6.901 Final Project

REBUILDING THE INTERNET

Amjad Afanah

Asadollah Kalantarian

Abdurrahman Kandil

Abdulrahman Tarbzouni

REBUILDING THE INTERNET

Abstract:

Despite the effectiveness of current security technologies, a major overhaul to the Internet's infrastructure and supporting protocols is needed in order to deal with the ever-increasing security demands of tomorrow's emerging technologies. In order to solve security problems inherent in the current Internet infrastructure, we need to implement one of the following approaches: (1) rebuild the Internet from scratch and renovate existing TCP/IP protocols, (2) add more security enhancement to the current infrastructure and upgrade security patches and authentication procedures. The idea of rebuilding the Internet and upgrading security protocols is great on paper; however, we must also look into the feasibility of such an "invention", and other questions of ownership, incentives, and control. We believe the debate that will surround the new Internet patent debate will mirror that of the software patent debate that is going on today.

REBUILDING THE INTERNET

Outline:

1.0 History & Background on the Internet
- *1.1 The Birth of the Internet*
- *1.2 The TCP/IP Protocol Suite*
- *1.3 The Evolution of the Internet*
- *1.4 The Creation of the World Wide Web & E-Mail*

2.0 Introduction to Vulnerability and Drawbacks of the Current Internet technology
- *2.1 Security: A Crucial Building Block in the Future Picture*
- *2.2 Internet Vulnerability & Security Risks*

3.0 In Depth Look at Internet Security Risks
- *3.1 Understanding TCP/IP*
- *3.2 Security Problems in the TCP/IP Protocol Suite*

4.0 Introduction to Possible Solutions
- *4.1 Rebuilding the Internet from Scratch*
- *4.2 Adding Security Enhancements to the Internet Infrastructure*
- *4.3 The Pros and Cons of Rebuilding the Internet*

5.0 Patent-Related Issues Surrounding Internet security solutions
- *5.1 Introduction to Patents*
- *5.2 How to patent Internet security solutions?*
- *5.3 The Software Patent Debate*
- *5.4 Are Patents the Only Incentive for Innovation*
- *5.5 Questions About Ownership of Internet Inventions*

1.0 History and Background on the Internet

1.1 The Birth of the Internet

In the 1960's, the Air Force was pursuing a reliable method for sustaining command and control in case of a nuclear attack. After extensive studies, Paul Baran of the RAND Institute suggested "packet switching" as the solution. This technology allowed a transmitted message to reach its destination through available routers regardless of any damages to other parts of the network. The Advanced Research Projects Agency (ARPA) believed that packet switching is the best answer to the agency's critical need for continuous information exchange between scientists and military sectors in case of a nuclear attack. The year 1969 marked the birth of the ARPANET; mother of our current INTERNET.[1]

In 1968, ARPA connected the ARPANET to four supercomputers at: University of California at Los Angeles, SRI (in Stanford), University of California at Santa Barbara, and University of Utah. The network was wired together via 50 Kbps circuits.[2]

1.2 The TCP/IP Protocol Suite

Development began on the protocol later to be called TCP/IP, it was developed by a group headed by Vinton Cerf from Stanford and Bob Kahn from DARPA. This new protocol was to allow diverse computer networks to interconnect and communicate with each other.

Vinton Cerf from Stanford and Bob Kahn from DARPA headed a group developing the protocol later to be called TCP/IP .The group's concern was to build a protocol capable of interconnecting different computer networks and allowing them to communicate freely

[1] (Smithsonian.yahoo.com), Birth of the Internet.

[2] Kristula, Dave, "*The History of the Internet*," March 1997

with each other.[3] Since ARPANET was initially supposed to connect four institutes, access was granted to professors and scientists only and was done from mainframes connected by nodes to ARPANET. Hence, TCP/IP was a purely practical technical attempt with no security considerations to interconnect different users through the network. Later on, this protocol was taken as a base for many updates on the ARPANET and today this protocol is considered the backbone of the current INTERNET. Moreover, that same protocol underlies every Internet application, from email to the Web to audio streaming.

Reasonably, that the main objective of ARPANET was only to maintain the constant flow of scientific information between research institutes. The only security measure that was a concern is keeping the network alive in case of a nuclear attack.

1.3 The Evolution of the Internet

The future uses of such a network were not clear back then. No one imagined that a military and scientific based network would someday evolve to a universal network holding crucial applications and sensitive information for nearly every aspect of daily lives. Simply, the Internet rapidly evolved from its predecessor ARPANET while holding on to many legacy features of the old network; most importantly is the lack of security, privacy, and rights management. There is no more confirming evidence than what Vinton Cerf co-inventor of TCP/IP—who's known as the "Father of the Internet"—said in a recent interview when he was asked what would he have done differently given he had the chance to go back and rebuild the Internet, his answer was "I would probably go in and integrate security into the system more fully than I did".[4]

---

[3] Kristula, Dave, "*The History of the Internet*," March 1997
[4] Wingfield, Nick, "*Still Netting after all these years*," CNET.com, March 3, 1997

Starting from 5 networks back in the 1960s, the Internet today interconnects 50,000 worldwide networks with an enormous exchange rate of about 20 trillion bytes a month.[5] The Internet is now an integral part of most of our daily activities, from checking personal email to ordering a pizza from Domino's Pizza's website.

1.4 The Creation of the World Wide Web & E-Mail

The advent of USENET made way for the creation of the Electronic Mail (Email). Then the World Wide Web was formed which made the Internet a more interactive platform for building applications and holding personal information. The WWW holds about 50% of all transactions conducted on the Internet. With all of these developments, the Internet dramatically transformed from a scientific research exchange platform to a universal communication platform covering the whole world which is portrayed as the most optimum way to conduct business and provide services whether it was Business 2 Business (B2B) or Business 2 Consumer (B2C).

2.0 Introduction to Vulnerability and Drawbacks of the Current Internet technology

2.1 Security: A Crucial Building Block in the Future Picture

Increasing commercial use of the Internet has heightened security and privacy concerns. With a credit or debit card, an Internet user can order almost anything from an Internet site and have it delivered to their home or office. Companies doing business over the Internet need sophisticated security measures to protect credit card, bank account, and social security numbers from unauthorized access as they pass across the Internet. Any organization that connects its intranet to the global Internet must carefully control the access

[5] Cerf, Vinton, "*Computer Networking: Global Infrastructure for the 21st Century*," 1995

points to ensure that outsiders cannot disrupt the organization's internal networks or gain unauthorized access to the organization's computer systems and data.

2.2 Internet Vulnerability & Security Risks

Digital disruptions or intrusions that could cause loss of life or that could be part of a coordinated terrorist attack have also become an increasing concern. For example, using the Internet to attack computer systems that control electric power grids, pipelines, water systems, or chemical refineries could cause the systems to fail, and the resulting failures could lead to fatalities and harm to the economy.

Also, the support for legacy code in the current infrastructure posed another threat of lack of privacy for individuals. This can be apparent in the less control the net user is having over the distribution of his personal information and preferences. Moreover, spam is becoming an increasingly annoying and time wasting drawback of using e-mail.

The pinnacle of problems is the ability of hackers to get unauthorized access to sensitive information. The extremely fast spread of viruses in the Internet is another bold vulnerability.

All of these drawbacks, vulnerabilities and weaknesses are reflections of the fast development that has been built on top of the old protocols and infrastructures that were used by ARPANET. The boom that the Internet has had required that organizations and companies move fast to adopt the old protocols and support the legacy structure of the old network. Thus, there wasn't enough time to reconsider some weak aspects of the old network and redefine them to cope with the demands of the new INTERNET. It was simply a chaos. After the transition has been made, scientists began to think about solving

the problems regarding the security side of the INTERNET. Updates after updates have been applied on top of the old protocols but with no effective use.

3.0 In Depth Look at Internet Security Risks

3.1 Understanding TCP/IP

In order to understand the problems associated with the Internet, we need to understand the TCP/IP architecture on which the Internet is based. This section discusses the TCP/IP architecture and provides a basic reference model that explains TCP/IP terminology and describes the fundamental concepts underlying the TCP/IP protocol suite.

The Internet model provided by the Department of Defence (DoD), known as the *DoD reference model*, describes four functional layers that make up the basic infrastructure of the Internet. While the original *DoD Protocol Model* was based on three basic functional layers: network access layer, host-to-host transport layer, and application layer, an additional layer, the *Internetwork layer*, has been added to describe how TCP/IP protocols interact with other layers and provide the basic packet delivery service for all networks (see Figure 1.1)[6].

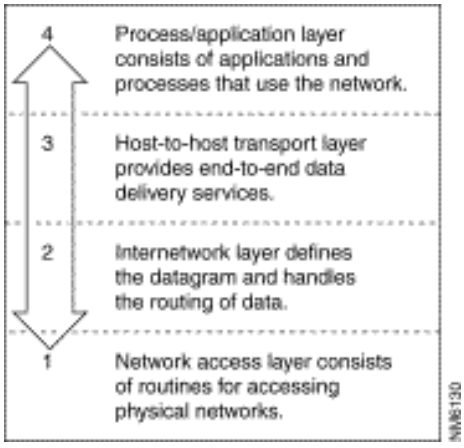

Figure 1.1 showing the *DoD Reference Model* of the Internet
Credit to: DDN Protocol Handbook, Volume 1.

[6] © 1992--2002 Cisco Systems, Inc. "Securing Your Network with the Cisco Centri Firewall"

Each of the layers in the reference model shown Figure 1.1 has its own set of functionalities. The *network access layer* is the lowest layer in the Internet reference model. This layer is responsible for delivering data to the other computers and devices that are attached to the network. The layer above the network access layer is called the *Internetwork layer*.[7] This layer is responsible for routing messages through Internetworks. The *host-to-host transport layer* provides end-to-end data integrity and establishes a highly reliable communication service for parties that want to carry out an extended two-way exchange. The top layer in the Internet reference model is the *application layer*. This layer provides functions for users and their programs, and is responsible for delivering applications. The TCP/IP protocol suite is used by all of the functional layers of the Internet and plays an important role in integrating the functionalities across different levels.

The most important protocol at the network access layer is the *Internet Protocol* (*IP*). Some of the functions performed by IP at the network access layer include encapsulating the IP datagrams into *frames* that are transmitted by the network. By checking the destination address in the header of an incoming packer, the IP protocol can determine whether to deliver the packet directly to the requested address or to pass it to a gateway for delivery. If the destination address is the address of a host on the directly attached network, the packet is delivered directly to the destination. If the destination address is not on the local network, the packet is passed to a gateway for delivery. *Gateways* and *routers* are devices that switch packets between the different physical networks. Deciding which gateway to use is called *routing*. IP makes the routing decision for each individual packet.

[7] © 1992--2002 Cisco Systems, Inc. "Securing Your Network with the Cisco Centri Firewall"

The Transmission Control Protocol (TCP) plays a vital role at the host-to-host transport layer. TCP provides reliable connections by ensuring that data is resubmitted when transmission results in an error (i.e. TCP provides end-to-end error detection and correction). Unlike IP, which contains no error detection or recovery code, TCP is a *reliable, connection-oriented, byte-stream* protocol.

3.2 Security Problems in the TCP/IP Protocol Suite

The fact that IP has no error detection or recovery capabilities has made the protocol unreliable and often vulnerable to security risk. There are a number of serious security flaws inherent in the TCP/IP protocols. Some of these flaws exist because hosts rely on IP source address for authentication. Others exist because network control mechanisms, and in particular routing protocols, have minimal or non-existent authentication.

There are a number of attacks that the TCP/IP protocol suite is susceptible to, including sequence number spoofing, routing attacks, source address spoofing, and authentication attacks.[8] Sequence number prediction in TCP is one of the more important security holes that was first described by Morris.[9] He suggested that a hacker may predict a TCP sequence number and construct a TCP packet sequence without ever receiving any responses from the server. Morris provided evidence for this security flaw by spoofing a trusted host on a local network and documenting his findings.

---

[8] *Bellovin, S.M., "Security Problems in the TCP/IP Protocol Suite"* - Computer Communication Review, Vol. 19, No. 2, pp. 32-48, April 1989

[9] Morris, R.T. 1985. *A Weakness in the 4.2BSD UNIX TCP/IP Software*. Computing Science Technical Report No. 117, AT&T Bell Laboratories, Murray Hill, New Jersey.

Source address spoofing is another security risk inherent in the TCP/IP protocols. IP source routing involves the target host using the reverse of the source route provided in a TCP open request for return traffic, and picking any IP source address desired, including that of a trusted machine on the target's local network. The outcome of an IP source routing attack is full control of all facilities available to target machines by the attacker.

Another security risk that limits the reliability of TCP/IP is the lack of authentication procedures within the *Exterior Gateway Protocol* (EGP). EGP is intended for communications between the core gateways. An exterior gateway is periodically polled by the core. One possible attack would be to impersonate a second exterior gateway for the same autonomous system. The core gateways are not equipped with a list of legitimate gateways to each autonomous system, making it easy for the attacker to use readily available routing information of exterior gateways connected to the network.

Because IP address-based authentication has numerous flaws, some implementations of TCP/IP use the *Authentication Server*. The Authentication Server plays the role of a trusted third party; if a server wishes to know the identity of its client, it may contact the Authentication Server and ask it for information about the user owning a particular connection. While, this method is more secure than simple address-based authentication, there are certain risks that this method is vulnerable to. A security problem that is inherent in the Authentication Server mechanism is that not all hosts are capable of running authentication servers. If the client cannot establish a connection with an Authentication Server, it does not matter who the user is claimed to be; the answer cannot be trusted. Additionally, the authentication message itself can be compromised by routing

table attacks. Such attacks can corrupt transferred messages and can result in the transmission of viruses to all connected hosts.

In summary, the lack of authentication procedures within TCP/IP has led to numerous flaws and security risks inherent in the current TCP/IP protocol suite. These flaws have resulted in the fast spread of viruses, identity theft and spam.

4.0 Introduction to Possible Solutions

4.1 Rebuilding the Internet from Scratch

The current Internet model does not account for any security related layer. Authentication, ID tagging to data is not part of the picture. Security should constitute a layer such that two sides should know and authenticate each other in every single transaction.

Some scientists think that the solution to Internet security problems lies in rebuilding the Internet's current infrastructure and protocols. The way to assure security in critical applications like e-commerce and e-mail can be achieved by simply taking security into consideration from day one in the development process of the new infrastructure. The TCP/IP protocol would be oriented around security as a first priority rather than technical efficiency. Other protocols would follow the same path. Piece by piece the whole infrastructure will be rebuilt around maximum security measures.

There are major obstacles to rebuilding the Internet from scratch. With more than 30 million World Wide Web sites and over 100 million Internet hosts, the transition to a new system is going to be very hard. Many businesses that depend on the Internet for a wide array of services (e.g. e-mail, e-commerce, etc…) will need to adjust to the new transition, a task that is more complicated than it seems. Additionally, with technology changing

everyday, there is no way to predict future security threats. Rebuilding the Internet may prevent current security threats, but there is no guarantee that the new system will stop future risks. Finally, the cost of rebuilding the Internet is very high and may discourage researchers from pursuing Internet security solutions.

The other important thing is a new initiative backed by computer organizations called the Next Generation Secure Computing Base (NGCSB) or Palladium. This is a trustworthy computing move which emphasized the importance of have secure platforms for information exchange. Simply put, the technology revolves around tying software to personal digital certificates in order to assure full security. In other words, every piece of information that is owned by a person will be linked to a digital certificate in a way that only certified applications and data can be read or written by the user.

4.2 Adding Security Enhancements to the Internet Infrastructure

An alternative solution to rebuilding the Internet is adding reliable security enhancements to the current Internet infrastructure. These enhancements would solve security flaws in authentication and IP routing. The two main enhancements that need to be added are: authentication and encryption. The best-known authentication mechanism is the Needham-Schroeder algorithm. It relies on each host sharing a key with an authentication server; a host wishing to establish a connection obtains a session key from the authentication server and passes a sealed version along to the destination. By implementing an authentication mechanism like the Needham-Schroeder algorithm, many of the security flaws within TCP/IP would vanish.

The second enhancement to add is e*ncryption*. Encrypting each packet as it leaves the host computer is an excellent method of guarding against disclosure of information. It also

works well against physical intrusions; an attacker who tapped in to an Ethernet cable, for example, would not be able to inject spurious packets.

Unfortunately there are certain limitations to adding security enhancements. With technology changing everyday, there is no way to predict future security threats. Thus adding security enhancements is not a long-term solution and merely adds complexity to the current Internet infrastructure. Additionally, there is a high cost associated with security enhancements. Encryption devices are expensive, often slow, hard to administer, and uncommon in the civilian sector. Finally, "inventing" security enhancements may give rise to patent-related problems. The debate over patenting Internet security solutions is described in more detail in Section 5.

4.3 The Pros and Cons of Rebuilding the Internet

How is all of this is going to help? Well, it's quite amazing. The rebuilding of the Internet infrastructure and using NGSCB are the perfect combination to achieve an ideally secure environment. With the rebuilding we are assuring that hackers won't gain access to any unauthorized information since all the vulnerabilities will be diminished. With NGSCB, spam and viruses will be abolished due to the fact that the user will only allow reading of certified information and applications. Hence, viruses cannot be certified by security organizations as "safe data" and accordingly won't get certified and accessed. In the same way, personal information will hold certificate tags that will be only readable by specific sites and no more lack of privacy will exist on the INTERNET.

On the other hand, liberals are opposing such initiatives that would assure a more secure INTERNET. Basically, they claim that such a renovation would cause the INTERNET to lose its freedom of information exchange. They say that such an act would

cause there certified information to be fully exposed to government authorities since they're going to be responsible of issuing personal certificates and as they see it, the NSA or any other security organization would do whatever to exploit this chance of dominance over information.

We believe that taking the two initiatives (rebuilding the Internet and using NGSCB like approaches) into action is worth all the efforts and time we're going to spend. By applying these techniques we will assure a brighter future of the information age. We will enjoy greater opportunities in a more secure INTERNET. Freedom will not be diminished but only minimized. There has to be scarifications, a price to pay. In fact, we're not paying much since the outcome is very rewarding. Today we're enjoying the unlimited capabilities of the e-world; just imagine what the progress would be if we were assured that any new addition to the network would certainly assure us security and functionality at the same time. We won't need to be concerned any more about such issues, it will all be fixed. A secure, functional e-world full of great opportunities!

5.0 Patent-Related Issues Surrounding Internet security solutions

The idea of rebuilding the Internet and using NGSCB-like approaches is great on paper, and the prospect of having such an idea materialize is very promising and encouraging. However, we must also look into the feasibility of such an "invention", and other questions of ownership, incentives, and control. There has been a debate over the patentability of very essential needs, and many argue that the Internet has now become a very essential part of our daily lives. Since the Internet is known for its openness and the fact that is a forum for the free exchange of ideas across the world, any tampering with the ownership or control of this Internet will almost definitely restrict the openness of the

Internet. There are many issues to discuss and elaborate upon surrounding the new rebuilt Internet and its patentability and we will attempt to address the most important questions in the next few pages.

5.1 Introduction to Patents

Before delving deep into the debate of the new rebuilt Internet and its patentability, let us define a patent as a set of exclusive rights granted by a state to a person for a fixed period of time in exchange for the regulated, public disclosure of certain details of a device, method, process or substance (known as an invention) which is new, inventive and useful. Since the new rebuilt Internet is new, inventive, and useful, it definitely meets the criteria for a patent. However, just because all of the criteria are met, doesn't mean that one should blindly be given a patent for this invention because the Internet as we know it is such an essential part of our daily lives and the prospect of having a person or organization having the exclusive rights for this patent is mind-boggling.

5.2 How to patent Internet security solutions?

Rebuilding the Internet and using NGSCB-like approaches require some sort of protection from copying, but since this potential invention is very different from most other conventional inventions, we are having a difficult time figuring out how it will be protected. Some may argue that since this new technology satisfies the requisites for a patent, then it should be protected by a patent and the exclusive rights should be granted to the inventor. However, as I mentioned before, the Internet is know for its openness and the fact that it is a forum for the free exchange of ideas across the world, and therefore patenting this new

Internet will definitely restrict this openness. Therefore, many other people argue that this new Internet should not be patentable.

Another interesting argument in favor of *not* allowing the Internet to be patented is the whole idea of the useful arts. Some people argue that an easy way of dodging the whole patentability of the Internet issue is by considering the Internet be a "useful art", thereby making it free and universal. Since the term "useful arts" is very vague, the Government can just say that the Internet falls under the domain of "useful arts", and therefore making it impossible for any inventor to have exclusive rights over it.

The Internet has quickly become a very important part of many people's daily lives, and it's hard to imagine what life would be like without the Internet. The Internet has many uses that are necessary for the daily function of many people, and many people now consider the Internet to be a necessity. Therefore, restricting the Internet by giving a patent to an inventor raises serious concerns with a lot of people. This brings us to the next important question: is there another way to give due credit to inventors besides giving them patents? We believe that this new Internet will and should *not* undergo the same process as all other patents, and that the inventor should *not* have the same exclusive rights to this new technology as the holders of other patents. We believe that the inventor of the new Internet should be given a restricted patent that will not give the inventor exclusive rights to the invention.

5.3 The Software Patent Debate

We believe the debate that will surround the new Internet patent debate will mirror that of the software patent debate that is going on today. Therefore, we believe that understanding the software patent debate will help point out some potential issues that might arise should a new, rebuilt Internet come into the scene. Since widely available software is a relatively new thing, it is sometimes unclear whether software should be covered by patent or copyright. According to the WTO[10], any software written is automatically covered by copyright. This means that the author of the software, the writer of the program code, has exclusive rights over that code and that the direct copying of the program code is illegal. Getting a patent for your software gives the author more restrictive power. For example, getting a patent for certain software covers the programming method itself.

If it is decided that this new rebuilt Internet cannot be patented, then there must be a way in which the inventor is compensated financially for the invention, or should there? Many people believe that America is the leading country in innovation because we have the best patent system in the world. Many argue that without the patent system, there would be no incentive for people to innovate and come up with new inventions and ideas. People with this line of thought think that inventors want to make sure that the hard work and money they put into their inventions will have some pay-offs, and therefore need some sort of financial compensation for their products.

[10] (Trade-Related Aspects of Intellectual Property Rights. April 15, 1994. http://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm visited December 14, 2005)

5.4 Are Patents the Only Incentive for Innovation?

If it was known that no patent will be granted to the inventor of the new, rebuilt Internet, will this important innovation happen because of need anyways? We believe that although the patent system gives *more* incentive for inventors to innovate and develop new products, people will still innovate and invent great things if there is a need for that product. Another important question to ask is: besides money, what other incentives do inventors have to dedicate a lot of time and money into making a new product? We believe that people don't invent things solely for the prospect of making money. Perhaps that might be the case with many companies that are inventing products with the sole purpose of selling them to make products. However, we believe that if there is a certain unmet need that will make the world a better place, then there will be people who are passionate about their work who will try to satisfy this unmet need by inventing something. Another incentive for inventing something is the advancement of science and the dissemination of knowledge, which will ultimately make this world a better place to live in.

5.5 Questions About Ownership of Internet Inventions

It is not inconceivable that, through a wild sequence of events, the new, rebuilt Internet is issued a patent. If this does happen and the new rebuilt Internet was to be patented, who would have control over it? Will ownership and exclusive rights be given to a single inventor, organization, or company? Another question to address in this case is that of fairness. Will the Government or other overarching body have partial ownership to make sure the inventors don't abuse their power and complicate the whole system? These are all serious questions that will be very difficult to answer, but that will ultimately pave the future of the Internet. These questions must be well thought out and resolved carefully and

meticulously, because if these issues are resolved quickly and haphazardly, then the consequences might be dire.

References

- (Smithsonian.yahoo.com), Birth of the Internet.
- Kristula, Dave, "*The History of the Internet*," March 1997
- Wingfield, Nick, "*Still Netting after all these years*," CNET.com, March 3, 1997
- Cerf, Vinton, "*Computer Networking: Global Infrastructure for the 21st Century*," 1995
- © 1992--2002 Cisco Systems, Inc. "Securing Your Network with the Cisco Centri Firewall"
- *Bellovin, S.M., "Security Problems in the TCP/IP Protocol Suite"* - Computer Communication Review, Vol. 19, No. 2, pp. 32-48, April 1989
- Morris, R.T. 1985. *A Weakness in the 4.2BSD UNIX TCP/IP Software*. Computing Science Technical Report No. 117, AT&T Bell Laboratories, Murray Hill, New Jersey.
- (Trade-Related Aspects of Intellectual Property Rights. April 15, 1994. http://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm visited December 14, 2005)