Chapter 1

Cyber Security and Cyber Trust

V Rao Vemuri
University of California, Davis

Introduction

History is undergoing the third in a succession of great changes in technology and cost of transportation. The 19th century was shaped by the falling cost of transporting goods; the 20th, by the falling cost of transporting people; and the 21st century will be dominated by the falling cost of transporting ideas and information. "Death of distance" is very much here.

The last two decades of the twentieth century witnessed a steep increase in the pervasiveness and ubiquity of digital technologies in our lives. The trip from mainframes to personal computers, laptops and PDAs took place at a breathtaking speed. RFID (Radio Frequency Identification Tag) embedded in everyday objects to smart toys and smart clothing is another journey that has already begun. Indeed much of what we do is getting inexorably tied to digital technologies.

With the declining costs associated with Internet access and information processing, more and more people are being lured to use computers. The rank and file of these users is not the literati of cyberworld – it is the ordinary person who is seeing the desktop computer, connected to the Internet, as another utility outlet – just plug in and use the services. And these folks are expecting a quality of service (QOS) that is commensurate with the QOS they are accustomed to with other utilities like electricity, gas and telephone. People's expectations are that such service is continuously available anytime and anywhere; reliable, secure and easy to use.

Nowadays, computers are being sold in department stores along with microwave ovens, TV sets and music players. Many households (in the US) that own an automobile probably own a computer too. Just like getting behind the wheel, turning the key and driving to the grocery store, people are expecting to get in front of the terminal, fire it up, log on and read mail, make reservations, find driving directions, play games and pay the bills. With the advent of wireless, some are able to perform these functions from anywhere using their laptops.

This rosy picture is not without its thorns. People are not able to perform these routine functions without facing a host of problems. Indeed the need to wait for a long time for the computer to boot up – even in dire emergencies - was caricatured in Hollywood films. The need to memorize usernames and the associated passwords and PINs – with each service provider imposing its own set of rules on the user – is a familiar headache. Is there a way one can help a user learn to choose good passwords and then memorize them? Should the technique of password-based authentication be the same for desktops and hand-held devices? Is there a way one can train users to learn a process of selecting

new passwords when the old one expires? When a user is required to memorize a host of passwords, is there someway one can help the user to manage the plethora of passwords? Would graphical passwords solve the problem? Are graphical passwords immune to dictionary attacks?

In addition to these there are many other problems. For example, the need to know the procedures for handling files with a host of extensions. A particularly vexing problem that is grabbing headlines is the issue of coping with virus and worm attacks!

Cyber Security

We, as a society, are paying a price for these developments. In 1982, a program called Elk Cloner, written for Apple II systems, is credited with being the first computer virus to appear "in the wild" -- that is, outside the single computer or lab where it was created. On November 2, 1988, Robert Morris, a Cornell University graduate student, purportedly launched one of the first computer worms to gain significant mainstream media attention. Around 6,000 major Unix machines were infected by the Morris worm. The General Accounting Office of the U. S. put the cost of the damage at $10 M - $100 M. Robert Morris was tried and convicted of violating the 1986 Computer Fraud and Abuse Act (Title 18). After appeals he was sentenced to three years probation, 400 hours of community service, and a fine of $10,000. During 2003-2004, virulent attacks by viruses and worms, such as CodeRed, Slammer and MyDoom, have taken a toll on organizations and individuals that rely on computers. The sad realization is that computer community is still vulnerable to attacks – after two decades of research and in the face of threats at prosecution.

Table 1 is one estimate of the damage in U. S. dollars caused by viruses and worms alone. These costs include services and hardware needed to remove viruses from networks, shore up defenses and repair damage.

Table 1. Computer Economics' Estimate of Damages Caused by Viruses and Worms

Virus/worm	**Year**	**Cost** (billions)
Melissa	1999	$1.10
LoveBug	2000	$8.75
Code Red	2001	$2.75
Slammer	2003	$1.25
SoBig.F	2003	$1.10

The years 2003-2004 seem to be especially harsh on computer security professionals. In the immediate aftermath of MyDoom attack in early 2003, a New York Times article, "Geeks Put the Unssavy on Alert: Learn or Log Off," dated Feb 5, 2004, quotes the president of the World Wide Web Artists Consortium, as lamenting, "It takes affirmative action on the part of the clueless user to become infected.... How to beat this into these people's heads?" A similar know-all geekish attitude exhibited by U. S. automobile

manufacturers in the sixties paved the way for the high-quality Japanese imports we are enjoying today! "The tension over the MyDoom virus underscores a growing friction between technophiles and what they see as a breed of technophobes who want to enjoy the benefits of digital technology without making the effort to use it responsibly," concludes the New York Times.

The reason one hears more about viruses and worms is because they impact everyone and the media also gives these events high coverage since every user can identify with them. However, the damage caused by these nuisance makers – high as it is – pales in front of the damage caused by someone stealing confidential information from high profile organizations (e.g. a bank) – which is rarely disclosed in public or even within closed groups. This is done to protect the interests of the organization. One exception to this trend can be cited. On February 10, 2004, Associated Press reported the discovery of a major vulnerability in the Windows operating system, although researchers at eEye discovered the problem more than six months earlier. "Microsoft Corp. warned customers ... about unusually serious security problems with its Windows software that could let hackers quietly break into their computers to steal files, delete data or eavesdrop on sensitive information." As some of Microsoft's built-in security features -- such as its Kerberos cryptography system -- rely on the flawed software, the breadth of systems affected is probably the largest ever. Computer systems that control critically important infrastructures, like power and water utilities, are now vulnerable. Intrusion detection systems, therefore, play a supporting role in identifying virus/worm spreads and a key role in protecting organizations with confidential data.

Indeed, products are available to block viruses and worms at the gateway to an organization, at the desktop level, at the server level and at application level (e.g. Messaging Servers). Once such technology is in place, there should be strong processes to monitor and track viruses and worms. What is needed is teamwork between management personnel who are aware and will provide focus, system administrators who are trained in countering these threats and end users who are aware (Don't open unknown attachments from strangers!). Virus and worm control is a classic example of the requirement for technology, processes and people to secure an environment. It is these inter-relationships that make security complex.

The computer community's effort to develop patches every time a new virus is detected is somewhat analogous to the medical community's effort to look for known pathogens in a community's blood supply before a transfusion is attempted. In the early days of the AIDS epidemic, many innocent people were inadvertently infected via blood transfusions because the doctors at that time had no idea about what causes AIDS. There is no reason to believe that the current blood supply is any safer because we still have no idea what other hitherto unidentified viruses are lurking in there. What is potentially more useful than screening for known pathogens is something analogous to pasteurization – a process by which *all* pathogens are eliminated. In the case of milk, one simply heats the milk. In the case of blood, we have no analog to pasteurization. Computer security community also needs a process analogous to the pasteurization process. Any hope of finding such an analogy is not dependent upon luck, it can only come from a deeper understanding of the

current crop of intrusion detection methods. Many subtle issues are making it difficult to exploit this pasteurization metaphor in the context of computer security.

With the popularity of wireless and mobile networks, attacks have taken a different flavor. Attacks need not be concentrated over a particular direction or link and hence are difficult to detect. Every bit of message is transmitted through an open medium and thus intruders have free access to the data. In such a scenario, security becomes even more challenging. Lack of resources available at the mobile device for processing and encoding of messages makes these considerations much harder to meet than conventional networks.

Cyber Trust

Associated with security, but not synonymous with security, are other issues – privacy and trust. Privacy – from a business point of view – is influenced by how personal information is collected and stored. Almost all businesses collect some information about their customers. They must find a way to manage that information in a responsible manner. How an organization manages confidential information with which it is entrusted speaks a lot about that organization's respect for its customers. Major companies like JetBlue, Mrs. Fields Cookies and Victoria's Secret have learned their lesson with great dismay and cost. Hospitals learned their lesson when they outsourced some of their transcription work to untrustworthy offshore companies.

Trust is a critical element in web-based communities, e-commerce and in influencing the attitudes of just plain folks toward web-based information systems. Trustworthiness is a concept that is intertwined with dependability and security. The attributes of dependability are reliability, availability, integrity and safety while the attributes of security are confidentiality, availability, and integrity. Like pornography, it is easier to recognize an untrustworthy system when you see one than to define it. For example, the National Science Foundation made an attempt to define their vision of CyberTrust, by seeking answers to questions such as:

Can just plain folks justifiably rely on computer-based systems to perform critical functions securely?

Can people justifiably rely on computer-based systems to process, store and communicate sensitive information securely?

Can people justifiably rely on a well-trained and diverse workforce to develop, configure, modify, and operate essential computer-based systems?

Today, one of the most common things happening when a user uses a computer is the trail of records, such as HTTP logs and cookies, left behind. Records of user activity are invaluable tools for research, but every hidden history file is a potential threat to security and individual privacy. Because of this conflict and other proprietary considerations it is becoming almost impossible for academic researchers to work with realistic data.

Consider a simple user transaction. From a naïve user's point of view, trust comes from flexibility of the operation sequence and transparency to what is happening. The solution to the twin problems of security and trust is not to remove all records of activity or make records hard to access, but to provide feedback to users so they know what is being recorded about their transaction and give the user some control and access to what is being recorded about that transaction. This means that we must first understand how people view different types of records of their activity. A user may not mind to leave behind aggregated access patterns so some search engine can be built based on page ranks derived from these access patterns.

Trustworthiness of, say web sites, can be improved by process-oriented, design-oriented or security-oriented features. Different domains inspire trust in different ways. Branding is popular business strategy. Customers flock to a familiar – not necessarily a better – brand. Brand recognition and reputation go hand in hand. To earn that reputation, companies should publish reliable reports of their performance (say, on-time arrival statistics) or they may seek certification from a third party (say, Verisign certification for secure data transfer) and so on. A popular mechanism for building reputation is by tracking the past behavior of earlier participants. Under its Feedback Forum initiative eBay seeks feedback from users and makes it available to all. Amazon.com allows users to submit their own book reviews. Such peer-rating schemes have their own drawbacks.

In view of these considerations, designers of CyberTrust are facing three basic challenges.

Challenge #1: The Distribution of Expertise

This refers to the distribution of knowledge or expertise about computing systems throughout society. The relationships between different categories of users can be visualized as a pyramid built up of several layers. The base level is by far the biggest, for it consists of ordinary people who possess relatively little technical expertise, whose interest in computers is based on the latters' capacity to facilitate communication for transactions, and who often lack access to the expert consultants that users with technical expertise take for granted. The next level is one containing fewer people who routinely use a digital infrastructure to complete work tasks. Doing so requires them to be savvy, sophisticated users (e.g. many business and industry users), although they often have access to technical assistance through formal and informal pathways at work. The third level is that of the individuals with technical expertise in information technology and engineering. Our pyramid is capped by a still smaller number of computing professionals who design and build systems (hardware and software), and whose technical competence provides deeper knowledge of how a computer functions. They typically take for granted operational knowledge that is utterly incomprehensible to most other users.

Challenge #2: Proliferating Devices and Functionality

The second challenge is the proliferation of computing systems, the variety of digital devices, and their increasing functionality. Examples abound:

- Cars are becoming laden with digital devices that increase functionality: navigation systems, sensors that alert drivers when they drift from the center of a lane, remote unlocking from a central place, tracking the position of cars, plug and play diagnostics of vehicles, etc.
- Toys are getting smarter.
- Products from companies such as Nokia are concealing the technology and emphasizing the usability by careful study of every day users and simplifying design and functionality.

Such digital devices are characterized by, among other things:

- shrinking device sizes (e.g. laptop versus desktop)
- greater mobility (e.g. PDAs)
- the specialization of device functionality (and, paradoxically, increasingly diverse functionality of individual devices)(e.g. "smart" cellular phone/cameras)
- a variety of operating systems
- the embedding digital devices in various products (e.g. automobiles with GPS capability)
- incorporating them into larger, geographically distributed systems (e.g. cellular phones that allow users to point and click at a vending machine that then automatically charges the soft drink to their bank account)

Challenge #3: Burgeoning Purposes

Accompanying the proliferation of digital devices and their incorporation into society is an expansion of the purposes to which they are put. It was not so long ago that experts contemplated how ordinary households would ever use personal computers (and be convinced to buy one) which seemed destined to remain in the realms of work and education. The implication here is that concerns about trustworthy computing systems may have as much to do with the nature of information sent, stored, and received as it does with the devices *per se*. Ordinary users may be relatively unconcerned, for example, about the trustworthiness of digital devices and the systems of which they are part, than they are concerned about the use and misuse of particular categories of information. These include:

- health and medical records, such as test results
- personal and family finance, investment and banking data
- specific purchases and larger patterns of consumption
- recreational activities, hobbies, and networks of friends and family
- physical location and movements between locations
- political affiliations.
- educational and training certifications and transcripts

What the Future Holds

No one predicted the Internet and the WWW as we are experiencing them today, although there are people who claim that they “invented” the Internet. No one predicted viruses, worms, spam, phishing, identity theft, and a host of other ills that we are putting up with. So, it would be foolhardy to make predictions in a text book like this. However, there is one prediction we can safely make: Usage of computers, in some form or another will continue to increase. We will continue to face challenges to our security and privacy. Even if the underlying technology changes, there is commonality in the challenges brought forth by these technologies.

The rest of this book introduces some of the techniques and methods that are likely to survive and find their way into the cyber world and help us combat the attendant ills.