ITU-T Workshop

“New Horizons for Security Standardization”

Abstract

Geneva, 3 –4 October 2005

Speaker:	Miroslaw Kula **GTECH Corporation**
Session:	**4**: **Stakeholder Perspectives**
Title of Presentation:	**IT Systems Security in High Speed Transaction Processing** How is it different and? Can standardization help?

Building, deploying and operating high speed Transaction Processing (TP) systems is a discipline wherein many challenging aspects of Information Technology and Networking intersect, thereby creating an environment where well-established, commonly-used technical solutions are often deemed inadequate.

All successful providers of product and services for high speed TP markets quickly realize that making incremental improvements to established design patterns and frameworks do not yield satisfactory results when trying to meet the extreme requirements of throughput, response time, availability, and very strict cost constraints required by these systems. Targeted, specialized solution architectures and design patterns are consequently created, at a minimum for those components of the systems that are located directly on the transaction path.

Under these circumstances, maintaining adequate system security is not a trivial matter. The topic becomes even more interesting if and when one is committed to a high level of system openness by following technology and industry standards.

As the industry develops IT and Networking standards, to what degree do we need to be cognizant of their impact on performance and cost of the systems they are meant to be adopted in?

Should a measure of complexity, performance impact, and, potentially, increased system cost be one of the metrics and/or adoption criteria for any standard under consideration?

Security is a dimension of an IT system that is difficult to address when performance and cost perspectives are seriously considered. Generally, security only matters when it fails. When it works properly its quality is considered higher the more “invisible” it is. Is it possible to introduce IT security measures that never fail, do not materially impact performance, and are added at a relatively negligible cost? Can these three demands be reconciled? Can standardization help?