Samenvatting

Dit hoofdstuk biedt een beknopte Nederlandse samenvatting van dit academisch proefschrift met als titel *"Het bouwen van een betrouwbaar besturingssysteem: Foutbestendigheid in MINIX 3"*. Hoofdstuk 7 bevat een uitgebreidere Engelse samenvatting en gaat dieper in op de onderzoeksbijdragen.

Een van de grootste problemen met computers is dat ze niet voldoen aan de verwachtingen van gebruikers ten aanzien van betrouwbaarheid, beschikbaarheid, veiligheid, etc. Een onderzoek onder Windows-gebruikers liet bijvoorbeeld zien dat 77% van de klanten 1 tot 5 fatale fouten per maand ondervindt en de overige 23% van de klanten maandelijks zelfs meer dan 5 fatale fouten ervaart. De oorzaak van deze problemen ligt in het besturingssysteem ("operating system") dat een centrale rol heeft in vrijwel elk computersysteem. De meeste fouten zijn terug te leiden tot stuurprogramma's voor randapparatuur ("device drivers") die relatief foutgevoelig zijn. Dergelijke stuurprogramma's zijn nauw geïntegreerd in het besturingssysteem, waardoor fouten zich gemakkelijk kunnen verspreiden en het hele besturingssysteem kunnen ontregelen. Dit probleem doet zich niet alleen voor bij standaard besturingssystemen voor de PC, zoals Windows, Linux, FreeBSD en MacOS. Besturingssystemen voor mobiele apparatuur (bijvoorbeeld telefoons, PDAs, fotocamera's, etc.) en ingebedde computers (bijvoorbeeld in auto's, pinautomaten, medische apparatuur, etc.) zijn veelal gebaseerd op een vergelijkbaar ontwerp waardoor ze soortgelijke problemen kennen.

Onbetrouwbare besturingssystemen veroorzaken niet alleen persoonlijke frustraties, maar hebben ook grote maatschappelijke consequenties zoals economische schade en veiligheidsrisico's. Dit onderzoek heeft zich daarom tot doel gesteld om een uitermate betrouwbaar besturingssysteem te bouwen dat fouten in stuurprogramma's kan weerstaan en herstellen. Deze doelstellingen zijn gerealiseerd door het besturingssysteem foutbestendig ("fault tolerant") te maken zodat het normaal kan blijven functioneren ondanks het optreden van veel voorkomende problemen. Hierbij hebben we voortgebouwd op recente technologische vooruitgang en ingespeeld op de veranderende eisen en wensen van gebruikers. Aan de ene kant biedt moderne computer hardware betere ondersteuning voor het afschermen van foutgevoelige stuurprogramma's. Aan de andere kant is de rekenkracht van computers zodanig toegenomen dat technieken die voorheen te kostbaar waren nu praktisch

toepasbaar zijn. Daarnaast is de snelheid van desktop PCs tegenwoordig ruim voldoende en leggen steeds meer gebruikers de nadruk op betrouwbaarheid.

In dit onderzoek promoten we het gebruik van een modulair besturingssysteem ("multiserver operating system") dat compatibiliteit met UNIX waarborgt, maar stuurprogramma's en systeemtoepassingen net als gewone gebruikerstoepassingen in een onafhankelijk proces uitvoert. Dit model combineert hardware-bescherming met software-technieken om stuurprogramma's te isoleren, zodat getriggerde fouten minder schade kunnen aanrichten. In ons ontwerp hebben we twee strategieën toegepast om de foutbestendigheid verder te verhogen: (1) fout isolatie ("fault isolation") om de tijd tussen fatale fouten te vergroten ("mean time to failure") en (2) foutherstellend vermogen ("failure resilience") om de benodigde tijd voor het repareren van fouten te verkleinen ("mean time to recover"). Beide aspecten zijn in gelijke mate van belang voor het verhogen van de beschikbaarheid van het besturingssysteem. Naast de hogere foutbestendigheid bieden modulaire besturingssystemen ook vele andere voordelen: een korte ontwikkelingscyclus, een vertrouwd programmeermodel en eenvoudig systeembeheer.

Om onze ideeën te kunnen testen, hebben we van het open-source besturingssysteem MINIX 3 gebruikt. MINIX 3 voert stuurprogramma's, systeemtoepassingen en gebruikerstoepassingen uit in onafhankelijke processen. Slechts een klein deel van het besturingssysteem, bestaande uit zo'n 7500 regels programmacode, draait met alle rechten van de computer en controleert de rest van het systeem. Communicatie tussen de verschillende onderdelen van het besturingssysteem is alleen mogelijk door berichten van proces naar proces te kopiëren. Wanneer een gebruikerstoepassing bijvoorbeeld een bestand van de harde schijf wil lezen, moet deze een bericht sturen naar de systeemtoepassing voor het bestandssysteem, dat vervolgens een bericht stuurt naar het stuurprogramma voor de harde schijf. Eén van de uitbreidingen op MINIX 3 is een systeemtoepassing die alle stuurprogramma's beheert ("driver manager"). Deze component maakt het mogelijk om systeemtoepassingen en stuurprogramma's te starten en te stoppen zonder de computer opnieuw te hoeven starten. Het zorgt er tevens voor dat de stuurprogramma's strikt van elkaar en van de rest van het besturingssysteem worden afgeschermd en het kan veel voorkomende fouten in stuurprogramma's detecteren en automatisch herstellen.

Hoewel veel van de gebruikte ideeën en technieken op zich niet nieuw zijn, was hun gecombineerde potentieel om de betrouwbaarheid van besturingssystemen te verbeteren nog niet voldoende onderzocht en overtuigend aangetoond. Door dit te doen met behulp van MINIX 3 levert dit proefschrift de volgende wetenschappelijke en praktische bijdragen:

- Het laat zien hoe de betrouwbaarheid van besturingssystemen kan worden verbeterd met behoud van het vertrouwde UNIX-programmeermodel. In tegenstelling tot aanverwant onderzoek, is alleen het binnenwerk van het besturingssysteem vernieuwd. Hierdoor kan compatibiliteit met bestaande software worden behouden en is praktische toepassing stapgewijs mogelijk.

- Het classificeert de geprivilegieerde verrichtingen van stuurprogramma's die ten grondslag liggen aan het verspreiden van fouten en bespreekt voor elke klasse een reeks fout-isolatie technieken om de schade die fouten kunnen veroorzaken te beperken. Dit resultaat is van belang voor elke poging om stuurprogramma's af te zonderen ongeacht het besturingssysteem.

- Het introduceert een ontwerp dat het besturingssysteem in staat stelt om een breed scala aan fouten in belangrijke componenten automatisch te detecteren en te repareren zonder gebruikerstoepassingen te onderbreken en zonder tussenkomst van de gebruiker. Veel van deze ideeën zijn van toepassing in een bredere context dan besturingssystemen alleen.

- Het evalueert de effectiviteit van het gepresenteerde ontwerp door middel van uitgebreide tests met door software nagebootste fouten. In tegenstelling tot eerdere projecten, zijn letterlijk miljoenen fouten nagebootst, waardoor ook veel sporadisch voorkomende fouten opgespoord konden worden en verbeterde betrouwbaarheid met een hoge mate van zekerheid is aangetoond.

- Het beschrijft hoe recente hardware virtualisatie technieken gebruikt kunnen worden om beperkingen van bestaande fout-isolatie technieken te overwinnen. Tegelijkertijd bespreekt het enkele resterende tekortkomingen in huidige PC-hardware waardoor zelfs volledig afgezonderde stuurprogramma's het besturingssysteem nog steeds kunnen laten vastlopen.

- Tot slot heeft dit onderzoek niet alleen geleid tot een ontwerp, maar is dit ontwerp ook geïmplementeerd, met als resultaat het besturingssysteem MINIX 3 dat publiek beschikbaar is via de officiële website http://www.minix3.org/. Dit foutbestendige besturingssysteem maakt duidelijk dat de voorgestelde aanpak praktisch toepasbaar is.

Samenvattend kunnen we concluderen dat met dit onderzoek naar het bouwen van een foutbestendig besturingssysteem, dat bestand is tegen de gevaren van de foutgevoelige stuurprogramma's, een stap is gezet in de richting van meer betrouwbare besturingssystemen.