

Profiel MINIX 3



Amsterdam, 13 februari 2006

MINIX 3: een veilig en betrouwbaar besturingssysteem



Sinds kort is een nieuw open-source besturingssysteem voor de PC beschikbaar: MINIX 3. Dit besturingssysteem is ontwikkeld aan de Vrije Universiteit Amsterdam met het oog op *veiligheid* en *betrouwbaarheid*. MINIX 3 is klein van opzet en heeft een nieuwe, modulaire opbouw waardoor het systeem niet kwetsbaar is voor veel van de bestaande problemen met besturingssystemen zoals Windows, maar ook Linux. MINIX 3 is gratis verkrijgbaar en in de eerste maanden na de release is het systeem al meer dan 50.000 maal gedownload.

Door Jorrit Herder, Herbert Bos, Ben Gras, Philip Homburg en Andrew S. Tanenbaum

Hoewel veel mensen Linux en Mac OS zien als concurrenten van het alom bekende Windows, zijn deze besturingssystemen op dezelfde leest geschoeid en hebben ze daarmee veelal dezelfde tekortkomingen als Windows. Al deze systemen hebben een *monolitisch ontwerp* waarbij het hele besturingssysteem als één groot programma, ook wel de de 'kernel' genoemd, draait---zonder bescherming tussen de verschillende functies en met alle mogelijke toegangsrechten. Door de benodigde interactie met de hardware zitten device drivers (stuurprogramma's) ook in de kernel van deze systemen. Dit ontwerp leidt ertoe dat een enkele fout in een willekeurige device driver, bijvoorbeeld de printer driver, het hele systeem kan laten 'crashen'. MINIX 3 daarentegen, heeft een modulaire opbouw waardoor dergelijke problemen kunnen worden voorkomen. Daarnaast kunnen veel fouten zelfs automatisch worden verholpen zonder dat de gebruiker hier iets voor hoeft te doen. In dit artikel zullen we het ontwerp van MINIX 3 in meer detail presenteren en laten zien hoe het bijdraagt aan de veiligheid en betrouwbaarheid van besturingssystemen.

MINIX 3 vanuit historisch perspectief

Het besturingssysteem MINIX kent een rijke historie, die teruggaat naar de jaren tachtig van de vorige eeuw. De eerste versie van MINIX is in 1987 geschreven door Prof. Andrew S. Tanenbaum van de Vrije Universiteit Amsterdam en was bedoeld als onderwijsinstrument. MINIX heeft een voor die tijd revolutionair *multiserver ontwerp* waarbij belangrijke onderdelen van het besturingssysteem, waaronder het bestandsysteem en het geheugenbeheer, als onafhankelijke programma's bovenop een kleine 'microkernel' draaien. Zoals we straks zullen zien, biedt deze modulaire structuur vele voordelen ten opzichte van monolitische systemen. De kleine omvang en modulaire opbouw van MINIX maken het besturingssysteem eenvoudig te doorgronden. De source code van MINIX is gepubliceerd als appendix in het bijbehorende boek "Operating Systems Design and Implementation". Wereldwijd gebruiken vele universiteiten MINIX nu voor hun onderwijs over de basisprincipes van besturingssystemen.

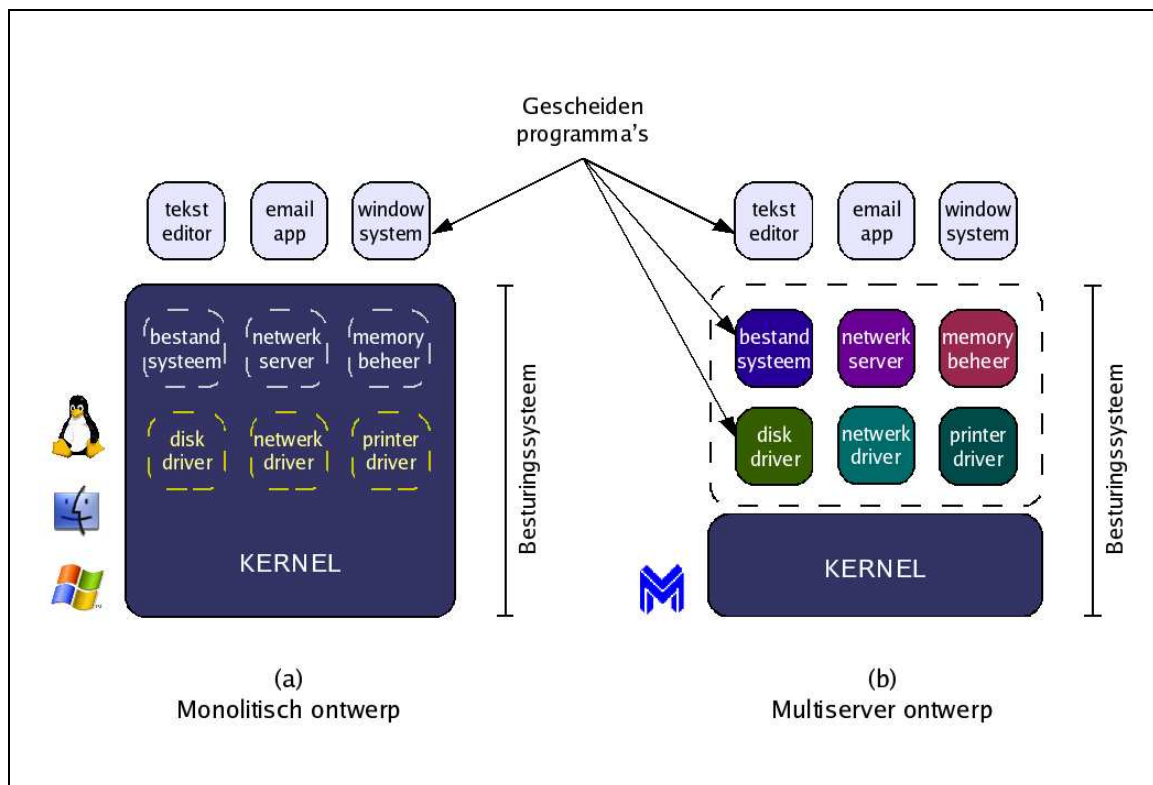
Eerdere versies van MINIX inspireerden Linus Torvalds tot het schrijven van het bekende open-source besturingssysteem Linux. Hoewel Torvalds zowel het MINIX boek als het besturingssysteem tot zijn beschikking had, heeft hij niet voor een multiserver ontwerp gekozen. In plaats daarvan heeft hij Linux een traditioneel, monolithisch ontwerp gegeven waarbij alle functies van het besturingssysteem weer in de kernel zitten. Deze stap terug in de tijd resulteerde in 1992 in een wereld-beroemde discussie tussen Tanenbaum en Torvalds op de USENET nieuwsgroep comp.os.minix: "Linux is obsolete" (Linux is achterhaald).

Door de tekortkomingen aan standaard besturingssystemen zoals Windows and Linux, is het onderzoek aan en de ontwikkeling van MINIX in 2003 weer opgepakt door de afdeling Computer Systemen van de Vrije Universiteit Amsterdam. Tijdens zijn afstuderen en daarna als promovendus heeft Jorrit Herder het ontwerp van MINIX geanalyseerd en het systeem omgebouwd tot een geheel modulaair systeem waarbij nu ook alle device drivers als aparte programma's buiten de kernel draaien. Verdere ontwikkeling met het oog op veiligheid en betrouwbaarheid heeft geleid tot de eerste publieke release van MINIX 3 eind 2005, die in de eerste maanden na de bekendmaking al meer dan 50.000 maal is gedownload.

Hoe werkt MINIX 3?

Voor de gebruiker werkt MINIX 3 net als andere besturingssystemen. Het besturingssysteem stuurt de hardware aan en biedt de gebruiker een vriendelijke interface om de computer te bedienen. MINIX 3 ondersteunt meerdere gebruikers tegelijkertijd en heeft dezelfde mogelijkheden als een normaal UNIX systeem. De standaard command line interface ondersteunt meerdere 'virtual terminals'. Er zijn al meer dan 300 UNIX programma's geschreven voor of overgezet naar MINIX 3, waaronder verschillende shells (*ash, bash, rsh*), tekst editors (*ed, emacs, vi, elle*), compilers en interpreters (*awk, cc, gcc, perl, python*), netwerk programma's (*telnet, ftp, lynx, mail, talk, wget*), bestand hulpmiddelen (*cat, cp, mv, dd, tar, zip*), systeembeheer hulpprogramma's (*adduser, backup, fsck, mkfs, mount, cron*), etc. En recent is ook een grafische interface, het *X Window System*, naar MINIX 3 overgezet.

Tot zover de overkomsten met UNIX. Technisch gezien zit MINIX 3 echter heel anders in elkaar. Zoals reeds genoemd, hebben traditionele UNIX systemen een monolitisch ontwerp, waarbij het hele besturingssysteem in de kernel zit. Dit maakt het systeem kwetsbaar, omdat de kernel alle mogelijke rechten heeft en zelfs een kleine fout de werking van het hele systeem kan verstoren. MINIX 3 heeft daarentegen een multiserver ontwerp, waarbij de kernel sterk is gereduceerd en het besturingssysteem is gesplitst in onafhankelijke modules met beperkte rechten. De microkernel bevat alleen de meest basale functionaliteit om de rest van het besturingssysteem te ondersteunen. De MINIX 3 kernel houdt bijvoorbeeld bij welke programma's actief zijn, bepaalt welk programma wanneer en hoe lang mag draaien en levert eenvoudige functies waarmee de modules van het besturingssysteem met elkaar kunnen communiceren. Dergelijke communicatie gebeurt door kleine berichten uit te wisselen. Alle functies die niet per se in de kernel hoeven te zitten, zoals het bestandssysteem, geheugenbeheer en alle device drivers die de hardware aansturen, draaien als aparte programma's. Deze programma's werken samen om de functionaliteit van een UNIX besturingssysteem te bieden. Het verschil tussen MINIX 3 en het traditionele monolitische ontwerp dat onder andere door Windows, MacOS en Linux wordt gebruikt, is geïllustreerd in figuur 1.



Figuur 1: (a) Structuur van monolitische systemen zoals Linux en Windows zonder bescherming tussen de verschillende functies; (b) Het multiserver ontwerp van MINIX 3 waarbij alle modules van het besturingssysteem als gescheiden programma's draaien.

Veiligheid en betrouwbaarheid van MINIX 3

De modulaire structuur van MINIX 3 is zeer belangrijk voor de veiligheid en betrouwbaarheid van het besturingssysteem. Doordat het besturingssysteem niet langer één geheel vormt, is het mogelijk om bescherming tussen de verschillende modules aan te brengen, zodat fouten in één module zich niet kunnen verspreiden naar andere modules. Ook is het mogelijk de rechten van elke module nauwkeurig af te bakenen, waardoor de schade die een fout zou kunnen aanrichten tot een minimum beperkt blijft. Deze bescherming van MINIX 3 is vergelijkbaar met het gebruik van compartimenten bij schepen: als een lek optreedt, stroomt alleen dat bepaalde compartiment vol en niet het hele ruim, zodat het schip blijft varen.

Uit onderzoek naar de betrouwbaarheid van besturingssystemen blijkt dat de device drivers in Linux 3 tot 7 maal meer fouten bevatten dan de rest van de kernel. Dergelijke fouten kunnen in traditionele besturingssystemen tot grote problemen leiden omdat een fout in de driver van je printer het hele systeem kan aantasten. Onder Windows wordt bijvoorbeeld 85% van alle crashes door drivers veroorzaakt. Daarom zijn in MINIX 3 alle device drivers afgeschermd van de rest van het systeem. Zo draait de printer driver als een apart programma en heeft alleen toegang tot de printer. Een eventuele fout kan ertoe leiden dat de printer niet meer aangestuurd kan worden, maar kan niet langer het hele systeem ontregelen.

Omdat de kernel alle rechten heeft en dus de bescherming tussen de programma's kan omzeilen, is het zeer belangrijk dat de kernel correct functioneert. Er zijn verschillende studies gedaan naar de dichtheid van fouten in software met uitkomsten tot maar liefst 75 fouten per 1000 regels code. Om het aantal fatale fouten te beperken, is het dus van groot belang om de kernel zo klein mogelijk te maken. De Linux kernel omvat zo'n 2,5 miljoen regels code, wat met een voorzichtige schatting van 10 fouten per 1000 regels code betekent dat deze 25.000 fouten bevat. Bij Windows is het probleem zelfs een factor 10 groter. De kernel van MINIX 3 omvat daarentegen slechts 4000 regels code, waardoor het aantal fouten in het meest kwetsbare deel van het besturingssysteem veel kleiner zal zijn. De beperkte omvang van de kernel maakt het systeem ook eenvoudig te begrijpen en te bouwen, wat de kans op fouten nog kleiner maakt.

Een ander aspect van MINIX 3 dat tot meer betrouwbaarheid leidt, is de mogelijkheid om automatisch fouten te herstellen. De modules van het besturingssysteem worden gecontroleerd door een speciale module, de *reincarnatie server* geheten, die verantwoordelijk is voor de juiste werking van het systeem. Wanneer een netwerk driver onverhoopt vastloopt, wordt deze automatisch verwijderd uit het systeem en vervangen door een nieuw exemplaar. Ook kan de systeembeheerder automatisch met een e-mail op de hoogte gebracht worden van het probleem. Dit alles gebeurt zonder interventie van de gebruiker en leidt slechts tot een kleine vertraging van het systeem. Eventuele openstaande netwerk verbindingen worden niet beïnvloed, zodat bijvoorbeeld de Internet browser blijft werken. Experimenten laten zien dat het ophalen van een groot bestand van Internet slechts 8% langer duurt wanneer er elke 4 seconden een fout optreedt in de netwerk driver en deze herhaaldelijk opnieuw gestart moet worden. Deze eigenschappen maken MINIX 3 niet alleen geschikt voor de PC, maar ook voor systemen die zeer betrouwbaar moeten zijn, zoals de ingebedde computers van auto's, vliegtuigen of ruimtesondes.

MINIX 3 is niet alleen betrouwbaar, maar ook een veilig besturingssysteem. De bescherming van MINIX 3 voorkomt namelijk ook veel beveiligingsproblemen die worden veroorzaakt door fouten in de software. Veel virussen en wormen maken bijvoorbeeld misbruik van zogeheten 'buffer overrun' fouten om hun eigen code in het systeem te injecteren en uit te voeren. Doordat de code van alle programma's door MINIX 3 beschermd wordt, is het uitvoeren van geïnjecteerde code niet langer mogelijk en zijn zulke fouten veel moeilijker te misbruiken. Wanneer een aanval leidt tot een foutieve handeling of afwijkend gedrag in een deel van het besturingssysteem, dan merkt de reincarnatie server dit direct en zal de slecht functionerende module vervangen door een nieuw exemplaar. Een interessant voorbeeld is de zogenaamde 'ping of death' waardoor een kwaadwillend persoon een Windows server kon laten crashen met een enkel fout verzoek vanaf het Internet. Moderne varianten van de ping of death zijn recentelijk aangetroffen in de interactie met de 'remote desktop server' van Windows. Een dergelijke aanval zal in MINIX 3 slechts een lokale fout veroorzaken, waarna het besturingssysteem zich in de meeste gevallen automatisch kan herstellen.

Tot slot

MINIX 3 is een nieuwe besturingssysteem dat is ontworpen met het oog op de veiligheid en betrouwbaarheid voor de eindgebruiker. In tegenstelling tot traditionele systemen zoals Linux en Windows is het besturingssysteem opgesplitst in gescheiden modules met beperkte rechten, zodat programmeerfouten en andere problemen zich niet door het systeem kunnen verspreiden. Hierdoor wordt de schade die een fout kan aanrichten beperkt. Doordat de modules van MINIX 3 klein en eenvoudig zijn, kunnen ze gemakkelijk begrepen en beheerd worden, waardoor de kans op fouten vermindert. Omdat de werking van het besturingssysteem continu gecontroleerd wordt en foutieve modules automatisch gedetecteerd en vervangen worden, is MINIX 3 uiterst geschikt voor systemen die zeer betrouwbaar moeten zijn.

Momenteel wordt er aan de Vrije Universiteit Amsterdam actief onderzoek gedaan om de veiligheid en betrouwbaarheid van MINIX 3 nog beter te maken en het systeem verder te ontwikkelen. Daarnaast is er een groeiende gemeenschap van geïnteresseerden en vrijwilligers die aan het systeem bijdragen.

Het MINIX 3 besturingssysteem, alle source code, documentatie, nieuws en achtergronden zijn te vinden op de officiële website: www.minix3.org. Probeer MINIX 3 ook zelf!

Meer informatie

- Bezoek de officiële MINIX 3 website (www.minix3.org) voor een download en meer informatie of ga naar de nieuwsgroep (comp.os.minix) voor discussies over MINIX 3.
- "Operating Systems Design and Implementation, 3e editie." Andrew S. Tanenbaum en Albert S. Woodhull. Prentice-Hall, 2006. ISBN: 0-13-142938-8.
- Voor meer informatie of vragen over MINIX 3 kunt u ook contact opnemen met Jorrit Herder <jnherder@cs.vu.nl> van de Vrije Universiteit Amsterdam.