



The State of Information Security: The Risk of Attack is Unacceptable

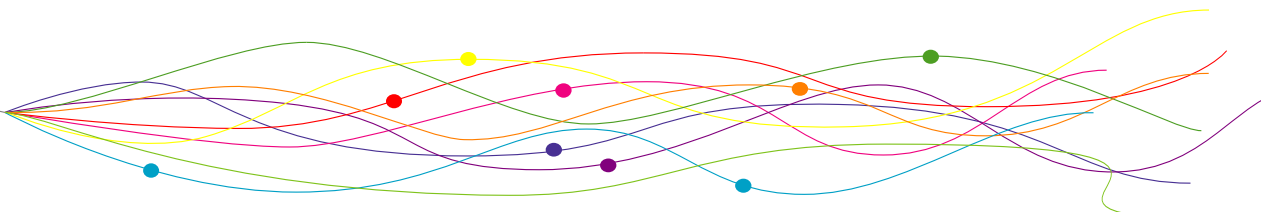
Computers are everywhere in our lives. In addition to giving us virtually instant worldwide communications capabilities, computers literally allow us to run our businesses, our commerce, and our government...including highly complex military systems that are integral to our national security. Without these systems, our current way of life comes crashing to a halt.

The genesis of interconnectivity brought on by the internet and the world wide web has caused an explosion of connections, resulting in an evolving incredibly complex system of systems. And there are holes in those systems...gaping security weaknesses. The complexity of it all continues to grow minute by minute, and the holes are getting larger and more numerous, surpassing our ability to stay ahead of security issues. The dike is leaking, so to speak, and with our current approach to cyber-security, we simply cannot plug every hole. We are vulnerable to a catastrophic cyber attack today...right now...and it's inevitable that hackers, whether individuals or nations, will continue to take advantage of openings in their efforts to deal the United States a critical blow.

The current state of our information security is "broken at best," contends Harry Haury, CEO of NuParadigm Government Systems, Inc, and noted government computing systems authority. In a paper titled "Explosion of Connections: Information Security is Broken, Ineffective at Best," prepared for the Office of the Secretary of Defense(OSD), Haury claims the current security methodologies and standards of practice for connecting systems, secure storage and the transfer of information are impractical and unsustainable into the future. We're merely putting a finger into the dike whenever breaches to information security are realized; we're reacting to new holes and fixing them with patches, putting ourselves on an unsustainable path that is resulting in overly complex systems that are un-sustainable into the future. While we're plugging the holes in the dike, the entire structure threatens to collapse around us

Haury uses a number of scenarios to convey the magnitude of the current risk, scenarios that are completely possible right now given the current state of our IA frameworks. He asks us to imagine a Christmas-time attack where cyber-attackers target systems that automate credit transactions and they pour in hundreds of millions of fraudulent credit card orders. The torrent of misinformation bankrupts the credit card companies under the impossibility of untangling the real from the fake transactions, retailers can't sell their products without a trustworthy electronic credit system, and the nation's economy is brought to a halt. Or how about a physical attack on critical internet cable hubs? This would literally disrupt all our communications...internet, phones, etc....right down to our electrical grid. Done in the deep throes of winter, thousands of lives could be lost as power systems fail. And what about our military information systems? They control the operations of our sophisticated attack and defense equipment. A cyber-invader could literally turn our own systems against us, causing misguided attacks damaging ourselves and our allies, possibly causing tens of thousands of deaths.

"The vulnerability of our critical systems to attack proves it is time to take these issues seriously; meaningful and comprehensive efforts need to be undertaken immediately to protect our networks, systems and data with the highest national priority," says Haury. The long term solution is to build better systems where structure is inherently sustainable, requiring a new paradigm, a new approach to the future protection of information, especially in terms of electronic transfer of data, systems connectivity and interoperability. Says Haury, "While most IA / security subject matter experts (SMEs) would agree that there are serious IA issues, the broader issue is how to step back and fix the problem rather than continuing the current approach of piecemeal patches reacting to security vulnerabilities – adding complexity without addressing the root causes." Haury advocates a new approach that relies on "a new architecture that is simpler, systemically consistent, significantly more flexible, sustainable and most importantly



affordable.” This new architecture uses a “data centric model that will...work with legacy and new systems alike,” says Haury. We need to focus on protecting the data itself, rather than the devices it is stored on and transmitted through. We tend to protect information pretty well when it is residing in servers and storage devices, but we drop the ball when we put information in motion and transmit it over a network or across the word-wide-web, where it remains extremely vulnerable to attack. The new goal needs to be protecting information wherever it lives, whether in storage or in transit.

The time to start developing and implementing this new paradigm is now, before the inevitable inability to maintain the current approach overwhelms us, causing ever more critical breaches. In Haury’s opinion, “the Department of Defense and Intelligence community will keep throwing massive amounts of money away on an approach that cannot work, creates unsustainable complexity, and is always in reactivity mode versus investing a relatively small amount of funds to rebuild IA capabilities for the emerging systems paradigms.” With the greater exposure we’re facing with information flowing through the web, and with the net centric issue of more and more people, devices, information and services being interconnected within and across networks, we simply have to take a new approach to security.

Under the new paradigm espoused by Haury, we can fill the protection gap that exists as information travels between systems by establishing “an end-to-end trust model, which is standards based and open architecture that can support anonymity and non-repudiation but also addresses directly the ability of one community, system or participating entity to trust another.” In other words, managing the flow of information needs to involve security and encryption that can accurately recognize and authenticate authority throughout all data channels, where information lives in a constant state of secured encryption as it travels, yet still completely supports the needs of multiple users to access and use that data when it is appropriate.

Haury suggests we’re kidding ourselves when we think the current oversight of security features and assurances is being managed effectively – it’s not, as a rule. Constant changes made to hardware, software and other critical parts of systems make it unrealistic on a practical level. What we need is a new capability for securing meta-data, the data that tells us about other data, and we need to improve our ability to authorize an object and transmit it along with its associated data information, all within a secure communications network.

Haury stresses that the first important step is for us to recognize and agree that the current approach is unsustainable, and a new paradigm needs to be put into place sooner rather than later. Addressing these problems will take a universal dedication and of course, a significant investment. But the investment in this type of change will be extremely modest versus the inevitable costs of continuing down the current path, especially if catastrophic security breaches occur before the old paradigm is fixed. With the current reactive approach of monitoring for security breaches, then jumping in to close the gaps as they occur, we’ll inevitably lose the battle. As more and more breaches occur beyond our ability to keep up, the more sophisticated assailants will inevitably exploit these gaps, and the worst of potential outcomes could be cataclysmic. The most frightening thing right now is that too few recognize or acknowledge the magnitude of this problem, and the inevitability of the coming wave of serious electronic security invasions if we don’t act proactively. Right now...to quote an old tale with an apt metaphor... “The Emperor has no Clothes”.

According to Haury, we need to develop a new approach that “centers on the creation of an enterprise trust environment and the controlling, limiting of privilege in arbitrarily complex intersecting systems of systems.” Haury is telling us that encryption of data is not enough. We need to develop business and government-wide systems where access to information is overseen and governed on multiple levels, where data can only be transmitted to individuals with the right level of authority...only to those who have a right to it. These systems need protocols that rigidly define levels of authority, and can accurately identify who has access to these levels. We need to be able to



fully trust the sources of information requests, ensuring that users are who they say they are. These multiple layers of defense are inherently rather simple concepts to develop and employ, but they create multiple barriers that are incredibly tough for hackers to penetrate. This is what Haury calls “an end to end framework for assuring, distributing and implementing trust.”

Imagine it this way. As human beings, we can walk down a street, and no matter where we are...whether at the park, or in a store, or in an office building...we have the ability to quickly recognize individual people and immediately assess how well we know them. If we don't know an individual, we pass on by...perhaps with a tacit nod of acknowledgement of their presence, or a simple “hello”. We know they're there, but no communication of information is exchanged at any level. However, when we come across an individual we know, we open up the lines of communication, and dependent upon how well we know a person, we regulate the level of intimacy that communication is allowed to reach. Your best friend may gain access to your most intimate secrets. A casual acquaintance may get a fair amount of information from you...but not the intimate details. Someone you see often, but don't really know...like a store clerk...may only get the most superficial information from you. We innately judge the character of each individual, with their character being related to their level of trustworthiness, allowing us to govern the control of information shared in our daily interactions.

Haury argues that our regulation of electronic information can be controlled in much the same way, by building our systems with the right recognition and trust protocols that allow information access only to those who have the specific authority. And it doesn't matter if that information is located on a server, or on its way through a router or hub, or travelling over the world wide web or internet, or residing on an individual workstation or laptop...we have the ability now to instill our data with the information needed to give it a character that can be distinctly and accurately recognized, and we have the ability to establish reliable identification systems to give users truly unique identities...allowing systems to govern the control of information it shares and with whom. Just as we recognize the identity of someone walking down the street, we can develop our systems to accurately recognize and identify users, and then give access according to the integrity, authorities and trustworthiness of any given user.

To realistically protect and secure our businesses, our economy and our nation against cyber-threats, now and into the future, we've got to implement this new way of thinking immediately. No longer can we afford to hold a reactive stance, plugging security breaches as they occur, putting fingers in the dike. The fact is our current approach will quickly gain so much complexity it will become utterly unsustainable, allowing more and larger breaches to open up, dramatically increasing our exposure to risk. Sadly, it seems we are largely ignoring the magnitude of the damage that could be inflicted right now. As Haury warns us, “our infrastructure has become so vulnerable to compromise that it is already a massive national security issue ranging from ecommerce to the Department of Defense.” We have the opportunity to act proactively, today, to dramatically improve the security of our information and our systems in general. We can regain that strong feeling of security with the deployment of this new way of thinking, this new paradigm.....or we can wait and wonder why we are picking up the pieces after a trainwreck that could have been avoided.

