De Flip Feng Shui-aanvalstechniek: vraag en antwoord

Hoe werkt de Flip Feng Shui-aanvalstechniek op hoofdlijnen?	Een aanvaller huurt een virtuele server op dezelfde host als uw virtuele server. De aanvaller zorgt dat de hypervisor vervolgens een bepaald stuk geheugen dat uw server en de zijne gemeen hebben, ontdubbelt. Dat betekent dat beide systemen bepaalde informatie die ze allebei verwerken, in het zelfde deel van het fysieke geheugen opslaan. Met behulp van de zogenaamde rowhammer-techniek[1] is de aanvaller in staat de informatie in dit geheugen te veranderen zonder dat de hypervisor of uw virtuele server dit merkt. Hierdoor is hij in staat uw virtuele server te bewegen tot het installeren van malware of het toestaan van logins door ongeautoriseerde personen.
Welke systemen zijn kwetsbaar?	Alle virtuele servers die zijn ondergebracht op hosts die geheugenontdubbeling (memory deduplication) toepassen.
Ik ben eigenaar van een host: hoe kan ik de kwetsbaarheid wegnemen?	Schakel geheugenontdubbeling (memory deduplication) uit in de configuratie van uw hypervisor. Bij oude versies van sommige hypervisors staat ontdubbeling standaard ingeschakeld.
Geheugenontdubbeling levert me een groot efficiëntievoordeel op. Kan ik de kwetsbaarheid niet op een andere manier wegnemen?	Het artikel van de onderzoekers beschrijft enkele alternatieve maatregelen. Zero-page deduplication is een minder vergaande vorm van geheugenontdubbeling. Als u deze hanteert, is Flip Feng Shui niet meer uit te voeren op uw host. Deze vorm van geheugenontdubbeling levert u minder efficiëntievoordeel op dan volledige geheugenontdubbeling. Ook als het interne geheugen van uw host niet gevoelig is voor bekende rowhammer-technieken, is Flip Feng Shui niet uit te voeren. U kunt echter niet eenvoudig nagaan of het interne geheugen in uw server tegen bekende rowhammer-technieken bestand is. Ook worden er regelmatig nieuwe rowhammer-technieken gevonden, waarvoor het interne geheugen in uw server dus hernieuwd vatbaar kan zijn.
Ik gebruik ECC-geheugen in mijn host. Is de aanvalstechniek dan nog mogelijk op mijn host?	Het gebruik van ECC-geheugen maakt het uitvoeren van de aanvalstechniek moeilijker. De host merkt enkele bitflips dan op en kan ervoor corrigeren. Een aanval vergt dan twee keer zoveel bitflips en wordt navenant moeilijker. De onderzoekers hebben waargenomen dat ook meervoudige bitflips voorkomen. Het gebruik van ECC-geheugen voorkomt de aanvalstechniek dus niet volledig.
Ik ben eigenaar van een virtuele server: hoe kan ik de kwetsbaarheid wegnemen?	U kunt de kwetsbaarheid niet zelf wegnemen. Dring er bij de aanbieder van uw virtuele server op aan dat hij geheugenontdubbeling (memory deduplication) uitschakelt op de host waarop uw virtuele server ondergebracht is.
Hoe waarschijnlijk is het dat ik met de aanvalstechniek te maken krijg?	De onderzoekers hebben de code die ze hebben geschreven om misbruik van de kwetsbaarheid te maken, niet gepubliceerd. Voor een aanvaller met weinig kennis en middelen is de aanval daarom lastig uit te voeren. Voor een aanvaller met ruime kennis en middelen is de informatie in het onderzoeksrapport voldoende om de aanval uit te kunnen voeren. Een criminele organisatie of buitenlandse inlichtingendienst is hier waarschijnlijk goed toe in staat. Daarbij geldt echter wel dat hij zijn aanvalscode zal moeten aanpassen voor het specifieke besturingssysteem dat u op uw virtuele server gebruikt.
Hoe is de aanvaller in staat de virtuele server binnen te dringen?	In het onderzoeksrapport beschrijven de auteurs twee aanvallen op Debian en Ubuntu als voorbeeld. Met de eerste van deze aanvallen weet een aanvaller binnen te dringen in een server. De aanvaller richt zich op het aanpassen van een instelling van OpenSSH. Hij maakt een kleine wijziging in een publieke sleutel die is geautoriseerd om op de server in te loggen. Door deze wijziging kan hij de sleutel eenvoudig kraken. Zo verschaft hij zich toegang tot de server.
Hoe is de aanvaller in staat de virtuele server malware te laten installeren?	In het onderzoeksrapport beschrijven de auteurs twee aanvallen op Debian en Ubuntu als voorbeeld. Met de tweede van deze aanvallen weet een aanvaller de server malware te laten installeren. De aanvaller richt zich op het aanpassen van instellingen van softwarebeheerapplicatie apt. Hij brengt kleine wijzigingen aan in de URL waarvandaan apt software downloadt. Zo zorgt hij dat de server malware installeert die zich voordoet als een softwareupdate. Hij omzeilt de integriteitscontrole door ook een kleine wijziging te maken in de publieke PGP-sleutel waarmee apt de software controleert.
Is deze aanvalstechniek ook te gebruiken tegen andere virtuele	Ja. De aanvalstechniek maakt geen gebruik van specifieke eigenschappen van servers, dus een aanvaller kan de aanvalstechniek ook toepassen op andere virtuele machines. Hij moet dan echter

[1] Zie bijvoorbeeld https://en.wikipedia.org/wiki/Row_hammer.

machines dan servers, bijvoorbeeld op een werkstation?	al wel toegang hebben tot een andere virtuele machine op dezelfde host. De kans daarop is veel groter bij een host waar servers met allerlei verschillende beheerders draaien.
Wat maakt deze aanvalstechniek anders dan andere soortgelijke technieken?	Eerder ontdekte aanvalstechnieken, zogenaamde side channels, richten zich op het afluisteren van vertrouwelijke gegevens van een virtuele server op dezelfde host. Dit is de eerste aanvalstechniek die een aanvaller in staat stelt wijzigingen in het geheugen van een andere virtuele server aan te brengen. Zo kan hij de virtuele server direct aanvallen.
Waarom heet de aanvalstechniek Flip Feng Shui?	De naam van de aanvalstechniek valt in twee delen uiteen. 'Flip' slaat op de bitflips die de aanvaller weet te bewerkstelligen op uw virtuele server. 'Feng Shui' is een Chinese filosofie over het in overeenstemming brengen van zaken met hun omgeving. De manier waarop virtuele servers bij deze aanval wijzigingen van hun buren overnemen, doet hier sterk aan denken.
Waar kan ik meer informatie vinden over de aanvalstechniek?	De onderzoekers hebben hun resultaten gepresenteerd op het USENIX Security Symposium 2016. Hun slides en onderzoeksrapport zijn beschikbaar op https://www.vusec.net/projects/flip-feng-shui/.