"Apparently, the only thing Americans learned from Prohibition is that it doesn't work to prohibit *alcohol*." – M. Miller

THE CENTER FOR INFOSEC STUDIES AND RESEARCH
INVITED LECTURE SERIES

Immunity from Viruses, Safety from Geeks Bearing Gifts

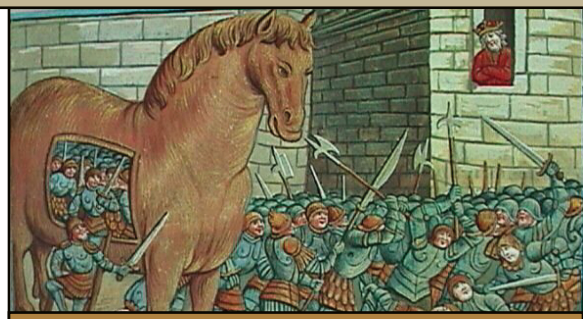
Mark S. Miller
CTO - Combex, Inc., Open Source Coordinator - ERights.org

Thursday, May 9th at 1400 in Spanagel 421

Why is it so hard to make our computer systems safe from viruses? Why are these systems so vulnerable to Trojan horses? Because the security model they are built on is incapable of limiting access at the right level of granularity. The fact that was forgotten (by non-capability practitioners) is that we grant privileges to people and enforce access control on processes or objects. That's why your email program can launch a virus; it runs with the privileges granted to you.

This talk is centered on a demo of CapDesk, our capability-based distributed desktop and application installation/launching framework. CapDesk uses no passwords, no user group lists, no firewalls, yet supplies a computing world invulnerable to viruses and Trojan horses. We'll show a web browser built on these principles but with malicious components activated under CapDesk, and compare the results of the attack with an attack on a Winix (Windows or Unix, it makes no difference) desktop using the same code.

CapDesk is built on E, our distributed capability language. Capabilities bundle designation with authority. Capability practitioners have long understood the great economy of mechanism this bundling provides for security programming -- benefits we experienced while building CapDesk. CapDesk additionally applies this bundling principle to its user interface architecture, in order to provide similar benefits to our users.



Mr. Miller is the co-inventor of the agoric paradigm of market-based distributed secure computation. A co-founder of the Vulcan project at Xerox PARC, he is a pioneering designer of secure distributed programming languages including Vulcan for Xerox PARC, Trusty Scheme for Autodesk, Joule for Agorics, Tclio for Sun Labs, and E for Electric Communities, ERights.org, and Combex. At Autodesk, he was the chief architect of a pioneering hypertext system that anticipated many of the Web's virtues. He is a co-founder of Agorics, a successful startup company established to capitalize on the agoric computing vision. He is a co-director of the Agorics Project at George Mason University, researching market-based computing ideas. Mr. Miller is an inventor on 7 patents in the areas of cryptographic protocols, automated combination-auctions, and distributed secure object systems.