

# THREAT AND VULNERABILITY MODEL FOR INFORMATION SECURITY

Report to the  
President's Commission  
on Critical Infrastructure Protection  
1997



This report was submitted to the President's Commission on Critical Infrastructure Protection, and informed its deliberations and recommendations. This report represents the opinions and conclusions solely of its developers.

---

---

# Contents

---

---

	Page
<b>Acknowledgments</b> .....	<b>iii</b>
<b>Part One: Introduction</b> .....	<b>1</b>
<b>Part Two: Adversary Model</b> .....	<b>3</b>
<b>Part Three: Vulnerability Landscape</b> .....	<b>4</b>
<b>Section One: Attack Process</b> .....	<b>4</b>
<b>Section Two: Security and Residual Vulnerabilities in     The Physical World</b> .....	<b>5</b>
<b>Section Three: Security and Residual Vulnerabilities in     The Virtual World</b> .....	<b>6</b>
<b>Section Four: A Rational Response to the Vulnerability     Landscape</b> .....	<b>8</b>
<b>Section Five: Security as a Product</b> .....	<b>11</b>
<b>Part Four: Future Trends</b> .....	<b>12</b>
<b>Appendices</b>	
<b>Appendix A: Detailed Adversary Model</b> .....	<b>A-1</b>
<b>Appendix B: Detailed Vulnerability Review – Availability</b> .....	<b>B-1</b>
<b>Appendix C: Detailed Vulnerability Review – Authenticity</b> .....	<b>C-1</b>
<b>Appendix D: Detailed Vulnerability Review – Integrity</b> .....	<b>D-1</b>
<b>Appendix E: Detailed Vulnerability Review – Privacy</b> .....	<b>E-1</b>
<b>Appendix F: Detailed Vulnerability Review – Life Cycle</b> .....	<b>F-1</b>
<b>Appendix G: Glossary</b> .....	<b>G-1</b>

---

---

# Acknowledgments

---

---

The Commission thanks the following individuals from the Department of Defense for their participation in the preparation of this report, their insights and their assistance in assuring its completeness: Alexander A. Abler, Richard M. George, Terry W. Oxford, Jerome P. Roddy, Christopher M. Salter, Omar S. Saydjari, Donald N. Simard, Jay W. Turner, James Wallner and Neal I. Ziring.

The Commission also gratefully acknowledges the leadership provided by Commissioner Joseph J. Moorcones and the insights and perspective provided by Commissioner Nancy J. Wong.

# Part One

---

---

## Introduction

---

---

This report describes a threat and vulnerability model, based on the investment decisions an adversary makes in attacking systems. It illustrates what new risks have been created for our critical infrastructures as a consequence of their increased reliance on network technology. This report outlines several future trends which the government could consider as it decides the appropriate steps to guard against future catastrophes. The report concludes with several appendices which examine some of the issues and concepts in more detail.

What new risks have been created for our critical infrastructures such as electrical power systems, telecommunications, and banking and finance, as a consequence of their increased reliance on network technology for their operation? In his testimony to Congress, former Director of Central Intelligence John Deutch expressed his fear that an adversary of our nation will use cyber attacks to “seriously jeopardize our national and economic security” since, in the words of the President’s Commission on Critical Infrastructure Protection, “...the dependency on the flow of information has created new vulnerabilities that present risk not previously considered.”

Studies show that application of technologies will place our infrastructures at greater risk if no actions are taken to secure them. The near term threat is that networks have enabled consolidations in these critical infrastructures which have put these infrastructures in the path of greater physical harm. Centralization of the nervous systems of these infrastructures has also widened the damage that a terrorist or natural disaster can inflict.

The real risk, however, is to our economic future and national security. We all live in a safer, efficient and more enriched world by virtue of wider bands of communication and increased interdependence brought about by common, international networks. However, consequences of inadequate security in this new age can undermine public confidence, thus impeding the Information Age from reaching its full economic and social potential.

In any analysis, the goal is to not exaggerate the dangers, but to take rational precautions commensurate with the level of risk.

The following sections form a basis for a rational investment strategy to address the threats in the near and long term. First a model is derived for how adversaries operate based on their capabilities and risk tolerance. Next, the process is outlined for how adversaries successfully

attack a target. A vulnerability model for the expanded world of networks is built upon the well understood model for the physical world. An underlying theme is that improved security requires a balanced investment across many dimensions. An investment to fix one problem may not make sense given other vulnerabilities in a system. Investment decisions for countermeasures are based on the investment decisions adversaries might make.

It should also be noted what is meant by the words “adversary” and “attack” in the context of this paper. An adversary is an individual or entity who wishes to cause some sort of economic, political, military or other harm for a variety of motivations. An attack is the actual event which inflicts the harm.

The appendices include a detailed adversary model description and the implications of technology trends for assessing risk. The reason for this projection is that the effectiveness of the adversaries changes as the landscape changes. Some adversaries become more significant while others may have to work harder to retain the same level of threat.

*Over time, misuse of information technology will have the power to do greater harm.  
Start now to cultivate needed security.*

# Part Two

---

---

## Adversary Model

---

---

The Adversary Model characterizes adversaries in terms of their associated objectives and their levels of available resources and risk tolerance. Appendix A describes this model in greater detail.

*Resources and access determine what adversaries **can** do; risk tolerance and objectives determine what they are **willing** to do.*

An adversary, when choosing to attack, has budget constraints consisting of money, expertise, access, manpower, time, and risk, and expects to find some return on his investment which in some way benefits the adversary. Some attacks require a great deal of access but not much expertise, like a car bomb, while other attacks require a great deal of computational power, but no access, like breaking an encryption algorithm. So each adversary, who may have different types of resources, must choose from a set of attacks which are affordable to him. Given the set of all affordable attacks, a rational adversary will, therefore, choose the attack which maximizes his return on investment. That is, the adversary wishes to minimize his cost in terms of money and risk, and maximize his benefits.

*An adversary follows the path of least resistance.*

<b>Adversary</b>	<b>Resources</b>	<b>Risk Tolerance</b>
Insider	High	High
Info Warrior	High	High
National Intelligence	High	Med
Terrorist	Med	High
Organized Crime	Med	Med
Industrial Espionage	Med	Low
Hacker	Low	Low

A well-funded adversary can trade money for access by paying off an insider, can trade money for expertise by buying technology, and can trade money for risk by executing a more sophisticated attack.

## Part Three

---

---

# Vulnerability Landscape

---

---

The vulnerability landscape is made up of a series of peaks and valleys. The valleys represent the adversaries' opportunities for attack. These opportunities for attack are called vulnerabilities. The adversary may attack in the physical world: breaking and entering, bombing strategic targets, taking human life, etc. Today the adversary may also attack in the virtual world. Attacks against the physical infrastructure in the virtual world can be conducted instantaneously and remotely, without warning. Protection must be provided for vulnerabilities in both worlds in equal measure.

---

## Attack Process

---

Adversaries follow these four steps for every successful attack:

- 1. Identify the specific target which will be attacked. Identify the specifics of the attack which will accomplish the desired objectives.**
- 2. Gain access at the appropriate level to the target.**
- 3. Alter the target in some intended way, which may include erasing the evidence of the attack.**
- 4. Complete the attack.**

In order to protect against attack from one's adversary, the intended victim needs to prevent the adversary from successfully completing only one of these steps. The goal for the security designer is to find the most cost-effective method.

# Security and Residual Vulnerabilities in the Physical World

## Physical Security

Physical security speaks to the problem the world has been trying to solve since there has been a notion of ownership. Fences, locks, guards, and identification badges are all tools of physical security. Today's organizations know how to take security measures commensurate with the physical threat; they know their adversaries and what countermeasures are sufficient to protect their assets.

The security mechanisms are layered to produce a solution. Behind the fence, guards patrol the perimeter of a locked building. The five dollar locks on the doors might be sufficient given the guard and fence. Remembering that the adversary often takes the path of least resistance, an intruder, if he encounters a locked door, will break through a glass window. Therefore, a ten dollar lock might be wasteful given access to the window.

*Second Axiom of Security: Layered security solutions reinforce each other so that the sum is greater than its parts.*

*Corollary: Each layer is only as strong as its weakest point*

<b>Protection Level</b>	<b>Protection Measures</b>	<b>Residual Vulnerabilities</b>
Vulnerable	Nothing	Thieves and vandals have unrestricted access to physical assets.
Due Care	Fences, locks, and alarms	Response time to a break-in is slow.
Best Practice	Guards	Insider or highly sophisticated thieves can get by guards.

## The Trust Model in the Physical World

The trust model is how an organization determines whom to trust with its assets. For instance, those who are to be employed by the institution might have their applications verified, their references interviewed, and their criminal record checked. Once employed, picture identification might be issued. In the physical world, it is easy to identify those individuals who are trusted, and those who are not.

<b>TABLE II-2. Trust Model in the Physical World</b>		
<b>Protection Level</b>	<b>Protection Measures</b>	<b>Residual Vulnerabilities</b>
Vulnerable	Nothing	Untrusted outsiders have unrestricted access.
Due Care	Car stickers, badges, uniforms (recognition)	Forged credentials are trivial.
Best Practice	Enhanced credentials, electronic badges	The insider remains a real threat. Also, more sophisticated adversaries can forge credentials and impersonate legitimate employees.

### **The Life-Cycle of Physical Assets**

A company engaging in industrial espionage might choose to bug the telephones or copiers destined for his competitor's offices. The adversary must choose when and where to conduct this attack. The office equipment is vulnerable during its entire life-cycle: on the drawing board, in the plant, at the loading dock, in the workplace, or even after disposal. Depending on the access afforded to him, the adversary may choose to alter or swap the equipment during production, shipment, installation, normal operations, or maintenance.

<b>TABLE II-3. Life-Cycle of Physical Assets</b>		
<b>Protection Level</b>	<b>Protection Measures</b>	<b>Residual Vulnerabilities</b>
Vulnerable	Nothing	Equipment can be altered or swapped by anyone.
Due Care	Buy equipment from a reputable dealer.	Equipment can be altered or swapped during operation or maintenance.
Best Practice	Inspect the equipment periodically and service equipment at a reputable repair shop.	Adversary needs to operate or have access to a front organization that looks reputable to his target.

## **Security and Residual Vulnerabilities in the Virtual World**

The virtual world is the world of networked computers, where work and commerce are conducted electronically. The virtual world includes wide area networks, like the Internet, where the communications backbone may be publicly owned and operated, and it includes local

networks where all of the information resources are privately owned and operated. The trend is for these separate networks to interconnect since duplication and redundancy are too expensive.

*“To a first order approximation, all computers are networked together.”*  
R. Morris

## Virtual Security

---

As the world increases its reliance on electronic commerce, more adversaries will be enticed to exploit networks. From anywhere in the world, the adversary can eavesdrop on electronic conversations or break into private networks and steal documents without fear of immediate apprehension.

<b>TABLE II-4. Virtual Security</b>		
<b>Protection Level</b>	<b>Protection Measures</b>	<b>Residual Vulnerabilities</b>
Vulnerable	Nothing	Adversary has unrestricted access to electronic information at large and within the LAN.
Due Care	Network firewalls, virus scanning, link encryption	Adversary can use e-mail and the web-browser to infiltrate. Adversary remains anonymous.
Best Practice	Security infrastructure with end user software encryption.	Insider still has access. A sophisticated adversary needs to hack his way through the firewall and break two layers of encryption.

Without any network security, data is at perpetual risk, in transit and at rest. Constructing a firewall is analogous to building walls and installing locks on doors. Encrypting messages creates the secure corridors for a conversation between two parties and a safe for stored data.

### The Virtual Trust Model

The problem for the virtual world is how to extend the same level of trust in individuals from the physical world to the virtual world without the physical presence of the individual to draw upon. For example, in the physical world, an adversary who wishes to masquerade as a trusted member of a community takes the personal risk of being apprehended. In the virtual world, a spy can come across the border and impersonate as a trusted member of the organization without physical risk because he never has to leave “home.”

*“Information warfare offers a veil of anonymity to potential attackers.”*  
Defense Science Board

<b>TABLE II-5. The Virtual Trust Model</b>		
<b>Protection Level</b>	<b>Protection Measures</b>	<b>Residual Vulnerabilities</b>
Vulnerable	Nothing	Adversary has unrestricted access in the virtual world.
Due Care	User accounts with passwords, and audit	Adversary can sniff or guess passwords and masquerade.
Best Practice	Identity certificates issues by a trusted authority.	The insider remains the biggest threat. Adversary can steal identity secrets or forge ID certificates.

### **The Life-Cycle of Software**

Software running on a network of computers is becoming the work environment of the virtual world. It is, therefore, important to maintain the integrity of accredited software during its life-cycle. The software developer could inadvertently leave a back door in the latest release of the operating system. An adversary could put a Trojan Horse in a popular net browser and distribute for free over the Internet. An adversary could write a virus which attacks the accounting software and deliver it as an executable attachment to an e-mail message.

<b>TABLE II-6. The Life-Cycle of Virtual Assets</b>		
<b>Protection Level</b>	<b>Protection Measures</b>	<b>Residual Vulnerabilities</b>
Vulnerable	Nothing	Software can be altered or swapped by anyone during distribution or operation.
Due Care	Buy shrink-wrapped, accredited software from a reputable source, and use a robust operating system	Software or data can be altered remotely by a virus in the executable attachment of an e-mail or web site.
Best Practice	Digitally signed accredited software.	Adversary needs to alter the application software, plus the security software which verifies the signature.

## **A Rational Response to the Vulnerability Landscape**

The vulnerability landscape is broad, and protective countermeasures must be applied evenly across the landscape to prevent those adversaries which present the greatest threat from attacking successfully. Keeping in mind that blocking one of the steps necessary for a successful attack is

sufficient to deter an adversary, the security designer should make rational investment decisions when applying countermeasures. That is, it doesn't make sense to spend more money improving the locks on the front door when the adversary is apt to break through the glass window. It also doesn't make sense to spend \$100 on protective countermeasures to protect \$10 worth of assets. Simple countermeasures, education, policy and procedures are rational, cost-effective means of mitigating the risks posed by the vulnerability landscape. These simple steps can significantly raise the risk and sophistication needed by the adversary to conduct a successful attack.

The following chart summarizes the vulnerability landscape, the rational countermeasures associated with each residual vulnerability, and the level of resources, risk, and access needed by an adversary to exploit the vulnerability.

<b>TABLE II-7. Vulnerability Landscape</b>				
	<b>Protective Countermeasure</b>	<b>Residual Vulnerability</b>	<b>Cost of Attack</b>	
			<b>Resource</b>	<b>Risk</b>
Physical Security	Nothing	Thieves and vandals have unrestricted physical access	Low	Low
	Locks, fences and alarms	Slow response time to physical break-ins	Low	Med
	Guards	Insiders are still a threat, as well as sophisticated thieves	Med	High
Physical Trust Model	Nothing	Untrusted outsiders have unrestricted access	Low	Low
	Picture badges, uniforms	Forging credentials is trivial	Med	Med
	Electronic badges	Insiders are still a threat as well as sophisticated forgery	High	Med
Product Life Cycle	Nothing	Anyone can alter equipment anytime, anywhere	Med	Low
	Reputable source	Equipment can be altered during operations or maintenance	Med	Med
	Inspection and reputable service	Adversary needs to operate a front organization	High	Med

Virtual Security	Nothing	Adversary has unrestricted access to electronic information	Low	Low
	Firewalls and virus scanning	Adversary can attack anonymously through e-mail or web-browsing	Low	Low
	Security infrastructure with encryption	Insiders are still a threat as well as the sophisticated adversary hacking past the firewall or breaking encryption	High	Med
Virtual Trust Model	Nothing	Adversary has unrestricted access in the virtual world	Low	Low
	User accounts with passwords and audit	Adversary can sniff or steal passwords and masquerade	Low	Med
	Identification certificates	Insiders are still a threat, as well as a sophisticated adversary forging certificates	High	Med
Software Life Cycle	Nothing	Anyone can alter software anytime	Low	Low
	Shrink-wrapped, accredited software and a robust operating system.	Data can be altered by a virus from e-mail or web-browsing	Low	Med
	Digitally signed accredited software	Adversary must alter both application and verifying software	Med	Med

## Analysis

---

Risk is higher to the adversary in the physical world than in the virtual world because it is harder to detect and apprehend the criminal in the virtual world.

*“Never underestimate the amount of money, time, and effort someone will expend to thwart a security system.”*

Bruce Schneier

By applying due care in each of these categories, the attacks get technically harder and more risky. Inexpensive, simple countermeasures sufficiently raise the bar by eliminating opportunities for adversaries to conduct some of the attacks.

By applying best practice in each of the categories, most adversaries are eliminated from most attacks. However, it is impossible to eliminate either the insider or the Info Warrior from successfully conducting any attack of his choosing. Those adversaries will simply choose the least costly, and least risky attacks which accomplish their objectives.

Notice that the best practice for countermeasures in the virtual world is not achievable with current technology.

## **Security as a Product**

For a security technology to be successful it must have the attributes of any successful technology. In this case, the attributes are:

- cost
- ease of use
- compatibility
- amount of overhead
- security

If a security product costs too much, if it's too hard to use, can't be used to send messages to a partner or customer, or causes performance of a system to degrade, then it will not be used and no security will be achieved. What is worse, products will be bought that meet the first four criteria but that provide poor security.

A measure must be found for security that allows market forces to drive improvement. Market forces act best when there is agreement on standards. For instance, cryptographic standards create a larger market for interoperable security products. Current efforts on influencing standards are splintered and not a priority of most government organizations. Government must participate in key standards bodies with the uncompromising goal of making that standard the best possible given any unique knowledge the government has acquired through its operational experience and its R&D investments.

# Part Four

---

---

## Future Trends

---

---

### Overview

---

We can divide future trends into three general areas: direct technology changes, business sector changes, and social changes. Each helps to drive the other. Many of the technologies that will drive business and social change over the coming decade are already on the market, or emerging from industry and university labs. Some of the changes driven by these technologies will make our critical infrastructures more vulnerable, while others will give us greater ability to protect them.

Given the current, accelerating pace of change, predictions of technical and business evolution even three years in the future are suspect. Only by regularly revisiting projections of relevant trends can we hope to identify new or shifting risks to our critical infrastructures.

Recent efforts by the Administration to relax export controls, create an international market for cryptography, and foster key management infrastructure are all part of a sound investment strategy. Additional steps can be taken to build public confidence in the rapidly changing information technologies. For it is in the acceptance of these technologies that the United States will find its future economic success and its national security in the Information Age.

There are some obvious movements in our technology, business culture, and social fabric that have implications for the protection of critical infrastructure and competitiveness. This section explores a few such trends.

In general, American society is still on the uphill curve of the third wave addressed in a well-known economic model. Information and communications technology will continue to proliferate, gain ubiquity, encourage new business models, and subtly affect personal and social roles.

*First Wave: Agriculture*  
*Second Wave: Industry*  
*Third Wave: Information*

Alvin Toffler

## Direct Technology Trends

---

Introduction of new technologies, their refinement, and new applications of existing technologies, create a nearly impenetrable turbulence around current business and personal life. It is very difficult to separate important long-term movements from momentary fashions. The list below attempts to identify technical trends that will have long-term impact.

- Telecommunications services will continue to diversify.

The number of companies providing communication service of all kinds to consumers and businesses is rising rapidly. Formerly quite distinct, various communications service sectors now exhibit substantial overlap. In the next 5-10 years, we can expect to see evolution of new types of communication service, as well as an increase in the ability of existing providers to offer broader ranges of service.

There are two primary implications for national infrastructure. First, diversity of telecommunications structure will protect users from catastrophic disruption only if present short-term trends in overloading the existing public switched telephone network (PSTN) are reversed. Second, the trend toward offering any service over any medium will expose business and consumers to greater individual risk of focused attack, because more avenues for attack will exist. The overall effect of this trend will be to defocus our vulnerabilities, making telecommunication service providers themselves less important targets.

- Data networking will become the chief driver and foundation for all telecommunications.

Today and in the near future, data networks will increasingly host other communication services. Voice, fax, video, telemetry, and other services will be loaded onto data networks instead of using dedicated systems. Further, data communication services will increasingly be moved onto public global data network. The fabric of the global PSTN is already digital; this will be pushed outward until it reaches individual employees and consumers.

There are subtle implications for our national infrastructures in this trend. Boundaries between business sectors based on their use of different media will be blurred. For example, video entertainment service (today: CATV) and real-time voice communication service (today: phone companies) will be provided by the same companies, and competition will increase in both areas. Infrastructure providers, such as power companies and public utilities, will probably employ the public data network to transmit their monitoring and control information, instead of the current common practice of using private circuits. This migration may expose these utility companies to network-based threats that they can ignore today.

*Diversity is an effective defense against large-scale attack. Present-day practice of putting all our telecommunications eggs in one PSTN basket cannot and will not continue.*

- Wireless communication systems will become ubiquitous.

Both satellite and surface-bound wireless communications are growing rapidly, and will continue to become more widespread over the next few years. By 2010, we can expect to see most of the globe accessible to high-bandwidth space-borne links, and all populated areas in developed countries covered by multiple, competing surface systems. The present-day association of network connectivity with a physical connection will evaporate.

- Remote-sensing technology, especially satellite imaging, will become cheaper and more widely available.

Space-borne imaging is already being offered for sale to the public in several countries. This information is tremendously useful for some industries, and due to market pressures, its availability is sure to increase.

Some of our national infrastructures have vital components that are large enough to be visible from space (e.g. many water projects can be seen from orbit by even primitive imaging satellites). As imaging technology gets better, it will become a means for some adversaries to identify and study potential targets. Sectors that may become more vulnerable due to this future trend include: power, water, railroad, farming, and some facets of telecommunications.

*The government monopoly on space-borne intelligence gathering is over.*

- Mobile use of information system assets will increase.

There has been steady improvement in the technology to support mobility for information system users. Distributed computing, cellular telephony, network remote access, and telecommuting are all on the increase even today. In the coming decade, new forms of mobile information access will become important, with virtual reality intersecting with mobile computing to create “telepresence.”

The potential of widespread mobile network access to affect our critical national infrastructures is not yet clear. Certainly, it will strengthen the ability of an attacker to remain anonymous.

- Network agents will proliferate.

Technology is emerging that will support the creation and proliferation of autonomous network agents, software entities which conduct information retrieval and other business on behalf of network users. The technologies that support agents, as well as the business activities those agents conduct, have the potential to open new vulnerabilities.

To the extent that our economy depends on information, network agents will add a valuable new capability to the toolbox of workers and decision-makers. However, the computational basis needed to support this capability can open new vulnerabilities. A few years from now, as this technology begins to mature, the need for greater flexibility will strain our information security infrastructure. In order to reap the potential benefits of network agents, our security systems will need to support very flexible authorization, access control, delegation, and non-repudiation features.

- Public-Key Infrastructure (PKI) Providers will proliferate.

Public and business awareness of network security issues has been and will continue to increase. The only technology that currently offers hope for large-scale, interoperable, robust information security is public key cryptography. However, to be most useful, this technology requires a service infrastructure which supports the enrollment and management of security participants.

Companies that provide PKI services will grow rapidly over the next decade. Competition will be intense, but the availability of usable standards will prevent the market from coalescing to a single provider.

In a sense, the services of PKI providers underpin the entire security model of our future information systems. The issuance of digital credentials is a supremely serious step in a world where large financial transactions, personal business, and government activities are conducted on-line. The ultimate costs and overhead involved in providing this service are not yet clear, but only with a good, robust, secure PKI will our country be able to reap the full economic benefits of global networking.

Lastly, over the next decade, PKI service may enter more sectors of our society. If conditions are favorable, PKI may offer another path for disparate elements of our society to enter the economic mainstream. This highly desirable end can be achieved only if the costs associated with PKI can be held down.

- GPS will become the primary navigational and timing baseline for applications worldwide.

As Global Positioning System (GPS) receiver hardware continues to drop in price, use of the system will greatly increase. The ability to know your exact location on the globe is

tremendously convenient. The fact that the service is free after capital outlay makes the system even more attractive. Further, some applications employ the GPS as a timebase.

As use of GPS becomes very widespread, it becomes a very tempting target for an adversary. While the actual GPS transmitters are inaccessible, there may be a potential for denial of service, disruption, and loss of integrity via ground-based jamming or spoofing.

*GPS will become a primary mechanism for locating things in all four dimensions.*

Some trends apply directly to the promises and threats posed by these technology trends. First, network security depends on cryptography, and any factors stifling the development and adoption of good cryptographic security will stifle and delay the benefits of network security while encouraging fraud and other crime. Second, the legal framework under which PKI companies can thrive must be established. Only by providing a workable business environment for this service can we foster its growth and widespread use. Third, robust international standards are vital to the growth of wireless communication and mobile computing. Finally, government entities have performed a great deal of research in many technical areas, including PKI, remote imaging, and wireless communication. Sharing this research and technical progress with the private sector will encourage growth and might even improve the competitiveness of U.S. businesses.

In general, the technical progress we expect in the coming years will aid both attackers and defenders. The technologies for defense will need support and encouragement, because market pressure to provide new operational features is stronger than pressure to tighten security.

## **Business and Government Sector Trends**

---

The technology trends identified in the last section will have profound effects on many areas of business, industry, and government. The availability of cheap, fast physical transportation fundamentally altered business and society in the first half of this century; availability of cheap, fast information transport has the potential to similarly shape the next decade and beyond.

The most fundamental trend in all sectors is the move from supplementing business practice with information technology to *basing* the business on it. While most such businesses maintain manual, fallback procedures for use when the information technology is unavailable, such procedures will increasingly be discarded or abandoned under competitive pressure. The implication is clear: our increased reliance on information systems for basic activities makes our national economy dependent on the availability and integrity of these systems.

- Telecommunications customers will participate in administration of the media they utilize.

Service providers will increasingly allow business and individual customers to regulate and control the bandwidth they pay to use. This decentralization trend is inevitable as customer requirements diversify and competition among providers heats up.

Distributed control of the telecommunication infrastructure may open up new vulnerabilities. Opportunities for fraud, service theft, and outright denial of service may greatly expand.

- Financial services will migrate onto the Internet.

Financial services firms will increasingly allow their individual and corporate customers to interact with their accounts and initiate activities over the public data network.

Already, protocols and products marking the beginning of this trend have appeared. The coming decade will see first a fragmentation and then a consolidation within this area, with the financial services sector eventually settling on a few interoperable systems and protocols. Integrity and confidentiality will be critical to its adoption, especially given the importance of public confidence in this area.

- Medical informatics will migrate onto the Internet.

Consolidation and competitive pressures in the health care industry will force hospitals, HMOs, doctors, and even patients to employ the public data network. Today, this trend can be most clearly discerned in radiology, where medical images are quite commonly sent over the Internet instead of by physical means.

Some states have legislated medical privacy, forcing health care providers to employ encryption and other security mechanisms. This trend will continue and expand. However, integrity and authentication will also emerge as important concerns with increased deployment of medical and other personal information service on the Internet.

*“Every employee is fully committed to the principle that before any medical record goes out on the wire, it will be encrypted.”*

Kaiser-Permanente, HMO

- Judicial and law enforcement officials will depend more heavily on computer databases.

The business of tracking criminals and crime has adopted information technology (IT), and is being pushed to depend on IT by budget reductions and increasingly complex criminal procedures.

There are grave legal issues to be faced in this area. Some of these issues are: assurance of the integrity of legal records, assurance of the confidentiality of the defendants, victims, and litigants, assurance of authority for the users of these systems, and assurance of audit capabilities.

A related trend in this arena is the increase in connectivity among judicial and law enforcement systems at different government levels. Before another decade has passed, law enforcement officers of almost any jurisdiction (municipal, state, federal, special) will have real-time access to information resources for all the other jurisdictions. This may pose additional concerns for our national law enforcement infrastructure; security safeguards will certainly vary widely among different law enforcement entities.

- Information system software and hardware manufacture will become increasingly global.

Even today, most of the computer and network hardware on which we have come to depend is manufactured outside North America. International competition is a strong force, and it will affect or soon begin to affect countries where much of our IT products are made.

Lack of oversight in early phases of a product's lifecycle has very severe security implications. In general, assignation of trust based solely on the origin of hardware or software will not be possible. Other means for establishing trust will have to be devised.

A related future trend will be the emergence of "gold standard" security products and services targeted at high-value environments. These products and services will be characterized by domestic, limited-access facilities, bonded workers, high-overhead procedures, and solutions unique to particular customers' requirements. The buyers for these expensive products and services will be in the financial services, heavy industry, government, and criminal sectors.

- Large organizations will continue to centralize management of their facilities.

In every sector that engages in management of geographically distributed assets, there is a clear trend toward centralized monitoring and control. Improvements in network ubiquity and equipment prices will support this trend. This trend will affect transportation (trucking, railroads), energy (electricity, gas, oil), water, and all aspects of telecommunications.

Competitive pressures will force organizations to centralize, and also to use the least expensive medium to host the communications required. In most cases, this will mean the public network. As critical national infrastructure providers come to depend on the Internet to support their real-time management and control, the reliability of the network will become much more important.

- The Federal government can encourage the seamless integration of strong security into all commercial information technology products, through the deregulation of cryptography and information security technology. The orderly removal of export controls will give this movement a tremendous boost.

The government can encourage the development and production of strong security products to make them more readily available. Market-driven products will be more cost-effective, compatible and user-friendly than current government regulated products. Security will become “invisible” to the user. U.S. industry will likely become the leader in secure information technology.

There is the potential of loss due to national intelligence information obtained from the interception of unencrypted messages being lost. Also, law enforcement wire taps will become more costly and difficult. Government will have to carefully weigh the costs and benefits of all the equities involved.

- The Federal government will be in a position to encourage the development and use of Security Management Infrastructures (SMI) by buying and using standards-compliant equipment and products.

The Federal government makes up about 5 percent of the market for information technology. However, this fraction still represents the largest single segment of the market and carries with it billions of dollars in purchasing power and market incentive. The federal investment dollar will help stimulate the development of strong security products. The need to interoperate with government systems will be further incentive to build and use compatible products. It is important to remember that investing in cutting-edge technology has some risks associated with it. Some investment in losers will be inevitable, and the cases of Beta-Max and 8-track tapes are good examples that the market can sometimes bypass innovators.

- The Federal government will establish and define the legal liability framework for information security.

Questions and uncertainty about the liability associated with a security management infrastructure (SMI) have been a major deterrent to its deployment, but by removing some of the uncertainty, industry will be more willing to provide the products and services needed to provide an SMI.

- The Federal government will continue to encourage and support international standards in the area of security.

Standardization is essential for interoperability across products and technologies, and will foster commercial development and wide-spread proliferation of information security technology. The standards bodies also serve as a forum for government influence.

On the negative side, the wide-spread proliferation of security products will diminish the collection of unencrypted messages for both law enforcement and national intelligence.

- The Federal government will continue to subsidize R&D for technology transfer, especially for information security technologies.

Some R&D investment from the public sector for prototyping security technologies will continue to be needed to mitigate the market's perceived risk for independently developing these products, and as electronic commerce and the information industry take off, the expected return on investment in security management infrastructure (SMI) technology will be tremendous.

- The Federal government continues evaluating and assessing security products (including services and standards), and makes the results publicly available.

The Federal government is in a unique position to provide an unbiased brokerage service. Expertise currently exists within the Federal government within the intelligence community. Making its capability more widely available may require some level of reorganization within the Federal government.

An unbiased assessment will be useful to the consumer of security products. The results of the security evaluations will help to educate the vendors of security products.

In general, as businesses and governments place more dependence on information technologies, they will place greater emphasis on their reliability and integrity. By establishing clear precedents for security services in government systems and in procurement, government can leverage its modest market influence to encourage development of secure products that will be needed by businesses and individuals.

Two business trends are particularly ominous with respect to the vulnerability of critical national infrastructures. First, the trend among large organizations to centralize the management of their facilities and resources; the communication medium they will use for this management will be the public network. Second, the trend among telecommunication providers to let their customers administer their network resources being leased to them; this will expose the network to greater danger of disruption, possibly from the very parties who most depend on it. There is no simple technical fix for this dilemma; market pressures will have to resolve it, although the establishment of a legal framework for security issues could help provide the impetus for more solid security.

## Social Trends

---

Significant social changes will accompany the technological and institutional trends that we will see over the next decade. As these changes will affect large segments of the population, they will also have some implications for our national competitiveness and for the integrity of our national infrastructures.

In general, the social trends identified below are driven by technical innovation. This is a natural aspect of the transition from a second to a third wave society.

- Internet access will become an expected part of personal and working life.

Currently, less than 20 percent of the U.S. populace has regular access to the Internet. By 2010, this will probably grow to over 80 percent. Use of electronic mail for personal and business purposes will be the social norm.

For the U.S. to remain at the forefront of nations in productivity and technical prowess, we must support the Internet and help it to become reliable enough to be the primary media basis for the interactions that support our daily lives.

*By the end of 1996, about 80 percent of all Danish citizens had access to the Internet.*

- The economic importance of intellectual property will increase.

As our society becomes increasingly bound to information technology, the assets best supported by that realm will become even more important. Demand for software, entertainment, knowledge bases, and other 'infoware' will drive a larger share of our markets.

However, the fungibility of intellectual property is predicated on the ability to control and charge for its use. Security mechanisms of all sorts will be required, and a legal framework will have to be established. These necessities will emerge, but their quality will help to determine how big a boost to our economy this sector can give. Further, our competitive position with respect to other nations will depend in large part on the ability to control our intellectual property. This issue has already become important in our diplomatic relationships, and will become more so in the coming decade.

- Information technology-related crime will proliferate.

Introduction of new areas of economic opportunity traditionally spawn new areas for criminal activity. Safeguards, standards, and legal frameworks for controlling new forms of crime will have to be established.

One very subtle social aspect of this problem has not been well addressed. There is a certain deterrent effect derived from society's attitudes toward undesirable or harmful activities. There is currently no trend toward establishing a moral or social framework for IT-related ethics. If consensus for an ethical baseline for our third wave society does not emerge, then the potential benefits of the information-based society may be severely curtailed. Attempts have been made among specialist groups (computer scientists, lawyers, notaries public) to establish such an ethical base, but no such dialog is occurring in the mainstream.

Social forces are very slippery, and difficult to direct. If our nation is to continue to reap the educational, professional, and economic benefits of information technology, we must ensure that virtual space reflects the values we hold in the physical world.

# Appendix A

---

---

## Detailed Adversary Model

---

---

There are a large number of malicious parties motivated and equipped to attack our information systems and infrastructures. They can be characterized by three criteria: their material resources, their expertise and skills, and their tolerance for risk. In general, a greater value for any of these criteria makes an adversary more dangerous.

*Resources and expertise determine what adversaries **can** do, risk tolerance and goals determine what they are **willing** to do.*

In addition to classifying adversaries according to their abilities, we also attribute general goals to each type. The goals held by a potential attacker will help determine the vulnerabilities they choose to exploit.

---

### Adversary Characteristics

---

**Objectives:** An adversary's objectives are the events or desired outcomes which motivate the adversary to conduct some attack.

For purposes of discussion, each class of adversary is given a rating of high, medium, or low for the following characteristics.

**Resources:** Resources includes the money, technical expertise, and access available to an adversary. Note that if an adversary has a lot of money but not much technical sophistication (like a drug cartel), then the adversary can simply buy the necessary expertise (like drug cartels do).

- A **High** resource rating indicates that the adversary has the money or expertise normally associated with a national level organization, such as an annual budget in the billions of dollars.
- A **Medium** resource rating indicates the money or expertise associated with large corporations, such as a budget in the millions of dollars.

- A **Low** resource rating indicates financial or technical resources typically associated with small organizations or individuals, such as a budget less than a million dollars.

**Risk Tolerance:** An adversary’s level of risk tolerance indicates the severity of the consequences of being caught that the adversary is willing to accept. Desperation, fear, retaliation, exposure, and the opportunity for future attacks all factor into the adversary’s risk tolerance.

- A **High** rating in risk tolerance indicates a very desperate adversary, willing to accept any consequence in order to carry out his mission. Often, adversaries willing to incur this amount of risk considers themselves in a state of war.
- A **Medium** rating in risk tolerance indicates an adversary willing to risk his job, or serve jail time, but might not be willing to risk his life.
- A **Low** rating in risk tolerance indicates an adversary who is not willing to risk personal harm.

<b>TABLE A-1. Adversary Characteristics</b>					
<b>Adversary</b>	<b>Objectives</b>	<b>Money</b>	<b>Expertise</b>	<b>Access</b>	<b>Risk Tolerance</b>
Insider	revenge, retribution, financial gain, institutional change	Low	Low	High	High
National Intelligence	information, political military, and economic advantage	High	High	Med	Med
InfoWarrior	military advantage, chaos, damage to target	High	Med	Med	High
Terrorist	visibility/publicity, chaos, political change	Med	Low	Low	High
Industrial Espionage	competitive advantage	Med	Med	Med	Low
Organized Crime	monetary gain	Med	Med	Med	Med
Hacker	thrill, challenge, prestige, notoriety	Low	Med	Med	Low

---

## Malicious Insider

---

The malicious insider is a very dangerous and insidious adversary. By definition, the insider already has a high level of access to the systems or infrastructures they attack. This allows the insider to ignore some or all of the security measures that might deter an outsider. Because of this high level of access, the insider has all of the organization's own resources to use against itself. The goals of the insider include revenge, financial gain, institutional change, and occasionally publicity for a cause. Malicious insiders may have a very high risk tolerance, because they may believe they are acting for a higher purpose.

**EXAMPLE:**

Aldrich Ames, a highly placed individual at the CIA, was trusted with the identities of some of the nation's most valuable operatives in the Eastern Bloc. By selling these names to the KGB, Ames inflicted an tremendous amount of damage to the US intelligence community.

---

## Info Warrior

---

An Info Warrior is a military adversary who undermines their target's ability to wage war by attacking their information or network infrastructure. An Info Warrior has the same high resources of national intelligence, but differs from national intelligence in two respects: its focus on the target's ability to wage war, and its tolerance of short-term risk that would be intolerable to long-term intelligence interests. The objectives of the Info Warrior are basically military advantage and chaos. Some of the particular facilities that an Info Warrior might choose to target include: command and control facilities, telecommunications, logistics and supply facilities, weapons systems, and transportation lines.

**EXAMPLE:**

Operation Desert Storm is the best example of an Info War to date. The coalition forces systematically destroyed Saddam's ability to wage conventional war by targeting his command and control infrastructure with a combination of electromagnetic jamming and old fashion bombing raids. Without the command and control capability, Iraq's massive ground troops were useless.

---

## National Intelligence

---

A national intelligence effort is a very capable and rich adversary. However, a national intelligence adversary is highly risk adverse. The national intelligence adversary may use his immense resources to gain access without risk that is not available to any other adversary except the insider. The objectives of this adversary are to gain long-term political, economic, and military advantage by collecting and distributing information. Obtaining that information may entail actively attacking information, telecommunications, and even physical systems.

The operations of a national intelligence adversary can be divided into several types. Some of these are:

- **Traditional SIGINT:** Passive collection of information; low risk, but expensive due to volume and processing requirements.
- **Active SIGINT:** Introducing intelligence-friendly features into security systems, in order to facilitate identification or collection of information that the systems were installed to protect. This is risky, but can result in high intelligence return.
- **Active Exploitation:** Broader than Active SIGINT, this activity involves introducing intelligence-friendly features into all forms of automated equipment to allow the adversary access. This access may be employed at a later time to identify and collect information.

**EXAMPLE:**

A foreign intelligence organization inserts exploitable features into a foreign company's product line. Once these products are used by the targets, the foreign intelligence organization can exploit the system and collect intelligence.

---

## Terrorist

---

This adversary includes a broad-range of ideology-motivated organizations, both foreign and US-domestic. Most of the threats associated with this group involve availability and integrity attacks. The objectives of the terrorist include chaos, publicity, and revenge. Since the terrorist considers himself in a state of war, he endures a high tolerance for risk. Since terrorist groups are typically from ThirdWorld countries or are outside the mainstream organizations, they will not have as much money, expertise, or access as a nationally funded intelligence or Info War attacker.

**EXAMPLE:**

By intercepting the airline reservations of a highly visible government official, a terrorist group is able to target the flight that will maximize the effect of their bombing attempt.

---

## **Organized Crime**

---

Organized crime is a type of adversary that identifies and exploits vulnerabilities with the goals of making money and gaining power. As electronic commerce becomes widespread, criminal elements will become more active in cyber-attacks. Because this adversary has a stake in preserving the status quo and its place in it, its risk tolerance is lower than that of terrorists and Info Warriors.

**EXAMPLE:**

Organized crime has been very successful lately in using the computer as a weapon. Some financial institutions around the globe are reporting that their computer systems have been remotely held hostage, and that if the banks do not deliver the ransom money, the bank robbers will crash the computers. Since the banks cannot afford the loss of public confidence, they typically pay and keep the incident confidential.

---

## **Industrial Espionage**

---

Industry seeks competitive advantage by obtaining its competitor's trade secrets and logistics. Their attacks are highly targeted to gain the specific information sought. A company will devote the necessary resources towards industrial espionage to achieve an acceptable return on investment. This adversary has an interest in preserving their reputation in the community they do business, and therefore their risk tolerance is low.

**EXAMPLE:**

An overseas aircraft manufacturer wishes to disgrace a U.S. rival. They attack the LAN on which the embedded software for a new plane is being developed, and insert malicious code that causes the aircraft's performance to degrade only in a specific geographic region. In U.S. tests, the aircraft performs well; at an overseas air show it performs badly, and the U.S. firm loses business.

## **Hacker**

The hacker is typically defined as an individual with technology expertise, engaged in compromising computer and telecommunication systems for personal pleasure. Their resource level is low and they are risk adverse, but they may have no fear of prosecution, so, hackers may engage in illegal activities without any perceived risk. The primary danger posed by the hacker community is their potential, in aggregate, to erode public trust and confidence in public network and communication infrastructures.

**EXAMPLE:**

A hacker penetrates the computer security on the network of a metropolitan police department, and modifies the configuration of the department's automated telephone system. Callers to the police department emergency number, 911, get a derisive message and no connection to an emergency operator.

# Appendix B

---

---

## Detailed Vulnerability Review - Availability

---

---

Availability of an information system is the ability of the system to provide the user-required functions in a manner that meets timeliness and structure requirements. Availability is primarily concerned with ensuring that the system works when you need it.

This section describes security vulnerabilities that compromise availability. With the increased reliance on networked computer systems to perform critical functions, it is important to examine the effects of denial-of-service attacks on overall system performance. Denial of service prevents or inhibits the normal use of an information system. These attacks can be segmented into three general categories: disruption, blockage and delay.

- **Disruptive attacks** attempt to disrupt data by using system features to cause the user to become flustered to the point where they will either disable the feature or not use the system. An example of a disruptive attack is to force the system to drop every 19<sup>th</sup> bit. This is not an integrity issue because the user knows the data is bad. In fact in most cases, the user will assume that the line is noisy. In some systems this may be tolerable, but in others the user may turn off what they believe to be the cause, maybe the firewall, or move to a slower transmission device.
- **Blocking attacks** attempt to identify critical resources and critical paths that are shared by both the target and the attacker. The attacker then tries to occupy the resource or path, blocking the target's access to the resource. An example of this type of an attack is when a dial-up connection is required. An attacker then dials in, occupying the line and preventing the target from having access. Firewalls offer excellent security services, but also make excellent targets for blocking attacks because they are almost always a critical path shared by an attacker and the target.
- **Delay attacks** attempt to cause time-critical data to be delayed, thus reducing its value, or rendering it useless. The main purpose of this attack is not to block or disrupt the information, but to cause the target to act on outdated or incorrect information. An example of this type of attack is an attacker changing a routing table to delay the posting of current stock prices to a seller. The attacker could then detect a trend prior to the target and buy or sell at a strong advantage.

All of these attacks can be combined and often evolve from one to another. The Morris Internet Worm is an excellent example. On November 1, 1988, a computer worm (a type of computer virus) was discovered on a computer system in Pennsylvania around 6:00 p.m. Eastern Standard Time. By 10:00 p.m., the worm had reached BARnet on the West Coast and had rendered the Internet unusable.

A key feature of the worm was its method of moving from machine to machine. The software written by Morris used a procedure to roll a 15-sided die so that there was only a 1-in-15 chance that the worm would move on and therefore go undetected. But due to a programming error, the actual code caused the worm to replicate 14 out of 15 times. This moved the worm to first a delay attack, causing the infected system to slow down; then to a blocking attack where the worm occupied major transfer nodes on the Internet. In fact, when Morris found his error, he tried to e-mail the solution to kill the worm, but the Internet was already blocked. If a Morris-like worm were to infect the Internet today, the cost in public trust would be incalculable.

A more direct example is the attack on WebCom, a major Internet service provider (ISP). For over 40 hours, WebCom was attacked by a 200 message-per-second flooding attack on what would have been a very busy shopping weekend. The attack effectively blocked over 3,000 websites. The attack was traced back to CANet, an ISP in Ontario, Canada. Unable to stop the attack, all traffic from CANet was blocked by MCI to allow WebCom to return to service.

***Flooding: Producing excess requests for services so other users can't use the system.***

In the past, the availability of a system was a function of fault-tolerant design of hardware and software reliability. In a highly-interconnected world, a competitor can command almost unlimited resources to bring a system down. Strong mechanisms must be developed to limit a user's ability to occupy resources and control other systems. Strong authentication and integrity methods are steps in the right direction.

***Without strong access controls, any system that allows public access can be blocked from service.***

# Appendix C

---

---

## Detailed Vulnerability Review - Authenticity

---

---

Authenticity is a means by which proof of identity is produced, allowing decisions to be made to grant access to information, capabilities and resources. In the non-network world, authenticity is often based on credentials (photo identification cards) or seals (notaries). In the network world, authenticity is primarily based on what one knows (passwords), and less often on what someone knows and has (Smartcards or WatchWords), and least often on what makes a person unique (biometrics).

### Forms of Identification and Authentication

---

Identification and authentication (I&A) are mechanisms and procedures which are commonly encountered in everyday life. People are issued credentials (drivers license, passport, employee ID), which are used as an identification mechanism. The seals on credentials authenticate them as original and not counterfeit copies. *Identification* is who I claim to be, *authentication* is the proof I am who I claim to be.

### Identification in Network Systems

---

Network systems also employ identification mechanisms. These are usually based on a piece of information only the authorized user knows: a password. Passwords are inadequate to protect anything critical because, in a network environment, they must be broadcast across the network in the clear where they can easily be collected. Once stolen, a password can be used to impersonate the authorized user. The inadequacy of passwords in a network has been addressed by a number of efforts [i.e. *Kerberos* and *S/KEY*] which address the threat of easy collection of clear text passwords on the network. While these efforts greatly reduce risk, they still do not address the case of counterfeiting a password once it is stolen or guessed.

SmartCards and WatchWords are mechanisms which increase the cost of counterfeiting a user's identity by providing a means where a remote computer can issue a challenge which requires the SmartCard or WatchWord to respond correctly. These mechanisms require user-entered information to activate them (a password or a PIN). The mechanism is more robust than passwords alone because they require something the user knows (the password or PIN) and something they own (the SmartCard or WatchWord). Counterfeiting requires compromising information stored in the SmartCard or WatchWord which requires access to the device.

Biometrics are another form of identification which are based on physical characteristics which are believed to be unique to an individual, and reproducible and can be measured by a computer. These include: eye scans, fingerprints, hand writing voice and face recognition. Some systems store the biometric information on a SmartCard or token so it can easily be transported by the user. Using a biometric system as an identification system requires measuring the individual and comparing the result to the stored information. In addition to what is known (password/PIN) and what is owned (token), a biometric system adds information on who you are. These systems are probably the strongest identification systems available today.

## **Authentication in Network Systems**

---

A common deficiency in all the identification mechanisms is a lack of universal agreement about what is required to authenticate a person or entity. A driver's license is universally accepted as identification credentials due to the trust of the procedures to acquire a license. There is no universally accepted identification mechanism in the network world.

The discussion of the identification mechanisms above (passwords, SmartCards and Biometrics) did not discuss authentication. Recall that authentication is the evidence that an individual (or entity) is who (or what) they claim to be. Password-only mechanisms provide no proof that the claim should be accepted. Systems like Kerberos attempt to address the authentication needs but are a closed system serving a small community. Tokens provide elements to build a stronger authentication mechanism with, since they must be issued, are hard to counterfeit, and can contain proof that they are issued by a trusted party (digital signatures).

An authentication system should be able to answer a number of critical questions including:

- Are the credentials authentic?
- Is the identified party authorized to access the protected source?
- Was the identified party authorized at the time the request was generated, received or fulfilled?

An authentication should be universally recognized and available for use. Legislation to ensure that authentication providers (VeriSign) are protected and supported would facilitate this deficiency being addressed.

---

# Foundations of Security

---

*An adversary will choose the least costly attack he can find.*

**Corollary.** *A security system (mechanisms and procedures) is only as reliable or trustworthy as the protection against the easiest attack.*

Adversaries get to choose where and when they will attack a system. The security engineer's responsibility is to invest information security dollars wisely in the areas which represent the highest risk. Where security countermeasures are unavailable, the engineer should employ detection mechanisms (alarms) which indicate a system has been attacked. Periodic audits and inspections are also valuable tools to use to plug the holes in the system.

## Areas of Vulnerabilities

---

- Authentication Vulnerability 1 - Security Administrator Clones Credentials

The trustworthiness of an identification and authentication mechanism is rooted with the issuing authority and the workstation used to enroll users. Cloned (or counterfeit) certificates could be created which provide complete privileges of the cloned entity. If cloning is successful, the confidence in the system will be greatly compromised.

The security administrator enrolls users into the system. A compromised security administrator or a corrupted workstation could retain copies of credentials. The requirements for security administrator and life cycle support for the security enrollment workstation must be more strict than for other users and workstations.

The impact of a successful attack on security administration is the compromise of all the credentials created by that security administration. Additionally, confidence would be eroded about the trustworthiness of the system.

**EXAMPLE:**

New, or upgrades to, computer software is always being installed on computers. Software installation usually requires system administrator (root or super-user) privileges. Such software is an attractive opportunity for an adversary to modify security-critical programs. A robust set of procedures may be reduced to the least-trustworthy site at a computer software vendor or distributor's site.

*Every component is not equal. Implementing extraordinary mechanisms and procedures may be appropriate for more critical parts of the system.*

- Authentication Vulnerability 2 - System Administrator Privileges Gained and Authentication Decision Mechanism is Altered

Access control decisions are based on identity and authentication (I&A) mechanisms. Once I&A is performed, a decision to grant or withhold access to a resource must be enforced. If the access-granting mechanism can be altered, the I&A mechanism is ineffective.

Adversaries that can attack a computer system and acquire system privileges can replace critical security-related mechanisms. It is not uncommon to read reports where hackers have carried out such attacks successfully.

This vulnerability, if exploited on a critical system, would remove the I&A mechanism that the user is dependent upon. In effect, the adversary becomes the most privileged insider.

# Appendix D

---

---

## Detailed Vulnerability Review - Integrity

---

---

Integrity of a collection of data is the accuracy of the data, in the sense that the data accurately reflects the intentions of its users and creators. Also, integrity involves the environment in which data or systems reside. The integrity of data is not preserved if the origin of the data is altered. In some cases, we may directly associate extra information with a collection of data, information specifically formulated to help ensure integrity. The integrity of a complex system or infrastructure is the reliability we can place in the system that it indeed performs its intended function without deviation. Often, the integrity of a system is directly dependent on the integrity of the data it contains and controls.

---

### What is Integrity?

---

This section describes security vulnerabilities that compromise integrity, and thereby cause harm to individuals and organizations. In general, the parties harmed by integrity attacks will be those that depend on the accuracy and reliability of their support systems. It is typically the dependence on accuracy, the trust in a system or data collection's immunity to disruptive change or alteration, that exposes the user of a system to harm. Further, public confidence in data or systems may be substantially reduced by any appearance of inaccuracy or imprecision.

### Physical Integrity

---

In the physical world, integrity is typically assured by physical means. The accuracy of a financial instrument like a check is determined by the condition of the paper and the ink. Similarly, the correct operation of a physical system like a railroad tunnel can be determined by physically inspecting it for cracks or leaks.

Various integrity assurance mechanisms are accepted in the physical worlds. For example, notary seals are used to guarantee the integrity of ink signatures. The physical integrity of cosmetics and

medications are protected by snug cellophane seals. In most cases, the mechanism for verifying integrity is physical inspection.

## **Digital Integrity**

---

In the digital domain, integrity is very difficult to test or ensure. A software system, computer network, or database will not reveal integrity shortcomings to a casual observer. Our nation's increasing reliance on accurate and reliable information and telecommunications systems makes us more vulnerable to their failure.

*Digital data can be tracelessly modified.*

Data integrity is a sub-part of the overall integrity issue. A great deal of information on which our government and businesses depend is stored primarily in computer systems. If these systems were to come under attack, substantial cost and lost productivity could be incurred to fix them or to employ less-vulnerable back-up systems or procedures.

Data integrity is more than just the content of a database, fax, web site, or computer network. The context in which the data exists must also be reliable and accurate for us to depend on it. The time at which data was created, who created it, and for whom it was intended may all be important.

*The context of digital information is just as important as the content.*

---

## **Areas of Vulnerability**

---

This list below describes several types of vulnerabilities that can threaten the integrity of computer and telecommunications systems. Each one is described in very general terms, and includes an assessment of the ability and willingness of identified adversaries to carry it out. Also, each attack description includes an estimate of its potential impact. Some of the attacks are illustrated by concrete technical examples.

- Integrity Vulnerability 1 - Alter E-mail Messages

Current e-mail technology does not provide any means to ensure the integrity of messages. It is not always possible to detect alterations to messages. In the case of e-mail messages, an attacker may choose to alter the body of a message, or the time it was

sent, or the identity of the sender. (This vulnerability introduces both implementation and trust structure risk.)

Adversaries with a medium level of resources, or with access to systems that route e-mail, will be able to perform this attack. The level of expertise required is not high. However, the volume of e-mail and the difficulty of selecting messages to modify that will cause significant harm make this attack expensive to carry out on a large scale.

The potential impact of this attack is modest at present, because reliance on e-mail for critical decisions is currently low. Also, adequate alternative channels exist (e.g. fax, telephone) to allow for confirmation of e-mail information. In the future, this attack may be very dangerous: as we continue to rely on e-mail to conduct business, the potential loss resulting from falsified messages increases.

**EXAMPLE:**

A bid for a government contract is to be sent via e-mail to the procuring agency. A rival bidder uses well-known network attack techniques to gain control of the first bidder's Internet Service Provider. Exercising this control, they arrange to preview and alter the bid. As a result, the first bidder loses the contract. Costly and disruptive litigation ensues.

- Integrity Vulnerability 2 - Alter Corporate Databases

A corporate database, such as a payroll or billing database, must meet strict criteria for integrity. If the contents of the database were altered, the daily operations or even the long-term future of a company could be endangered. Alterations to data can be very subtle, and may even go undetected for years at a time. Similarly, the software that is used to manage the database may be altered to achieve an adversary's goals.

Modern database systems vary in the amount of integrity assurance they provide. Typically, the amount of expertise and expense needed to compromise a corporate database will be directly related to its size; the larger systems tend to have better integrity mechanisms. However, the centralized nature of most small-to-medium databases makes targeting them straightforward. An adversary with modest resources will only be able to target smaller database systems. An adversary with a medium resource level will be able to target large organizations' database installations, and the most capable of them will be able to attack many large organizations simultaneously. Corporate database systems are particularly vulnerable to attacks by malicious insiders, because they are typically centrally administered and accessible to many members of the organization. (This type of vulnerability yields primarily implementation risk for an adversary.)

*Disgruntled insiders pose a serious integrity threat to data that is at rest.*

The potential impact of an attack on a corporate database is limited by the extent to which the organization's resources and activities are controlled by that database. Detection of altered records can be very difficult; thus the effect can be extended over an indefinite period of time. In many cases, back-up paper records or manual procedures may exist to validate and/or repair the database; periodic audits of databases may be employed to help detect data integrity compromise. An area where this issue merits particular attention is the growing field of medical informatics; particularly in radiology, the integrity of computer databases has been a very serious concern.

- Integrity Vulnerability 3 - Alter or Vandalize Public Information

As public data networks continue to become more popular, both consumers and businesses will increasingly rely on information posted publicly rather than on direct communication. Currently, the systems which host such information and make it available are vulnerable to a very broad range of network and computer attacks. This vulnerability is not, for the most part, inherent in the technology, but is instead the consequence of ill-advised, improper, or faulty application of it. Various mechanisms exist to ensure the integrity of public information in transit from the provider to the consumer, but almost none to ensure its integrity in the interval between creation and transmission. (This kind of vulnerability yields primarily implementation risk. Implementation risk in this context typically means a security design is good; however when a user implements the design and does not implement the design *as intended*, then risk has been incurred due to poor implementation which has circumvented security.)

*Integrity of the World Wide Web entails safeguarding both storage and transmission.*

An adversary equipped with modest network hardware and resources can target and, in many cases, successfully alter information provided on public web sites and possibly on other network services.

**EXAMPLE:**

Currently, public comments on network discussion groups are archived and made available on the Web. An attacker might choose to target a political candidate by altering their public remarks made years ago. Judicious modification could reduce the credibility of the candidate, and cause their defeat in an election. Current technology would offer the victim few means for refuting the evidence, and essentially no means for tracing the attacker.

To the extent that organizations depend on public information services to present their public face, they are vulnerable to integrity attacks on that information. Today, the danger is mostly bad publicity, but it will not remain so.

EXAMPLE:

A Microsoft WordBasic™ virus is injected into the computer of a large corporation. It would quickly propagate to many of the computers in the organization. Such a virus could modify contracts under the control of an outside malicious entity such as a rival company, and ensure that the modifications were included only on printing hardcopy, and never on the display. In this way, the rival company could gain financial advantages. The move toward “paperless workflow” makes this scenario more plausible.

- Integrity Vulnerability 4 - Alter Network Control Information

The operation of large computer networks is wholly dependent on control and configuration information that resides on constituent network devices. Kinds of information include low-level data like network routing configuration, and higher-level information like the names of computers on the network.

An adversary could substantially disrupt the operation of the network by altering network control information, but they can also perform more subtle tricks, slowing information flow or making it available for intercept. The dependence of computer networks on their control information has implications for availability and privacy as well as integrity. (Network control information integrity vulnerabilities introduce both trust structure and implementation risk.)

A knowledgeable adversary with a modest level of resources could, with luck and skill, alter the network information enough to affect a small number of targets. Attackers with large amounts of resources would alter the network control information in a wide variety of ways, allowing them to create widespread disruption or precisely focused compromise.

*Network name services are critical to operation, and are currently not protected.*

The impact of an attack against the configuration of a network can vary widely. Some of the possible attacks are:

- Compromising network name services to prevent customer access to an organization, or to allow impersonation, (authenticity and privacy threats).
- Concentrating traffic through a bottleneck, slowing performance and creating a means for substantial disruption of service (availability threat).
- Changing the flow of messages through the network to permit convenient capture or alteration to a single point (privacy threat).

**EXAMPLE:**

A hostile intelligence service installs a high-speed network connection, and alters network control information to force large amounts of data to flow through their sites. This level of control would offer them the freedom to alter traffic at any time. For example, they might alter software being downloaded to protect a developer's workstation at VeriSign, Inc. With their malicious software injected, later compromise of the security services provided by VeriSign, Inc. would be very easy.

The type of adversary that poses a very serious threat in this area is the Info Warrior. The resiliency of modern network architectures will usually permit attacks to be cleaned up quickly; service disruptions and wide-area compromises would not be long-lived. However, an Info Warrior might create and exploit short-term compromise to open a particular objective for further exploitation or even physical attack.

---

## **Conclusions**

---

The operations of our businesses, governments, utilities, and other institutions are dependent on the integrity of information systems and the data that they store and transport. Reliability of these systems has always been an important issue, and therefore many critical systems are backed up by manual procedures, policies and support personnel. An individual attack against the integrity of our information and communications infrastructure components is unlikely to cause a serious crisis at the present time. However, we have a large number of diverse systems at risk, and the resources required to attack them are not prohibitively high. Integrity assurance mechanisms are necessary to support continued reliance on digital information systems.

# Appendix E

---

---

## Detailed Vulnerability Review - Privacy

---

---

### Privacy

Privacy is the desire to keep data from being disclosed to anyone but the intended recipient. Most methods established to maintain privacy of data involve either hiding, limiting access to, or disguising information.

Governments are driven to keep certain information private because their adversaries would likely derive tremendous political, economic and military advantage from those secrets. For the commercial sector, financial considerations usually drive the implementation of privacy mechanisms. In addition to a weakened competitive position, governments and commerce may also suffer from a significant loss of public trust when critical information is divulged.

*Privacy can be maintained by denying an adversary the ability to acquire important information, or by denying him the ability to read it, or both.*

Concealment can be an effective means to keep one's information private. For instance, in the case of wireless data, transmission security techniques can be used to create low probability of detection and low probability of intercept to hide the signal, and hence the underlying information, from an unauthorized listener. Another means to acquire privacy is by denying access to information. In the electronic sense, an operating system might address this with an access control list and through management of user privileges. The most common privacy mechanism is disguising information through cryptographic means.

In theory, strong cryptography coupled with sound implementations will stand up to analytic attacks by even the most sophisticated and well-financed adversary (a national or multi-national intelligence capability). However, implementing cryptographic algorithms and protocols to deny targeted attacks capable of being carried out by much less capable adversaries has proven to be very difficult. Also, even a strong cryptographic scheme with all its functionality (key generation and distribution, randomization, certificate management and other infrastructure) operating securely might be circumvented by a well-placed insider.

The Walker/Whitworth case is a classic example of privacy circumvention. A U.S. Navy employee with access to highly-classified keying material sold that information to a foreign government, who is then able to decrypt sensitive communications secured by the U.S. cryptographic system employing those keys. The employee is trusted because he passed various employment screening tests, as defined by the Trust Model, to gain access to sensitive classified information. Removing keying material from secured premises is a violation of both trust and physical constraints. The decision by the foreign intelligence service to engage in this mission speaks to their risk tolerance, for they certainly recognized their likelihood of being exposed. Also, since the adversary sought only keying material, we might infer that the intelligence organization had gained familiarity with the classified cryptographic system and was collecting ciphers. However, they decided to buy an insider rather than focusing their resources toward passively attacking the cipher. In spite of the robustness of the cryptography, its implementation relied on delivery of hard-copy key, common for systems of that vintage. This proved to be the Achilles Heel of the system.

The recently-solved 40- and 48-bit RC5 challenge problems posed by RSA Data Security, Inc. represent another exploitable vulnerability in a privacy mechanism. In this case, no proof yet exists that the RC5 cryptographic algorithm is weak, but if used in conjunction with a key size that is indeed too small, adversaries with even modest resources will be able to recover keys through cryptanalysis. The 40-bit key was recovered by a graduate student with access to university resources (about 250 high-performance workstations) while the longer key required a cooperative effort over the Internet encompassing about 3,500 computers.

Electronic mail is embroiled with privacy issues. A typical requirement is that only the sender and intended recipient be able to read the transmission. Archived data may also require the same level of confidentiality. Further, some systems levy a transmission security requirement whereby persons other than the sender and intended receiver cannot even detect the existence of a message.

Privacy of content is usually handled by cryptographic means. However, for e-mail, in addition to the strong crypto and secure implementation warnings, we have additional concerns regarding network interface nodes and message transfer agents. Network nodes are points of access and are targeted by intruders. In fact, system administration might require monitoring of mail which implies decryption and re-encryption at relay nodes, thus potentially exposing the underlying plain text. Mail forwarders or message transfer agents are a consequence of the store-and-forward nature of e-mail. Again, these agents may also be points of vulnerability.

Encryption is also the most common method for addressing the transmission security of e-mail messages. In this case, the encrypted e-mail message is embedded within a larger transmission which may even be destined for a different addressee, who acts as an intermediary. This outer transmission is also encrypted and hence the hidden inner e-mail message is now super-encrypted.

As another example, the use of hardware cryptographic tokens is now becoming more popular. SmartCards, especially, have seen a surge in interest in the United States this past year. The conglomeration of security capabilities of these cards expose them to serious vulnerabilities. An adversary able to introduce a new version of a device driver or system software onto a user's computer, could cause the user to begin using the same cryptographic key for all secure e-mail messages. With the current API and e-mail security standards, the attack would be nearly undetectable. The potential impact of this class of attack would depend directly on the importance of the e-mail sent by the particular target. For example, an organized crime adversary might target officials at the Drug Enforcement Administration (DEA) or Bureau of Alcohol, Tobacco and Firearms (ATF).

# Appendix F

---

---

## Detailed Vulnerability Review - Life Cycle

---

---

Any information technology can be exploited any time in its life cycle by an adversary who has sufficient knowledge of, and access to, the product. Access to the product, however, is non-trivial to come by. The adversary must either be trusted by the company that designs or produces the product, or have access to the product after its manufacture. The adversary must either intervene in the distribution channel, be trusted to install or perform maintenance on the equipment, or gain surreptitious access in its operating environment. In addition, any adversary can take advantage of inept disposal procedures for products that stored data.

*Life Cycle Stages: Design, Production, Distribution, Installation, Operation, Maintenance, Retirement.*

---

### Life Cycle Attacks

---

There are three components to a life cycle attack: identification, access, and execution. The adversary desires to alter or substitute the product. Consequently, the adversary must first identify or anticipate the specific products that will be in use. Next, a decision must be made when and where to gain access. What can be accomplished once access is obtained must be determined. Finally, the risk and cost of executing the attack must be weighed against the expected pay-off.

The level of access required to constantly carry out life cycle attacks precludes most adversaries. This is currently the world of spy-vs.-spy. A government (and its agents) can insinuate itself into the distribution chain. Government agents can also infiltrate an organization's facility. The stakes are high so the risk is acceptable. The Info Warrior wants to deny use of the technology in order to cripple an adversary's ability to wage war.

## Rational Response

---

Simple measures can be taken to reduce the threat of a life cycle attack. Most countermeasures try to eliminate the covert channel back to the adversary. One channel is the electromagnetic emanations from the equipment. This risk can be diminished by locating the equipment in the middle of a building, which can put the emanations out of an adversary's reach. This is not always feasible. Another option is to extend the inspectable space of the facility. Foil-backed wall board can be installed to block the emanations. An adversary can also piggyback on the electrical signals such as power lines. Filters can be installed to mask out covert signals. Last of all, inspections can be made periodically in order to detect whether an adversary modified the environment, including the products. These simple steps can significantly raise the risk and sophistication needed to conduct a life cycle attack. Note however, that no space can be made secure, and inspections will never be effective if guards cannot keep out infiltrators or if the organization cannot screen effectively those trusted to have access.

## Residual Threat

---

The information technology based on networks has created new opportunities for adversaries exploiting the life cycle of products. In the old world, phone lines could be filtered to stop covert channels. Applications supported on a network of workstations can have multiple paths for a covert channel. In addition, applications implemented in software can be modified remotely by malicious executable content. The adversary can modify products without having physical access. Moreover, the trend is to have increased reliance on remote maintenance of information systems. Technicians will be centrally-located and fix problems at a distance. That capability to fix is another avenue of attack for an adversary.

*Access obtained through malicious software allows adversaries to modify products without incurring physical risk.*

As information technology becomes integrated into the nation's commerce, the profit motive will entice organized crime into exploiting the life cycles of products. The functionality of information technology is outpacing the ability to secure the technology.

# Appendix G

---

---

## Glossary

---

---

Many common terms are routinely used throughout this document. To avoid any confusion, we list how these terms are defined, and the documented sources. Where there exist multiple meanings, bullet points are used for clarification.

### Access

- Capability and opportunity to gain knowledge of or to alter information or material.
- Ability and means to communicate with (i.e., input to or receive output from), or otherwise make use of any information, resource, or component in an automated information system. NOTE: C An individual does not have “access” if the proper authority or a physical, technical, or procedural measure prevents them from obtaining knowledge or having an opportunity to alter information, material, resources, or components.
- A specific type of interaction between a subject (i.e., person, process, or input device) and an object (i.e., an automated information system resource such as a record, file, program, or output device) that results in the flow of information from one to the other. Also, the ability and opportunity to obtain knowledge of classified, sensitive unclassified, or unclassified information.
- Permission, liberty, or ability to enter, approach, communicate with, or pass to and from. [Webster’s 9th New Collegiate Dictionary]

### Adversary

- Person or organization that must be denied access to critical information. NOTE: Synonymous with competitor.
- Person or organization that seek to gain military or competitive advantage over a country.

## **Attack**

- Act of trying to defeat automated information system safeguards. NOTE: An attack may be active, resulting in the alteration of data; or passive, resulting in the release of data. The fact that an attack is made does not necessarily mean that it will succeed. The degree of success depends on the vulnerability of the system or activity and the effectiveness of existing countermeasures.
- An attempt to gain information or advantage.

## **Automated Information Systems (AIS)**

Any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware.

### NOTES:

- Included are computers, word processing systems, networks, or other electronic information handling systems, and associated equipment.
- The term "AIS" includes stand-alone systems, communications systems, and computer network systems of all sizes, whether digital, analog, or hybrid; associated peripheral devices and software; process control computers; security components; embedded computer systems; communications switching computers; PCs; workstations; microcomputers; intelligent terminals; word processors; office automation systems; application and operating system software; firmware; and other AIS technologies, as may be developed.

## **Communications Security (COMSEC)**

Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. NOTE: Communications security includes crypto security, transmission security, emission security, and physical security of COMSEC material.

## **Countermeasure**

- Action, device, procedure, technique, or other measure that reduces the vulnerability of an automated information system.

- Action, device, procedure, technique, or other measure that reduces the vulnerability of any equipment that electronically processes information as well as facilities and automated information system.
- Anything which effectively negates an adversary's ability to exploit vulnerabilities.

### **Exploitation**

The process of obtaining intelligence information from any source and taking advantage of collected information.

### **Information Security (INFOSEC)**

- The result of any system of policies and procedures for identifying, controlling, and protecting, from unauthorized disclosure, information that requires protection.
- The discipline covering the protection of classified National Security information by the application of the rules and procedures established by Executive Order.
- The protection afforded by combined measures of computer security and communications security.

NOTE: See *Information Systems Security*.

### **Information System (IS)**

Any telecommunications and/or computer related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.

### **Information Systems Security (INFOSEC)**

- The protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

- A composite of means to protect telecommunications systems and automated information systems, and the information they process.
- The protection afforded information systems in order to preserve the availability, integrity and confidentiality of the systems and the information they contain.

## **Information Warfare**

- Information-based Warfare is an approach to armed conflict focusing on the management and use of information in all its forms and at all levels to achieve a decisive military advantage especially in the joint and combined environment. Information-based Warfare is both offensive and defensive in nature -- ranging from measures that prohibit the enemy from exploiting information to corresponding measures to assure the integrity, availability, and interoperability of friendly information assets.
- While ultimately military in nature, Information-based Warfare is also waged in political, economic, and social arenas and is applicable over the entire national security continuum from peace to war and from 'tooth to tail.' [Working definition recognized by the Information Resources Management College of the National Defense University as of 11/16/93.]
- An electronic conflict in which information is a strategic asset worthy of conquest or destruction. Computers and other communications and information systems become attractive first-strike targets. [Information Warfare: Chaos on the Electronic Superhighway (1994) by Winn Schwartau]

## **NSTISSI**

National Security Telecommunications and Information Systems Security.

## **Penetration**

- Unauthorized act of bypassing the security mechanisms of a cryptographic system or automated information system.
- The act of overcoming one or more measures designed to protect an organization's operation, activity, facilities, information or personnel.
- Unauthorized access to a cryptographic system or automated information system.

## **Perceived Threat**

---

- Estimate of possible present and future resource allocation and capabilities of an adversary to gain information. Synonymous with potential threat.
- Estimate of an adversaries desire and resources necessary to gain access to and advantage of an information system.

## **Risk**

---

- A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting adverse impact. NOTE: Risk is the loss potential that exists as the result of threat and vulnerability pairs. It is a combination of the likelihood of an attack (from a threat source) and the likelihood that a threat occurrence will result in an adverse impact (e.g., denial of service), and the severity of the resulting adverse impact. Reducing either the threat or the vulnerability reduces the risk.
- A measure of the potential degree of loss of protected information.
- The possibility that a particular threat will exploit a particular vulnerability of the system.

## **Security Countermeasures**

---

Countermeasures that are aimed at specific threats and vulnerabilities (operations security procedures; camouflage, concealment, and other denial techniques) or involve more active techniques (counter-imagery programs, counter-SIGINT operations; and telecommunications and computer security) as well as activities traditionally perceived as security.

## **Security Threat**

---

The technical and operational capability of an adversary to detect and to exploit vulnerability.

## **Threat**

---

Existence of an *adversary* with the capability to *attack* (exploit a *vulnerability*) a system.

- Capabilities, intentions, and attack methods of adversaries to exploit, or any circumstance or event with the potential to cause harm to information or an information system.

- The capability of an adversary coupled with his intentions to undertake any actions detrimental to the success of program activities or operation. See *security threat*.

## **Vulnerability**

- Weakness in an information system, or cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited.
- A weakness in an information system or component (e.g., security procedures, hardware design, internal controls) that could be exploited.
- The susceptibility of facilities, operations, activities or programs to exploitation.
- Potentially exploitable weaknesses/deficiencies in a device, system, algorithm, policy, or posture.
- Required facets or features of a system or product which can be exploited.