical practitioners to be critical of the physicians of George Washington's day if they were delivering the standard of care that other physicians of that era were giving to their patients. It would appear that Dr. James Craik, Dr. Elisha Cullen Dick, and Dr. Gustavus Richard Brown were well trained as physicians, were honest and caring, and gave the kind of medical care that their peers would have given. Today we know that many of their methods were wrong and we would do things differently… Today we find the removal of about eighty two ounces of blood (about five pints or units of blood) from a sick patient in less than sixteen hours to be incredible. However this was the method of treatment being taught in those days. It was the treatment of choice for many diseases and the complications of using this method were not comprehended by the physicians of that day."

Certainly it would be improper to blame those four physicians for having practiced medicine as they had been taught. On the other hand, the entire medical profession can certainly be held to account for its failure over thousands of years to examine the assumptions behind the very common and very intrusive practice of bloodletting.

The complications of using bloodletting were not comprehended, but patients and their families and friends must have had their private doubts. When a person as prominent as George Washington dies suddenly after the application of a practice of which people are skeptical, some amount of doubting will be done in public. As the French media were obsessed with news from America in the early nineteenth century, perhaps the story of Washington's treatment and outcome was a catalyst for Dr. Louis's decision to be the first in nineteen centuries to take the time to quantitatively analyze the outcomes of bloodletting procedures.

The Epistemology of Information Security Best Practices

To protect an information resource, information security technology in the form of firewalls, application firewalls, intrusion detection and prevention systems and other systems establish information security by identifying the intentions and character of the sender of a stream of bits.

One might ask whether it is possible to identify the intentions and character of the sender of a stream of bits. To do so, however, would be to ignore the decades of development of best practices in the field of information security technology.

Where did those practices come from? Indeed, what is the epistemology of the assumptions behind most information security technology?

From *Quiet Enjoyment, First Edition by* Wes Kussmaul

Open Range Cowboys

When we spend time on the Internet, we inhabit territory that was settled by a group of people with needs and views very different from our own. For sure, the territory could not have been settled without them – the Internet could never have been settled, or built, without the open-range cowboys.

Cowboys know how to handle themselves on the open range. Further, an open-range cowboy has no use for buildings – office buildings, schools, department stores, or any other type of enclosure. The cowboy is just fine sleeping under the stars.

If you asked a nineteenth-century cowboy out on the plains what he thought of the tendency of open spaces to make commerce impossible, he would probably have to think about what commerce was and what it had to do with his life.

If you asked that cowboy what he thought of the tendency of open spaces to present unacceptable hazards to children, he would have considered the question really odd. After all, how often did he encounter children? "What would kids be doing out here on the open plains?"

But our children are spending time online, chatting away with strangers under the open sky. Our important files are sitting out there in the open, in piles between the sagebrush bushes. Critical resources by which we manage utility and information infrastructures are strewn around the desert sand as though they were so many prospectors' pickaxes.

Why has the world paid so much attention to the open-range cowboys? Why do we treat our Internet as though it still fits their romantic but delusional notion of their frontier Internet? Why does the world resist the construction of useful online bounded spaces?

The answer is that the new online space developed in a manner very similar to the development of the American West. As with the West, there are strong traditions to be dealt with. The romantic notion that the plains must remain open is one of the strongest of the Internet traditions. Tradition has a reputation as something that is built over long periods of time, but there are Internet traditions that are [as strong as] those of the Roman Catholic Church. The strongest of those is the open-plains tradition.

A True Cowboy Story from the Open Plains

Digital Equipment Corporation's operating system called VMS was the first interactive system to really make commercially available a complete set of secure access and privilege controls. It combined a number of identifiers of an account with a number of privileges that an account or a process had. In other words, VMS was kind of like the real urban world, asking the questions, "Who are you? What company do you work for and in what capacity? What are you authorized to do and where are you

authorized to be?" That's a fine place to start thinking about where to design the entrances and common areas and walls and doors with and without locks in a new office building.

Now, a lot of programmers who were used to Digital's earlier operating systems did not like those boundaries. They were used to being cowboys on the open range of computing, having all the address space rangeland available for their roaming. But even if we assume that roaming was with the intent of being productive, that presented a problem. Though the cowboys knew that more people were using their computer systems and therefore things had to change, they were nevertheless as hostile and vocal as were the open-range cowboys of the Old West about the new boundaries.

The people who built VMS tried to explain to management in their customer companies why their computer had become too important and too complex to allow the cowboys to continue to roam free. But the cowboys were right down the hall in the engineering computing department, while Digital was a vendor from somewhere in central Massachusetts. So the customers told the vendor: "Our technical people say the access and privilege controls in VMS cramp their style. They say they make them less productive." Well, of course. And wouldn't we all like to have unfettered access to the situation room at the White House, and the anchor desk at NBC, and for that matter the offices of the IRS. Wouldn't that kind of freedom make one more "productive" in entirely new endeavors? I needn't go into the good reasons why it is not easy to get such access to the White House and NBC and the IRS.

But management didn't understand what Digital was trying to tell them – that the reason their software people were saying, "Don't fence me in" was precisely the reason they needed to be fenced in. Think about it: when was the last time someone told you they needed stronger controls imposed on themselves to prevent them from doing you harm?

The "technical folks" were the in-house experts. They insisted on being allowed to roam free.

TECO

Digital offered a solution to keep the technical cowboys happy with VMS – it was called TECO. It sounded innocent enough; it was called an "editor." But calling TECO an editor is like calling a nuclear weapon a large heavy object. TECO was an editor that could go anywhere and do anything within a VMS system.

TECO was great fun to use. It was one of those editors that assumed you could keep an entire detailed picture of the file you were working on in your head; it was macho to work in TECO for half an hour without ever asking it to display the contents of the file you were working on. You could move mountains with a few very terse commands. You could inadvertently destroy the company's receivables files with a single misplaced punctuation mark. At best, in the hands of a well-intentioned worker, TECO was a big hazard. In the wrong hands TECO was as dangerous as an angry open-rangeland cowboy with a score to settle in modern downtown Oklahoma City. ("Boss, he's not going to do any harm, all he's got in that truck is diesel fuel and fertilizer.")

VMS was distributed with a warning: unless you have a very specific reason for keeping TECO, the first thing you should do is make sure it does not get installed with the operating system. If for some reason it gets installed, get rid of it right away. But at most VMS sites, if you typed "teco" at the command prompt, there it was. TECO typically got installed – and kept. Why? Why would those responsible for such systems leave such a hazard lying around?

Systems people understood how dangerous it could be. But it could also be immense-

ly useful. And after all, who did the installation of an operating system but those who would use it most. Management typically never saw the distribution package, and if they did their attitude was "My software people said they needed it." Sure, and your facilities department could probably move walls more quickly if you'd only let them use dynamite to do the job like they asked.

The irony is that without TECO, VMS is one of the most rock-solid-secure and rugged systems around, a marvel of software engineering.

The TECO story has an exact parallel in the Internet world. Somehow the open-range cowboys have got us convinced that the construction of walls and the designation of specific uses and behavior for specific enclosed spaces are tantamount to destruction of the First Amendment. And the bad consequences of the open-range tradition don't stop with hazards that are visible on the screen. The tradition leads us to believe that we are in a kind of free will heaven, when in fact it is appallingly easy for any company or government, or even an individual with money, to snoop on our every move while we are on the Net.

What we are talking about in this book strikes the Internet's open-range cowboys as fencing in the old West.

There was a time when the best use of the western American plains was as open rangeland, not owned by anybody, free for anybody to use to graze and drive cattle. But the population grew to the point where title deeds and fences became necessary. Then came residential settlements, then towns, then Kansas City. Kansas City defines a space that is "highly developed," meaning there are buildings with rooms designated for particular uses by particular groups of people, many surpassing Cowboy Will's wide-eyed "… seven stories high! 'Bout as high as a buildin' oughtta grow!"1

Today, the notion of open rangeland is romantically compelling and totally impractical. For precisely the same reasons, the notion of an unbounded open Internet as anything but the solid ground beneath the bounded and controlled spaces defined by the buildings above is equally romantic and equally impractical. It's reminiscent of the 42nd Street cowboys in New York City (John Voigt in Midnight Cowboy) acting out a persona that is ridiculously out of place.

The Internet is sometimes still characterized as a highway system. If only we thought of it as just that, and asked ourselves what happens after highways are built. While we do use highways to get to parks and open land, most of what we transport ourselves to with highways are office parks, hotels, conference centers, meeting places, and residences. For those of us who do not spend our days cruising the Interstates just for the joy of being on the open road, those bounded spaces are what make our physical highways truly useful.

Why should it be any different with our online spaces? Should our online highways not also bring us to bounded, secure, manageable online spaces? Is it not precisely the absence of such spaces that causes the problems that we write about?

Furthermore, our physical highways themselves are not exactly places of anarchy. Vehicles are registered, and every vehicle registration is linked to a driver's license or corporate identity or other means of holding people responsible for the drivers' actions.

Why, then, is our online highway system (1) a place of total anarchy (2) host to a huge number of roadside stands, bars, rest areas, and other public facilities that common sense tells us should be bounded spaces? For some reason we let those who built the highway tell us that everything is a highway, that you can't use the highway to get to places that are not highways.

Why do we conduct business by the side of the highway? Why do we let our kids hang out unsupervised in Times Square, where

filters called ordinances keep some of the pornography from their view but do nothing to prevent strangers from approaching them?

We do these things because the open-range cowboys who best understand the land beneath this new space, and who truly love that land, tell us that's the way it must be. While we can understand and respect their perspective, we must understand that their perspective is not our perspective. They generally do not need the same things we do. The rest of us need bounded spaces as much in the online world as we need a roof over our heads where we live and where we work and where our kids go to school.

We cannot afford to let our policies be made and our spaces designed and governed from the open-range mindset, just because the people there have a better understanding of Internet technology than the rest of us.

From *Quiet Enjoyment, Second Edition by* Wes Kussmaul

When Henry Bessemer and Joseph Monier invented structural steel and reinforced concrete in the middle of the nineteenth century, they and their colleagues were sure that fifteen story buildings would quickly pop up all over the developed world. Cities would be transformed; the world would be changed.

Decades later there were still no fifteen story buildings. Cities looked pretty much the same as they had before the miraculous new materials had been made available. And so the materials scientists, to varying degrees, lost faith in their inventions. Steel and concrete, they concluded, were a great idea but impractical for wide deployment.

So what had caused society's inability or unwillingness to make effective use of structural steel and reinforced concrete?

Let's start with building codes.

Building codes have been around since at least the time of the Code of Hammurabi, which mandated that, among other things, "If a builder builds a house for someone, and does not construct it properly, and the house which he built falls in and kills its owner, then that builder shall be put to death." Later, the Law of Moses as expressed in Deuteronomy chapter 22 verse 8, gets specific about roofing: "In case you build a new house, you must also make a parapet for your roof, that you may not place bloodguilt upon your house because someone falling might fall from it."

The spirit of the late Enlightenment, along with burgeoning populations, brought the science of urban planning to the fore in the early nineteenth century. Around the same time as the invention of structural steel and concrete, London's Metropolitan Buildings Office was formed in 1845 to regulate the construction and use of buildings.

Among the first of the new, enlightened building codes was the stricture that streets were to be at least 40 feet (12 meters) wide, or the width to be the same as the highest building in the street, whichever was the greatest.

See a problem there? A fifteen story building will have to front on a street that is as wide as the building is tall. Obviously the inventors of the new construction materials and the writers of the new building codes were not on the same page.

Now if you asked the materials inventors and the writers of the new building codes about future prospects, they would each have responded with an enthusiastic picture of future buildings better able to serve the needs of people in comfort and safety. And if you looked at those two pictures you'd realize they had very little in common, that they could not both have been fulfilled in reality without major rewrites. There was not only no communication between the two groups, there was not an ounce of common understanding of reality between them.

Let's pretend it's 1847. Pretend you and I know only what we would have known if we

lived then. Let's list ten reasons why fifteen story buildings won't work. Here's my take on the problem:

1. The only cranes in existence are of no use here. Regardless of how good steel and concrete are, once you've built the first few floors there is no way to get those materials to the top floors, so there is no way to construct a 15 story building.
2. It will be impossible to get tenants for those floors because no one wants to walk up more than six flights of stairs.
3. Building codes make such buildings a legal impossibility, as illustrated above. Just spending time planning such a building is folly. Our building permit application would generate peals of laughter.
4. Similarly, very few architects have heard of these new materials, let alone have the requisite familiarity with them. No design professionals know how to design such a structure.
5. Same with contractors. No builders are able to construct the building.
6. Where is financing for such a structure to be obtained? Potential lenders and equity investors have never heard a 15 story building. Which one would step forward and be the first?
7. The real estate brokerage profession is very primitive and not at all ready to deal with the process of leasing space in such a building.
8. There is no body of tenancy law for such a complex structure. How is quiet enjoyment defined in such a building?
9. The density of outhouses in urban areas already makes for barely tolerable sanitary conditions. Picture the outhouse density required for a fifteen story building (or perhaps it's something you really don't want to picture…) Indoor plumbing is required, and very few people know how to design and build these newfangled indoor plumbing systems.
10. Actually, the new indoor plumbing isn't enough, unless all toilets are located on the first few floors. Getting water to the upper floors and wastewater safely down will require version 2.0 of indoor plumbing, and at present we're at about version 0.7. Tenants on the upper floors will need to learn to ignore the call of nature.

If you had posed the notion of fifteen story buildings in 1847 those would have been cited as insurmountable problems even to the great minds of the day. And indeed, given the technology of the day they were insurmountable. But it wasn't simply a matter of unavailable technology. There was also a mindset obstacle.

A couple of decades later the problems still seemed insurmountable but in fact they were not. Most of the solutions had been developed to a sufficient extent; but those solutions had yet to enter the understanding of those who could deploy them. The result was surprising and disappointing delay in the construction of tall buildings.

Fast forward to the present. Tower cranes and elevators and indoor plumbing are part of common everyday experience. It doesn't take a great mind to envision a fifteen story building; everyone in an urban setting uses buildings two or three times that tall all the time. With a combination of experience with concrete and steel buildings and a little common sense, plus the tidbit about building codes above, anyone could probably write a few paragraphs about "what's needed to build real world 15 story buildings out of concrete and steel."

When it comes to PKI, we are in 1875. That is, *the technologies, methods, and procedures for solving our information security problems have been in existence for a few decades, but those who could put them to effective use are not aware of them.*

PKI is a very high quality set of building materials, produced by brilliant materials

scientists for the construction of what we characterize as digital buildings.

Materials scientists may or may not be familiar with things like building codes and occupancy permits and professional licensing and professional liability of architects, contractors and building inspectors. Certainly the inventors of steel and reinforced concrete weren't thinking about the need for elevators. And cranes. And about the liability of public officials who were being called upon to put their professional licenses and reputations on the line for some very unproven technology.

And why should materials scientists concern themselves with such things? That's not their job! That's the job of the rest of society. In other words, it's up to you and me to understand how this marvelous construction material called PKI can be made to fit into the real world to solve real world problems.

Time to replace "best practices" with better practices

The information security problem is an effect of a bigger problem. That problem is inauthenticity.

Replacing inauthenticity with authenticity will solve a multitude of problems. Security is just one of them.

Here's how to bring the benefits of Authenticity to your organization:

- Start with measurably reliable digital certificates and their accompanying PENs
  (Read Quiet Enjoyment, 2nd Edition, to learn how this is being accomplished.)
- Address trackability-related privacy concerns by emulating highway management practices
  (Read Quiet Enjoyment, 2nd Edition, to learn how this is being accomplished.)
- Replace the catch-the-bad-guys mindset with accountability by means of pervasive digital signatures from measurably reliable identity credentials
  (Read Quiet Enjoyment, 2nd Edition, to learn how this is being accomplished.)
- Replace open-rangeland-fortification architecture with useful and manageable structures that allow productive work to get done
  (Read Quiet Enjoyment, 2nd Edition, to learn how this is being accomplished.)

What is QEI?

Quiet Enjoyment is the conveyed right to possess, use, and enjoy a facility in peace and without interference.

Most network security products and services are all about identifying the bad guys and capturing or killing their packets, treating security management as a kind of warfare. But how can you run a business on a battlefield?

In the physical world we have a better way of creating and managing bounded, secure and manageable spaces where we can get things done. They're called *buildings*.

Move your facilities away from the battlefields, information highways, intranets, extranets, VPNs and other tunnels whose ends are open to the outdoors. Now, with the **Quiet Enjoyment Infrastructure**, your online facilities can be as secure, manageable and understandable as your physical office.

The **Quiet Enjoyment Infrastructure** consists of technologies, standards and methods that turn your online facilities into office suites, meeting rooms, reception areas, and other familiar spaces that have proven themselves over the years.

QEI is a PKI that:

- Answers point-by-point the Schneier and Ellison 10 Risks and other PKI critiques
- Builds on the original Universal ID idea
- Provides an identity source with an important (often overlooked) ingredient
- Addresses Universal ID concerns with robust privacy protection
- Imports effective methods and procedures from the world of physical buildings

The Quiet Enjoyment Infrastructure consists of Twelve Components in Three Groups:

Part I of QEI
PEOPLE: The Authenticity Infrastructure

Question 1: *Authenticity calls for pervasive digital signatures by reliably identified human beings. How do you protect the private keys, while making them available for digital signatures?*
Answer:
1. PEN Component
Nothing we do with computers, cell phones, PDAs, or other information appliances will be secure until there is a sound way to keep files, directories, keys, identifiers, and other important items in a truly protected space. Many efforts such as TPM and UEFI Secure Boot attempt to accomplish this, but each will fail unless it is part of an integrated system that allows the user to determine whom to trust, and which uses a reliable source of identity credentials.

Question 2: R*eliable digital identity certificates, professional licenses and occupancy permits call for a reliable source of issuing public authority that is independent of any geographic jurisdiction. Where do we find such a source of duly constituted global public authority?*
Answer:
2. Public Authority Component.
On March 7, 2005 the City of Osmio was chartered at the Geneva headquarters of the oldest international governance body in the world, the International Telecommunication Union. Osmio's Vital Records Department is a certification authority that limits its practice to identity certificates. The Professional Licensing Department will issue licenses that will allow architects, contractors, and building inspectors to sign plans for facilities and occupancy permits. Osmio's authority is strictly limited to those who choose to accept it, and its governance is as participatory as that of a small New England town.

Question 3: *How do you establish identity in the first place?*
Answer:
3. Enrollment Component
Enrollment can be costly or not, depending upon the level of rigor needed by relying parties. The Enrollment Component ensures that evidence supporting a claim of identity is gathered properly for the requisite level of rigor and presented along with the public key in a certificate signing request to the Osmio Vital Records Department.

Question 4: *When someone identifies herself to you, how do you know how reliable is that claim of identity?*
Answer:
4. Reliable Identities Component
The foundational identity certificate is accompanied by other certificates and by an identity quality record. A relying party might know very little about the person identified other than the identity quality information and the fact that the identity certificate has not been revoked. But that is sufficient to establish accountability.

Question 5: *Personal control of information about oneself has been a long-sought goal of privacy activists. How can a universal identity credential restore privacy rather than erode it even further?*
Answer:
5. Personal Information Ownership Component
The foundation of real privacy is your own control over information that identifies you. Without such strong controls, individuals will rightfully resist the idea of a strong identity infrastructure. Because the companies that accumulate information about you regard that information as their own corporate asset, the PIOI provides technological and legal tools by which you can reclaim that asset as your own personal property.

Question 6: *We value anonymity, but at the same time we want others to be accountable. What happens when someone whose privacy is protected anonymously harms me, my community, or my country?*
Answer:
6. Accountability Component
As QEI must protect your privacy, it must also protect your right to recourse if you are harmed by someone whose privacy is similarly protected. Law enforcement must also be able to seek a court order to intercept communications when a legitimate court deems it necessary to protect public safety. The Accountability Component ensures that due process prevails.

Part II of QEI
PLACES: The InDoors Infrastructure

Question 7: *By what standards are we assured that an information facility is habitable, that is, secure and manageable?*
Answer:
7. Building Codes Component
Your information is never secure in a private, cryptographic tunnel if it is exposed at the ends of the tunnel. Indeed, a tunnel can be less secure than the outdoor space around it, because it gives its occupants a false sense of security. Building codes are sets of standards and procedures that ensure the integrity of the virtual buildings that enclose, for example, the ends of tunnels.

Question 8: *How do we bring the benefits of InDoor spaces to our computers and phones?*
Answer:
8. Indoor Operating System
We can work around the vulnerabilities of popular operating systems so that the components of QEI provide genuinely secure, manageable, usable, and private space inside those operating systems. An even better solution for the long term will be to gracefully exchange the vulnerable and cranky old operating system foundation for a more reliable, secure, and manageable one, while keeping most of the familiar user interface and applications programming interfaces.

Question 9: *Who decides whether a facility is habitable, that is, that it conforms to building codes?*
Answer:
9. Professional Licensing Component
As with physical real estate, our bounded online spaces need qualified architects, contractors, property management people and building inspectors to ensure that they serve our purposes. As with physical real estate, the Professional Licensing Component provides a system of certification of their credentials and of the results of their work.

Question 10: *How do we bring privacy and authenticity to social media?*
Answer:
10. Community Component
Where are these online buildings built? Who owns them? Who pays for them? How do they connect to each other in a rational way? We find our answer in the surprising intersection between skills and methods in the media industry and those of the urban planning profession.

Question 11: *Can the outdoor public transport system also benefit from QEI?*
Answer:
11. Public Roadways Component
The roadway system, the Internet, is far ahead of the virtual real estate it needs to connect – the secure online places where people can safely gather. Its protocols, like those for the next generation of concrete Interstate highways, are well established. But the facilities that control the Internet are entirely too vulnerable to terrorists and vandals. Access controls based upon strongly established identities must be in place.

Part III of QEI
THINGS: The Common Vocabulary Infrastructure

Question 12: *Strict definitions of terms reduces confusion in the world of building codes and permits. Can terminology standards reduce rampant "FUD factor" confusion in information technology?*
Answer:
12. Common Vocabulary Component
What information technology provides to the online world is no more mysterious than what architects, contractors, and property managers provide to the physical world. The Common Vocabulary Component requires the use of standardized terminology in the permitting of new facilities. By using the well-understood language of real estate, management can finally direct information technology, rather than the other way around.

References

Arbittier, D. (2011). Bloodletting antiques. Retrieved from http://www.medicalantiques.com/medical/Scarifications_and_Bleeder_Medical_Antiques.htm

Brain, P. (2009). *Galen on bloodletting: A study of the origins, development and validity of his opinions, and a translation of the three works.* Cambridge, ENG: Cambridge University Press

Hanna, B. (2011). Lead talk at Equine Guelph's first *Integrative Therapies Night*. Guelph, ON

Fielding Hudson Garrison (1914), *An introduction to the history of medicine: with medical chronology, bibliographic data, and test questions.* London & Philadelphia, W.B. Saunders

Pfleeger, C. P. (2002). *Security in computing.* Boston, MA: Pearson Education

Tipton, H. F. (2003). *Information security management handbook.* Boca Raton, FL: CRC Press

Wallenborn, W. M. (1997) *George Washington's Terminal Illness: A Modern Medical Analysis of the Last Illness and Death of George Washington*

Morabia, Alfredo (2006) *Pierre-Charles-Alexandre Louis and the evaluation of bloodletting,* Journal of the Royal Society of Medicine 2006 March; 99(3): 158–160. PMCID: PMC1383766

(2011, November 17). http://en.wikipedia.org/wiki/Bloodletting

(2012, November 30). http://en.wikipedia.org/wiki/Information_security