Escaping Cyber Flatland

Stephen L Squires, PhD

Abstract for Invited Keynote
Security and Privacy Engineering (SPREE) Workshop
June 16, 2011
Carnegie Mellon University
Pittsburg, PA

There are three generally believed assumptions about Cyber Space.

1. The "hackers" have an asymmetrical advantage over their targets and always will …
2. If this problem could have been solved since the invention of the transistor then it would have …
3. Even if there was an effective solution now it is too late …

These are the assumptions of Cyber Flatland.
Every one of these assumptions is wrong

… outside of Cyber Flatland!

The fundamental trends, limits, and alternative futures of Cyber Space will be characterized starting from the invention of the transistor over 50 years ago. The threats in Cyber Space are real and have been increasing as the value of the information increased and the systems became more interconnected and accessible. The CERT Curves that were first published in the open following the formation of the CERT at the SEI have demonstrated continued geometric growth in terms of vulnerabilities, exploits, and incidents. The systems in other sectors that may not be as interconnected as the open Internet systems do not, in general, use any technology that is fundamentally stronger than the systems on the open Internet. The use of certain relatively stronger crypto systems, firewalls, user authentication, and personal security reviews have only provided relative separation among otherwise weak systems.
All these systems are essentially operating in Cyber Flatland.

The concept of Cyber Flatland will be introduced and characterized as limiting the ability to bend and break the continued geometric growth of the CERT Curves. An alternative future will be introduced and characterized in terms of a system of technologies to enable effective engineerable geometric advantage over the threats in a given context. The system of technologies is based on advanced results that have emerged since the first DARPA investment in IT and IS in cooperation with NSA in the mid 1960s. Advanced results were produced and demonstrated decades before their time. Advanced IS was generally not adopted because of the apparent near term economic advantage of the extraordinary growth of IT, accelerated by the Internet, without any significant IS advances. The export control policies of the Cold War era also slowed the transition. As a result, IS transition was artificially retarded relative to IT advances. Escaping Cyber Flatland can be achieved by recognizing the additional dimensions that advanced IS brings to IT and the ability to cost effectively engineer systems to achieve effective geometric advantage over the threats in a given system context.

The challenge of the early 21st century is to understand the fundamental science, technology, and policy history of IT and IS over past 60 years. Application of the additional dimensions will provide the opportunity to gracefully transition advanced IS to existing and new IT systems. Recognizing the additional dimensions of Cyber Space is an essential first step for Escaping Cyber Flatland.