Futures Abstracts

The essential pieces for solving the cyber security puzzle are described in terms of what is needed to gain strategic advantage over the increasing threats of the early 21st century at a time when information systems are becoming critical and pervasive.

Historical Context: Fundamental Trends, Limitations, Alternative Futures

Modern information technology began to emerge at the end of World War II with the invention of the von Neumann computer architecture in 1945 and the transistor in 1947. The impact of these inventions was accelerated with the invention of the integrated circuit along with progressively more advanced technologies for processing, storing, and communicating information through the end of the 20th century. The Internet and Scalable Parallel Systems further accelerated the process in the 1980s along with the development of the associated software and systems to enable ubiquitous information systems with wired and wireless access. These advances have enabled extraordinary growth including information systems that have become critical to a wide range of activities including National Security.

Threats in Cyber Space: Global Characterization

The continued growth of the Internet is challenged by increasing threats. The challenges are limiting the transition of information systems from the ubiquitous systems of the 20th century to the more advanced pervasive systems needed for the 21st century that are also capable of supporting critical applications. The horrendous events of 9/11 illustrate the need to overcome these challenges and achieve critical and pervasive trustworthy information systems. A characterization of threats in cyber space from individual hackers to the higher grade threats of criminal activities to transnational terrorists and beyond to advanced information warfare of nation states is described in general terms. The continued geometric growth in vulnerabilities, exploits, and incidents is explained in terms of the limitations of the existing generally used information system technology base. An overall framework is presented.

Intrinsic Trust: Essential Pieces

A new approach to achieving trusted systems, called Intrinsic Trust is presented with an explanation of how it overcomes threats in cyber space by providing effective geometric advantage. The approach builds on selected existing and emerging technologies to enable fundamental strength of information systems on the existing Internet by 2012 while preparing for the further advances needed for Internet 2020.

Internet 2020: Achieving Critical Pieces by 2012

A vision for the Internet achievable by 2020 is presented. Internet 2020 will be as fundamentally more advanced than the existing Internet as the existing Internet was from the plain old telephone system (POTS) that existed before the Internet. Internet 2020 will operate as an evolutionary extension of the Internet while having revolutionary capabilities including Intrinsic Trust. The critical pieces for solving the cyber security puzzle through Intrinsic Trust can be available by 2012 for critical applications.

Integrated Reality: Achieving Strategic Advantage

A vision for fundamentally more advanced systems, called Integrated Reality, enabled by Internet 2020 is presented. Integrated Reality includes Terabits to desktop Teraops systems that provide full immersion virtual reality operating at the limits of human acuity. The system includes access to extraordinary performance services operating in the context of distributed sensor networks. Integrated Reality systems will, among other things, support the use of ensembles of faster than real time simulations of high fidelity physics based models. A variety of applications will be described across the private and public sectors in a global context including critical and pervasive trusted systems for finding and connecting the dots.