.net column

.NET Code Access Security

Vandaag de dag zijn veel computersystemen onderling gekoppeld en worden ze vaak bloot gesteld aan code die afkomstig is uit verschillende, vaak onbekende bronnen. Code kan als bijlage zijn toegevoegd aan een e-mail of worden gedownload over het internet. Helaas hebben veel computergebruikers uit eerste hand ervaren wat het effect is van destructieve mobiele code zoals virussen en wormen, die data kunnen beschadigen of vernietigen.

De meeste security mechanismen geven rechten aan gebruikers op basis van hun logon credentials (combinatie gebruikersnaam en wachtwoord) en beperken de toegang tot resources (vaak bestanden en mappen) waarvoor de gebruiker bevoegd is. Deze aanpak houdt echter geen rekening met de volgende aspecten:

- Gebruikers verkrijgen, zoals gezegd, code uit verschillende bronnen, waarbij niet alle bronnen betrouwbaar blijken te zijn;
- Code kan bugs of kwetsbaarheden bevatten die benut kunnen worden door destructieve code;
- Code doet soms dingen, waar de gebruiker geen weet van heeft.

Het resultaat hiervan is dat computersystemen kunnen worden beschadigd en gevoelige gegevens kunnen worden verstuurd als gebruikers deze destructieve- of 'buggy' software gebruiken. Voor het security mechanisme van de meeste besturingssystemen geldt dat elk onderdeel van de code volledig 'vertrouwd' moet worden om uitgevoerd te kunnen worden, behalve wellicht voor scripts op een webpagina.

Hierdoor is er behoefte aan een breed toepasbaar security mechanisme, dat toestaat dat code afkomstig van het ene computersysteem veilig kan executeren op een ander computersysteem, zelfs als er geen relatie is tussen de systemen.

Om een computersysteem te beschermen tegen destructieve mobiele code biedt het .NET Framework een security mechanisme dat code access security wordt genoemd. Code access security maakt het mogelijk om aan code verschillende niveaus van vertrouwen toe te kennen, afhankelijk van de herkomst van de code en andere aspecten van de identiteit van de code, zoals bijvoorbeeld de aanwezigheid van een digitale handtekening. Code access security dwingt de verschillende niveaus van vertrouwde code ook af, waardoor de hoeveelheid code die volledig vertrouwd moet worden om correct te kunnen executeren kan worden geminimaliseerd.

Code access security werkt volgens het principe dat de code (assembly) zelf een bepaalde mate van bewijs overhandigt aan de Common Language Runtime. Dit bewijs wordt door de CLR gebruikt om op basis van de ingestelde security policy te bepalen welke set van rechten (permissions) wordt toegekend aan de assembly. Indien de mobiele code een beveiligde resource wil benaderen, bijvoorbeeld het filesysteem, dan wordt er door de betreffende klasse uit de .NET Framework class library een zogenaamde demand permission uitgevoerd voor het benaderen van het filesysteem. Dit heeft tot gevolg dat de CLR zal controleren of het benodigde recht wel is toegekend aan de assembly en zo niet, dan wordt een security exception gegenereerd.

Met de komst van code access security is een nieuw security model geïntroduceerd dat bescherming geeft tegen destructieve mobiele code. Code access security maakt een scheiding tussen de credentials waarmee de gebruiker is ingelogd (dus ook waarmee processen worden gestart) en de rechten die aan de code worden toegekend. Zo is het mogelijk dat, ondanks het feit dat een applicatie draait met administrator credentials, de code toch geen toegang krijgt tot bepaalde systeemresources. Het verzorgen van code access security is een samenspel van de Common Language Runtime en de .NET Framework class library. De .NET Framework class library zal voor alle beveiligde resources een demand permission afdwingen, waarbij de CLR verantwoordelijk is voor de controle of de assembly wel beschikt over het benodigde recht.

Ing. Xander Buffart is werkzaam als IT-architect bij Info Support te Veenendaal (e-mail: xanderb@infosupport.com).