Safely Redistributing Untrusted Code Using .NET

Abstract:
Reusing software components is a textbook software engineering best practice. Developers reuse components written by others, combining them in unique ways to create new software products. Reusing software components can create a significant security risk, as these reused components may behave badly, either by malicious intent or negligence on the part of their authors.

The .NET framework provides fine-grained mechanisms for specifying how software should be trusted. Permissions are granted based on the source of software, and where it currently resides (on the local disk, or in a particular internet zone). Unfortunately, these trust guarantees are difficult to manage, and there is no guarantee that an end-user receiving a redistributed untrusted component will correctly set its trust level.

We provide a framework with a set of easily understood trust levels, and a simple mechanism for applying these trust levels both to already-compiled applications and libraries within the .NET framework. This will allow both end-users and software developers to leverage the work of others, while maintaining guarantees that this software will not, intentionally or otherwise, cause damage to their systems or leak confidential information. This tool should provide significant opportunities for code reuse with security and should be easily extended to handle related applications, such as those using compiled Java class libraries.

Dr. Martin C. Carlisle
US Air Force Academy

Reception to follow in CSSE Lounge (Dunstan 103)