Open source software voor Defensie

Lkol B. Smid MBT

Ante Pugnantibus Adsum

Inleiding

Defensie is afhankelijk geworden van ICT. Effectief en efficiënt optreden van eenheden vereist integratie van sensoren, wapensystemen en bevelvoeringondersteunende systemen en zonder de inzet van computers en de daarop aanwezige software is dit onmogelijk.
Met het aannemen van de motie Vendrik in 2002 werd de basis gelegd voor de toepassing van Open source software binnen de overheid. De doelstelling van deze motie was het actief stimuleren van Open source software in de publieke sector door concrete en ambitieuze doelstellingen. Eén van deze doelstellingen was ervoor te zorgen dat in 2006 alle door de publieke sector gebruikte software aan open standaarden zou voldoen. Het programmabureau Nederland open in Verbinding (NoiV) ondersteunt overheden bij de uitvoering van op deze motie gebaseerd beleid. Toch blijkt het gebruik van Open source software niet zo eenvoudig, al was het maar door de diverse inzichten over de kwaliteit en inzetmogelijkheden van deze software en de onduidelijkheid over de aanbesteding ervan.

In dit artikel wil ik kort ingaan op het ontstaan, het belang en de mogelijkheden van Open source software voor Defensie. Gezien de complexiteit van het onderwerp zal ik mij beperken tot een globaal overzicht. De geïnteresseerde lezer kan de links in de voetnoten gebruiken voor verdere informatie.

Geschiedenis

De geschiedenis van Open source software begint in de jaren 80 van de vorige eeuw als Richard Stallman, een doorgewinterde software ontwikkelaar aan het Massachusetts Institute of Technology, zich gaat inzetten voor wat hij vrije software noemt. Zijn doel is software te gaan ontwikkelen waarvan de broncode vrij beschikbaar is voor bestudering en aanpassing en zeker te stellen dat aanpassingen op hun beurt ook weer vrij beschikbaar zijn. Hij start daartoe het GNU-project en richt in 1985 de Free Software Foundation op, die als juridische bescherming van deze software de GPL-licentie[1] (GNU Public Licence) uitbrengt. Begin jaren 90 krijgt de beweging een enorme impuls doordat de door Linus Torvalds ontwikkelde Linux kernel deel van het GNU-project gaat uitmaken en onder de GPL-licentie beschikbaar wordt gesteld. Inmiddels werken over de hele wereld vrijwilligers en bedrijven aan een gestage uitbreiding en kwaliteitsverbetering van Open source software. Het idee dat deze software wordt gemaakt door wereldvreemde nerds in achterkamertjes kan hiermee naar het land der fabelen worden verwezen.

Het idee van Open source als concept blijkt inmiddels ook bruikbaar buiten de

software-industrie. Zo zijn er initiatieven op het gebied van auto's[2], OpenCola en Vores Øl Bier. Hierbij zijn ontwerpen en recepten vrij beschikbaar voor gebruik en verfijning, mits deze daarna weer vrijgegeven worden.

Open source of Open standaard

Als we spreken over Open source software dan wordt vaak de relatie gelegd met het begrip open standaarden. Hoewel in bijna alle Open source software open standaarden worden geïmplementeerd zijn de twee begrippen niet synoniem. Bij Open source software gaat het primair over de vrijheid om wijzigingen te mogen aanbrengen aan bestaande software.
Bij open standaarden gaat het om het voldoen aan door internationale instanties vastgestelde standaarden. Onder open standaarden vallen onder meer de door de Internet Engineering Task Force (IETF[3]) vastgestelde standaarden voor het Internet en de door de Institute of Electrical and Electronics Engineers (IEEE) vastgestelde standaarden op onder meer communicatiegebied.
Open standaarden bieden daarmee de mogelijkheid van (informatie-)uitwisseling tussen producten van verschillende fabrikanten en meer algemeen tot technische interoperabiliteit. Hierdoor zijn hopen standaarden een effectief middel tegen leveranciersafhankelijkheid.

Open source software en open standaarden zijn dus onvergelijkbare grootheden, maar beiden van groot belang voor systeemontwikkeling.

Open source versus Closed source

Het overgrote deel van door Defensie gebruikte applicaties zijn niet van het type Open source. De broncode is niet vrij beschikbaar wat dit type software de naam closed source geeft. Ook mag dit type software niet worden aangepast of verder verspreid.
Vanaf de komst van de eerste Open source software is de publieke discussie over de voor- en nadelen van de ene soort ten opzichte van de andere soort losgebarsten en het debat hierover zal nog wel even voortduren. De belangrijkste argumenten die hierbij worden gehanteerd zijn:

Kosten
Omdat Open source software door de GPL-licentie vrij verspreid mag worden, scoort dit type software natuurlijk goed als het gaat om aanschafkosten, zeker als het gaat om een schaalgrootte zoals we die bij Defensie kennen. Ditzelfde geldt voor de onderhoudskosten zoals updates. Dit is één van de redenen voor de grootschalige toepassing van Open source in serverparken.

Flexibiliteit
Door de vrij beschikbare broncode kan de software worden aangepast ten behoeve van integratie in grotere software projecten of afwijkende gebruiksomstandigheden binnen Defensie. Een bijkomend voordeel is dat in Open source software bijna altijd open standaarden worden gebruikt.

Gebruikersvriendelijkheid
Hier heeft Open source een inhaalrace achter de rug, omdat de software van huis uit door ingewijden werd gebruikt en grafische gebruikersinterfaces ontbraken. De laatste jaren is de gebruikersvriendelijkheid echter zodanig toegenomen dat Open source distributies als OpenSuse, Red Hat en Ubuntu zich in een steeds stijgend aantal gebruikers mogen verheugen.
Door het ontbreken van een overkoepelende architectuur voor Open source software is de integratie van applicaties soms minder goed geregeld als bij die van closed source software. Dit verschil tussen open- en closed source software wordt treffend beschreven in Eric S. Raymonds boek The Cathedral & the Bazaar[4].

Veiligheid
Het is inmiddels duidelijk dat het credo "security through obscurity", dat vaak als argument door fabrikanten van closed source software wordt gehanteerd, niet opgaat. Erkende internationaal bekende experts als Bruce Schneier[5] hebben aangegeven dat Open source een voorwaarde moet zijn voor beveiliging omdat de code geïnspecteerd kan worden. Dit heeft echter alleen zin als de organisatie ook beschikt over personeel die deze inspectie kan uitvoeren.

Ondersteuning
De ondersteuning van closed source software is inmiddels niet meer alleen een zaak van de community die de software voortbrengt. In de afgelopen jaren zijn grote internationale bedrijven[6] gaan meewerken aan Open source software en hebben zij winstgevende bedrijfsmodellen rond het onderhoud ervan ontwikkeld.

Implementatie
Als nadeel van Open source software wordt vaak de kosten voor omscholing genoemd. Deze kosten moeten echter worden opgebracht bij elke overgang naar een ander product en zijn daarom niet specifiek voor het gebruik van Open source software.
Wel is een gedegen begeleiding van de overgang naar Open source software voor zowel eindgebruikers als systeembeheerders van doorslaggevend belang gebleken voor het succes van de implementatie en moet speciale aandacht worden besteed aan data migratie.

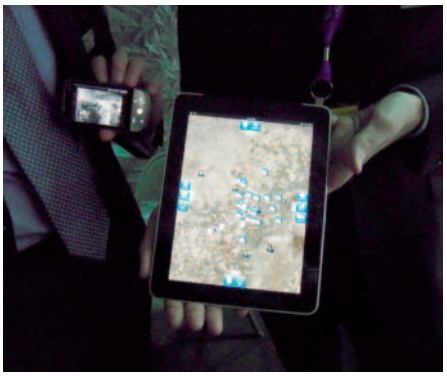
Het belang van Open source software voor Defensie

Het belang van Open source software komt voornamelijk uit de aspecten kosten, flexibiliteit en veiligheid.
Het aspect kosten volgt, zoals eerder aangegeven, rechtstreeks uit de schaalgrootte binnen Defensie. Hierbij moet in de eerste plaats worden gedacht aan toepassing in de kantooromgeving.
Het aspect flexibiliteit volgt uit de, uit kostenoverwegingen genomen, beslissing om Defensie voor bevelvoeringsondersteunende systemen te laten optreden als systeemintegrator. Integratie van sensoren, bevelvoeringondersteunende- en wapensystemen op landgebonden en maritieme platformen kan slechts plaatsvinden op basis van open standaarden en Open source software.
Het aspect veiligheid heeft volop de aandacht gelet op de steeds toenemende dreiging van cyberwarfare. De toepassing van Open source besturingssystemen met speciale maatregelen op beveiligingsgebied zoals SELinux[7] en varianten van de Berkeley Software Distributie (BSD) zijn hiervan voorbeelden.

Gebruik van Open source software

Kijken we naar het gebruik van Open source binnen Defensie dan valt allereerst het gebruik[8] binnen de Amerikaanse DoD op. In projecten als GRASS[9], een Open source geografisch informatie systeem dat in de jaren 80 en 90 van de vorige eeuw door de U.S. Army Construction Engineering Research Laboratories is gebouwd en nog steeds verder wordt ontwikkeld, is ervaring opgedaan met de toepassing van dit soort software.

Tegenwoordig wordt er binnen de DoD zeer veel Open source software toegepast en is het beleid gericht op het minimaliseren[10] van obstakels voor het gebruik. Actuele experimenten met informatiesystemen voor uitgestegen soldaten laten zien dat toepassing van Open source besturingssystemen als Android de snelle realisatie van operationeel te beproeven systemen[11, 12] mogelijk maakt.



Open source informatiesysteem voor de uitgestegen soldaat

Gebruik binnen de Nederlandse Defensie laat een wat genuanceerder beeld zien.
Beleidsmatig is de toepassing van Open source software verankerd in de beleidslijnen ICT-08: Defensie kiest voor open standaarden en ICT-09: Defensie kiest voor het gebruik van Open source producten.
Enerzijds wordt er binnen Ivent, het CAMS en C2SC volop gebruik gemaakt van Open source software. Voorbeelden van gebruik in de kantooromgeving zijn de experimenten Telestick en de alternatieve Mulan werkplek, beiden gebaseerd op de Ubuntu[13] distributie. Bij de realisatie van systemen voor de operationele omgeving als Guardion, Titaan, Isis, Osiris en Afsis wordt gebruik gemaakt van een veelheid van Open source componenten.
Daarnaast wordt er binnen de HDIO actief gewerkt aan beleid voor het gebruik van Open source software.
Anderzijds blijkt de verwerving van Open source software nog onvoldoende ingebed bij de overheid zoals Mathieu Paapst in zijn dit jaar gepresenteerde tussenrapportage van zijn promotieonderzoek[14] aantoont. Defensie vormt hierop helaas geen uitzondering.

Hoe nu verder?

Zoals aangegeven kan Open source software bijdragen aan kostenreductie, systeemintegratie en veiligheid. Er moet echter voor worden gewaakt om Open source software tot doel op zich te verheffen. De toepassing van Open source software moet aantoonbare toegevoegde waarde opleveren op de aangegeven aspecten. Daarnaast kan ook de toepassing van open standaarden, zoals vastgelegd in de NATO Interoperability Standards and Profiles (NISP[15]), bijdragen aan leveranciersonafhankelijkheid.
We moeten ons hierbij realiseren dat niet alle closed source applicaties vervangen kunnen worden door Open source equivalenten. Ook moet bij de implementatie veel aandacht worden besteed aan de begeleiding van gebruikers en systeembeheerders en de migratie van data. Voorzichtigheid bij migratie is dus geboden, zoals vele voorbeelden uit de civiele wereld[16] ons leren. Een aanpak gebaseerd op het principe “Open source tenzij” gecombineerd met het “comply or explain principe” lijkt hier het meest effectief.
Hierbij is gelijktijdige actie om meerdere fronten het meest zinvol. Op overheidsniveau moet de Algemene Regelgeving bij IT-overeenkomsten (ARBIT[17]) verder in overeenstemming worden gebracht met de motie Vendrik en de uitwerking door NoIV om de verwerving van op open software gebaseerde systemen te vergemakkelijken. Bij HDIO zal het beleid betreffende Open source software verder moeten worden uitgewerkt. Bij Ivent en binnen de DMO zal de toepassing in experimenten en systemen onverminderd moeten doorgaan en moeten leiden tot vermindering van kosten en verhoging van veiligheid.

Conclusie

Open source software biedt Defensie voordelen op het gebied van licentiekosten, flexibiliteit en veiligheid. Activiteiten met Open source software door Ivent , CAMS en C2SC moeten daarom, waar mogelijk, verder worden uitgebreid zodat naast de top-down benadering ook een serieuze bottom-up benadering gaat plaatsvinden. Beperkingen dan wel onduidelijkheden op verwervingsgebied moeten worden weggenomen, zodat Open source software volwaardig kan worden meegenomen bij aanbestedingen. Als Defensie ten volle wil profiteren van de kansen die de stormachtige ontwikkelingen in met name de mobiele telefonie doormaken, is het negeren van deze software geen optie.

Lkol Bert Smid MBT (1956) is sinds 1995 in diverse rollen betrokken bij de ontwikkeling van softwarezware systemen. Vanaf de oprichting van het C2SC in 2001 is hij hoofd van de sectie Systeemontwikkeling. In 2006 is hij overgegaan van de Verbindingsdienst naar de Technische Staf. Zijn vrije tijd besteedt hij, naast hardlopen en stijldansen, aan open source software in het algemeen en de Ubuntu-distributie in het bijzonder. Bert Smid is getrouwd met Gerry en vader van Sander (1981) en Michiel (1984).

1. www.gnu.org/licenses/gpl.html
2. www.theoscarproject.org
3. www.ietf.org
4. http://www.opensource.nl/bazaar.html
5. http://www.schneier.com/
6. *www.**linuxfoundation.org**/sites/main/files/publications/**whowriteslinux**.pdf*
7. http://www.nsa.gov/research/selinux/
8. http://cio-nii.defense.gov/sites/oss/index.shtml
9. http://grass.fbk.eu/
10. http://cio-nii.defense.gov/sites/oss/2009OSS.pdf
11. http://www.wired.com/dangerroom/2010/10/special-forces-want-android-apps-for-warzone-john-mad-dens/#ixzz13mvTjml9
12 http://www.wired.com/dangerroom/2010/10/tracking-the-bad-guys-yeah-theres-an-app-for-that/
13 http://www.ubuntu.com/
14 http://www.rug.nl/staff/m.h.paapst/ICTbeleidenaanbestedingspraktijk.pdf
15 http://en.wikipedia.org/wiki/NATO_Interoperability_Standards_and_Profiles
16 http://www.ch-open.ch/presse/pressemitteilungen/pressemitteilung100920.html
17 https://zoek.officielebekendmakingen.nl/stcrt-2010-11138.html