Bert Greevenbosch
Fraunhofer-Institut für Integrierte Schaltungen, Abteilung Audio
Am Wolfsmantel 33, 91058 Erlangen, Duitsland
bert.greevenbosch@iis.fraunhofer.de

Column Wiskundigen in den vreemde

Werken bij de oosterburen

Bert Greevenbosch, nu drie jaar verbonden aan het Fraunhofer Institut für Integrierte Schaltungen in Erlangen, Duitsland, studeerde in 2005 af bij Derk Pik in Leiden op een onderwerp op het grensgebied tussen audio en wiskunde. Door deelname aan een studentenuitwisselingsproject met China, kreeg hij de smaak van het reizen goed te pakken, en vond een passende onderzoeksbaan.

Mijn studie wiskunde aan de Universiteit Leiden heb ik in 2005 afgesloten met een afstudeerproject op het gebied van audio. Ik heb mij in die tijd beziggehouden met het scheiden van audiosignalen, waarbij de focus lag op het extraheren van één bepaald muziekinstrument uit een opname van meerdere instrumenten. Het project heeft mijn interesse voor digitale signaalverwerking gewekt en omdat ik na mijn studie naar het buitenland wilde, was een sollicitatie bij het *Fraunhofer Institut für Integrierte Schaltungen IIS* (kort: Fraunhofer IIS) in Erlangen, Duitsland een voor de hand liggende keus. Het Fraunhofer IIS is een van de 56 instituten van het Fraunhofer Gesellschaft. Al deze instituten houden zich bezig met toegepaste wetenschap. Elk instituut richt zich op een eigen onderzoeksveld en de instituten werken in hoge mate onafhankelijk van elkaar. Fraunhofer IIS is het grootste Fraunhofer instituut en houdt zich onder andere bezig met de ontwikkeling van audio- en videocodecs, medische technologie, digitale radio en satellietnavigatiesystemen. Een van de bekendste ontwikkelingen van Fraunhofer IIS is het audioformaat MP3.

Ik werk in de audioafdeling en heb als werkterrein de ontwikkeling en standaardisering van Digital Rights Management (DRM)-systemen. Bij deze systemen wordt een digitale inhoud (bijvoorbeeld een film) cryptografisch versleuteld geleverd. De sleutel wordt apart, in een licentie, gegeven. Naast de sleutel staan in die licentie ook de gebruiksvoorwaarden, zoals het maximaal aantal keren dat de inhoud afgespeeld kan worden of de datum tot wanneer de licentie geldig is.

Naast het feit dat DRM-systemen het maken van roofkopieën moeilijker moeten maken, maken ze ook nieuwe businessmodellen mogelijk. Zo maakt DRM een online-videotheek mogelijk, waarbij de gebruiker bijvoorbeeld voor een klein bedrag het recht koopt om een film drie dagen te huren. De gebruiker krijgt dan de versleutelde film plus een licentie om de film drie dagen te kunnen afspelen. Na drie dagen verloopt de licentie, tenzij de gebruiker de huur verlengt door het kopen van een nieuwe licentie.

In technisch opzicht komt het verkopen of verhuren van inhoud dus neer op het verkopen van licenties. Om er zeker van te zijn dat licenties nageleefd worden, moet de sleutel tot de inhoud cryptografisch beveiligd worden geleverd. Het hoofdbestanddeel in de ontwikkeling van DRM-systemen is daarom het ontwikkelen van cryptografische protocollen en sleutelmanagement. Verder moet worden vastgelegd hoe een DRM-apparaat met licenties om moet gaan. Het apparaat moet er bijvoorbeeld voor zorgen dat een inhoud die drie keer afgespeeld mag worden, inderdaad niet meer dan drie keer afgespeeld wordt. Het is daarom belangrijk dat de protocollen en apparaatspecificaties goed geanalyseerd en beveiligd worden om te voorkomen dat hackers de licentievoorwaarden kunnen omzeilen.

Het DRM-systeem waar ik aan werk, OMA DRM, wordt niet alleen ontwikkeld door het Fraunhofer IIS. Aan de ontwikkeling van de standaard wordt deelgenomen door meerdere bedrijven uit de hele wereld binnen een standaardiseringslichaam genaamd de Open Mobile Alliance™ (OMA). Deze organisatie stelt een technische specificatie van de standaard op, een document waarin precies beschreven staat hoe een OMA DRM-implementatie eruit moet zien.

Om zo'n wereldwijd project in goede banen te leiden, zijn regelmatig conferenties nodig. Daarom vlieg ik bijna maandelijks naar allerlei landen in Azië, Amerika en Europa. Tijdens deze conferenties doen de deelnemende bedrijven, waaronder ook het Fraunhofer IIS, technische voorstellen. Die worden in de specificatie opgenomen, mits ze voldoende ondersteuning krijgen. Het is daarom niet alleen belangrijk om met goede voorstellen te komen, maar minstens zo belangrijk is dat duidelijk uitgelegd wordt waarom die voorstellen goed zijn.

Het leven bij de oosterburen is aangenaam en aan tradities is geen gebrek. In de winter wemelt het hier van de kerstmarkten, compleet met Glühwein- en Bratwurstbuden. In mei zeggen de Erlangers dat de berg roept, wat betekent dat er weer Bergkrichweih is: een festival vergelijkbaar met het Oktoberfest in München. Op het werk wordt op z'n tijd op Weißwürste mit süßem Senf getrakteerd, meestal rond 11:45u, want volgens de traditie moeten die worstjes voor 12 uur gegeten zijn.