SBIR cyber security

Projecttitel:	**Secure Information Grid**
Bedrijf:	**Coblue Cybersecurity**
In samenwerking met:	**n/a**

Projectsamenvatting

De doelstelling van het Secure Grid project was tweeledig. Ten eerste had het project als doel om een "**Secure Information Grid**" te ontwikkelen: een software infrastructuur- en middleware-laag die zorgt voor veilige opslag en communicatie van data. Secure Grid technologie is gebaseerd op decentrale dataopslag in combinatie met geavanceerde cryptografie. Het resultaat is een infrastructuurlaag die zeer robuust is tegen kwaadwillenden (hackers, DDoS aanvallen, etc.), schaalbaar is, en data decentraal versleuteld opslaat. In Figuur 1 worden verschillende eigenschappen van het Secure Information Grid genoemd. Bedrijfsapplicaties ontwikkeld op Secure Grid erven deze kwaliteiten. Zo maakt deze technologie het mogelijk om 'secure-by-design' applicaties te ontwikkelen. Het cybersecurity probleem wordt hiermee bij de wortel aangepakt.

De tweede doelstelling van het project was het ontwikkelen van een veilige *collaboratie tool* op basis van Secure Grid technologie die direct inzetbaar is binnen het Nederlandse bedrijfsleven (inclusief grootbedrijf). Dit product noemen we **Storro**.

Storro is een gebruiksvriendelijke en zeer veilige manier om samenwerking en bestandsdeling te realiseren. Storro faciliteert: revisiebeheer (altijd mogelijk om terug te gaan naar historische versies), real-time back-up, audit trail en samenwerking in één gebruiksvriendelijke sterk geïntegreerde omgeving.

Deze nieuwe applicatie kan gezien worden als een veilige variant op huidige cloud storage en bestandsdelingdiensten. Toch zijn er enkele belangrijke verschillen met de huidige alternatieven voor deze dienst, zowel in technische zin als in functionele zin, zoals:

Geavanceerde cryptografie. Storro maakt gebruik van de hoogste standaarden op het gebied van software-encryptie. Ook biedt het de mogelijkheid het bestandssysteem aan te koppelen als mountable/drive. Dit betekent dat de bestanden nooit onversleuteld op de harde schrijf staan (zoals ook in TrueCrypt wordt gedaan).

Decryptiesleutels uitsluitend in het bezit is van de bestandeigenaar(s). Qua techniek is een eerste belangrijk verschil dat de encryptie- en decryptiesleutel uitsluitend in het bezit is van de bestandeigenaar(s). Het probleem bij bijvoorbeeld Dropbox is dat de encryptiesleutels in het bezit zijn van Dropbox. Dit maakt Dropbox zelf een ideaal doelwit voor hackers en kwaadwillenden – met een enkele hack kan de hacker toegang krijgen tot talloze documenten en bestanden. Storro werkt zonder een centraal key storage system. Dit maakt Storro minder kwetsbaar.

Decentrale opslag. Een ander technisch verschil zit in de distributie van opslagcapaciteit. Met Storro worden bestanden decentraal opgeslagen. Dit betekent dat er geen centrale database is, maar dat alle data in kleine stukken wordt verdeeld en versleuteld wordt gedistribueerd over het netwerk van de secure collaboration tool gebruikers. Door de encryptie blijven bestanden beveiligd tegen ongeautoriseerde toegang. De 'file hartslag sensor' registreert hoe vaak een stuk data bestaat in het netwerk. Wanneer de redundantie van het data stuk te laag is, wordt deze gekopieerd om de redundantie op pijl te houden. Wanneer het systeem dat een bestand bevat uit het netwerk wordt genomen (door bijvoorbeeld een herinstallatie, schade, of diefstal) blijft de data veilig opgeslagen in het netwerk. Met andere woorden, Storro biedt een veilige en continue off-site back-up dienst. En door het werken zonder een centrale component is Storro zeer robuust en schaalbaar.

Rechtensysteem cryptografische afgedwongen. Het rechtenbeheer binnen Storro wordt cryptografsich afgedwongen. Met andere woorden: de autorisaties van gebruikers worden niet softwarematig bepaald, maar wordt bepaald door het wel of niet bezitten van de juiste sleutel die nodig is om een document te ontsleutelen. Dit geeft een zeer sterke beveiliging tegen ongeautoriseerde verspreiding van en toegang tot documenten. Het rechtensysteem biedt ook verregaande functionaliteit voor het afdwingen van bedrijfsbeleid. Een gebruiker kan specifieke autorisaties voor lezen en schrijven, maar in de toekomst ook voor bijvoorbeeld downloaden, printen en versturen, op bestandsniveau vastleggen. Zo kan de informatiebeveiliging binnen een bedrijf daadwerkelijk op het dataniveau plaatsvinden.

Geïntegreerd versiebeheer. Daarnaast biedt de secure collaboration tool ook de functionaliteit van een geïntegreerd versiebeheer. Hierdoor wordt het mogelijk om de bewerkingsgeschiedenis van een document (of databestand) te bekijken en kunnen voorgaande versies van een document worden teruggehaald.

Toepassingen

Door het combineren van deze eigenschappen kunnen verschillende toepassing worden ontsloten. Zo kan aan een aantal use cases worden voldaan. Momenteel hebben wij 15 verschillende use cases geïdentificeerd, die zijn weergegeven in de onderstaande figuur.

Voor vragen over het beschreven project kan contact opgenomen worden met Coblue via info@coblue.eu of telefonisch op 053-8200924.