Some Perspectives on Cybersecurity: 2012

1 Introduction

As a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and “solutions” ranging from the technical to the legislative. While buzzwords like cybersecurity may make for good headlines, serious discussions of security and the Internet require a shared understanding of what is meant by cybersecurity.

The landscape covered by the term cybersecurity includes many types of problems and an even greater number of solutions. Some of the solutions are technical and some are not, and can be solved through education, policy, or regulation. As a result of this scope and range of solutions, there are many stakeholders involved in solving cybersecurity issues including individual users, standards and policy development organizations, product developers, enterprises, non-governmental organizations, and governments. All of these stakeholders need to work collaboratively to achieve the goal of a safe, secure, and robust Internet.

The Internet model of developing collaborative standards and policies in an open and broad based consensus process by international experts is one of the best vehicles for achieving real security. This model has been successful in improving cybersecurity with the deployment of secure virtual private networks (VPNs) and encryption protocols, DNS Security Extensions (DNSSEC), secure protocols for data exchange and a more secure routing system through the development of security enhancements to BGP. This model of consensus and international cooperation will instill confidence and create an environment of trust in order to address the many challenges of improving cybersecurity. Unfortunately, there are potential threats to this open consensus based model including corporations pushing proprietary solutions and governments pressing for back door access mechanisms.

The purpose of this paper is not to “solve” cybersecurity but rather to break down some of the different elements of the cybersecurity problem and to identify the ongoing work by different organizations and stakeholders to address these different elements. It is our hope that by approaching the issue from this perspective, the reader will gain an understanding of different ways to frame the issue and to think about solutions. We also hope that this framework provides readers with insight into the wide range of organizations working together to address the technical elements of cybersecurity.

1.1 Background

The Internet has fundamentally transformed our society and economy. As the Internet becomes truly global and accessible at every point of the earth, its impact, influence, and importance will continue to grow. As well, a new generation of Internet savvy citizens who grew up with the Net and are comfortable with its many dimensions are driving new applications, services and uses.

The open Internet, as we know it today, has been a boon for humanity. It has not only allowed businesses of all sorts to become more efficient, but enabled new forms of production and distribution, and economic models such as open source software and click-based marketing. It also has the potential to be a significant instrument in addressing social ills and other significant challenges, such as dissemination of information during natural disasters, monitoring global climate change and helping people reduce energy consumption via "smart meters".

But there is a dark side to this digital revolution, one in which individuals and businesses may be scared away themselves or restricted by governments in their use of the Internet. Online fraud and identity theft are common, and there is an ongoing challenge to address flows of illegal information and incorrect data. These negatives mean that the benefits of the Internet are countered with real and direct costs. And yet, the final result of this balance calculation is not universally agreed.

While our current firewalls, anti-virus and anti-spam measures and Internet security practices can improve cybersecurity, the increasing complexity of the system and its open nature poses new challenges. As reported at the New Security Paradigms Workshop [NSPW], a variety of seemingly straightforward preventive measures, such as requirements for strong passwords, have given us a false sense of protection against potential attacks. In fact, the report says, we aren't paying enough attention to more potent threats. Recent highly publicized discoveries of world wide "ghost nets", fundamental flaws in Internet security infrastructure as shown by the Diginotar incident [DIGINOTAR], and cyber-attacks against companies like Google [NYT-GOOGLE] or entire nations like Estonia [WIKI-ESTONIA2007] indicate that there are still serious vulnerabilities to be addressed and new ones that we haven't even imagined yet. If large attacks became commonplace – and seemingly unstoppable – our confidence in the Internet may be significantly eroded or come to an abrupt halt.

To avoid this fate, increased use of carefully thought out measures to improve confidence, safety and security will be needed. Unfortunately, some current proposals to improve security themselves pose a danger to the open, generative Internet. Some national governments are erecting borders in cyberspace. Not all these efforts are aimed at imposing political control; indeed, some are intended to improve cybersecurity but nonetheless threaten the openness and functionality of the Internet. For example, the Australian government considered and then abandoned a proposal to require ISPs to implement filtering using a government-controlled list. The goal is to block "child sexual abuse imagery, bestiality, sexual violence, detailed instruction in crime, violence or drug use or material that advocates the doing of a terrorist act."[AUSTRALIA-DBCDE][AUSTRALIA-UPDATE] More than a dozen countries have plans to deploy mechanisms intended to block Internet content for political, social and security reasons [BORDER]. These plans pose a significant risk to global interoperability and the goal of an open, accessible, and generative Internet.

There is a growing need for fundamental work to deal with the concerns referred to by the term "cybersecurity." For this work to be constructive and effective, it is essential to start from a shared understanding of what is meant by cybersecurity.

1.2 Evolving Definition of Cybersecurity

Cybersecurity is a broad term that has evolved over time with no clear consensus on its exact meaning. It can stand for an almost endless list of different Internet security related themes, including technical problems and vulnerabilities, social and behavioral issues, and criminal activity. The possible solutions include technical standards and products, operational practices, user education, policies, regulation, and legislation.

For the purposes of this document, cybersecurity is defined as anything that includes security problems specific to the Internet and their technical and non-technical solutions. Not every crime that occurs on the Internet is covered by the term cybersecurity. A crime is a crime, and simply moving it to the Internet doesn't make it special. When crimes are committed using the Internet, they may be novel and make good headlines, but ordering items from a catalog retailer and trying to pay for them with a stolen credit card is simply fraud via the Internet—not "cyberfraud."

Some types of legal and security issues that are not specific to the Internet, such as unauthorized reproduction and distribution of copyrighted materials such as movies, or illegal content such as images of child abuse, although important, have not been included here. While the Internet may be an enabling conduit for these activities, they have been omitted to keep the focus on technological solutions to common security problems, rather than include "everything bad that can happen over the Internet."

Both cybersecurity problems specifically and other criminal activity carried out using the Internet are not going to be solved with technology alone, but rather via close cooperation and coordination by all Internet stakeholders, including business, organizational and individual users, governments and law enforcement agencies, and policy makers worldwide. This must be combined with active efforts aimed at Internet literacy for all Internet users, including parents, children, and educators. The social component of cyber-crime cannot be fixed without user engagement.

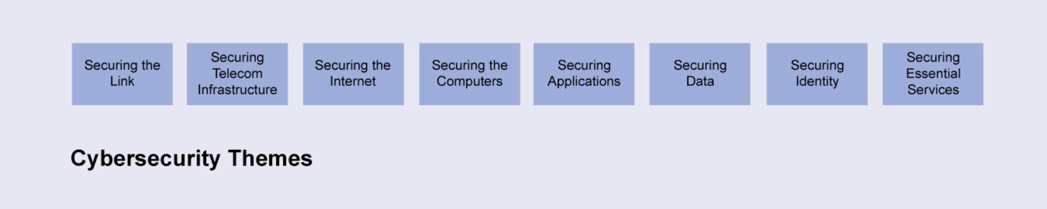

Figure 1 – Cybersecurity Themes

2 Cybersecurity Themes

The chart in Figure 1 is a simple deconstruction of many of the elements of cybersecurity. The diagram is not intended to be exhaustive, but to provide a simple framework to discuss the many aspects of cybersecurity. Each block in the diagram represents a general category of security services. Because the scope of cybersecurity is so broad, it is helpful to break it down into these general categories or themes. The following sections discuss each of the themes in more detail.

2.1 Securing the Link

Internet packets inherently have no security. They are completely open and anyone with a simple software tool can easily inspect the contents of each packet as it is transmitted across the network. This is a basic building block of the Internet architecture. To prevent unauthorized "sniffing" or eavesdropping, it was quickly recognized that there needed to be a way to encrypt the transmission of sensitive data. There are a number of approaches to do this, including encryption at the data link layer (MACSec and Wi-Fi Protected Access), encryption at the IP layer (IPSec), and encryption at the application layer (SSL/TLS and SSH, among others). These technical solutions are discussed in the Sniffing section of this document.

While Internet eavesdropping can be technically difficult in normal residential and business deployments, the growing use of open and public Wi-Fi and other wireless technologies has made it clear that eavesdropping is a continuing problem. For example, in October 2010, Eric Butler released a tool called “Firesheep” to demonstrate how simple it is to eavesdrop on unencrypted Facebook traffic in public wireless networks. Butler’s stated goal was to encourage web sites to make greater use of encryption (such as SSL/TLS) to protect user data in flight, a challenge Facebook accepted, but which didn’t change the behavior of the rest of the Internet. [FIRESHEEP]

IPsec, SSL, SSH and other IP and application layer encryption protocols are specified by the Internet Engineering Task Force (IETF) in a series of Request for Comment (RFC) documents addressing various components and extensions. The IEEE 802 LAN/MAN Standards Committee addresses security for wired and wireless local and metropolitan networks including Ethernet, Bluetooth, Wi-Fi, and WiMax. An industry consortium, the Wi-Fi Alliance, also participates in definition of wireless security with their Wi-Fi Protected Access (WPA and WPA2) standard, a profile based on the IEEE 802.11 standards.

2.2 Securing Telecom Infrastructure and Internet Infrastructure

Internet security and telecom security have traditionally been distinguished from each other when defining cybersecurity, because each of these has its own particular technology infrastructure and related standards organizations. Lumping them together can muddy the issues, as the solutions to secure a national telecommunications infrastructure—highly regulated closed systems with a few significant players in every market, hierarchically organized, natural monopolies, and with aging physical plants—are different from those needed to secure the Internet’s infrastructure—largely unregulated open systems, building on top of multiple national and international telecommunications infrastructures, and with no clear organizational center. Increasingly, cybersecurity includes security issues with respect to telecommunication networks such as cell phone, satellite, broadcast and microwave facilities. As Internet technologies are used more frequently to deploy traditional telecom services, such as in delivering telephone service to home Internet subscribers, cooperation and collaboration are becoming increasingly important for successfully improving the state of security of the Internet.

When policy makers discuss the lack of standards for cybersecurity they are generally referring to the problems related to Internet infrastructure and computer security, as this infrastructure is in the hands of the private sector and thus largely unregulated or self-regulated. Telecommunications infrastructure is the exception as it has always been under the supervision of various national telecommunications regulatory agencies or government-owned telecom carriers. Because of the long-standing tradition of telecommunications development and regulation, most telecommunications networks are treated as separate entities for the purposes of security. For example, Angola’s approach to securing their national telecommunications infrastructure is not linked to the security of Zambia’s infrastructure any more than it is to Algeria’s. In these cases, international telecom standards agencies such as the UN International Telecommunications Union (ITU) are responsible for developing effective recommendations and standards.

While not a treaty organization, the IETF is also active in developing telecommunications network security standards, particularly as these networks utilize a range of IETF-standardized protocols.

Law enforcement agencies may also cooperate with both the ITU and IETF in designing security standards to meet their own requirements, such as for lawful intercept (tapping) of voice telephone signaling and audio traffic.

Internet infrastructure security is different from national telecommunications infrastructure security or corporate enterprise security because it must address the challenge of securing a global network of networks, rather than a country-by-country or company-by-company set of networks. The Internet is a global overlay network of agreed-upon protocols, where the underlying infrastructure and the individual connected networks are managed and controlled by many separate organizations, both public and private. This means that the biggest challenges faced by those working toward Internet security arise from the autonomy and organizational and business diversity of the interconnected individual networks constituting the Internet.

The main organization charged with developing security standards for the Internet is the IETF. There are several working groups in the IETF that are specifically addressing the development of security protocols including IPSec and TLS. In addition, the IETF has directed that all protocol documents must have a "Security Considerations" section addressing the security implications of that protocol. Additional information can be found at www.ietf.org.

The IETF has established a security operations working group, OPSEC, which plans to produce best practices documents on more than a dozen operational security issues. These documents will capture current practices related to secure operation based on real-world experience. Each document will list:

- Threats addressed;
- Current practices for addressing the threat;
- Protocols, tools and technologies extant at the time of writing that are used to address the threat; and
- The possibility that a solution does not exist within existing tools or technologies.

The output of OPSEC will provide guidance to the telecom operators community, the IETF community of protocol developers and to implementers of these protocols. Six of the proposed best practices documents have been published as RFCs as of November 2012 with an additional six best practices documents in active development. In addition to these surveys, OPSEC is producing a taxonomy of the various cybersecurity standards that are being developed by standards organizations around the world. [OPSEC-TAXONOMY]

2.3 Securing Computers

Whenever a device is connected to the Internet, it is susceptible to intrusion. Overwhelmingly, the most successful attacks from hackers, criminals and other bad actors have been against servers and end-user computers connected to the Internet. Many organizations go to great pains to install firewalls and end-point security systems, usually called “anti-malware” or “anti-virus” tools. At the same time, hackers are continually testing and exploring for weakness in firewalls and networked computers. The result is an escalating conflict between computer owners, who want to maintain control over their systems, and hackers, who want these computers and the data on them for their own purposes.

No one knows exactly how successful the hackers are in their mission. Many attacks are never reported. Competitive pressures also often inhibit sharing of intrusion data between organizations and discourage collaboration on different approaches to security. Discussions are ongoing in various forums on how to effectively gather and share this type of data.

The reasons that hackers want to control computers have varied over time. Fifteen years ago, the major drivers for cyber-crime were pure vandalism. This evolved into criminals using the Internet to extort money, steal passwords and financial information (such as credit card numbers), and to build botnets that could be used for sending spam, committing fraud, stealing identity information, and executing denial of service attacks against specific web sites. Some of these techniques are also being used in a much more sophisticated form by national governments or other criminals-for-hire for espionage, disruption of communication and services, and other offensive purposes.

The tools used to attack computers include malware, Trojan horses, botnets, phishing, distributed denial of service (DDoS) and man-in-the-middle attacks. These are discussed in greater detail, along with some of the protective technologies, in the “Cybersecurity Problems and Protective Technologies” section of this paper.

Keeping computers secure, whether servers or user desktops, laptops and smart phones, is the focus of a wide variety of groups within the IT and Internet communities. The table below helps to identify some of the major players and their areas of interest.

Organization	Area of Interest
Software companies, such as Eset, F-Secure, Kaspersky, McAfee, Sophos, Symantec, and Trend Micro	Production of anti-malware tools for servers, for user desktops and laptops, and for use in embedded devices such as firewalls
Firewall companies, such as Check Point Software, Cisco Systems, Juniper Networks, and SonicWALL	Production of network firewall devices to secure organizational networks by providing a boundary between the network and the Internet
Hardware companies, such as AMD and Intel	Production of computers with embedded security (such as self-encrypting hard drives and the Trusted Platform Module) to guard against cyber-intrusion
Trusted Computing Group (an industry consortium)	Development of standards for protection of end-system devices, such as self-encrypting hard drives, hardware authentication devices, and network access control
IETF	Development of standards for Network Endpoint Assessment, to ensure the “health” of devices before they are allowed to connect to networks and the Internet

2.4 Securing Internet Applications

Any application on a device, such as a personal computer or a smart phone, connected and communicating over the Internet is an "Internet Application". For the purpose of illustration, two of the most common Internet applications, electronic mail (email) and web browsing, are examined in this section. However, there are many Internet applications and the number continues to grow as new uses of the Internet become accepted. Protecting these applications falls into a general category of application-layer security, one more part of cybersecurity.

2.4.1 Securing Email

Anyone who uses electronic mail will be familiar with one security issue: spam, or unsolicited commercial bulk email. Protecting email from spam has largely fallen to commercial software and appliance vendors, such as Barracuda Networks, Cisco/IronPort, McAfee, Proofpoint, Symantec, and Trend Micro. Service providers such as Google/Postini and Microsoft have built “in-the-cloud” solutions to help to secure email against spam, and a number of companies such as Spamhaus provide black lists and reputation services.

The main standards organization working specifically in the anti-spam arena is MAAWG, the Messaging Anti-Abuse Working Group, which maintains a liaison relationship with the IETF and other smaller standards organizations and industry alliances. Based on the work of the MAAWG, the IETF formed a working group to help standardize reports of spam. Messaging anti-abuse operations between independent services often require sending reports on observed fraud, spam, virus or other abuse activity. A standardized report format enables automated processing. The IETF’s MARF (messaging abuse reporting format) working group has developed a series of RFCs detailing a method and format that can be used by interested organizations to report spam in a standardized way. [MARF]

Email is susceptible to a second threat, impersonation. Because the design of the Internet email protocols did not envision use by a large community that would be susceptible to wide-scale impersonation, such attacks are still easy to do. The IETF has developed Domain-Keys Identified Mail (DKIM), a series of standards that help to detect impersonated email. DKIM also can help by blocking types of spam that involve impersonation, such as phishing emails purporting to be from a bank.[1] [DKIM]

2.4.2 Securing Web Applications

Web-based applications, such as Facebook social networking, eBay auctions, and Yahoo! Mail, represent the most common use of the Internet for many consumers. For businesses, both specialized and general-purpose e-commerce applications such as credit card authorization tools or on-line inventory management may be more important. In either case, though, the web servers and software that provide these applications may call for specialized security. These products are known as web application firewalls, and they are operated by the owner of the web-based application, not the consumer.

The main goal of web application firewalls is to protect both web users and web servers against security faults that may be hidden in the application. For example, a particular type of attack known as “SQL injection” can be used against susceptible web applications to bypass the application and speak directly to the database behind the application. SQL injection attacks, when successful, can give the attacker the ability to download private information from web application databases (such as usernames, addresses, passwords, and even credit card numbers) or to upload content to a trusted web site that could place malware on an unsuspecting user’s

[1] “Phishing” is the creation of web sites that have the look and feel of legitimate sites. The user is often directed to these sites through an e-mail message or similar sounding names or spelling. They are then directed to enter passwords, account numbers and other personal information.

computer. Web application firewalls (and to some extent, Intrusion Prevention Systems) can help to detect and block these types of attacks, giving an additional layer of security.

The World Wide Web Consortium (W3C) is largely responsible for stewardship of all web-based standards. The W3C has created two working groups related to applications and security, the Web Applications Working Group [W3C-APP] and the Web Application Security Working Group [W3C-SEC]. The IETF also chartered a working group on Web Security in October 2010, to help provide both standards and advice to software developers to help reduce uncertainty. Most of the specific work on web application firewalls has been done by the vendors of these products, and by the developers of the popular web browsers, particularly Microsoft and Mozilla. With the vast amount of activity in the field of web application security, many in the technical community believe that more coordination on a framework would be useful. [HODGES]

2.5 Securing Data

Data security and privacy (including consent) are other areas commonly included under the term cybersecurity.

Data security is any strategy or measure – legal, technical, social or other – employed to protect data. As the ultimate trans-border data conduit, the Internet allows people all over the world to send and receive data from anywhere. Different Internet protocols provide varying degrees of data security. In some situations, Internet users also expect the data they send and receive will be secured, for example, when communicating with their bank, government or healthcare provider. In other situations, the data they send or receive, for example, the content of entries in Wikipedia, may not be secured in transit.

Internet users may also wish to protect stored data from third party access or tampering. This data may be held locally by the Internet user (e.g. on their PC or Smartphone) or by a service provider (e.g. a bank, government agency, social network provider, file storage provider etc.). The **data security** aspect of cybersecurity deals with securing this data in transit and while stored.

Privacy, in the online environment, is concerned with the protection of personal data. Recently, a modern definition of privacy has emerged focusing on the sharing of private data online:

> *Privacy is the consensual sharing of data in an explicit context with an expectation of scope*

Policy and legal frameworks for privacy and data protection tend to focus on personal data (or personal information), which the OECD Privacy Guidelines define as “any information relating to an identified or identifiable individual”.[OECD] Data about corporations, organizations, and individuals who have died is typically excluded. Traditionally, technical frameworks for data exchange via the Internet concentrated on **data security** rather than **privacy**. However, with the relatively recent explosion in data exchange among Internet users fueled by more accessible and easy to use tools (e.g. cheaper devices, social media websites, blogging software, mobile access and apps, etc.), the Internet technical community is investing considerable resources on the development of privacy-respecting technical tools and privacy enhancements to Internet protocols.

The main organizations working in this area are national legislatures and affiliated government bodies. The privacy of personal information has been the subject of legislation on every continent.

In the United States, legislation has generally been weak at the federal level with some notable exceptions like health care privacy (HIPAA, the Health Insurance Portability and Accountability Act). This leaves the states to step in and provide stronger protections for consumers. California was an early leader in this area with legislation in many areas related to data protection. Many other US states have developed their own legislation in this area as well, although this has left the US with a patchwork of different regulations and requirements. In response to a concern about the lack of federal-level online privacy rules, U.S. Department of Commerce is conducting a comprehensive review of the nexus between privacy policy and innovation in the Internet economy and has initiated a public process and series of workshops toward that end. [US-NTIA]

Some examples of international data protection rules are shown in the table below.

Name	Covers
European Directive on Data Protection	Covers the transparency, legitimate use, and proportionality of use of personal information on all EU citizens, as well as how that data may be transferred both within and outside of the EU
Australian Commonwealth Privacy Act	Appropriate collection, holding, use, correction, disclosure, and transfer of personal information by both public and private sector organizations
Canada Protection of Personal Information in the Private Sector	Covers non-governmental collection, use and disclosure of personal information, the individual right of privacy of and the appropriateness of organizational collection, use and disclosure of personal information.
Taiwan Computer-Processed Personal Data Protection Law	Covers both public (governmental) and non-public (private sector) use of personal data, including appropriateness, permissions, disclosure, and penalties for misuse of personal data.
OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data	Covers an international consensus on collection and management of personal information. Assists governments and businesses by offering guidelines on protection of privacy and personal data, as well as transborder data flows
APEC (Asia-Pacific Economic Cooperation) Privacy Framework	Covers a regional consensus on the development of privacy protection while avoiding barriers to information flow.

2.6 Securing Identity

In the early days of the Internet, it was quickly recognized that for many commercial applications to succeed, mechanisms built on principles of trust and secure identity management were needed to authorize and authenticate Internet users.[2] A secure link is only good as long as the end points are considered to be legitimate entities that are authorized to carry out a given transaction.

[2] Identification is the attachment of a label to an entity, such as a username to a person sitting behind a keyboard. Authentication is the process of verifying that the entity being identified is who they claim to be, typically using a technique such as a secret password.

Originally, the expression cybersecurity was largely thought of in these terms – as a positive phrase to enable services and capabilities for the Internet.

Mechanisms to increase trust and validate identity would enable the Internet to provide channels for secure, reliable, and private communication between entities, which can be clearly authenticated in a mutually understood manner. These mechanisms should have reasonable means for entities to manage and protect the details of their identity.

Although many of the issues related to securing identity are legislative, there are privacy and security protocols which can help secure the process of authentication and authorization of end users. The organizations most involved in identity and trust solutions include national governments and their agencies, such as the US NIST, private-sector and public-sector organizations including OASIS, W3C, OpenID, the Kantara Initiative, and the IETF, all discussed below.

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit consortium originally chartered to work on the SGML (Standard Generalized Markup Language), focusing on document markup and preparation. While SGML was not a huge success, a descendent standard, XML (eXtensible Markup Language) has been widely adopted, and OASIS has become active in many related standards. OASIS' Security Services committee developed SAML (Security Assertion Markup Language) which is a widely used base for many advanced identity protocols. [OASIS]

The US National Institute of Standards and Technology (NIST) has prepared a National Strategy for Trusted Identities in Cyberspace [NSTIC]. This government-sponsored strategy "envisions a cyber world - the Identity Ecosystem - that improves upon the passwords currently used to log-in online. It would include a vibrant marketplace that allows people to choose among multiple identity providers - both private and public - that would issue trusted credentials that prove identity."

The OpenID Foundation, another active organization in the area of securing identity, was founded in 2007. OpenID is an international non-profit organization of individuals and companies committed to enabling, promoting and protecting OpenID technologies. [OPENID]

The Kantara Initiative was founded in 2009. It is intended to be a focal point for collaboration to address issues shared across the identity community. Their mission is to "foster identity community harmonization, interoperability, innovation, and broad adoption through the development of open identity specifications, operational frameworks, education programs, deployment and usage best practices for privacy-respecting, secure access to online services." [KANTARA]

The IETF's OAuth Working Group is also active in the standardization of trust and identity protocols, and is continuing development of OAuth, an "open protocol to allow security authorization in a simple and standard method from web, mobile, and desktop applications." Version 2 of the OAuth protocol was published as a proposed standard in October 2012. [OAUTH-V2], [LYNCH2011], [CERF2011], [GRANT2011]

2.7 Securing Essential Services

Essential services, such as the electric power grid and municipal water systems, are increasingly dependent on data networks, called SCADA (Supervisory Control And Data Acquisition), for their normal operation. When essential services are attacked, the potential damage goes far beyond the damages caused by sending spam advertising fake watches and sexual enhancement drugs.

The consequences of a successful attack against a computer operating or controlling these types of critical infrastructure are dire. Disabling a web server may be inconvenient and result in some loss of income and extra costs, but bringing down the electrical grid has more serious and far reaching effects on public safety. Thus it is important to pay particular attention to the threat such attacks and the associated responses would represent to governance and proper functioning of the global Internet.

These threats are new, and for the most part, theoretical. However, SCADA systems are not run in the same way as typical enterprise networks, with regularly scheduled security patches and downtime for upgrades and maintenance. SCADA networks have computers embedded deep inside that are programmed to do very specialized attacks very reliabily, with a much lower emphasis on protection from attacks. The major forms of protection for networks controlling essential services have been twofold: air gap and security through obscurity.

The phrase “air gap security” refers to a common security practice with critical control systems. Network and system security, it is thought, is simple: just ensure there is no physical connection between the control systems and the Internet. No physical connection—an air gap—means that no malware can infect a system disconnected from all others, and no one can take control of a system with no network connections. While this type of security was easy to enforce several years ago, it has becoming increasingly difficult to ensure these air gaps, given the pervasiveness of the Internet in every aspect of our lives and businesses, including that of utility companies. Because essential systems are networked with each other, all it takes is one compromised system at the periphery to take down the entire chain. For example, it is believed that the Stuxnet Worm that disabled hundreds of centrifuges in Iran’s Natanz fuel enrichment plant was able to jump over the air gap between the plant’s SCADA network and the Internet when a technician plugged an infected computer into the plant network. [STUXNET-NYT]

A second type of security, “security through obscurity,” suggests that networks supporting essential services are inherently protected because many of the control systems and protocols were largely unknown to potential attackers. But as these systems have become valuable targets for criminals, there is additional incentive to learn about, and break into, obscure systems. This is increasingly true as custom-written and real-time operating systems are replaced with lower-cost off-the-shelf software such as Windows and Linux, with known security vulnerabilities that may not be patched due to the nature of these networks.

Military organizations, as well as standards bodies like NIST in the US, are now starting to address the challenge of securing systems supporting national critical infrastructure.

3 Cybersecurity Problems and Technology Solutions

Cybersecurity is an active area of research and development in the information technology community, with participants from all parts of the IT ecosystem. Many of the cybersecurity themes discussed above have common security problems that must be solved as part of the continuing maturation of the Internet as a secure and trusted part of our lives.

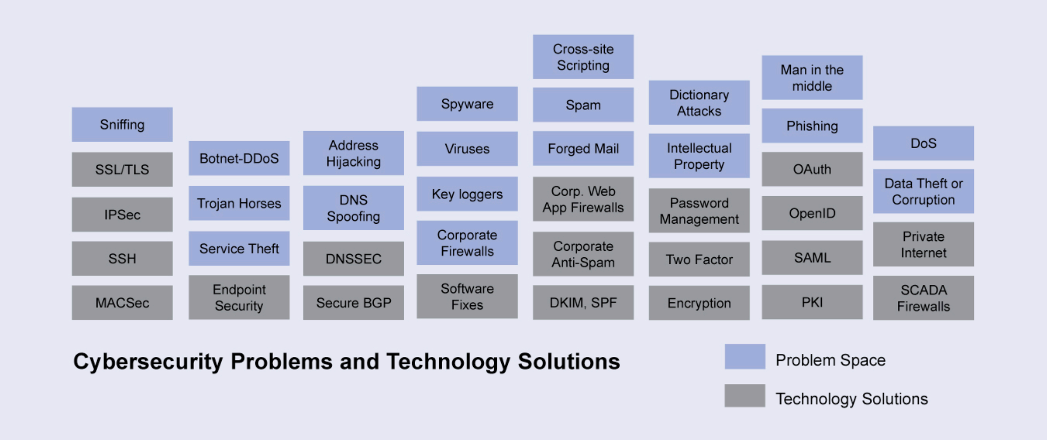

Figure 2: Cybersecurity Problems and Technology Solutions

Figure 2 summarizes some of the major problem areas of cybersecurity and indicates where some of those problem areas have technological solutions that have been developed by commercial entities, standards organizations, and Internet users.

Finding a technological solution to a cybersecurity problem doesn't make the problem go away; it simply offers an opportunity to solve it. For example, end-to-end encryption using SSL/TLS is a well-known technology that can be used as a part of the answer in many of the themes listed above. However, it has not been universally adopted, partly for historical reasons and organizational inertia, and partly out of ignorance or misinformation. Having well-known solutions to well-known problems doesn't bring much value if the solutions are not used.

The sections below give a cross-section overview of some of the major cybersecurity problems and the solutions that are being actively developed and maintained in the Internet community. In many cases, the solutions listed are well known and mature; in the rest, the solutions are areas of active research and development throughout the community. Because many of these cybersecurity problems can be used in multiple cybersecurity themes, they don't map directly to the list of themes earlier in this document but are common to the whole area of cybersecurity.

3.1 Solving Eavesdropping with Encryption

The problem of eavesdropping can be solved with encryption (and authentication) of messages. This encryption can occur at various layers of the network. In some cases, multiple encryption schemes may be applied at the same time, depending on network and application architecture. The common approaches are:

Layer	Solution
Lowest (physical and data link)	Proprietary Link encryption; IEEE wireless standard 802.11; IEEE wired standard 802.3 MACSec
Network (IPv4 and IPv6 level)	IETF IPSec IP Security (and IKE Internet Key Exchange) standards
Application	SSL, TLS, SSH, PGP, S/MIME

Link-layer encryption can be provided by the mature wireless standard IEEE 802.11 (and the industry-based profile called Wi-Fi Protected Access, WPA) or the new IEEE 802.1 data link encryption standard, commonly called MACSec. While 802.11 and WPA security are commonly implemented today, MACSec is not in use because it is a new standard and requires new network equipment. Older link-layer encryption tools, such as point-to-point encryption devices , have been deployed in wide area network (WAN) environments, especially by the financial services and military communities.

Network layer encryption is common in many enterprises using the IPsec [IPSEC] and IKE standards. The generic term for this type of encryption is VPN, Virtual Private Network, since the use of these protocols can create a protected and encrypted network-within-a-network. These standards were developed by the IETF based on earlier work done in other security and standardization organizations. Enterprises linking branches together over the Internet are the most frequent users of IPSec, but this standard can also be used for remote access, bringing individual users back to the corporate network through an encrypting VPN client installed on their laptop or desktop.

Application-layer encryption can be provided by many different protocols. The best-known example is SSL (Secure Socket Layer), recently replaced by Transport Layer Security [TLS]. SSL/TLS is the most common application-layer encryption protocol used in most financial and security based transactions. In the Web world it is signified by the web prefix “https:” In addition to SSL/TLS, other application security protocols supporting encryption include SSH (Secure Shell) [SSH] for remote login capability and S/MIME [SMIME-MSG] [SMIME-CERT] for encrypting e-mail. All of these application security protocols use X.509 certificates [X509] for the public key infrastructure. A number of recent incidents involving the issuance of these certificates illustrate some of the inherent flaws in this approach [COMODO] [DIGINOTAR]. There are efforts in multiple technical organizations to address some of these issues.

All these protocols have a long history of development through various technical standards organizations. Many have spawned development in other organizations looking at more secure variations. IPsec, for example, is a successor of the ISO standard Network Layer Security Protocol (NLSP) based on the SP3 protocol that was published by NIST, but designed by the Secure Data Network System project of the US National Security Agency (NSA).

3.2 Solving Malware using Firewalls and End-Point Security Tools

One of the largest areas of potential for improving cybersecurity is the protection of computers themselves. These are often called “end-point” security solutions, because the computer, whether it is a web server, a smart phone, a laptop, or a desktop in someone’s home or office, is one of two ends of a connection on the Internet.

3.2.1 Types of Malware

The generic term for viruses, spyware, Trojan horses, and key loggers is “malware,” short for “malicious software.” Malware is software that is downloaded by the user, often unintentionally by clicking on what appears to an innocuous web site or advertisement or opening an email message. The software embeds itself in the computer operating system with a range of possible effects. It can be a simple nuisance that constantly bombards the user with unwanted pop up ads. On the other hand the software can be more sinister; for example, through “key logging” where it listens for passwords and other personal information typed on the keyboard, and saves them for uploading to criminals at a later date.

Another use for malware is the creation of botnets, abbreviated from Ro**bot Net**works. Botnets are created by sophisticated types of malware designed to infect many systems at once, and then turn control of the systems over to a human being who can use them as a massive parallel processing network. Botnets can be used to send unsolicited commercial email (spam), to act as fake web servers to steal credentials and other information from end users, and to attack other computers to disable or overwhelm them (Distributed Denial of Service, DDoS attacks).

Recent research indicates the magnitude of the problem. A typical botnet built to recruit enterprise machines is about 1,000-strong, while a large spamming botnet can be anywhere from 50,000 to hundreds of thousands of machines. According to Dark Reading [DR] the average number of botnets found in an enterprise has remained relatively steady during the past couple of years, with as much as 5 to 7 percent of all corporate systems infected by botnets.

Securing the computers connected to the Internet against malware has been divided into two major areas: firewalls, which build a protective ring around an organization's network, and end-point security software and hardware, which focus on detecting and blocking malicious software from taking control of the end point.

3.2.2 Using Firewalls

A common approach to securing end points is to create a boundary around the organizational network using firewalls. For most computers, the firewall acts as a one-way valve, allowing the system inside to connect out towards the Internet, while prohibiting connections from the outside to the inside. For a few systems, such as email and web servers, incoming connections need to be allowed, but these are restricted to particular applications on particular servers. This creates challenges of configuration and control, especially with new multi-media applications. For example, Voice over IP (VoIP) and Video Conferencing don't function if they are choked by a firewall, so the IT group must add rules to allow traffic through the firewall to accommodate these complicated services. If an error has been made by the IT group or the firewall vendor in designing the firewall's VoIP or video conferencing features, unintended traffic could be allowed into the corporate network.

Over time, the growth of rules and exceptions has itself become an object of concern. Because each rule added is known as "punching a hole" through the firewall, organizational firewalls have been referred to as "Swiss cheese," and their effectiveness as a way to protect computers is in doubt.

More importantly, most firewalls allow internal computers relatively unrestricted access to the Internet to browse web sites and read email. Because malicious software can be delivered to the end user's computer over these very common channels, the firewall by itself is not very effective at blocking threats. Firewalls and packet inspection technologies also coexist badly with other protective measures such as encrypted content, VPN/tunneling, and SOAP. This is because all of these open up ways for malicious payloads to pass through. This has led to an ecosystem of assistive technologies, including:

- Firewalls with anti-malware tools embedded (usually called "UTM," for Unified Threat Mitigation);

- Application-aware firewalls (usually called Next Generation firewalls) which both have embedded anti-malware tools and are able to control the use of Internet applications such as Facebook and Skype that a traditional firewall cannot control; and
- Secure web gateways (also called proxy servers) with embedded anti-malware tools embedded.

3.2.3 Using End-Point Security Software and Hardware

Malware can arrive on computers in many ways. One of the most common is when a user inadvertently downloads software from an infected or disreputable website, or receives the software as part of an email message. Malware can also be passed through corporate and home networks (which are often loosely secured) by sharing of USB flash drives. Cyber-criminals have also developed more innovative ways to attack end-user systems, such as through public Wi-Fi connections [WIFI].

Malware exists for every type of computer in common use, including Macintosh OS X, Unix and Linux systems, as well as smart phones and other devices such as digital music players and tablet computers running embedded operating systems.

This problem is so widespread that organizational IT staff universally recommends the use of end-point security software (often called anti-virus or anti-malware) tools on all devices. It is common for enterprises to require that any computer attached to their network have installed end-point security tools set by corporate standards. This is true in almost every sphere, from higher education and government to military and corporate networks.

End-point security tools can contain several components to assist in protection against malware, including:

Tool	Description
Anti-malware	Protects against viruses and spyware (malware) by detecting malware when it is downloaded or executed
Intrusion Prevention	Protects by detecting the behavior of malware, rather than the malware itself, when it attempts to infect the operating system, to infect other systems, or to join a botnet
Host Firewall	Blocks inbound and outbound connections to an end-system based on security policy

3.3 Technical solutions to secure Internet infrastructure

Although the Internet is seen as ubiquitous and reliable, its own infrastructure is vulnerable to attacks. However, an attack against the Internet infrastructure is a double edged sword for many potential criminals – a successful disruption of the Internet infrastructure would preclude it being used for any purpose, including communications by the “bad guys” or as a platform for further attacks. An attack against the Internet infrastructure itself would vastly disrupt commercial communications around the world (although it would be unlikely to disrupt secure military communication systems), and so such an approach would appeal to individuals or groups who wish to make strongly destructive political statements. As has been seen with the cyber-protests accompanying events such as the release by Wikileaks of classified diplomatic cables, attacks can come from unexpected sources at unexpected times.[3]

Some key points of vulnerability for the Internet are the core routing protocols of the network (BGP) and the Internet naming system (DNS). Ongoing technical work on BGP and DNS Security is discussed below in 3.3.1 and 3.3.2. The physical routers, as well as the forwarding and management planes of the Internet, are also susceptible to cyber-attacks, but these are largely single-domain security issues internal to a network operator and so are usually addressed at the organizational level, or as telecom security issues.

These issues have not gone unnoticed. The US Department of Homeland Security has published a roadmap for fixing the Internet's protocols [ROADMAP]. Readers interested in more details on the security issues related to DNS and BGP may want to refer to [NIST-BGPSEC], a publication of the US National Institute of Standards and Technology (NIST).

Historically, however, there have been few intentional widespread attacks against the Internet's infrastructure. DNS attacks are the most frequent, but have not widely affected the infrastructure. Instead, they are being used to target specific individuals and organizations. BGP incidents are not uncommon, but they are generally caused by human error and configuration errors rather than malicious actors or intentional disruptions.

3.3.1 Securing DNS data with DNSSEC

The Domain Name System (DNS) is a highly successful and critical part of the Internet infrastructure. Without it, the Internet would not function. DNS allows people to use easily remembered and recognizable names for web sites and e-mail addresses, which are then converted into the numerical format used in the Internet's internal protocols.

Multiple potential DNS attacks have been described, both in theory and in practical demonstrations:

- The DNS is a globally distributed database, whose performance critically depends on the use of caching. Unfortunately it was discovered that the common DNS software implementations are vulnerable to spoofing attacks whereby an attacker can fool a cache into accepting false DNS data.
- Man-in-the-middle attacks can be accomplished when a device can be inserted into the path between DNS clients and DNS servers (or two DNS servers) and redirect or modify DNS information.
- Administrative attacks on the DNS can be used to redirect an organization's DNS traffic by guessing passwords on domain name registrars or convincing registrars to give unauthorized personnel access.

Internet engineers recognized some time ago that there was a strong incentive to make the DNS secure because of its important function of translating human recognizable addresses into those used by the routers and computers connected to the Internet.

[3] It should be noted that the cyber-protests surrounding the Wikileaks releases were not actually Internet infrastructure attacks as discussed here, but denial of service attacks against organizations seen as supporting the US Government position on Wikileaks.

As early as 1995, research [ATKINS2004] was started on a more secure replacement of DNS, and DNSSEC became an IETF working group. DNSSEC is a set of extensions to the DNS that provide authentication and integrity checking of DNS data. In 1997, the first DNSSEC standard, known as RFC2065, was developed. A revised DNSSEC specification was completed in 2005, with some additional features standardized in 2008.

Authentication in DNSSEC ensures that zone administrator can provide authoritative information for any particular DNS domain, while integrity checking ensures that information in the DNS cannot be modified (accidentally or maliciously) while in transit or in storage. That means that DNSSEC, among other things, helps to protect against attacks that insert false information into the DNS to redirect Internet users to deceptive or criminal web sites, so-called "hijacking" of web sites.

After several years of intense technical study and testing, the first production DNSSEC deployment in a top-level domain was completed in Sweden in 2007. After agreement was reached on how it would be deployed globally, DNSSEC is now being deployed around the world. In July 2010 the DNS root zone was signed.

It is important to note that the Domain Name System Security Extension (DNSSEC) is not designed to end cyber-attacks against the DNS, but to make those attacks detectable. Wide-scale deployment of DNSSEC could help resolve many other security problems as well, such as secure key distribution for e-mail addresses.

Because of the way DNSSEC is implemented it allows many other technologies to use the same set of security protocols to safely distribute the all-important encryption key required for a range of purposes, such as SSH and IPSec. So not only will DNSSEC provide a basis to address the security of challenges of the DNS; it will enable strengthening of other critical parts of the Internet. [DANE]. Having said this, DNSSEC will need to address the same issues associated with CA compromise as illustrated in the Diginotar and Comodo incidents referenced earlier.

3.3.2 BGP Security

As the Internet's inter-domain routing protocol, the Border Gateway Protocol (BGP) is the glue that holds the Internet together. But a major limitation of BGP is that it does not adequately address security. Recent high-profile outages clearly showed that the Internet routing infrastructure is susceptible to attacks with a global impact.

The routing tables maintained by Internet Service Providers (ISPs) and dynamically updated by BGP are the basis for all inter-organizational routing. Since BGP is inherently inter-domain and not under the control of any single management authority, it is possible for routing errors to be inserted deliberately or accidentally by organizations including both ISPs and any organization with a large enough Internet presence to participate in the BGP protocol, such as a company with two independent Internet connections. Errors can cause severe disruption of the Internet. Weekly reports produced by several organizations, including APNIC (the Asia-Pacific Network Information Center) and the University of Oregon, along with Internet researchers such as Geoff Huston, show that configuration errors affect about 1% of all routing table entries at any given time, once again underlining the fact that the current system is highly vulnerable to human errors, and a wide range of malicious attacks. Yet BGP has proven to be amazingly resilient at the same time.

One of the mis-configurations of Internet routers running BGP, often referred to as “BGP hijacking,” isn’t new. It happens frequently, though generally the hijack is unintentional. Nonetheless, such errors can result in a widespread denial-of-service attack or outage, as was the case when Pakistan Telecom inadvertently hijacked YouTube traffic.

In that incident, the Pakistani telecom company intended to block only Pakistanis from accessing YouTube in order to prevent them from viewing content the Pakistan government deemed objectionable. Instead, the company and its upstream provider mistakenly advertised to routers that it was the best route through which to send YouTube traffic. For nearly two hours browsers from many sites across the Internet attempting to reach YouTube fell into a black hole in Pakistan. [BGPHIJACK]

BGP hijacking is the insertion of unauthorized IP routes into the BGP routing tables. At this time, there is no single unambiguous database that matches IP routes to the organizations allowed to insert, or advertise, them. The current authorization process is essentially manual, with each organization joining the Internet having the responsibility of approving the set of IP routes that can be advertised to their peers. While the IETF Best Practices recommendations suggest that each BGP peer should only allow the specific routes that have been administratively approved, this practice is not widely followed. In addition, as one moves further from the connected organization towards the Internet core, the ability to authorize and authenticate updates becomes impossibly complex. Policy-based tools, such as the Internet Routing Registry (irr.net), which attempt to provide authoritative lists of authorized networks and network service providers, have been successful but are not universally adopted and require considerable manual intervention in routing configuration.

The Secure Inter-Domain Routing (SIDR) working group within the IETF was formed in November 2005 to reduce vulnerabilities in the Internet’s BGP routing system. SIDR aims to reduce the risk of service providers hijacking networks by advertising unauthorized IP routes, and will create standards for a certification infrastructure called Resource PKI (RPKI). This certification infrastructure verifies the allocations of Internet Number Resources (INRs) including blocks of IP addresses and Autonomous System numbers (ASNs). This infrastructure follows the existing INR distribution structure within IANA, the Regional Internet Registries (RIRs) and the Internet Service Providers (ISPs) issuing certificates for the relevant resources. This allows organizations that are the holders of specific IP address to authorize a specific network (denoted by an ASN) to advertise these addresses. This authorization is published using a digitally signed object, called Route Origination Authorization (ROA), that third parties can validate using RPKI, giving the potential for automated checking, even at the Internet core, of all routing updates. If an organization attempted to inject an unauthorized IP route into the BGP routing tables, this would be detectable. [SIDR]

The SIDR working group has published a number of documents laying the framework for RPKI and Route Origin Authorization. The specifications are standardized and published as RFCs, and all the Regional Internet Registries (RIRs) are currently deploying services to support RPKI. However, significant effort will need to be expended by every organization participating in Internet BGP routing (currently over 37,000 organizations) to make use of these new capabilities in their routing management infrastructure.

3.4 Technical solutions to secure authentication systems

Authentication of end users to Internet-based applications represents a continuing tension in both public and private sector. The goals of security, privacy and usability are often at odds with each other. The easier it is to authenticate, the easier it is for someone to intercept or steal authentication information and use it to impersonate a valid user. On the other hand, if authentication is onerous and time-consuming, even though security is increased, end users may decide not to use the application because it is too much bother. Or, in the face of difficult-to-use authentication systems, users could build their own workarounds and shortcuts to make the authentication process easier but, at the same time, less secure.

Protecting authentication falls into two broad categories: protecting the information itself, and making it easier for users to authenticate securely.

3.4.1 Protecting Authentication Databases

The databases that hold authentication information are referred to as Identity Data Management systems (IdM) [IDM]. They are commonly a subset of many databases containing much larger sets of personal data and which usually contain user name and password information required for authentication. These databases may also contain other pertinent information related to authorization, for example whether a user has been authorized to see certain content at a remote site. The most popular protocols used in these systems are directory systems such as LDAP [LDAP] and X.500 [X500]. RADIUS [RADIUS] servers using LDAP and X.500 are common tools used to simplify access to authentication information by providing a simple Application Programming Interface (API) to the more complicated directory systems.

Any breach of the IdM database opens up the entire set of personal data stored in the database to an attacker. In some cases, it would also allow the attacker to impersonate a legitimate user to authenticate to other systems around the world. As a result, attacks against IdM systems are usually one of the preferred methods to breach security of a web application.

Insiders with access to the IdM are usually the weakest link in maintaining the security of IdM systems. Brute force approaches such as “dictionary attacks”, where attackers try commonly used names and passwords to gain access to the IdM system, are among the more popular and successful approaches for external attackers.

Defenses against dictionary attacks include asking users to change their passwords every few weeks or months and using complex passwords made up of numerical and alphabetic characters that would not be found in commonly used names or passwords. On the server side, the primary defense is encryption of the password database to protect against unauthorized access. In some cases, the encryption has proven to be ineffective and even encrypted databases have resulted in compromised passwords.

A more practical, although more expensive, approach to password protection is to add two-factor authentication. Two-factor authentication adds some other factor in addition to the username and password. This factor is required for the authentication to complete. For example, a small token may be assigned to a user that displays a “password of the minute” that must be combined with the normal user password. Other innovative techniques, such as sending a password to a mobile phone, adding in biometric tools such as fingerprints, or displaying a Quick Response (QR) code as part of the authentication dialog are also used. [TIQR]

3.4.2 Using Open Authentication Standards and PKI

As the number of Internet applications requiring authentication has grown, so too have the number of authentication databases. As mentioned above, in some cases encryption of these databases has proven to be ineffective with the result being compromised passwords. One area of considerable interest in cybersecurity is trying to reduce the risk of having these databases by reducing the number of databases or reducing the amount of data stored in these databases, while at the same time developing open protocols that allow authentication information to be passed between applications securely.

A number of techniques are used to steal authentication information directly from end users, including both phishing and man-in-the-middle attacks. Phishing is an activity where hackers establish a false identity on the Internet, pretending to be a bank or store web site, where they entrap unsuspecting visitors who are there to carry out commercial transactions and trick them into providing detailed personal information such as bank account numbers, and passwords. "Man in the middle" attacks are computers deployed across the Internet that can intercept common queries and messages from a user, and then redirect them elsewhere, or provide erroneous data in response to a user request. A frequent threat posted by man-in-the-middle attacks is the theft of authentication information.

Both phishing and man-in-the-middle attacks can be defeated through the mutual identification and authorization of both end points of communication, enabling both parties to have reasonable assurance that they are who they claim to be.

Considerable research and development has gone into the work of establishing identity and trust under the rubric of cybersecurity, and we are now starting to see the first products and services emerge from standards bodies and research organizations. In the academic world Shibboleth [Shibboleth] is now the preferred tool for federated identity, while in the commercial world tools such as OpenID [OPENID] and OpenAuth [OPEN AUTH] are slowly gaining acceptance. Security Assertion Markup Language (SAML) [SAML] is the underlying technology used for many authentication applications used by OpenID and OpenAuth. It is an XML-based standard for exchanging authentication, entitlement, authorization data and other user attributes. SAML allows business entities to make assertions regarding the identity, attributes, and entitlements of a subject (often a human user) to other entities, such as a partner company or another enterprise application. SAML is a product of the OASIS Security Services Technical Committee [OASIS].

4 Concluding Thoughts

Cybersecurity is a broad term that has evolved over time with no clear consensus on its exact meaning. Public awareness of the status of cybersecurity is colored by the often-sensational lapses in security that occupy the media. The exposure of personal information, stolen financial data, and spread of malware and viruses all give the impression of danger and chaos, of the imminent collapse of the Internet. In fact, the sky is not falling; but there could be storms on the horizon. There's certainly reason to be cautious, but the overall balance weighs heavily on the side of value. The Internet has become a tool for knowledge, communication, expression and commerce, a trusted resource and a powerful force for personal freedom.

This paper has demonstrated that cybersecurity solutions are widespread and complex – as we move forward to address new challenges, we must ensure that the open and innovative spirit of the Internet is not compromised. Solutions to cybersecurity problems must also further the goal of all Internet users: an open, accessible, and trustworthy Internet. The openness of the Internet is one of its key strengths, making it a major worldwide source of creativity, innovation, and growth. Ultimately, success in addressing cybersecurity problems lies in multi-stakeholder cooperation and collaboration, not new command-and-control systems.

References:

[ABAR] American Bar Association-appointed special cyber-prosecutors http://www.cfr.org/publication/22832/internet_governance_in_an_age_of_cyber_insecurity.html

[ALBRIGHT] Remarks of Madeleine K. Albright at the meeting of the North Atlantic Council with the Group of Experts on NATO's New Strategic Concept, May 17, 2010 http://www.nato.int/cps/en/natolive/opinions_63678.htm

[ATKINS] Atkins, D. and Austein R. (2004). RFC 3833, "Threat Analysis of the Domain Name System (DNS)", August, 2004 Available: http://www.rfc-editor.org/rfc/rfc3833.txt.

[AUSTRALIA-DBCDE] Australian Government Department of Broadband, Communications, and the Digital Economy. (2011). *Internet Service Provider (ISP) filtering*. Available: http://www.dbcde.gov.au/all_funding_programs_and_support/cybersafety_plan/internet_service_provider_isp_filtering. Last accessed 25 March 2012

[AUSTRALIA-UPDATE] http://arstechnica.com/tech-policy/2012/11/australia-comes-to-its-senses-abandons-national-internet-filtering-regime/

[BGPHIJACK] YouTube Hijacking: A RIPE NCC RIS case Study (http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)

[BORDER] Reporters without Borders http://en.rsf.org/internet.html

[CECC] Council of Europe Convention on Cybercrime http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp

[CERF2011] Cerf, V. (2011). The Battle for Internet Openness. *IEEE Internet Computing*. 15 (5), 104.

[CLARKE] Richard A. Clarke *Cyber-War* http://www.wired.com/threatlevel/2010/04/cyberwar-richard-clarke/

[COICA] Wikipedia, "Combating Online Infringement and Counterfeits Act" http://en.wikipedia.org/wiki/Combating_Online_Infringement_and_Counterfeits_Act

[COMODO] Leonhard, Woody. "Weaknesses in SSL certification exposed by Comodo security breach." InfoWorld Tech Watch. InfoWorld, 24 Mar. 2011. Web. Web. 27 Jul. 2012. <http://www.infoworld.com/t/authentication/weaknesses-in-ssl-certification-exposed-comodo-security-breach-593>.

[CYBERCOM] Burghardt, Tom, "The Launching of U.S. Cyber Command (CYBERCOM), Center for Research on Globalisation, Quebec, Canada, http://www.globalresearch.ca/index.php?context=va&aid=14186

[DANE] DNS-based Authentication of Named Entities Working Group - http://tools.ietf.org/wg/dane

[DIGINOTAR] Whitney, Lance. "Comodohacker returns in DigiNotar incident." CNET: News: Security & Privacy. CNET, 6 Sep. 2011. Web. Web. 27 Jul. 2012. <http://news.cnet.com/8301-1009_3-20102027-83/comodohacker-returns-in-diginotar-incident/>.

[DKIM] http://tools.ietf.org/wg/dkim/

[DR] Dark Reading – http://www.darkreading.com/index.jhtml

[FBI] 2005 FBI survey http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf

[FIRESHEEP] http://codebutler.com/firesheep/?c=1

[GRANT2011] Grant, J.A. (2011). The National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy through Standards. *IEEE Internet Computing*. 15 (6), 80-84.

[HERSH] Seymour Hersh, "The Online Threat" http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh

[HODGES] Hodges and Steingruebl, "The Need for a Coherent Web Security Policy Framework", Web 2.0 Security and Privacy 2010 Conference, http://w2spconf.com/2010/papers/p11.pdf

[IC3] Internet Crime Complaint Center Report http://www.ic3.gov/default.aspx

[IDM] Identity Data Management systems (IdM) http://en.wikipedia.org/wiki/Identity_management

[IPSEC] IPsec http://datatracker.ietf.org/wg/ipsec/charter/

[IWM] Information Warfare Monitor http://www.infowar-monitor.net/

[KANTARA] The Kantara Initiative http://kantarainitiative.org/

[LDAP] Zeilenga, K. (ed) (2006). RFC 4510, "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map," June, 2006. Available: http://www.rfc-editor.org/rfc/rfc4510.txt.

[LOPPSI] http://fr.wikipedia.org/wiki/Loi_d'orientation_et_de_programmation_pour_la_performance_de_la_s%C3%A9curit%C3%A9_int%C3%A9rieure

[LYNCH2011] Lynch, L. (2011). Inside the Identity Management Game. *IEEE Internet Computing*. 15 (5), 78-82.

[MARF] http://tools.ietf.org/wg/marf/

[NIST-BGPSEC] http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf

[NSPW] New Security Paradigms Workshop http://www.nspw.org/

[NSTIC] National Institute of Standards and Technology. (2011). *Making Online Transactions Safer, Faster, and More Private.* Available: http://www.nist.gov/nstic/. Last accessed 22 March 2012.

[NYT-ENERGY] http://www.nytimes.com/2010/01/26/world/26cyber.html

[NYT-GOOGLE] http://www.nytimes.com/2010/01/13/world/asia/13beijing.html

[OASIS] OASIS Security Services Technical Committee http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

[OECD] Organization for Economic Cooperation and Development. (1980). *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* Available: http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html. Last accessed 25 March 2012.

[OPENID] http://openid.net/

[OAUTH V2] Hardt, D. RFC 6749, "The OAuth 2.0 Authorization Framework", October 2012. Available: http://www.rfc-editor.org/rfc/rfc6749.txt Last accessed 23 October 2012.

[OPSEC] Internet Engineering Task Force. (2012). *Operational Security Capabilities for IP Network Infrastructure (opsec).* Available: http://datatracker.ietf.org/wg/opsec/. Last accessed 25 March 2012.

[OPSEC-TAXONOMY] C. Lonvick and D. Spak. (2011). *Security Best Practices Efforts and Documents (Internet Draft).* Available: http://tools.ietf.org/html/draft-ietf-opsec-efforts-18. Last accessed 25 March 2012.

[PATHWAYS] Seventh Worldwide Security Conference International Pathways to Cybersecurity http://www.ewi.info/international-pathways-cybersecurity-0

[PGP] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and Thayer, R. (2007). RFC 4880, “OpenPGP Message Format”, November, 2007. Available: http://www.rfc-editor.org/rfc/rfc4880.txt. Last accessed 25 March 2012.

[RADIUS] Rigney, C., Willens, S., Rubens, A., Simpson, W. (2000). RFC 2865, “Remote Authentication Dial In User Service (RADIUS),” June, 2000. Available: http://www.rfc-editor.org/rfc/rfc2865.txt. Last accessed 25 March 2012.

[REVIEW] Defense Department’s Quadrennial Defense Review http://www.defense.gov/qdr/

[ROADMAP] Department of Homeland Security’s roadmap for fixing the Internet’s protocols http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

[SAML]Security Assertion Markup Language (SAML) http://en.wikipedia.org/wiki/Security_Assertion_Markup_Language

[SHADOWS] http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0

[Shibboleth] http://shibboleth.internet2.edu/

[SIDR] http://tools.ietf.org/wg/sidr/charters

[SKYPE] Ten countries threatening to block Skype and Google http://www.voip-sol.com/10-isps-and-countries-known-to-have-blocked-voip/

[SMIME-MSG] Ramsdell, B., Turner, S. RFC 5751, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification," January 2010. Available: http://www.rfc-editor.org/rfc/rfc5751.txt.

[SMIME-CERT] Ramsdell, B., Turner, S. RFC 5750, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling," January 2010. Available: http://www.rfc-editor.org/rfc/rfc5750.txt.

[SSH] Ylonen, T., Lonvick, C. (ed). (2006). RFC 4251, “Secure Shell (SSH) Protocol Architecture,” January, 2006. Available: http://www.rfc-editor.org/rfc/rfc2865.txt. Last accessed 25 March 2012.

[STUXNET] Falliere, Nicolas; Murchu, Liam; Chien, Eric (Symantec Security Response) W32.Stuxnet Dossier (Feb, 2011) http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

[STUXNET-NYT] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[TIQR] Jan Michielson. (2011) *TIQR User Manual.* Available: https://tiqr.org/wp-content/uploads/2011/05/tiqr_manual_v1.0.pdf. Last accessed 25 March 2012.

[TLS] Dierks, T., Rescorla, E. (2008). RFC 5246, “The Transport Layer Security (TLS) Protocol, Version 1.2,” August, 2008. Available: http://www.rfc-editor.org/rfc/rfc5246.txt. Last accessed 25 March 2012

[US-NTIA] http://www.ntia.doc.gov/category/privacy

[W3C-APP] Web Applications Working Group Charter, World Wide Web Consortium. http://www.w3.org/2010/webapps/charter/

[W3C-SEC] Web Application Security Working Group, World Wide Web Consortium, http://www.w3.org/2011/webappsec/

[WIFI] http://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-Wi-Fi-Security-Threats.htm

[WIKI-ESTONIA2007] 2007 Cyberattacks on Estonia (from Wikipedia) http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[X500] X.500, “Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services.” http://en.wikipedia.org/wiki/X.500

[X509] X.509, “Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks.” http://en.wikipedia.org/wiki/X.509

Internet Society
Galerie Jean-Malbuisson 15
CH-1204 Geneva, Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445

1775 Wiehle Ave.
Suite 201
Reston, VA 20190
USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881

Email: info@isoc.org
www.internetsociety.org