Universiteit van Amsterdam

Virtualisatie

Virtualisatie en Virussen

20 mei 2016

Tutor:
Robin Klusman

Practicumgroep:
A2

Cursus:
Besturingssystemen

Student:
Sander Hansen
10995080

1 Inleiding

In dit literatuuronderzoek zal er gekeken worden naar het gebruik van virtualisatie om computers te beschermen tegen virussen. Het begrip virtualisatie, dat nader zal worden toegelicht, biedt perspectief op het gebied van het beschermen tegen virussen.

Omdat computers door bijna iedereen gebruikt worden tegenwoordig, hebben virussen ook op vrijwel iedereen effect. Het is daarom belangrijk dat er onderzoek gedaan wordt naar deze virussen, waarbij virtualisatie een steeds grotere rol gaat spelen. De maatschappelijke relevantie is hier logischerwijs uit te concluderen. Dat ook bedrijven hier mee bezig zijn toont het patent dat is aangevraagd op het beschermen van anti-virus *software* met behulp van virtualisatie aan. [Wang et al.(2012)Wang, Lorch, and Parno]

Er is veel onderzoek gedaan naar wat virtualisatie kan beteken bij de bescherming tegen virussen en onderzoek daar van. Openbare onderzoeken die de verschillende aspecten hiervan toelichten en vergelijken zijn er echter nog niet. Daarom is het belangrijk om te kijken waar we op dit moment staan met de bescherming van computers tegen virussen met behulp van virtualisatie.

1.1 Vraagstelling

Omdat de maatschappelijke relevantie groot is en er veel onderzoek naar losse onderdelen binnen dit gebied is gedaan, maar deze nog niet aan elkaar zijn gekoppeld. Kunnen we de volgende vraag stellen;

Hoe kan virtualisatie gebruikt worden om computers te beschermen tegen virussen?

1.2 Virtualisatie

Allereerst is het belangrijk om te begrijpen wat virtualisatie inhoudt en wanneer dit toegepast kan worden. Virtualisatie maakt het mogelijk om op dezelfde hardware meerdere besturingssystemen tegelijkertijd te laten draaien. Om virtualisatie mogelijk te maken kan er gebruik gemaakt worden van speciale *software* die de *hardware* vanuit een hoofdbesturingssysteem onderverdeeld over verschillende gastsystemen. Deze gastsystemen gedragen zich dan meestal (afhankelijk van het soort virtualisatie) als autonome systemen.

Het is per definitie niet nodig om de *hardware* van een computer aan te passen om deze gebruik te laten maken van virtualisatie. Als de *hardware* van een bepaalde computer niet direct werkt met bepaalde virtualisatie *software* zal deze *software* de code van de *kernel* vertalen op binair niveau. Vervolgens kan de virtualisatie alsnog draaien op de machine. [Adams and Agesen(2006)]

Het is wel zo dat om randapparatuur te virtualiseren er wel extra aanpassingen nodig zijn. Echter wat voor aanpassingen hangt af van de virtualisatie *software* die gebruikt wordt. Het virtualiseren van randapparatuur kan vaak worden gerealiseerd door het installeren van een aantal *hardware* specifieke *drivers*. [Rossier(2012)]

Het is goed om te realiseren dat er meerdere soorten virtualisatie bestaan. Zo bestaat er para virtualisatie, een vorm van virtualisatie waarbij het gastsysteem zich ervan bewust is dat het gevirtualiseerd is. In plaats van de *hardware* direct aan te sturen zal het gastbesturingssysteem dit via het hoofdbesturingssysteem laten gebeuren. Bij volle virtualisatie daarentegen gedraagt het gastbesturingssysteem zich daadwerkelijk als autonoom systeem en stuurt het direct zijn (gevirtualiseerde) *hardware* aan.

Er bestaan verschillende *software* pakketten voor virtualisatie. Er is niet een bepaalde soort *software* die duidelijk het meest gebruikt wordt maar uitgaande van de namen die het meest voorkomen in onderzoeken lijken de volgende drie bedrijven die virtualisatie *software* maken het populairst; VMware, Oracle en VirtualBox. Het is echter niet duidelijk op welke schaal ze door welke bedrijven worden gebruikt, het blijft daarom gissen naar een antwoord.

2 Onderzoek naar virussen

Het is lastig om onderzoek te doen naar virussen. De definitie van een computervirus is volgens van Dale niet voor niets; '*programma dat data ongevraagd kan veranderen of vernietigen.*' [van Dale(2016)] Tijdens onderzoek naar deze virussen wordt er juist data verzameld om te leren hoe deze *software* precies werkt. Als deze data op een of andere manier weer veranderd of vernietigd wordt heeft het onderzoek dus weinig tot geen nut.

2.1 Scheiden van systemen

Virtualisatie kan het probleem dat bij virus onderzoek optreedt verhelpen. Vanuit een hoofdbesturingssysteem kunnen gastbesturingssystemen worden waargenomen. De gastsystemen kunnen worden geïnfecteerd met een bepaald virus terwijl het hoofdsysteem hiervoor niet vatbaar is. Dit doordat virtualisatie er voor zorgt dat de twee systemen volledig gescheiden zijn. Vervolgens kan het gastbesturingssysteem vanuit het hoofdbesturingssysteem worden waargenomen. Het uiteindelijke doel hiervan zal zijn om informatie over deze virussen te vergaren en in de toekomst de virussen te slim af te zijn.

2.2 Detecteren van virtualisatie

Het onderzoek naar virussen wordt echter gehinderd door *malware* dat virtualisatie kan detecteren. Als er wordt ontdekt dat er gebruik wordt gemaakt van virtualisatie kan de kwaadaardige *software* het onderzoek verstoren en op deze manier de onderzoeker verwarren.

Het ontdekken van virtualisatie kan bijvoorbeeld gebeuren door te zoeken naar communicatie kanalen tussen het hoofd- en het gastbesturingssysteem. Als deze worden gevonden duidt dit op virtualisatie. Vervolgens kan het virus gaan interfereren op dit communicatie kanaal waardoor er dus verkeerde gegevens worden verstuurd.

Het is daarom ook belangrijk om er voor te zorgen dat het virus de virtualisatie niet kan detecteren. De manier van verhullen is echter wel afhankelijk van de manier waarop deze geprobeerd wordt te ontdekken. De bovenstaande manier is volgens het onderzoek van Carpenter de meest gebruikte manier. [Carpenter et al.(2007)Carpenter, Liston, and Skoudis]

Het verhullen van deze manier kan gedaan worden door in de *software* die voor de virtualisatie zorgt een aantal aanpassingen in de instellingen te doen. Het gaat er hierbij om dat door de instellingen te veranderen, de taal waarmee de besturingssystemen met elkaar communiceren gewijzigd wordt. Hierdoor herkennen de virussen niet meer dat er gecommuniceerd wordt tussen hoofd- en gastbesturingssystemen en detecteren ze niet meer dat er gebruik gemaakt wordt van virtualisatie. Op die manier kan er dus betrouwbaarder onderzoek gedaan worden.

2.3 Deel conclusie

Virtualisatie kan systemen scheiden waardoor er op een veilige manier onderzoek naar virussen gedaan kan worden. Er moet om betrouwbare resultaten uit het onderzoek te krijgen wel gezorgd worden dat het virus de resultaten niet beïnvloed. Dit kan gedaan worden door de virtualisatie te verbergen.

VANAF HIER NAKIJKEN

3 Virtualisatie en virusscanners

Virusscanners zijn er voor ontworpen om computers zo goed mogelijk te beschermen tegen virussen. Het probleem is echter vaak dat zodra *malware* een computer heeft geïnfecteerd deze de virusscanner zal proberen uit te schakelen. Virtualisatie biedt wellicht een uitkomst voor dit probleem. Door de virusscanner op een apart virtueel systeem te laten draaien is deze niet meer vatbaar voor het virus.

3.1 Virtual Machine Introspection tools

Virtual Machine Introspection tools afgekort VMI tools, zijn tools die er ervoor zorgen dat een virtuele machine van buiten af kan worden waargenomen. Met behulp van deze tools kan een virusscanner het systeem dus in de gaten houden zonder dat het zelf gevaar loopt om geïnfecteerd te worden. [Garfinkel et al.(2003)Garfinkel, Rosenblum, et al.]

Er zijn veel verschillende manieren waarop een VMI tool kan werken, zo kan de tool slechts waarnemen en eventuele problemen doorgeven aan het besturingssystemen, maar het zou ook direct kunnen ingrijpen. Het detecteren van eventuele virussen kan ook op verschillende manieren gebeuren, als voorbeeld kunnen de *hash* tabellen van de instructie- en geheugen pagina's worden vergeleken. Mocht hier geen match tussen zijn dan is de instructie pagina waarschijnlijk corrupt. [Nance et al.(2008)Nance, Bishop, and Hay]

3.2 Actief waarnemen

Het probleem van de tools die gebruikt worden om de virtuele machines met elkaar te verbinden is dat deze afhankelijk zijn van passief waarnemen. Dit houdt in dat de virusscanners pas achteraf en niet preventief kunnen ingrijpen. Als er alleen maar passief waargenomen zou kunnen worden zou er geen toekomst zijn in de verdere ontwikkeling van een volledig anti-virus systeem dat draait op een virtuele machine.

In plaats van het systeem passief waar te nemen kan dit ook actief gebeuren. Met het actief waarnemen van een systeem wordt bedoelt dat er via een koppeling actief naar het waar te nemen systeem wordt gekeken en dat er op die manier ook preventief gehandeld kan worden.

Via deze koppeling kunnen handelingen die de computer uitvoert worden bekeken. Bij deze handelingen kan er gedacht worden aan het aan maken van processen, het schrijven naar een harde schijf en dergelijke. Deze processen kunnen dan beveiligd worden en verdachte activiteiten, die op *malware* zouden kunnen duiden, kunnen worden herkent. [Payne et al.(2008)Payne, Carbone, Sharif, and Lee]

3.3 Deel conclusie

Virtuele systemen zijn uiterst geschikt om virusscanners veiliger te maken. Door deze op een apart systeem te laten draaien zijn ze niet vatbaar voor de virussen zelf. Als er een koppeling tussen het systeem van de virusscanner en het te observeren systeem wordt geplaatst kunnen deze virusscanner op dezelfde manier werken als normale virusscanners.

4 Discussie

In dit onderzoek is er gekeken naar op welke verschillende manieren virtualisatie gebruikt kan worden bij het beschermen van computers tegen virussen. Het is gebleken dat virtualisatie op meerdere manieren kan worden ingezet bij het beschermen van computers tegen virussen.

Helaas zijn lang niet alle onderzoeken naar het gebruik van virtualisatie bij het beschermen van computers tegen virussen openbaar. Dit komt waarschijnlijk omdat er veel geld te verdienen is met bijvoorbeeld virusscanners en daarom dus ook met onderzoek wat betrekking heeft op virtualisatie en virussen. Dat is dan ook rede waarom er veel patenten op dit gebied zijn.

4.1 Conclusie

Virtualisatie biedt een veilige omgeving waarin systemen elkaar niet kunnen infecteren. Daardoor kan virtualisatie zowel bij onderzoek naar virussen als bij het daadwerkelijk verhelpen en beschermen tegen virussen worden gebruikt.

Referenties

[Adams and Agesen(2006)] Keith Adams and Ole Agesen. A comparison of software and hardware techniques for x86 virtualization. *ACM Sigplan Notices*, 41(11):2–13, 2006.

[Carpenter et al.(2007)Carpenter, Liston, and Skoudis] Matthew Carpenter, Tom Liston, and Ed Skoudis. Hiding virtualization from attackers and malware. *IEEE Security & Privacy*, (3):62–65, 2007.

[Garfinkel et al.(2003)Garfinkel, Rosenblum, et al.] Tal Garfinkel, Mendel Rosenblum, et al. A virtual machine introspection based architecture for intrusion detection. In *NDSS*, volume 3, pages 191–206, 2003.

[Nance et al.(2008)Nance, Bishop, and Hay] Kara Nance, Matt Bishop, and Brian Hay. Virtual machine introspection: Observation or interference? *IEEE Security & Privacy*, (5): 32–37, 2008.

[Payne et al.(2008)Payne, Carbone, Sharif, and Lee] Bryan D Payne, Martim Carbone, Monirul Sharif, and Wenke Lee. Lares: An architecture for secure active monitoring using virtualization. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 233–247. IEEE, 2008.

[Rossier(2012)] Daniel Rossier. Embeddedxen: A revisited architecture of the xen hypervisor to support arm-based embedded virtualization. *White paper, Switzerland*, 2012.

[van Dale(2016)] van Dale. Betekenis computervirus, 2016. URL `http://www.vandale.nl/opzoeken?pattern=computervirus&lang=nn#.VzrotlZ95D8`.

[Wang et al.(2012)Wang, Lorch, and Parno] J.H. Wang, J.R. Lorch, and B.J. Parno. Securing anti-virus software with virtualization, November 6 2012. URL `https://www.google.com/patents/US8307443`. US Patent 8,307,443.