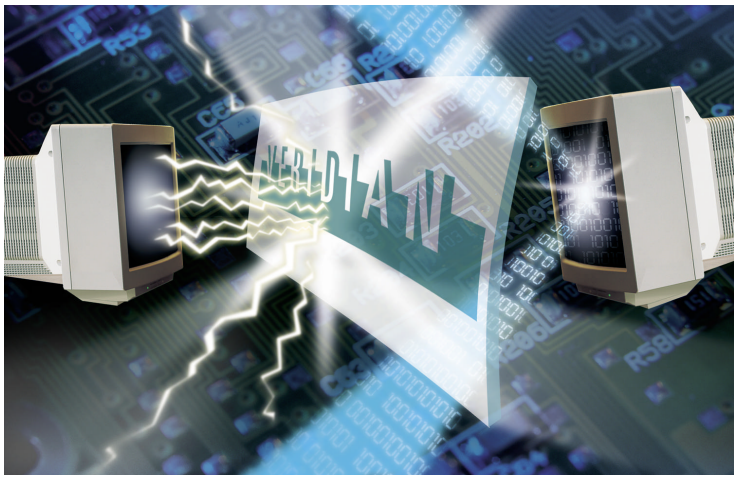
1100 NW Loop 410 • Suite 600
San Antonio, Texas 78213

VERIDIAN
Trident Data Systems

The Future of Information Security Technologies

As presented before the Conference on High Speed Computing
27 April 2000



John Steven Reel, Ph.D. · 210-442-4262 · John_Reel@tds.com

The Future of Information Security Technologies

As presented before the Conference on High Speed Computing

Abstract

Information security, and the technologies that provide such security, are a very hot topic throughout the information technology and business communities today. This paper, *The Future of Information Security Technologies* opens with a consideration of the current network environment. It answers the questions "where are these technologies?" and "where are the gaps in the technologies that are being addressed?" especially as they impact security. Next, the paper considers the field of network security technologies. It addresses the good, the bad and the undecided aspects of the field today. After setting the stage with this background information, the paper identifies the most important trends that will impact the network security industry in the coming few years: the federal government finally cares, the vanishing network perimeter, and the opportunity to achieve ubiquitous encryption. Toward the end of the paper, Dr. Reel presents two "killer" security-related applications. Finally, the paper closes with a discussion of the major needs in the information security field.

Table of Contents

Introduction

> *Men must pursue things which are just in present, and leave the future to the divine Providence. – Sir Francis Bacon*

As Sir Francis Bacon aptly states above, foretelling the future in any of life's endeavors is a challenge. To do so in a field experiencing such wholesale and rapid change as information technology is fraught with error. Then to compound that by considering a technology area which is not yet mature by any stretch of the imagination is sheer folly. Such is our task in this text.

Overview

We open this document by discussing the most pressing technology issue facing the county – perhaps the world – today. That issue is the lack of qualified technical personnel. If we cannot fix this problem, many of the other issues and opportunities will be mute.

Next we go into a discussion of the state of networking technology in general on the premise that without understanding the vector and the velocity of the technology environment in which we will be providing protection, any forecast will necessarily be flawed.

Then, we consider the current state of information security trends. First among these is the tremendous emphasis the *federal government* is beginning to show in the field of information security. The potential results of this interest are a significant increase in R&D spending in technologies that support information security as well as in spending toward a plethora of commercially-developed (COTS) security products. Second, we discuss the concept of the *vanishing perimeter*. Most information security products on the market today are point solutions based on the assumption that the perimeter of a network is well defined and controlled. This is no longer the case. The final trend we discuss is the move toward *ubiquitous encryption*. With the pervasiveness of the Secure Socket Layer (SSL) protocol and virtual private networking products, much more network traffic is encrypted today. We discuss the implications of this situation.

Having described these significant trends, we then describe two so-called "killer" applications. It has historically been demonstrated that for a new technology movement to really catch on and garner mass market adoption, there must be some innovative application of that technology that generates acceptance and excitement across the mainstream audience. VisiCALC served this purpose for the personal computer, and we might argue that e-mail and Mosaic did so for the Internet. The two applications that we discuss are

truly mobile network credentials and *enterprise management of the security realm*.

Finally, we close the paper with a discussion of the many areas that must be addressed by the technical community, as well as society, as a whole to allow effective information security to come into form.

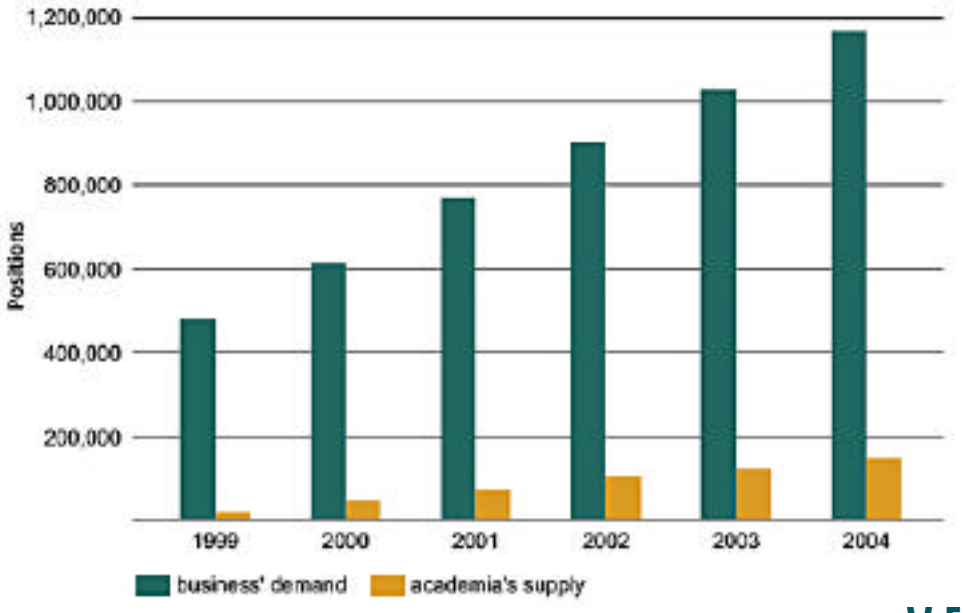
The Pressing Technology Issue

> *Frequently with serious works and ones of great import, some purple patch or other is stitched on, to show up far and wide.*
> *-- Horace*

Were Horace a CIO or Information Security Officer (ISO) in a Fortune Anything company today, he would open every briefing with a slide about the problem of recruiting and retaining quality technical resources. Moreover, that slide would have an animated purple background to be sure everyone understands the importance of the subject. Such is the degree of import with which we consider this issue.

First, let us start with an assumption that the information security labor pool is a subset of the overall IT labor pool.

Now, statistics indicate that the IT labor pool is shrinking. In January 1998, IDG reported that the IT industry needs approximately 137,000 new workers each year. Contrast this with the mere 24,000 IT graduates from US colleges and universities in 1997. This is an alarming situation, but it gets worse. There was a 42% drop in the number of IT graduates from 1986 to 1996. Further, the number of graduates is still declining approximately 4% per year. Following this trend,



we could have one million unfilled IT jobs by the year 2004. These trends are depicted in the graph above:

As an example to put this impending crisis in a more realistic light, if IBM hired *every single IT graduate* this year, it would still fall short of its recruiting requirements.

If we extend the crisis to the field of information security, the curve steepens due to the incredible growth in demand for such personnel. A 1998 CSI survey (reported in *Information Security Magazine*) of more than 300 corporations indicated the following statistics:

- From 1997 to 1998, there was a 64% increase in staff dedicated to information security
- From 1989 to 1998, there was a 300% increase in staff dedicated to information security
- The annual growth rate of information security staff was:
  - 68% at small companies
  - 27% at medium companies
  - 24% at large companies

These statistics indicate tremendous demand for information security professionals. Let us make that look worse by confirming that there are very few college graduates getting trained in information security. In fact, one of the oldest and largest computer science departments in the country is located at Purdue University. Purdue also hosts one of the largest computer security programs in the country, and in 1999 they graduated four students with Master's degrees in information security. FOUR. Many people are entering the field through self-study and using the very few certification programs such as the Certified Information Systems Security Professional (CISSP) [there are only 1,500 CISSP's to date]. Nothing is keeping pace with the demand however.

There is a point to all of these statistics and that point is — who is going to do all of this stuff? If we could perfectly communicate through this paper or some other forum omniscient foresight as to what is needed in this industry, there just are not enough people to build, implement and maintain it properly at this time.

Networking Technologies

> *'Tis true; there's magic in the web of it… --William Shakespeare*

We believe that the field of networking, especially information networking, is, in general, is maturing. There are tools and operations allowing reasonable expectations from enterprise management of networks today. We do much of that kind of work for substantial DoD networks at this time. The fundamental protocols used in networks – TCP, IP, ATM, even NetBEUI – are time tested, robust and trusted to perform. In fact, there is enough faith in these fundamental technologies that NASA is even planning to allow scientists to monitor and control space-based (on the shuttle, space station or satellites) experiments over the Internet. Further, the disciplines and methodologies for designing networks, implementing them, and maintaining them in operational environments are well understood.

Additionally, the physical plant necessary for widespread adoption of these technologies is in place and has capacity to grow rapidly as needed. Finally, there is a vast amount of vendor support – both products and services – to implement and maintain complex, high-volume, mission critical networks.

The primary improvements that we have seen in networking technologies, especially with respect to internetworking technologies are in the areas of on-ramp speed, throughput, and security. There has been a tremendous emphasis on getting the entire Internet user community faster connectivity into the network, and the wide range of high speed consumer-oriented access methods serves as witness to this trend. Of course, when you add users at an exponential rate and simultaneously make the content of web pages more visual, more interactive and more A/V driven, you must increase the throughput of the network overall. The graphic to the right demonstrates just how the speeds in the Internet realm have been increasing as compared to those of other technologies.

Internet Traffic Trends

Technology	Doubling Period
Semiconductor Performance	18 months (Moore's Law)
Computer Perf per Dollar	21 months (Roberts' Law)
Max I'net Trunk Speed	22 months
I'net Traffic Growth (1969-82)	21 months
I'net Traffic Growth (1983-97)	9 months
I'net Traffic Growth (1997-2008)	6 months
I'net rtr/switch max speed ('til '97)	22 months
I'net rtr/switch max speed (post '97)	6 months

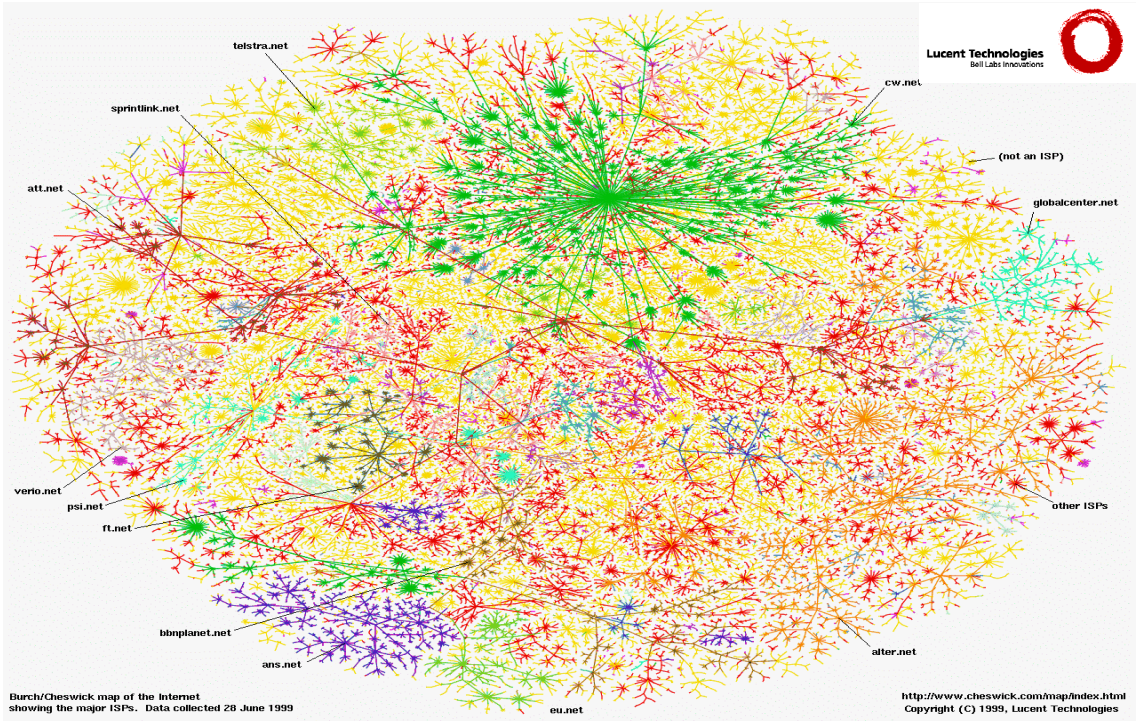
Source: Roberts, Lawrence. "Beyond Moore's Law: Internet Growth Trends." *Computer*. January 2000. pp. 117-9.

The Internet is a Complex Place...

> *Ruinous inheritance.* -- *Gaius*

As a point of illustration and as a final foundation for the following discussion, we must point out that securing the Internet, or even securing any significant enterprise connected to the Internet, is a very difficult undertaking. This difficulty is due largely to the "ruinous inheritance" we discussed in the prior section. All the protocols and design techniques and troubleshooting methods are well defined and accepted. None were defined or engineered with much thought about security because the Internet's underlying technologies were developed among a collegial group of scientists and engineers during the 1970's. Their only interest was to get their radical concepts working so they could then come up with new radical concepts. There was no motivation to steal information because everyone wanted to share information. There was no motivation to break systems because they all wanted to make systems work. Therefore, we in the security industry have inherited an architecture and a suite of protocols – as well as millions of lines of legacy operating systems, protocol stacks, and applications – with virtually no security infrastructure.

Take that legacy, and then consider the vastness and complexity of the Internet. The diagram below represents a map of the Internet done under a project at Bell Labs. Each terminal point in the map represents not a host, but a *network* or group of networks connected to the Internet.



With no security infrastructure and such tremendous complexity, we certainly face a challenge.

Networking Technologies – Remaining Gaps

> *The depth and dream of my desire,*
> *The bitter paths wherein I stray…* *-- Rudyard Kipling*

While networking technologies are stable and quite powerful, there are of course still needs and desires among the user community. There is always a need for higher throughput in the network for moving more data, moving it faster, and moving it to more places. Next, we also need the ability to provide, in an operational sense, additional services and capacities within the network. These include the ability to move voice over the data network, to move video over the data network, and to perform real-time collaboration over the data network. All of these capabilities translate to higher volume and speed in the network, but they also imply an underlying ability to provide quality of service (not existent in current Internet protocol suites) for network transmissions. To accomplish these new capabilities could require the development of many new protocols.

Another capability we need is reliable, irrefutable, common authentication on web. We need some reasonable level of assurance that jreel=[name=John S. Reel, company=Veridian-TDS, DoB=2/4/65, SSN=sss-ss-nnnn, AmEx=123456789, home_domain=tds.com, access_level=3, etc.]. That assurance should hold irrespective of where jreel logs in. Therefore, jreel should be able to log in from home, a satellite office, headquarters, or a client location with all the rights and privileges as from his work PC. This will also allow jreel to visit a web site and commit to purchases or other activities (survey inputs, document modifications, database inputs, etc.) while giving the host great confidence in *who* made those modifications.

Finally, we foresee that the era of multi-media is beginning to succumb to total media. Audio and video files now being "played" are moving toward fully interactive web content where the actors and decision branches are controlled – or at least influenced – by the user.

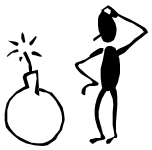
Network Security Issues

> *Our watchword is security.* *– William Pitt*

In discussing the state of network security issues, we have chosen to break the subject into three distinct categories. First we will discuss the areas where improvement is needed soon *The Bad*. Next we will discuss the positive aspects of the current state of network security technologies *The Good*. In the *Not So Sure* section, we discuss issues that will certainly impact our ability to

deliver secure, or securable, solutions, but we have not yet decided if there will be a positive influence or a negative influence by these issues.

The Bad



Relative to the field of general networking technologies, the field of information security has not yet begun to mature, and it may not ever mature as we would like to see. After all, the information security teams are always playing catch-up to other major technologies. Until we develop the discipline and priority needed to instill strong security underpinnings in all our network products, security will always fall far short of the dream.

Also, as compared with network management, there is no such capability as enterprise-level management of the security resource/state. Virtually all security-oriented solutions (think firewalls, intrusion detection systems, remote access controls, etc.) are currently point solutions. Vendors have finally begun to allow enterprise management of their own equipment to a limited degree, but there certainly are no strong tools for managing a heterogeneous, highly distributed environment on the market today. Much of this is caused through a lack of nationally, or internationally, accepted standards for such management and monitoring.

Not only can we not manage these devices, but we also cannot gain meaningful insight into what they are seeing and doing for us. Therefore, we have no way to extrapolate the true state of security within our systems at any given time.

Because we do not have the ability to manage a heterogeneous security environment, it is also currently impossible for us to automate policy enforcement/implementation. We are driven to make technological decisions with regard to managing security rather than making business decisions supported by the technology.

A real concern that we have today is that most information security solutions are getting very complicated, and complicated solutions are difficult to verify and maintain securely. As we get operating systems with 50 or 100 million lines of source code – developed all over the world – we must start looking at ways to build security solutions upon a more rigorous and mathematical basis.

Most technologies for securing information systems today are based on the premise that a given enterprise has a well-defined and defendable perimeter. This premise becomes less and less true each day making the paradigm for securing enterprises less and less applicable every day. Consider all of the ways we obfuscate the perimeter of networks today. We create extranets. We add virtual private networks (who have access through our firewalls). We allow remote access via telephone systems – often we have remote access via telephone systems even when we do not allow it. We open gaping holes in

our firewalls to accommodate new things all time: streaming video, voice over ip, e-commerce traffic, etc. Therefore, we advocate shrinking the security perimeter to a size that is more manageable – perhaps even to the single client or host level.

Yet another issue for *The Bad* elements surrounding information security is that virtually ALL solutions are focused exclusively on the TCP/IP protocol suite. The world is much, much more complex than just TCP/IP today. First, consider telecommunications networks and their protocols like Signaling System 7 (SS7) or SS5. Toll fraud in North America alone runs in the $4 billion per year range. That is hacking (ok, technically it is phreaking, but the result is the same – someone is talking a computer into giving them something they are not entitled to have). What about the ATM protocol? It is beginning to appear in network architectures going all the way to the desktop, and users are building applications such that the TCP/IP protocol suite will run over ATM. Then consider other systems that perform Supervisory Control and Data Acquisition (SCADA). These systems are used to manage petroleum refineries, building environmental controls, power distribution networks, manufacturing plants, etc. Many of the systems are highly distributed and weakly protected – largely because there are no technologies for protecting them.

Our final issue in this topic area relates to our legal system. It is fundamentally unequipped to deal with the issues surrounding cyber security. The law enforcement people, the prosecutors, the judges and the law are all ignorant to the subject area. As one example, when the FBI is tracking cyber criminals they cannot legally perform a trace route. Now, a trace route is a simple program that merely provides the user the addresses of each router between the user and some other node in the network. It is very helpful (and legal) for use in debugging network problems. However, it would also help the FBI quickly trace a hacker's path from home to the target. Somehow, a law enforcement person running trace route is actually performing an illegal search (for information) and seizure upon all of those routers in the path. So, to be legal, the agent must go to the first router and ask about the identity of the next router. Then he must go to court and get a search warrant for the next router. With the warrant, he must go to the router and ask about the next. And so on. This is the equivalent of having a police officer chasing an armed robber to call in and ask permission to cross the street before leaving his block. And then to call back at every turn or street crossing.

The Good

The best news on the information security front is that we have all the basic building blocks needed to provide high levels of security. Yes, we need to perform a lot of integration work, and we need to port some ideas to new domains, but the concepts remain the same.

Another piece of good news is that most of security is not technology-driven, but policy-driven. If we could just get businesses to define their own rules for handling information properly and then to train their people in the application of those standards, we could significantly improve the security without writing one line of code. Today, however, we have many very talented technical people writing code and creating the rules. Imagine the chaos that would occur if the business community approached the development of financial controls in accounting systems with the same level of disinterest.

One issue that has always been a problem when discussing computer security is the overhead that it takes to monitor the many factors and events. The news is improving on that front. We now have within our grasp the CPU power needed to encrypt everything everywhere s well as to support advanced levels of host-based security.

The Not So Sure

We are not yet sure about a number of movements within the information security community. First among those is the development of new Internet protocol standards such as IPv6. While it is true that these new protocols will have many new capabilities focused on security, there will be a long transition period where some compatibility between the protocols will be necessary. Certainly, this compatibility will create hacking opportunities. In addition, even if the newer versions of IP provide security enhancements, will the rollout into the network occur uniformly enough to promise truly enhanced security across the enterprise?

Next, we have been considering the long accepted premise that the entire security posture of the market will improve once all of the native network systems and their operating systems have high levels of security built directly into them versus having that capability added afterward. Our concern is that building complex security controls directly into the operating systems results in much added complexity – for the design, the development, the testing, the deployment and especially for the maintenance of the system. Might it not be better to create an external layer that would provide better protection in a more focused manner?

There are high levels of funding being discussed for information security initiatives throughout the federal government. As a company in this marketplace, we are very interested in the accuracy of the many projections for the real size of the security market. As technologists who care about improving our overall security posture, we look forward to increased levels of research and development funding as an opportunity to advance the state of the art. However, our experience has been that many dollars have been budgeted only to be pulled back for use on other initiatives with more temporal importance (Y2K, Bosnia, etc.). We sincerely hope that this latest

spate of highly publicized Internet attacks brings the proper attention and dollars into the market.

Trends

The Federal Government Cares

While it is true the Department of Defense and the national intelligence community have long been concerned with information security, their initiatives have not steeped other parts of the Government with similar concerns. Consequently, most civilian agencies have not budgeted for nor spent much money on this issue, and administrations over the years have not emphasized information security or assurance. This all began to change in 1996 with the creation of the President's Commission on Critical Infrastructure Protection (PCCIP). This commission was really focused on issues related to protecting critical infrastructures like energy, transportation and finance, but they continued to run into one consistent theme – network and information security.

One of their findings is very relevant to this discussion because it relates to research and development funding. The PCCIP estimated that the country as a whole would need to invest some $7 billion in research and development between the years 2000 and 2010 just to develop the technologies needed to protect the systems supporting our critical infrastructures. Note that the commissions estimates were not directed at defending the interconnection of these infrastructures nor their interdependencies. We estimate that developing the technologies to secure the interconnections/interdependencies will require an order of magnitude in additional investment (yes, $70 billion).

Other interesting activities have resulted from the work the PCCIP performed. The National Infrastructure Protection Center (the NIPC, under the FBI) was announced in February 1998 with a target funding of $64 million and a proposed staff of approximately 125 planned. In Presidential Decision Directive 63, President Clinton identified the mission for the NIPC as follows:

> *The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means for facilitating and coordinating the Federal Government's resources to an incident, mitigating attack.*

The news is even better as we look over the President's FY 2001 Budget. It contains $2 billion for critical infrastructure protection, much of which is dedicated to network and information security technology. Of that $2 billion, around $500 million is earmarked for applied research initiatives. Other monies are identified for such uses as the creation of computer intrusion networks for civilian agencies (the now infamous FIDNet), the creation of

private information sharing and analysis centers (or ISAC's), and the creation of "cybercorps"—a CERT-like Federal activity.

As a note of caution to the euphoria the security community may be feeling at this moment, this is definitely not *all* new money (only around $300 million of it is new)! Most, in fact, is money that was already budgeted in small bits and pieces across a spectrum of programs and projects. We are still not sure how much new money will result from these initiatives, but we do forecast with a cautious eye.

Commerce	$89 million	Security
Commerce	$48 million	Institute for Information Infrastructure Protection
GSA	$12 million	Office of Information Security
Justice	$4 million	PKI
NSA	$290 million	Security
NSF	$6.2 million	Federal Cyber Services Scholarships
NSF	$33 million	Security Research
NSF	$11.2 million	Security
OPM	$10.7 million	Federal Cyber Services Initiative
Treasury	$4 million	Security R&D in banking & Finance
Treasury	$7 million	Six federal PKI projects
USDA	$6.6 million	Agencywide cyber security

Where is the money in the President's 2001 budget for security going?

Vanishing Perimeters

The second trend we mention is that of the vanishing perimeter. By this we mean that it is getting harder and harder to truly define the perimeter of an enterprise's networks. Due to business requirements we make the perimeter fuzzy or unrecognizable through the installation of virtual private networks, the connection of client & supplier extranets, the granting of clients access into the system, uncontrolled dial-ups, extended intranets (such as via dial-up from homes with private networks and high-speed permanent network presences), etc. Where does the enterprise network stop and some other network, or the real Internet, begin?

Consider the following issues as you consider how definable or secure your perimeter really is:

- How many holes are punched in your firewall?
- How many modems exist behind your firewall?
- Are the vendors in your extranet as secure as you are? Will you be held liable if your vendor is hacked by someone coming through your network?
- Does your web site access data behind your firewall?
- Does it modify data back there?

The crux of the question is: considering that network perimeters are going away, how do we now provide protection to the enterprise? We contend that one viable approach is to shrink the domain of the perimeter. Rather than having a firewall protecting a network of thousands of computers, re-architect the network so a firewall can protect dozens of computers with enhanced and specially configured systems protecting the most crucial servers. Reducing the size of the perimeter makes the perimeter more definable and it makes the configuration and technology solution much simpler. Simple is safe – at least safer.

We also believe that we should reconsider how we will control configurations in the security environment. As was discussed earlier, we must be able to push policy out to our security enterprise rather than being a slave to the technology implementing that policy.

Ubiquitous Encryption

The final trend we discuss is the trend toward more and more encryption. It is now possible to encrypt all data on your hard drive and all of your network traffic. The applications and the throughput are there to handle this level of encryption today.

Additionally, more and more network traffic is being encrypted. Consider the proliferation of SSL-enabled web sites and SSL-driven e-commerce applications just in the past 18 months. Add to this traffic the explosion of the virtual private networking market of late. Infonetics projects that the VPN market in 2001 will reach $10.6 billion for services and $1.2 billion for products.

Further, in the total PKI market space, there has been a 20% growth per *quarter* in the number of security certificates issued since 1996. We feel this market is reaching critical mass and will soon become a de facto standard. The Department of Defense is preparing to base all of its network communications on PKI in the coming years.

Now that we have demonstrated something of a trend toward vast amounts of encrypted traffic in the Internet, why does it matter? Consider that the entire Internet founded upon open (unencoded) text-based communications. Almost all tools for analyzing network traffic and fixing problems rely on this, so the level of effort needed for administration and maintenance will be increased tremendously. This will also cause an additional factor of consideration for all design and development activity (applications, networks, systems, operating systems, protocols, etc.). Finally, most of the intrusion detection systems on the market today rely on the unencoded contents of the network traffic to detect attacks. If this traffic is encrypted, the intrusion detection system can not properly analyze the traffic without also having the keys used for the encryption. Providing all of your encryption keys to one host on the network creates an entirely new vulnerability.

Killer Applications

> *Nothing great was ever achieved without enthusiasm.*
> *– Ralph Waldo Emerson*

This section entitled *Killer Applications* is intended to impart two different applications that most would not consider security applications, but that are impossible without the trust that only security can provide. Our contention is that the developer and provider of these two solutions will walk away quite wealthy as well. Do you or does your company have the enthusiasm necessary to bring these applications to the marketplace?

Mobile Network Credentials/Capabilities

We have already discussed the idea that network users need trusted, mobile credentials in the network. Applications and operating systems must be able to develop a level of trust with a user based on those credentials, and the credentials should establish the users' expectations of the networks and systems.

We contend that network access is becoming (and should become) a service, and we need to allow service industries (hotels, airlines, telephone companies) an opportunity to provide network services at levels they cannot today. Without trusted and mobile network credentials, this just is not possible. Now, consider that virtually every traveling businessperson is tied to 15-20 pounds of equipment that they use to give themselves the network access, credentials and applications needed to do business on the road.

We want to <u>not</u> carry our laptops, but to be able to office in every hotel, airport, airplane, client, satellite location – and even automobile – we stop in. In order to provide this service, we need some underlying technologies.

- First, we need mobile network credentials that let us appear on our office LAN's while sitting 1000 miles away.
- Next, we need a diskless workstation wherever we may be with reasonably high-speed connectivity into the Internet.
- Finally, we must have network enabled applications. We can't have hotels and airlines guessing at what applications we will want to run, so we need applications that are smart enough to download only small parts of themselves as needed for what we are doing. While we are dreaming, we need this service to be very inexpensive, if not 'free' as a service to us.

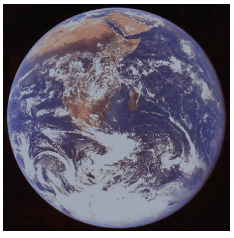
This application exists today albeit in a different domain – the cellular telephone industry. There are cellular telephones (and we are not talking about the new satellite telephones) now that you can purchase and use virtually worldwide. There is an identity built into the telephone on a small plug-in module (or smart card equivalent) that knows who you are and how to get billing information back to you. It knows what kinds of encryption you use and the quality of your credit with your telephone company. They have essentially solved this problem for us.

Now, once we have the application, let us consider what we might be able to do with it by imagining a businesswoman on a trip. She would arrive at her hotel and check in – sans laptop of course. She goes to her room and locates the network computer on the desk. She inserts her smart card identification into the reader and the system determines her identity and network configuration requirements. It then automatically creates a virtual presence for her on her home network handling all of the logons and encryption key sessions transparently. The hotel server would merely get a log of what company she had been connected with, for how long she was connected, and how much traffic she generated for billing purposes.

Now she starts to work. She can do the routine things like word processing, but let's think further out of the box than that. If her company is wise, they have installed the capability for her to have all of her phone calls routed from her office phone over the network to her virtual office in that hotel room. She can do conference calls, check her voice mail, change her message, dial local extensions, and put people on hold – all over the network. No one would know she was not in her office unless she told him or her. She could also do collaborative things with her team back home like jointly modify next week's presentation or work out a concept on a virtual white board.

Most of this stuff exists today – all we need is the network security framework to enable the extension of these capabilities beyond the crumbling perimeters or our enterprise networks.

Enterprise Management of Security Domain



We discussed earlier the tremendous need for the ability to view the state of security in our enterprise information systems and then to manage our security infrastructure at the enterprise level. This tool must be capable of managing a heterogeneous security environment, communicating the security state of the enterprise, projecting the future state after a few more potential moves by an attacker or mere network events, and proactively responding to situations.

This tool will allow us to know when bad things start happening, especially those things that appear to be related to a security incident. It will give our analysts the ability to perform what-if analyses to project just how bad a

situation could get and how the system and the hacker might react to various responses under consideration. It would also give our analysts the opportunity to install patches and configuration changes proactively and automatically in response to events or warnings from vendors.

Finally, this tool will allow us to manage the security enterprise as a function of the policy we set—not as a function of the technologies we choose.

This tool will break some rather new ground in three areas. First, it will allow my team to look at much more of my information infrastructure than just the part running over TCP/IP. We will be able to look into our telecommunications network, into our SCADA systems, into our facilities control systems, and even into our physical security systems. All of these various points of data will allow us tremendous insight into the information infrastructure. With this insight, we will be able to provide better management of the infrastructure as a whole. We will know how often fax machines are being used (should we keep paying for that dedicated telephone line?) and how often our users really use the video teleconferencing capabilities we have provided (should we expand or contract the capability?). We can then implement policy or technological changes and measure the change in the performance of the entire information infrastructure.

Finally, this tool will probably also need to consider breaking the geography paradigm — so many tools today base their view of networks and information systems upon the concept of links and nodes plotted upon maps of the world or of the United States. We feel we must break with this practice. "Near" does not carry the same connotation in a network that it does in the physical realm. Therefore, this tool may use virtual reality or three-dimensional techniques to allow us to envision and interact with network elements in completely different ways than we do today.

What do we really need?

> *I tell you naught for your comfort,*
> *Yea naught for your desire…* *-- G. K. Chesterton*

Re-Focus on Protecting the MISSION

Our first need in the information security technology community is to re-focus our objective. We have really focused in the past five years or so upon protecting the networks that enterprises use when what is important is not the network but the mission that the network, in part, enables. The legal office's computers probably contain far more sensitive information (from intellectual property to negotiation strategies) than the mail clerk's, yet today we largely

protect them both in the same manner. This re-focusing may require us to rethink fundamentally how we build networks and information systems from the ground up. Admittedly, doing so is hard, but if we begin to think in this manner, we will dramatically simplify the security solutions that we must implement.

System Security State

We have already discussed a bit about the need to gain visibility into the state of security within our enterprise. This starts with defining a baseline state – how else can you know if you are in trouble if you do not know where you started? Next we need tools to allow us to correlate events – not just pure security events but all kinds of anomalous and seemingly innocuous events – over a wide ranges of information sources and time horizons (near real time and long term). This will require the incorporation of expert systems, data mining, and data fusion technologies. Lastly, we need the ability to communicate this state and the changes to the state in meaningful ways to the analysts and company leadership who will depend upon *understanding* what is happening.

Enterprise-level Solutions

We have also discussed the need for solutions that span our enterprise. These tools allow us to manage a heterogeneous group of tools and technologies that help determine and improve the state of security in the enterprise.

Secure (or Securable) Underlying Technologies

We certainly need to improve the security – or more appropriately the securability – of the enterprise's underlying technologies. We need security features in protocols, better security options in operating systems, secure messaging capabilities, enhanced security in routers, etc.

Policies and Laws

As was also discussed earlier in this document, we need to make significant improvement in our legal infrastructure to foster better information security. This includes laws and treaties that allow law enforcement to respond to information attacks in real time across the world. It could also mean some form of regulation to standardize and impose some minimum level of mandatory detection, reporting, and investigation of events.

Beyond laws, it means developing a technology savvy judicial system – basically a subset of prosecutors and judges who really understand the business and technological implications of information security (and the lack thereof) as well as hacking and prudent system administration.

Appendix A - Other Resources

Web Site/Name	Description
www.ciao.com	Critical Infrastructure Assurance Office home page
www.ciao.gov/research.html#roadmap	Research roadmap from the PCCIP
www.pccip.gov	President's Commission on Critical Infrastructure Protection home page
http://csel.cs.colorado.edu/~ife/l14/EligibleReceiver.html	Article relating the story of the Eligible Receiver Exercise
Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare	Booklet from the Computer Security Institute
www.gocsi.com	Computer Security Institute home page
cm.bell-labs.com/cm/cs/who/ches/map/index.html	Internet mapping project at Bell Labs
www.securityfocus.com	technical and newsworthy security information

Appendix B -- About the Author

Dr. John Steven Reel

Dr. Reel has BS and Ph.D. degrees in Computer Science. He spent 9 years with the National Security Agency developing network-based software for deployment around the world. In 1995, he came to work for Trident Data Systems (now Veridian-Trident Data Systems) in their San Antonio operation. For 3.5 years, he worked in an advanced research and development facility dedicated to information security technology development and assessment. Since September 1998, he has been the Chief Technology Officer of Veridian-Trident. In 1998 he and five teammates were awarded a patent on a new technology to protect communications circuits from malicious use. In addition to his dissertation, *Radiant Object-Oriented Analysis and Design,* he has had one article published by IEEE Software Magazine (*Critical Success Factors in Software Projects*, May/June 1999). Further, he has given numerous talks and authored many white papers on IA/IO/IW/IP/IS concepts and technologies.

Dr. Reel serves on the External Advisory Board for the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. In addition, he serves as an advisor to the Security Panel of the President's Committee of Advisors on Science and Technology (PCAST).