ENVISAGE

STRIKING THE BALANCE:
SECURITY VS. UTILITY

Ari Vidali, CEO ENVISAGE Technologies Corp.

Presented to the NATO Advanced Research Workshop in Venice, Italy February 5-7, 2009

Abstract:

Maximum security requires by definition a "closed system" whereas maximum utility requires "openness." Is it possible to reconcile these two extremes? Can a highly secure system actually be easy to use?

With the exponential adoption of technology, highly interconnected computer & telecommunications systems have become an indispensible component of modern societies. Our reliance on information technology has penetrated almost every facet of daily life. Our critical services, financial systems, transportation and commerce rely upon the confidentiality, integrity and availability of these systems. Notwithstanding some promising advances, networked systems remain highly vulnerable to attack and exploitation by hackers, cyber criminals and terrorists despite the significant efforts and investments that have been put forth to detect, deter and mitigate these threats.

Most experts agree that the security of any information system is only as strong as its weakest link; the human beings who create and use them. This paper explores some of the root causes of the usability problem and how proper security practices are consistently being ignored or circumvented by the very users and organizations they were designed to protect.

We propose that this reality must be understood and addressed in order for systems engineers to architect effective, easy-to-use security solutions that enhance rather than limit system utility. In our paper, we propose that the security systems of the future must be highly convenient, largely transparent to end users, fully integrated across security domains, threat aware, and able to modify security policies "on the fly" in response to changing threat environments.

In a culture driven by convenience, one-stop-shopping and near universal access to information, system users will continue to find ways to circumvent even basic security protocols if they are too onerous and burdensome. While highly complex, inter-connected systems will always have flaws that can be exploited; the vast majority of attacks on cyber-infrastructure are made possible because of human nature.

Technology has become an indispensible tool for modern societies. Has our reliance upon technology become a two-edged sword? We argue that as hackers, cyber criminals, and terrorists become more technically sophisticated, the very technology that contributed to the rise of the western world is being exploited as one our greatest weaknesses by those with nefarious intent. Our paper concludes that to stem the tide, the security community must address some of these root causes of cyber insecurity.

Keywords: Security, Cyber security, Usability, Biometrics, Authentication, Human-computer interaction

"The more secure a system is, the harder it is to use.
The harder it is to use a system, the less secure it will be."
Brian R. Krause, Adducive

Introduction

It is September 11th, 2013. In a dimly lit room on the outskirts of Peshawar in Pakistan, five men stare into their computer monitors as their fingers rapidly tap on keyboards. Unbeknownst to them, their state-of-the-art equipment was funded by a relatively new drug cartel operated by Taliban warlords. With the massive financial resources derived from the burgeoning poppy trade, the cartel was able to ensure that the five had sufficient funds for their purposes.

Calling themselves the *New Islamic Martyrs Brigade*, the five men are about to launch a cyber attack on the Western World unlike anything ever seen before. Fueled by the propaganda they absorbed from radical Islamic websites, and violently motivated by the inflammatory rhetoric of impassioned fundamentalist clerics, they are driven by a single-minded objective: to deal a devastating blow to the very heart of western capitalism by crippling its vital information infrastructure.

After a year of careful planning, preparation, complex coding and target selection they are ready. For months they had been foiled in their attempt to crack the passwords of the eight critical edge routers vital to their plans. The systems administrators had used strong password authentication to protect them and combined with the cryptographic strength of the authentication mechanisms, they had been delayed in their progress. Luckily for them, an audit had required a new policy of changing the password every thirty days. Harried help desk staff had provided the forgotten password to a coworker in Instant Messaging rather than walking it down two floors, and the minor breach had been exploited. A well designed and near invisible piece of code was installed on the worker's computer and silently duplicated itself across the network capturing the

keystrokes executed on the compromised machines. It sent the logs to anonymous Yahoo accounts setup for this very purpose by the five men.

Just two weeks ago, the five received, via a PGP-encrypted message, the assurances of a highly-placed leader of the Hezbollah terrorist network that their efforts would be augmented by multiple simultaneous suicide bombings. The message also included instructions for coordinating their attacks with similar cyber terror cells in Iran and Venezuela who had amassed vast botnet armies to unleash upon the west at the appointed time. The five men had no doubt that their efforts would result in the "mother of all terror incidents." The careful planning, research, social engineering and brilliant coding had yielded not only a treasure trove of high-access accounts for vital systems, but also, had allowed them to study weaknesses in the security of the systems they intended to target.

At exactly 9:00 a.m. EST, an IT analyst at the New York Stock Exchange notices increased traffic on the NYSE backbone. At 9:10, all of the servers lock-up and stop functioning. At 9:45, the head of the NYSE issues a statement that all trading is suspended due to a malfunction. This is followed by statements from the NASDAQ that they too have suspended trading. As reporters investigate, rumors surface that the machines and backups have been compromised and the timetable for recovery is unknown. Investors around the world begin to panic forcing European stock markets to close after a 12 point decline panic selling and rumors of a pending meltdown in Asian indices. .

Halfway across the Globe, in London's Heathrow airport, air traffic control notices irregularities in its state-of-the art Pegasus-ATC traffic control systems. Installed just 4 years ago, the systems were said to be impervious to attack. Five minutes later, during heavy traffic, none of the primary or backup systems are working. The Prime Minister is briefed and decides to re-route all incoming flights to Gatwick but by then, it is too

late as two planes that were circling the airport under heavy fog collide. There are no survivors, the death toll is 467.

10:00 EST. All of the major news networks around the globe begin reporting on an urgent warning from the Center for Disease Control about water contamination in cities across America including Los Angeles, New York, Detroit, Miami, Des Moines, Atlanta, Chicago and Philadelphia. Officials deny that the CDC has issued any such reports, yet each of the contacts that typically received press releases had received the urgent warning. Grocery stores are without bottled water within the hour.

11:00 EST, explosions are reported at five rural elementary schools in the Midwest. Hundreds of children are injured; officials refuse to comment on the death toll citing the need to contact affected families. Cellular phones, already taxed with traffic from earlier incidents cannot respond to the load. Anxious parents across the country rush to take their children out of school, congesting freeways and impeding rescue efforts.

12:00 EST, 15 million users of the largest Voice over IP provider in the United States cannot receive a proper dial tone; instead they hear a pre-recorded message in broken English informing them of the impending destruction of their way of life. The botnet armies assembled by the Venezuelan and Iranian cells, exploiting a little known weakness in IPv6's IPsec implementation that, combined with an exploit of Cisco IOS's implementation of *stateless address auto-configuration*, are wreaking havoc with Cisco routers all across the Internet. Not since the Conficker worm outbreaks in 2008 and 2009 has such a rapid, widespread attack been seen. Already, 48% of the core routers on the Internet are down, locking up telecommunications across vast areas of the Internet. The general population is in a frenzy of panic. . .

At 12:01 EST, a secure call is routed to U.S. President who is aboard AirForce One travelling to an undisclosed location. The call, which is put through from the Situation Room, and which was originally received by the Secretary of Defense, is from a

middleman in the Ukraine who relays the terrorist's demand for an immediate withdrawal of all foreign military personnel from the Middle East including the emptying of bases in Iraq, Afghanistan, Saudi Arabia as well as the joint forces base of operations in Amman Jordan which was established in 2011. In addition, all shipments of arms or aid to Israel are to immediately cease. The White House has 72 hours to comply or further attacks will occur.

Back in Peshawar, the five men watch with glee as *Al Jazeera* reports on the devastation. They are deeply satisfied with the results of the first wave of their carefully planned attack. . .

Cyber Insecurity – A look at the current state of affairs

In the early 1980's network pioneers at DARPA[1] along with several academic institutions developed a successful open standard for linking computer networks together. The resulting TCP and later TCP/IP protocol ushered in the Internet age.

The basic concept that computer systems can be easily, cheaply and reliably linked together to exchange information has, within the span of three decades, revolutionized almost every facet of modern life and ushered in the era of pervasive computing, the Internet and the mobile communications revolution. It has been the very "openness" of these early implementations that was the driving factor in widespread adoption. And indeed, the growth of interconnected computer systems has been nothing less than staggering. Worldwide usage of networked computer systems has grown to an estimated 1.43 billion users which amounts to 21% of the world's total population.[2] In history, no prior technology has achieved such rapid adoption.

With such interconnectedness and widespread adoption comes the possibility that these tools can be used to harm the very societies that have come to rely heavily on them.

Our cyber-infrastructure -- including most of the technologies, protocols, and information systems that make up or reside in cyberspace -- was not originally designed with high security in mind. While systems security has improved, it has been added, after the fact, onto existing structures utilizing archaic authentication mechanisms that do not take into account the fallibility of human beings. This is due in part to the economics of technology development; most buyers are unwilling to spend the premium needed for true secure computing.

[1] The Defense Advanced Research Project Agency is an agency of the United States Department of Defense responsible for the development of new technology for use by the military.
[2] http://www.internetworldstats.com/stats.htm

This situation has not escaped the notice of disreputable actors who are finding ingenious ways to exploiting cyber-insecurity for monetary gain or with malicious intent. According to a report released by IBM in 2005[3], "there were more than 237 million overall security attacks in the first half of the year."

Our society's increasing reliance on these technologies coupled with the persistent, well publicized[4] vulnerabilities within our cyber infrastructure make it relatively easy to exploit, disrupt, disable or cause mayhem on critical systems.

In a recent report, the Congressional Research Service (CRC) outlined current terrorist capabilities for cyber attack and warned that terrorist organizations, state sponsors of terror and extremist groups are becoming increasingly aware of the essential role of critical information systems and will either develop their own capabilities for cyber attack, forge alliances with cybercriminals, or hire hackers to assist them in targeting critical infrastructure[5]. The CRC cites a key report from the House Homeland Security Committee, wherein FBI officials indicated that extremists have used identity theft and credit card fraud to support recent terrorist activities by Al Qaeda cells[6]. Finally, the report concludes that if the current trends continue, cyber attacks will certainly become "more numerous, faster, and more sophisticated" likely outpacing the ability of government agencies and private organizations to prevent, respond to and recover from concerted attacks.

---

[3] IBM Press Release, *Government, financial services and manufacturing sectors top targets of security attacks in first half of 2005,* August 2, 2005. http://www.ibm.com/news/ie/en/2005/08/ie_en_news_20050804.html

[4] A prominent example was made public at the July 2005 Black Hat computer security conference where an exploit was demonstrated to show how commonly used Internet routers could quickly be hacked. Victor Garza, *Security Researcher causes furor by releasing flaw in Cisco Systems IOS,* SearchSecurity.com, July 28, 2005.

[5] CRS Report for Congress: Terrorist *Capabilities for Cyberattack: Overview and Policy Issues*, January 22nd, 2007

[6] According to FBI Officials, Al Qaeda terrorist cells in Spain used stolen credit card information to make numerous purchases. Also, the FBI has recorded more than 9.3 million Americans as victims of identity theft in a 12-month period; June 2005. Report by the Democratic Staff of the House Homeland Security Committee, *Identity Theft and Terrorism*, July 1, 2005, p.10

Deputy Attorney General Mark Filip upon addressing the International Conference on Cyber Security stated that "Cyber crime and cyber terrorism are issues that transcend customary bureaucratic and national boundaries, and because both public and private Internet infrastructures are "closely linked," they transcend the usual public/private dichotomies as well[7]."

This "interlinked" system of systems allows for numerous attack vectors ranging from a single targeted breach to a widespread coordinated cyber attack. The objectives of a cyber attack include the flowing four areas[8]:

1. **Loss of integrity**, such that information could be modified improperly;
2. **Loss of availability**, where mission critical information systems are rendered unavailable to authorized users;
3. **Loss of confidentiality**, where critical information is disclosed to unauthorized users; and,
4. **Physical destruction**, where information systems create actual physical harm through commands that cause deliberate malfunctions.

Many experts agree that one likely scenario for a cyber attack would be its use in conjunction with a conventional physical, chemical, biological, radiological or nuclear (CBRN) terrorist attack. Such a scenario could include direct attacks against first responder communication infrastructure or 911 call centers simultaneously with the detonation of explosive devices.

The Internet, which has penetrated almost all of our daily lives and is critical to the functioning of our knowledge economies, was designed for research and information sharing. Almost all but the most sensitive information systems are either directly or indirectly connected to the Internet and are therefore vulnerable to its design flaws.

[7] *Law enforcement on the cyber beat*: Government Security News, January 8th, 2009
[8] U.S. Army Training and Doctrine command, Cyber Operations and Cyber Terrorism, Handbook No. 1.02 August 15th, 2005 P.II-1 and II-3

The continued and concerted Distributed Denial of Service(DDoS) attacks against the Net's DNS infrastructure is troubling in that many believe those responsible are merely conducting tests and that a full scale attack is a real possibility in the near future[9].

Many of these large scale attacks exploit weakly secured workstations from around the world turning these computers into "zombies" which in turn are aggregated into botnet armies which can be unleashed in devastating distributed denial of service attacks. Had the users of these workstations properly secured them, such attacks would be vastly more difficult as each workstation would have to be individually hacked.

Closed vs. Open Systems

It has been humorously stated that a computer is in fact quite easy to secure. Why, we can simply turn it off, lock it in a steel vault, destroy any key and ensure that it is not connected to anything. Voila, we now have a highly secure computing environment!

Unfortunately, while the computer in this scenario is highly secure in its impenetrable steel vault, it is also completely unusable consequently forcing anyone who needs to actually perform a productive task to seek out a machine that is significantly less secure.

On the flip side, a completely unsecured computer with no authentication requirement, connected to an un-firewalled public network is almost certain to be compromised[10], thus putting the user of that machine in danger of having their identity stolen by cyber criminals, their files damaged, the system rendered inoperable, or worse, sensitive information compromised and used for illegal activities.

---

[9] *DNS Attack: Only a Warning Shot*; http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208804344

[10] In November 2002, the Honeynet Project placed unpatched Windows 2000 computers on the Internet and found that they were being compromised after just five minutes. The Honeynet Project, "Forensics" (Jan. 29, 2003); http://honeynet.overt.org/index.php/Forensics.

It is logical to conclude, if people cannot use secure systems, they will seek to use systems that are less secure or will find ingenious ways to circumvent security policies. Ignoring best practices to get their work done will render the system less secure than before. For example, it is common to find that government personnel who cannot access their work email or files from home are regularly utilizing free internet email accounts such as Gmail or Yahoo to send messages and attachments to each other when they are not at their workstations. Thus, a theoretically secure system which is not usable does little to improve the situation and tends to create a false and dangerous sense of security within an organization.

So how do we strike a balance between the need for trusted, secure information systems and the convenience, ease of use and usability of our information systems? We need to design security solutions that are tailored specifically to the weakest link: human beings. To do so, we must understand the limitations and motivations of average people who use security solutions.

Security's Weakest Link

As Bruce Schneier wrote "Security is only as good as its weakest link, and people are the weakest link in the chain.[11]" Hackers and cybercriminals understand this phenomenon significantly better than most technology companies. While the "human factor" is generally accepted as a significant issue by the security community, the majority of the discussions and research surrounding cyber security are focused on the technical and policy challenges of securing cyberspace[12]. In addition there are a scarce number of resources including scholarly papers, blogs, books or articles devoted to the

[11] Schneier, B., *Secrets and Lies*, John Wiley & Sons, 2000

[12] Such as which technologies will be used, what standards will be implemented, what sorts of policies will need to be crafted to coordinate our security and law enforcement efforts nationally and internationally or the varying roles of government, academia and the private sector, in securing cyberspace.

subject of the usability of security solutions. Yet this issue is arguably one of the most glaring and pervasive root causes of cyber insecurity. Given the fact that most users interact with computer security on a daily basis, Angela Sasse, comments that the current state of affairs amounts to nothing less than a major usability crisis[13] and suggests that "unusable security systems are not only expensive, but ineffective."

This is because common security mechanisms have failed to acknowledge even the most rudimentary usability and human-computer interaction design principles such as minimizing user's mental workloads, task context or an understanding of user motivation and self-image. Our continued reliance on password authentication as a common security mechanism is proof that not much has changed in the last few decades.

As far back as 1999, Adams & Sasse conducted both interview and questionnaire studies with people inside and outside an international telecommunications company[14] and concluded that users:

- Could not cope with the proliferation of passwords,
- Received little instruction, training or support, and
- Were not motivated to behave in a secure manner.

A decade later, the average user's exposure to password authentication is even farther out of control. We are juggling everything from bill payments, eCommerce, social networking sites like MySpace, GoogleApps, Instant Messaging and an explosion of Web 2.0 Software as a Service (SaaS) offerings, credit and debit card PIN numbers, VoiceMail access codes, in addition to the numerous work and home related computer login accounts that most of us are required to maintain. It has been estimated that

[13] Sasse, Angela M., *Computer Security: Anatomy of a Usability Disaster, and a Plan for Recovery*, Department of Computer Science, University College of London
[14] Adams, A. and Sasse, M.A. (1999), Users are not the enemy, Communicatins of the ACM, Vol. 42, No. 12 December, 1999

today, the number of individual username/password combinations that the average person is required to contend with regularly is in the high teens. The number is significantly more than the average person can remember without an artificial aid. Unfortunately, the aid is often writing the passwords down, storing all of them in a single location or using the same password everywhere[15] thus defeating the purpose of strong password authentication.

Understanding the Usability Problem

Let us consider for a moment some basic principles of human memory and motivation and how these apply to security technology:

Human memory has limitations: Most of us are not good at remembering the random sequences of characters required by strong password authentication methods. Humans have trouble remembering more that 7 ± 2 unrelated characters. Moreover, there is a limit to the number of passwords we can remember. Finally, unaided recall is much more difficult that cued recall resulting in the proliferation of the "Security Question" or password reminders. While these "fixes" aid recall, they also introduce additional significant security risks.

Humans don't think randomly: We don't do well when we are required to invent a random string of characters and commit them to memory on the spot Pattern recognition is one of our strongest skills, so when asked to create many unique passwords, we unintentionally or intentionally introduce patterns.

Human memory decays over time: We cannot recall passwords we use infrequently. Conversely, we cannot forget (on command) memorized items we no longer need.

[15] Hackers and social engineers exploit this fact as it is much easier to direct their energies against soft targets to obtain one or two of a user's commonly used passwords which in turn are probably the same passwords used to access more sensitive systems at work.

Thus, when we are forced to change our passwords, we commonly forget the new one or confuse the new one with the old.

Humans are goal oriented: Security is not a goal most users strive for; rather it is seen to get in the way of their production tasks. People use technology in order to perform meaningful tasks. In this context, security is viewed as an "enabling task" or "hurdle" the user is required to overcome in order to perform their production task. "When security conflicts with a user's production task they often respond by circumventing security mechanisms, and perceive security as something that makes their life difficult[16]."

Security performance matches our motivation: Several research studies have concluded that users simply lack the motivation to expend the extra effort on security.[17] This is often due to a set of beliefs and behaviors on the part of those that do not comply with security practices. These include the notion that the threat of security is not "real"[18] and therefore the extra effort is not warranted and/or that users do not believe that their actions will make any significant difference anyway e.g. that a determined attacker will get access to their system regardless of what they do, or "no one else follows the rules, why should I?" This indicates that there is a cost/benefit equation that most users undertake when evaluating the effort they will put forth to secure their information. In this context, it is important to acknowledge that people will only expend the extra effort if they truly believe they are at risk.

[16] Sasse, Angela M., *Computer Security: Anatomy of a Usability Disaster, and a Plan for Recover*, Department of Computer Science, University College of London

[17] Weirch & Sasse, M.A, 2001: *Pretty Good Persuasion: A first step towards effective password security for the Real World. Proceedings of the New Security Paradigms Workshop 2001* (Sept. 10-13 Cloudcroft NM), pp. 137-143. ACM Press

[18] In an experiment conducted in 2004, regular commuters in London where asked if they would reveal their email passwords for a bar of chocolate. A troubling 34% revealed their passwords without needing to be bribed. Over 70% revealed information about themselves that could be used by identity thieves. BBC, Tuesday, 20 April, 2004: *Passwords revealed by sweet deal*. http://news.bbc.co.uk/1/hi/technology/3639679.stm

Humans are interpersonal: People like people, and they tend to want to be helpful to others. That is why social engineering is so effective. Also, it is this tendency which often leads to circumventing security best practices. If a colleague needs access to a file or a system, we are likely to help this person because as humans we value relationships more than organizational policies.

Human nature is the reason why social engineering is such an easy and lucrative means of attack for cybercriminals. Kevin Mitnick, the famous and controversial computer hacker of the late 20th Century was a master of social engineering techniques. In his book, *The Art of Deception*[19], he provided numerous examples of how he easily gained illegitimate access to computer systems using username and password combinations which he obtained by artfully duping end-users into giving him their credentials.

As none of the previous points are new revelations, why is it that we continue to use standard password authentication to secure our critical systems? Consider that not only is password authentication counter-intuitive to humans, in many cases, it relies on only a single "strong" security element; the password which as we have seen is inevitably being compromised by human behavior and limitations.

If we are to strengthen cyber security, the problem must be viewed as more than a technical challenge. Security as a system must be engineered around the people who use it, the context within which it is used, and its surrounding environmental conditions. The current lack of usability and human-computer interaction principles, almost guarantees that only the most sensitive data handled by the most security-conscious persons has a chance of being adequately protected. Yet even under these ideal circumstances breaches of security continue to crop up. For example, former CIA director John Deutsch, arguably a very security conscious person with significant motivation to protect Government secrets, lost his security clearance because he wrote a classified memo on his unprotected home computer. "The U.S. Department of

[19] Kevin Mitnick, *The Art of Deception*, 2002

Defense's Inspector General blasted Deutsch for particularly egregious violations of security protocol involving his doing classified work on an unsecured home computer, while serving in DOD posts in 1993 and 1995. An investigation into similar practices by Deutch, while director of the CIA, cost him his security clearance in 1999. "[20]

Anatomy of security mechanisms

The principle of strong security includes the common notion that in order to secure an information system we need a combination of multiple vectors to establish a trusted connection:

1.) Something I am – Identification – Who you are, positive identification
2.) Something I know – Authentication – Something only you uniquely know
3.) Something I have – A token, smart card, keycard etc.
4.) Somewhere I am – Location – a physical or logical "area" from where I can access a system. "e.g. IP filtering , Internet Zones)

To be secure, a system must incorporate at least 2 of these vectors to establish trust. In addition, once a user is positively identified and "trusted" we must also know what actions that user is authorized to perform on the system or in other words, his/her authorization level. Upon cursory review, password authentication conforms to security best practice by requiring two of the aforementioned vectors to authenticate a user and allow them access to an information system:

1.) Something I am → username and,
2.) Something I know→ password

Let us however, for a moment review standard password authentication in more detail. By accessing the login screen a user is prompted for a username and password to gain access to the system's functions. The username supposedly serves to identify the

[20] Forbes, Arik Hesseldahl, December, 1st, *2000. Disaster of the Day: The CIA* http://www.forbes.com/2000/12/01/1201disaster.html

individual seeking to gain access. In combination with the proper password, access is granted. In most cases, the username is ridiculously easy to guess as it almost universally based on publicly available information e.g. a person's email address, a subset thereof, their name or an abbreviation of their name. For Voicemail systems, the username is almost always the individual's phone number or mailbox number. Some financial systems try to mitigate this fact by utilizing identifiers that are considered "more secure" such a Social Security numbers, yet even these can be relatively easy to obtain over the internet for as little as ten US dollars.

Thus one of the most critical elements of our security system can be said to be ineffective at positively identifying a user, leaving only the password to stand in the way of a determined attacker. As we have seen, passwords are significantly less secure than we would like. Likewise because the 'identification" component of this authentication scheme is so weak, all it takes is a name, phone number or email address for any malicious attacker to acquire enough information to initiate an attack.

As if this state of affairs was not bad enough, there are numerous readily available tools that are designed to automatically exploit known weaknesses in operating systems and commonly used commercial software applications that can collect login credentials in order to assist a hacker in compromising vulnerable systems. These tools are both easily available for download from the Internet and can be utilized by relatively unsophisticated attackers.

In addition, password authentication is severely flawed from a usability perspective in that it requires 100% unaided recall of the non-meaningful items that make up strong passwords. Given the limitations of human memory outlined above, password authentication causes people to constantly compromise both the strength and secrecy of the password in question. It is not a stretch to conclude that both vectors (username and password) are compromised when it comes to password authentication.

This traditional scheme provides near zero non-repudiation support as there is no way for the system to positively identify the user beyond checking that the username and password combination matches what is stored in a database. Clearly, from a security perspective password authentication has utterly failed to provide adequate protection for sensitive systems and yet it continues to be one of the most commonly used security methods in cyberspace.

While we are not arguing that password authentication has no merit whatsoever, we are pointing out that it is an inadequate security mechanism for most systems and should be utilized only on the least critical systems. This brings us to an important conclusion: selection of the proper security system should be based upon an appropriate security risk assessment. In the U.S., before September 11th, many systems that support vital services had not been assessed for risk in the context of terrorism or cyber warfare. Today, with awareness on the rise, a number of military and sensitive governmental systems have implemented additional layers of security including the use of Common Access Cards (CAC) and or biometric security mechanisms to harden their systems.

Driving principles for Usable Security

To solve the usability problem, the security systems of the future must be highly convenient, largely transparent to end users, fully integrated across security domains, threat aware, and able to modify security policies "on the fly" in response to changing threat environments.

Convenience and transparency are absolutely critical if we are to solve the problem. As previously stated, the less a person encounters security as a hurdle to their production task, the more effective the solution will be. An example in the physical world would be a self-locking door. For those that do not have this convenience, many forget to properly lock their doors when leaving their homes.

Thus, in simple terms, our user's behavior indicates that they need security that is quick, convenient and easy to use. They want to know that their identity, files, systems and facilities are consistently secured in a manner that maintains their privacy, yet alerts them when a potential breach has occurred. While users are understanding of the need for authentication and are willing to provide credentials, it is unrealistic to ask them to provide too many different sets of credentials during their daily workflow. Users should be required to remember as few things as possible in order to access our systems. Also, security must be contextualized with user's production tasks and be appropriate for the sensitivity of the system and applicable threat environment.

So at a minimum, future security mechanisms should:

1. Positively identify a person (not a username)
2. Require strong passphrases
3. Be threat-aware i.e. able discern threats, take appropriate actions and notify appropriate user(s) or authorities of a breach. Also, they should be able to share information in order to act as a threat early warning system.

4. Adapt in real-time – allowing for additional security to be imposed during times of increased threat, automatically add layers of security to sensitive information when an attack is perceived.
5. Be largely transparent/convenient
6. Be integrated – allowing user credentials to be used for physical and virtual access
7. Be designed to safeguard our personal privacy

Positively identifying a person -- To establish objective trust and non-repudiation, requires that we look beyond the easily compromised username for positive identification. Biometric identification does this by using one or more unique and intrinsic physical (fingerprints, iris, retina, facial or hand geometry, palm vein patterns) or behavioral traits (typing dynamics, signature recognition, voice pattern) of an individual to establish a positive identity match. The advantages of biometric identification include:

1. Very easy to use/convenient – we don't forget our fingerprints or face and, unlike tokens, these cannot be "lost"
2. Limited Attack Surface – it is almost impossible for a remote attacker to access the information necessary to initiate a direct attack or steal the user's identity
3. Relatively fast – it can take under a second to verify a match
4. Increasingly accurate – accuracy has improved significantly over the last 2 years
5. Becoming cost effective – costs for biometric devices have come down significantly[21]

While biometrics has significant advantages, detractors point out that the technology is still problematic due to:

[21] The cost of a fingerprint sensor has fallen from around $20 dollars four years ago, to under $5 in 2007 and is being incorporated into everything from laptops and cell phones to USB keys and hard drives.

1. Inability to change a biometric – unlike a username, once a biometric signature is stolen, it is not easy to change and we only have a limited number of biometric identifiers.
2. Greater consequences - Criminals may be incentivized to cut off user's fingers, hands, other body parts or even kill in order to gain illicit access to secure systems.[22]
3. Surrounding systems weak – biometrics can still be compromised via system circumvention, verification fraud and enrollment fraud.[23]
4. Biometric verification is not 100% accurate - This is due to the need for match threshold values (similar to a metal detector) to take into account the changing characteristics of the Biometric. Faces age, fingers can be scarred and our voice may change due to a sore throat. Depending on the threshold settings, and the "noise" encountered when scanning the biometric, false verification can occur as well as false rejections.
5. Fabricated biometrics - It is theoretically possible to recreate source biometric data from associated templates thus possibly compromising the biometric.[24]

Nevertheless, biometric identification holds significant promise to the leverage numerous "immutable" physical and behavioral attributes which, when fused, could form the basis for identification systems that are nigh impervious to identity theft. These multi-modal or "fused" biometrics systems are more reliable due to their ability to acquire multiple pieces of evidence to identify a person. Imagine a computer,

[22] A common story we hear regarding this objection is about the man whose new Mercedes was carjacked. The car had a biometric lock and therefore the thieves removed the man's finger in order to start the car. Despite this popular story, many of today's biometric devices have "live" sensors in them that would actually incentivize a criminal to keep the individual alive as long as they need access. In addition, while this information can be coerced from someone by force, so can a username and the nature of the crime creates significant visibility for the perpetrators effectively removing the shield of anonymity cybercriminals hide behind.

[23] Wayne Penny, GSEC Certification Practical, SANS Institute 2002: *Biometrics: A Double Edged Sword*

[24] Andy Adler, School of Information Technology and Engineering, University of Ottawa, Ontario, Canada: *Sample images can be independently restored from face recognition templates*

vehicle or door that not only recognizes your face but scans your iris and asks you how your morning is going while analyzing the voice pattern of your response to positively identify you. Humans can instantly recognize each other. We do this by simultaneous synthesis of many visual, auditory and olfactory cues. In fact, our recognition is so keen that it works even when the subject in question has altered their appearance or sounds differently due to a cold. If a security system were as perceptive, it would be incredibly difficult to circumvent as an attacker would be required to fool multiple sensors simultaneously. In the future, we predict that multi-modal biometric technology will be able to mimic how humans recognize each other by fusing biometric sensors together and allowing security systems to evaluate our identity "holistically." In this scenario, match threshold values can be consolidated across multiple vectors enabling drastically improved recognition and the near elimination of false positives.[25] In other words, a user may have a swollen face, but the system would still recognize her because her height, iris and voice prints match.

Strong passphrases – Supporters of biometric authentication have gone so far as to suggest that the biometric is all that may be necessary to positively indentify a user and allow access to a sensitive system. While highly convenient and in some cases transparent for the user, we disagree on the grounds that while current biometric technology provides a significantly stronger mechanism for positive user identification, it still has sufficient vulnerabilities that must be addressed before we can completely eliminate strong two-factor authentication.

Since multi-modal biometrics are not yet cost effective for most implementations, one thing that could be done to increase the usability of most authentication systems is to eliminate the "strong password" and replace it with a the more usable "passphrase." It is much easier for humans to both create and remember a 47 character phrase like

[25] Brad Ulery, William Fellner, Peter Hallinan, Austin Hicklin,Craig Watson. *Evaluation of Selected Biometric Fusion Technique*: Studies of Biometric Fusion, July 20, 2006

"Securing my identity in 2009 is very important!" rather than a meaningless string of 8 random characters such as "!$3^1@Z&".

Numerous debates surround the topic of the cryptographic strength of a passphrase vs. the strong password and the related entropy[26] of each. Most agree however that the longer passphrase (30 characters or more is typical) enables increased cryptographic strength rendering many kinds of brute force attacks highly impractical. More importantly, because the passphrase is relatively easy to remember, we are far less likely to write it down.

Threat Awareness – A door is a physical barrier, if there is a lock on it, only authorized (key holders) are supposed to be allowed access. Yet, a thief can steal the key, pick the lock, break down the door or go through a window. In the physical world, we use alarm systems that include various sensors (contact, motion, pressure) to sense unauthorized intrusions. Once an intrusion is detected, an alarm sounds and authorities are dispatched to the property. At the network level, intrusion detection/prevention systems have evolved significantly allowing for real-time responses such as blocking suspicious traffic and automatically alerting administrators. When we look at most authentication systems however, they do little to proactively sense and defend against threats or alert account owners and administrators of a possible breach. In short, most are not threat aware. At best, they lock a user account after a certain number of login attempts and require reactivation and may log unsuccessful attempts in a log file or audit trail. While useful for forensic analysis *after* the system is compromised, this does little to prevent or deter an attacker that has stolen valid credentials. In addition, many attacks originate from inside the network by disgruntled employees utilizing their own credentials or those stolen from colleagues.

[26] Entropy is a measure of the uncertainty associated with a random variable. There are three components to entropy: the number of items chosen, the size of the set from which they are chosen, and the probability that each individual item is chosen. Since pass phrases are longer than passwords, they have the potential for higher entropy than passwords, (even if they are picked from the same character set) making them much harder to crack.

In order to secure systems from these sorts of threats, developers may be able to incorporate some of the lessons learned by the financial industry. Given the enormous costs associated with credit card fraud, many credit card companies have become adept at tracking individualized spending patterns (what cardholders typically buy, where they usually buy, average transaction sizes) and can proactively alert consumers of unorthodox spending patterns or charges originating from locations not commonly associated with the card holder. If we apply this principle to an authentication system, it would be able to perceive a threat by sensing anomalous behaviors in the user. For example, a user who is attempting to enter a building at an unusual hour or a login to a system from an atypical remote location. Biometric sensors could further enhance this approach by adapting speech recognition to detect stress or fear in the user's voice, scanning for pupil dilation or recognizing when an unknown person is standing too close to a user.

Adapt in real-time – Security systems should not only recognize threats but also be capable of adapting to these threats in real time. When no threat indicators are present, adaptive security systems should remain relatively transparent and not interfere with user's productive workflow. However, when a threat is identified, the system should be "smart" enough to adjust its behavior and increase its security posture in a manner commensurate with the threat it perceives. While we may be several years away from biometric fusion and artificial intelligence capable of judging threats based on user behaviors and situational awareness,we do have the technology today that could block access to systems for users who are being forced to reveal their credentials. Similar to a silent alarm system, a person who is under duress to reveal her password may provide a "safeword" instead. The system, upon receiving the "safeword" would automatically secure critical or sensitive data and "pretend" to allow the attacker access to the system while notifying authorities and logging all activity on the workstation.

Largely transparent and convenient – When Windows Vista was released, many of the complaints about the operating system were directed at the incessant security

messages that the operating system directed at the users. One "feature" that Microsoft added to Windows Vista is the ability to stop programs from starting to begin with. This was aimed at reducing the threat of viruses and malware so common on home computers. Microsoft implemented this in the form of the User Account Control (UAC). The UAC was incredibly "chatty" and constantly asked users whether they wanted a program to continue or if it should cancel the operation. While the purpose was to warn users when an unknown or unwanted program asked to start, Microsoft coded the service to display the message repeatedly for almost any non-Microsoft program. These messages were so frequent and annoying that most users simply ignore them and become used to clicking continue to get back to their production task. Microsoft's willful disregard for usability was further underscored by outrageous comments made at the RSA 2008, in San Francisco where Microsoft admitted that UAC was designed, specifically, to annoy. Microsoft's David Cross stated that "The reason we put UAC into the platform was to annoy users. I'm serious," said Cross.[27]

It is no surprise that soon after Vista was released, a slew of internet pages, blogs and forum posts sprang up with instructions on how to turn UAC off and according to Ars Technica's Ken Fisher, "…one of the most popular post-Vista install activities is disabling UAC."

So what have we learned? In this case, while the concepts of threat awareness and user notification were laudable additions to the Vista OS, the implementation was an unmitigated disaster and many Vista systems became significantly less secure as a result.

Integrated Security – Integrating application and network security is not a new concept; Single Sign-On does just that. Once single sign-on is in place, keeping the managed passwords can be changed to the strongest format allowed by the applications, and managed automatically. If they are never known by the user, they cannot be

[27] Ken Fisher, Ars Technica, April 11, 2008: *Vista's UAC security prompt was designed to annoy you*

disclosed, written down, or handled carelessly. However, if a single sign-on system is not reliable, users and administrators will not trust it, creating back doors or leaving critical systems vulnerable. In addition, many of today's implementations are prone to creating a single point of failure or a single point to break in. Usability is security, but reliability is important for both. The ability of single sign-on to eliminate the need for numerous sets of credentials is a drastic improvement in usability and if implemented correctly has significant advantages for increased cyber security. If we take this concept one step further, we could include physical access as an integrated component of our authentication system. There are companies today that have created locks which can not only read credentials[28] but also write data directly to back to the credential allowing administrators unprecedented access to monitor entry/exits from facilities[29] and quickly change access privileges when necessary without the expense of replacing hardware for sensitive areas.

When travelling, we use an internationally accepted passport which represents a "trusted" credential allowing us to legitimately enter or exit any country in the world. From a usability standpoint a unique, internationally recognized, trusted token that when used in conjunction with a passphrase, biometric or other identifier gives a user access to all their accounts, their vehicle, computer, and place of work could be an interesting concept to pursue. However, to be feasible, we would be faced with the Herculean tasks of ensuring it could not be forged, was easy and convenient to reissue a lost or stolen token, and incorporated a framework of strong safeguards to protect the personal privacy of the users.

Safeguard personal privacy – It cannot be stressed enough that if users don't trust that their privacy is being protected, or if the actions being taken by a security system are

[28] For example CoreStreet (http://www.corestreet.com) provides locks that can read and write to a token (FIPS 201 compliant smart card) thus allowing access physical access privileges to be denied (without the need for changing a lock) should the user's network and system access be revoked. The same goes for increasing a person's access rights to facilities for example when they have achieved security clearance. This has been a costly problem with standard locks and keys issued to employees.

[29] Which we have seen could be useful in establishing normal baselines of activities in order to detect unusual patterns of behavior to enhance our detection of anomalous events.

not disclosed to the users, they will not accept such a system or will intentionally bypass the system to protect their privacy. Several studies indicate that the majority of people who find out that software operates in a covert manner to compromise their privacy will discontinue use of that software application. The most important aspect of maintaining user trust is full disclosure of what the system may track and a clear understanding of the cost benefit of the technology[30]. People are rightfully afraid of an Orwellian scenario where every step they take in both cyberspace and the real world is monitored by "authorities" and will strongly resist any security technology that violates their privacy.

Yet, it is ironic that millions of people around the world post much of their personal data daily on the internet via social networking and other sites[31] and act as if they are completely unaware that most of their activities can be easily followed for they leave digital "breadcrumbs" wherever they go. Blogs, MySpace entries, IRC traffic, credit card records, phone records, internet activity logs, financial systems and even our healthcare records are exposing our digital DNA to potential attackers. Today, these "breadcrumbs" are distributed across the hundreds of web servers, applications and the individual systems making aggregating this information somewhat impractical. A single unifying identifier that can link all of these disparate systems together, while highly "usable" will open a Pandora 's Box of privacy issues that our societies may never be able to solve.

[30] There are countless examples of a user's voluntary willingness to part with personal information in order to increase convenience. After 9/11 several companies launched Registered traveler programs aimed a capitalizing on traveler's aggravation with increased security. Once such program "Clear" (http://www.flyclear.com) is now operating in 20 US Airports and in exchange for $199 per year and submitting personal information and a biometric for a background check, air travelers can access a special security lane with almost no wait time. In August 2008, a laptop with 33,000 Clear records was lost or stolen from the San Francisco Airport. Needless to say, the hard drive of that laptop was not encrypted proving once again that human error and lack of vigilance remain primary sources of cyber insecurity.

[31] It may be interesting to note that the vast majority of these users are individuals who have grown up with technology (Generation Y or the Millennials) and who don't seem to have the same suspicions or concerns regarding the security and privacy of their personal information.

The privacy challenges we face are enormous and cannot be exhaustively discussed in this paper. However, suffice it to say that the privacy question is of paramount importance to our security and that it has intersecting moral, policy, legal, and technology dimensions.

The Security System of the Future

It is September 1st, 2013. In a dimly lit room on the outskirts of Peshawar in Pakistan, five men stare into their computer monitors as their fingers rapidly tap the keyboards. . . Suddenly, they are startled by a loud explosion and a blinding flash of light. Before they can recover from the flash bangs, they are laying face down with the hands zip-tied behind their backs looking up at the threatening muzzles of silenced H&K MP5 submachine guns. The operators who wield them are the highly trained professionals of the International Cybercrime Task Force. The elite, international law enforcement unit was established by mutual treaty and has jurisdiction to arrest and bring before an international tribunal criminals wanted for cybercrimes. Accompanied by two armed Pakistani police officers, they make quick work of seizing the computer equipment for digital forensic analysis.

For almost a year, these men have been under close watch by the International Cybercrime Coalition (ICC) an International organization founded in 2011 with participants from over 40 Countries and almost all major software and networking vendors. The ICC which is tasked with blending information from all the participating country's cyber-security fusion centers, is closely linked with international law enforcement agencies. The ICC together with the cooperation of prominent technology companies including Microsoft, McAffee, Norton, Cisco, GoogleLabs, Barracuda, SonicWall and over 20 others leading technology providers developed an early warning framework that could be installed on any number of devices, was threat aware and could upload new threat models in real time.

The ICC was successful in developing a vast, opt-in early warning network dubbed Operation CyberShield which was launched by creating a successful marketing campaign for security awareness. Users, many fed up with the constant spam, viruses, malware and worms infecting their computers, were informed that they could assist cyber enforcement officials by downloading the free CyberShield software package.

CyberShield was designed to constantly monitor in-bound activity originating from their network connection and automatically alert users and the ICC authorities of suspicious hacking attempts on user's computers. Within six months of international campaigning over 5 million computers had the software installed. CISCO and Microsoft made the software an integrated option within their operating systems and numerous open source versions were released two months later. Pretty soon, the CyberShield network was growing at the rate of 10% per month.

By the time the men in Peshawar began their attempts to compromise critical machines, over 48 million computers, routers and firewalls on the internet were acting as early warning systems. Unfortunately for the plotters, several of these had the CyberShield system installed.

One hundred seventeen of these devices sent critical alerts to the ICC fusion center which, upon automated cross referencing of the involved MAC & IP hacker's source addresses, flagged the addresses for further observation.

But CyberShield was not just an early warning system. As administrators and users were alerted to the threat, they activated its "HoneyPot" mode; the software spawned a virtual machine that "pretended" to be the compromised host at the mercy of its attacker. CyberShield automatically redirected all traffic originating from the attacker's network address to the HoneyPot, all the while logging the illicit activities. The tables were now turned. . .

Back at the ICC fusion center headquarters, logs from the HoneyPots poured in and within hours, cyber security analysts had indentified the vulnerability and security patches developed by the involved vendors were automatically distributed through the CyberShield network to all of its connected machines. During this time, the five cyberterrorists remained blissfully unaware that their intrusion had been detected and that they were under counter-surveillance.

Later that day, authorities are able to decode an encrypted message from Hezbollah terrorist leaders and were made aware of the numerous conventional attacks that were planned to coincide with a massive cyberattack planned for the 11th of September. The message referred to similar groups in Venezuela and Iran and authorities begin cyber surveillance operations targeted at those countries subnets uncovering two additional cyber-cells involved in the attack.

ICC authorities increased threat levels across cyberspace and coordinated with Law Enforcement in the US and the UK investigating Hezbollah plots. The additional information gleaned from the computer logs seized in Pakistan provided investigators significant leads that led to the arrests of several cell members in the Midwest and East Coast involved in the scheme.

Numerous arrests are made the following week after additional evidence was gathered from the captured men's homes.

Conclusion

Technology has become an indispensible tool for modern societies, yet our cyber infrastructure remains highly vulnerable to attack. In this paper, we have explored some root causes of cyber-insecurity and conclude that a significant problem lies with humans. If we do not begin designing systems that squarely address human limitations and recognize that usable solutions are a crucial component of strong security, we will undoubtedly remain highly vulnerable and, within a decade, see our technology turned against us in continued, more sophisticated and damaging attacks.

As we designed the scenario outlined in the introduction, it was frightening to note how many possible avenues of cyber attack exist and how fragile and tenuous our economies and way of life actually are. As we pursued outlining both the problems and some possible solutions it became clear that there is no single "magic bullet" approach that will guarantee our safety. It is more a question of constant vigilance and the will to evolve our security solutions to deal with 21st Century threats.

Finally, to succeed in hardening our security across cyberspace will require unprecedented cooperation between nations, companies, academia and citizens as the challenges are both formidable and multi-dimensional. The price of not solving these problems may be nothing less than our way of life.