1. Introduction

The Internet is, by far, one of the most significant achievement in recent history. When it was designed and started as Arpanet in 1970s, the Internet was never intended to be secure or open for commercial use. In the 1980s, the Internet was structured to accommodate 4.3 billion potential network addresses. It afforded roughly one address for every person on earth. Yet today, with more than 50 million users on-line, the address space is getting short. The solution, yet to be implemented and deployed, is the Internet Protocol v6 (IPv6), or IP next generation IPng. IPv6 will offer better security and performance and will allow a wide range (up to $3 \times 10^{38}$) of nodes. Nodes will include almost any device anyone can imagine; even sensors, doors, and cars will have IP addresses so they can be controlled from afar. The Internet, as I hope, seems to be the infrastructure for the global village but without security, not only e-commerce is in danger, but also human lives could be at stake.

This paper summarizes the issues the panel will discuss and raise more questions than answers.

2. Internet Without Security

The Internet security has witnessed an explosive and exciting growth in the past two years. Under the surface of excitement lies a mine of technical and commercial challenges. Without solving these challenges, secure systems will not reach the expected potential. The Internet without security infrastructure in place is vulnerable to several attacks. Such attacks include: packet sniffing, monitoring and recording; active attacks (TCP/IP hijacking, IP spoofing); routing infrastructure attacks; protocol design/implementation flaws; and operations problems. Many of these problems exist due to the fact that Internet packets are not encrypted. However, before packet encryption becomes common, the key management problem must be addressed and proper key infrastructure must be deployed.

3. Securing the Internet

This panel is aiming at providing experts’ views about the future trends in Internet security. The panel will address several questions, such as: 1) What kind of certificate and public key infrastructure (PKIX vis-a-vis SPKI) is the appropriate one for the global Internet? 2) the state-of-the-art X.509 certificates solve authentication problem, but what about the authorization problem? 3) firewalls are used as “break walls” where the access from outside the enterprise is almost unattainable. This approach is limiting companies building extranets. What would be the approach to convert firewalls into “glass walls”? 4) what layer(s) (in the ISO model) will security be implemented in. Is it at the IP layer as the Simple Key-management for Internet Protocol (SKIP) and Internet Security Association and Key Management Protocol (ISAKMP) suggest, or at the transport layer as in the Secure Socket Layer (SSL) protocol, or at the application layer such as Secure Shell (SSH) or PGP/Smime e-mail. What are the advantages of such decisions?

4. Internet Security and Government Regulations

For the Internet to become a true infrastructure for the global village, it must continue to be unregulated. Several governments, however, have been trying very hard in the past few years to regulate encryption usage on the Internet. For example, in the U.S., the information industry is not allowed to export soft-
ware with strong cryptography. It is important to note that the Internet dissolves the geographical boundaries among nations.

The Panel will address the impact of the governmental regulations on the future of the Internet.

5. Java and Internet Security

The information industry is heading rapidly towards adopting Java as the programming language for the Internet. Will the Java Sandbox approach be sufficient to fulfill users’ and industrial needs for building the global information infrastructure?

6. Internet Security at the Internet Engineering Task Force (IETF)

At the IETF, there are several working groups related to Internet Security. The groups are:

- IPSEC (Internet Protocol Security);
- PKIX (Public Key Infrastructure based on X.509) and SPKI (Simple Public Key Infrastructure);
- DNSSEC (Secure Domain Name Service);
- Secure Shell (SSH);
- TLS (Transport Layer Security);
- Encrypted Mail (S/MIME, PGP);
- SOCKS (firewall traversals); and
- General Security Services (GSS).

The panel will give a brief update of the status of the IETF work.

7. Impact of New Technologies

7.1. Smart Cards

Industry studies indicate that there could be some 2.5 to 3 billion smart cards in use by the turn of the century. Major users of these joint smart card technologies are forecast to include telecommunications, banks, hotels, airlines and insurance companies as well as healthcare providers and governments. Smart cards, however, are limited in their processing power and storage capacity which most security algorithms require. How will the industry solve these shortages; and what impact smart cards have on enhancing individuals’ security?

7.2. Web Push Technology

The well known World Wide Web (WWW) is based upon the http (hyper text transfer protocol). The older version of the http protocol allows only information to be pulled by a client from a server. Recent proposals suggests a peer-to-peer relation between the client and the server, where the server will be able to push some content to client(s). Will push technology invade individuals’ privacy and create a flooded Internet; or should it be regulated to become subscription based?

8. Conclusion and Future Challenges

It is not fair fetched to think that any electric device can be connected to the Internet. These devices include small to complex ones. Most of the current security algorithms, such as RSA for example, are computational intensive and require substantial processing power. This power, however, is not available in small devices like sensors. Therefore, there is a need for designing a light-weight security algorithms.

What is going to drive the Internet security is the set of applications more than anything else. Will the information industry rise to the expectation and go beyond the desire to monopolize the Internet and work together to provide the needed applications? Will governments open the national boundaries and stop regulating the encryption technology? Will it be possible to build Intranet/Extranets and Virtual Private Networks with full security? Finally, will the Internet and e-commerce rise to the expectation and flourish in the global village? The answers to these questions are yet to be seen.