# Cybersicherheit und sichere Anwendungen

Wirksame Sicherheit mit Simulationstechnologie

www.windriver.com

WNDRVR

## KURZFASSUNG

**Cybersicherheit und die sichere Bereitstellung von Anwendungen sind Themen, die viele verschiedene Branchen betreffen — Luft- und Raumfahrt, Verteidigung, Energie, kritische Infrastrukturen, Industrieautomation, Medizintechnik oder Telekommunikation, um nur einige zu nennen. Diese Branchen haben eines gemeinsam — ein böswilliger Angriff über das Netzwerk kann unermessliche finanzielle oder physische Schäden verursachen oder sogar lebensbedrohliche Folgen haben. Doch es gibt Sicherheitsmaßnahmen und Lösungen aus der Cyberforschung, die sich auf sämtliche Bereiche anwenden lassen. Dieser Beitrag beleuchtet, warum sich Sicherheitslösungen mit virtueller Hardware und Systemsimulation produktiver entwickeln und testen lassen als mit Live-Systemen, die fortlaufend Angriffen ausgesetzt sind.**

## INHALT

## DIE WACHSENDE BEDROHUNG

Ausgeklügelte Cyberangriffe nehmen weltweit zu. Heute, mit der Ausweitung des Internet der Dinge (IoT) und der Gerätekonnektivität, erstrecken sich die Ziele von Cyberattacken über Verteidigung und IT hinaus auf kritische Infrastrukturen, Luft- und Raumfahrt, Automobil, Gesundheitswesen, Schwerindustrie, Transport und Kommunikation — also auf jedes Segment, in dem es digitale Informationen zu stehlen oder zu missbrauchen gibt oder in dem das Potenzial für Betriebsunterbrechungen oder Schäden besteht.

Der Schutz kritischer Systeme vor netzwerkbedingten Bedrohungen und die Verhinderung des Einsatzes infizierter Systeme sind Prioritäten sowohl für die Regierung als auch für die Industrie. Es sind heute Technologien verfügbar, die den Sicherheitsingenieuren einen erheblichen Vorteil bei der Bekämpfung von Bedrohungen verschaffen können. Doch zunächst sollten wir das aktuelle Modell für Forschung und Entwicklung im Bereich der Cybersicherheit überprüfen.

## CYBERABWEHR: „DE-KONSTRUKTION" VON ANGRIFFEN

Cyberabwehr bezieht sich auf das Bemühen, Wege zu finden, um Systeme gegen Angriffe zu schützen, einschließlich der Analyse, wie Angriffe geschehen, wie sie funktionieren, wie sie sich im Laufe der Zeit auswirken und ihre Auswirkungen sowie die Entwicklung von Gegenmaßnahmen. Das Verständnis der Art der Angriffe und das Aufdecken von System-Schwachstellen ist entscheidend für die Entwicklung wirksamer Verteidigungsmechanismen.

Die Verteidigung gegen Cyberattacken umfasst zwei Hauptaktivitäten:

- **Einsatz der Verteidigung:** Die Entwicklung und Bereitstellung eines koordinierten Pakets von Schutzfähigkeiten, die Konfiguration dieser Fähigkeiten zur Bereitstellung der erforderlichen Schutzmaßnahmen, die Verifizierung der Abwehr und die Aufrechterhaltung der Fähigkeiten mit ihren richtigen Konfigurationen.
- **Forensik:** Untersuchung, wie ein Angriff erfolgt, was der Angriff zu erreichen beabsichtigt, wie sich das eindringende Element verhält und wie das Angriffselement funktioniert. Das Verständnis für die Art eines Angriffs im Detail ist der Schlüssel zur Entwicklung geeigneter Cyber-Gegenmaßnahmen.

Die Entwicklung, der Einsatz und das Testen effektiver Cyber-Abwehrmaßnahmen in Embedded Geräten ist eine besondere Herausforderung. Embedded Geräte haben in der Regel Ressourcenbeschränkungen wie begrenzte Rechenleistung und Verarbeitungskapazität. Sie sind oft für einen einzigen, einzigartigen Zweck konzipiert und verwenden weniger verbreitete Busse und Schnittstellen. Die Einrichtung von Testlabors zur Durchführung von Cyber-Tests auf Systemebene an einer repräsentativen Auswahl von Geräten in großem Maßstab stellt eine logistische und kostenmäßige Herausforderung dar. Es ist auch schwierig, Sicherheitstests an Live-Systemen durchzuführen, ohne sie vollständig „einzufrieren", was nicht leicht zu bewerkstelligen ist, da die meisten Systeme jederzeit verfügbar sein müssen. Außerdem ist oft kein Backup oder redundanter Dienst verfügbar. Es ist zwar möglich, einen Hardware-Knoten herunterzufahren und die restlichen Systeme am Laufen zu halten, aber dies kann das Systemverhalten verzerren und daher kein Hinweis darauf sein, wie sich eine Sicherheitsmaßnahme in einem realen Angriffsszenario verhält.

Das Testen von Cyberabwehrsystemen umfasst Techniken wie Fuzz-Tests oder automatisierte Tests, bei denen ungültige, unerwartete oder zufällige Daten in ein System eingespeist werden, um die Ursachen für einen Systemausfall zu ermitteln, sowie Penetrationstests (oder „Pen-Test"), bei denen ein System angegriffen wird, um Sicherheitsschwächen aufzudecken, Zugriff auf Daten zu erhalten und Systemfunktionen zu übernehmen oder zu verhindern, und bei denen die Ergebnisse dann an den Systemeigentümer gemeldet werden.

Die Systembetreiber merken möglicherweise nicht einmal, dass sie angegriffen werden. Ausgeklügelte Angriffe können sich über einen langen Zeitraum hinweg entwickeln, mit scheinbar zufälligen Ereignissen, die isoliert betrachtet harmlos erscheinen, aber kollektiv und im Laufe der Zeit Schaden anrichten können. Die Cyberjagd kann schwer fassbar sein — intelligente Angriffe können zunächst als zufällige und einfache Fehler erscheinen. Cyberabwehr-Teams müssen Gegenmaßnahmen entwickeln, die ständig aktiv sind, die Angriffe erkennen und verhindern können und die versuchten Angriffe dem Sicherheitsteam melden.

Die Forensik ist im Wesentlichen eine Form des Reverse Engineering — Ermittler arbeiten sich rückwärts, um die Ursache eines Angriffs zu ermitteln. Viele ausgeklügelte Angriffe sind jedoch so konzipiert,

jedoch so konzipiert, dass sie ein Reverse Engineering verhindern — sie verstecken sich unterhalb der Betriebssystemebene, im BIOS oder in der Firmware. Diese Angriffe können auch Spuren von sich selbst löschen, so dass für ein Forensikteam wenig übrig bleibt, wenn der Angriff aufgedeckt wird. In einigen Fällen können Angriffe sogar erkennen, ob sie analysiert werden, und das Verhalten ändern, um die Entdeckung ihrer wahren Natur zu vermeiden.

## UNTERSUCHUNG VON ANGRIFFEN UND ENTWICKLUNG VON ABWEHRMASSNAHMEN IN EINER VIRTUELLEN UMGEBUNG

Wie können Sie also Forensik betreiben, wenn ausgeklügelte Malware dazu dient, Ermittlungsversuche zu vereiteln? Wie können Sie Schwachstellen in kritischen Infrastruktursystemen, die aus speziellen Embedded Geräten bestehen, erkennen und beheben? Wie können Sie tatsächlich klüger als Eindringlinge werden?

Wären die Kosten kein Thema, könnten Sie einen so genannten „Cyber-Schießstand" aufbauen, ein vollständig isoliertes Netzwerk aus physischen Computern, dessen einziger Zweck darin besteht, Cyber-Malware und Gegenmaßnahmen zu testen — vergleichbar mit einem Golfplatz für Schwungübungen oder einem Schießstand für Zielübungen. Aber dieses Unterfangen ist in der Regel sehr kostspielig und erfordert eine physische Ausrüstung — sei es ein ganzes Flugzeugcockpit, eine Kraftwerksausrüstung oder Instrumente für den Operationssaal, die alle in einem Labor zusammen verkabelt sind. Die Kosten und die physische Beschaffenheit einer Cyber-Range begrenzen seine Kapazität, die oft deutlich unter dem tatsächlichen Bedarf liegt. Darüber hinaus erfordern Cyber-Ranges in der Regel besondere Fähigkeiten in Verbindung mit den einzigartigen Eigenschaften und Schnittstellen eines bestimmten Systems. Angesichts dieser Einschränkungen und des daraus resultierenden Wertes ist eine physische Cyber-Range für viele Organisationen weder ausreichend noch kosteneffizient.

Eine weniger kostspielige, flexiblere und effektivere Alternative ist der Einsatz virtueller Hardware und einer vollständigen Systemsimulationstechnologie. Die Verwendung von virtueller Hardware und Simulation hat zwei Vorteile:

1. Es können Tests durchgeführt werden, die auf physischer Hardware nicht möglich sind, z.B. das „Austricksen" von Malware, so dass sie sich auf bestimmte Weise verhält und sich dadurch entblößt und nicht versteckt werden kann.
2. Es kann eine virtuelle Cyber-Range geschaffen werden, die so weit nötig vollständig skaliert ist, mit allen Varianten, die zur Erforschung der Systeme erforderlich sind, und auf die jeder Ingenieur des Cyber-Forschungs- und Entwicklungsteams zu-greifen kann.

Wind River® Simics® ist ein Beispiel für diese Art von Technologie. Simics ist ein vollständiger Systemsimulator; er simuliert nicht nur Prozessoren und Platinen, sondern komplette vernetzte Systeme, auf denen der gesamte Software-Stack unmodifiziert läuft, einschließlich BIOS, Firmware, Betriebssystem und Softwareanwendungen. Virtuelle Simics-Plattformen simulieren die Zielhardware, auf der die Software laufen soll.

Simics hat sich als ein effektives Forschungs- und Entwicklungswerkzeug für die Cybersicherheit in der Luft- und Raumfahrt und im Verteidigungssektor erwiesen, und diese Erfahrung ist auf andere Branchen übertragbar. Simics kann zur Unterstützung der Forschung und Entwicklung auf verschiedene Weise eingesetzt werden:

### Nicht nachweisbare Analyse

Software verhält sich auf einer virtuellen Simics-Plattform genauso wie auf physischer Hardware. Die gesamte Software, von der Anwendungsebene bis hinunter zum BIOS und zur Firmware, kann auf Simics unmodifiziert ausgeführt werden. Software-Build-Systeme und Entwicklungswerkzeuge müssen nicht modifiziert werden, und die Software wird auf dieselbe Weise geladen wie auf physischer Hardware. Das bedeutet, dass aus der Sicht der Software kein Unterschied zwischen Simics und physischer Hardware besteht. Und im Gegensatz zu einem Debug-Agent ist Simics nicht leicht zu erkennen, sodass Sie eine Selbstanalyse und eine „non-intrusive" Analyse eines Cyberangriffs durchführen können, da die Malware nicht weiß, dass sie auf Simics ausgeführt wird, was es schwierig macht, sich zu verstecken.

Cyber-Forensik-Ingenieure haben viele der gleichen Herausforderungen wie BIOS-Entwickler — sie müssen genau verstehen, wie Software auf niedriger Ebene funktioniert. Eine der Hauptanwendungen von Simics liegt in der Entwicklung von BIOS- und Firmware-Code, wobei die virtuelle Hardware in „High Fidelity" zum physischen Target entwickelt wird.

## Untersuchung von Angriffen: Kontrollpunkte und umgekehrte Ausführung

Die Untersuchung eines wahrscheinlichen Angriffs beinhaltet die Entwicklung eines Testfalls, der zeigt, wie der Angriff funktioniert. Und wenn auffälliges Verhalten auftritt, müssen die Forscher in der Lage sein, es zu reproduzieren und zu analysieren. Mit Simics-Kontrollpunkten und Funktionen zur umgekehrten Ausführung wird dies eine ziemlich einfache Angelegenheit. Mit einem System-Checkpoint kann ein kompletter Zustand des Systems gespeichert werden, von einem einzelnen Gerät bis hin zu Tausenden von Geräten, die wiedergegeben und von einem Team gemeinsam genutzt werden können. Mit der umgekehrten Ausführung können Cyberingenieure einfach die Zeit umkehren und dieselbe Ausführung mit vollständigem Determinismus erneut abspielen.

Darüber hinaus sind diese Funktionen nicht-invasiv, so dass das System nicht beobachten kann, dass es angehalten, umgekehrt, kontrolliert oder wiederhergestellt wird.

## Fehlerinjektion

Wenn es sich bei der „Hardware" tatsächlich um Software handelt, kann sie nach Bedarf geändert werden — beispielsweise können Hardwarefehler programmgesteuert in das System eingespeist werden. Bei vollständiger Kontrolle über die Zeit können Ingenieure das System im laufenden Betrieb ändern und modifizieren, um ein bestimmtes Verhalten zu erreichen, oder verschiedene Wege durch die Ausführungspfade nehmen. Diese Fähigkeit ist sowohl für Penetrations- als auch für Fuzz-Tests sehr nützlich. Da alles in Simics durch Scripting ausgeführt werden kann, kann die Fehlerinjektion automatisiert und so oft wie nötig wiederholt werden.

## Vollständige Inspektion

Als Ergänzung zu gewöhnlichen Blackbox-Analysen und -Tests ermöglicht Simics vollständige Whitebox-Tests und -Analysen. Simics ermöglicht einen vollständigen Einblick in das gesamte System und den Zugriff auf physischen und virtuellen Speicher. Alles auf dem Target kann unbemerkt und ununterbrochen gelesen werden, einschließlich MMU-Inhalte, Register und Disk-Inhalte. Jede Anweisung, jeder Speicherzugriff, jeder Gerätezugriff und jedes Netzwerkpaket kann zurückverfolgt und protokolliert werden. Und die Malware hat keine Ahnung, dass sie beobachtet wird.

## Zukünftiges Verhalten mit Hypersimulation beobachten

Da Malware manchmal so konzipiert ist, dass sie erst nach Wochen, Monaten oder sogar Jahren langfristige Auswirkungen hat, müssen Forscher untersuchen, was mit einem System in der Zukunft passieren kann und wie kleine Fehler im Laufe der Zeit zu größeren Problemen führen. Bei einem physischen System gibt es nur eine Möglichkeit, dies zu tun — das System laufen zu lassen und die Auswirkungen in Echtzeit zu überwachen. Durch Hypersimulation kann die Simulation die Zeit tatsächlich beschleunigen und das Systemverhalten in die Zukunft projizieren.

## Kein Quellcode erforderlich

Bei der Durchführung von Forensik kann man auf Situationen stoßen, in denen nur Software-Binärdateien verfügbar sind. Dieser Mangel an Quellcode könnte eine Untersuchung möglicherweise verlangsamen oder behindern. Da in Simics jedoch unmodifizierte Software ausgeführt wird, können Teile des Systems nur als Maschinencode verfügbar sein und dennoch durch die Nutzung der Funktionen von Simics ausgeführt und analysiert werden. Dies ist eine einzigartige Eigenschaft von Simics im Vergleich zu anderen Systemsimulationswerkzeugen.

## SICHERE BEREITSTELLUNG

Entwickler müssen sicher sein, dass neue Software und die damit verbundenen Produkte vor der Bereitstellung nicht beeinträchtigt wurden — dass das System zu Beginn und nach einem Update sicher bootet und funktioniert.

Die einfache Antwort wäre, jeden Teil der Software vor dem Einsatz und bei jeder Aktualisierung zu testen. Das Problem ist, dass die Sicherheit nur schwer richtig skaliert werden kann. Je komplexer die Software und das Computersystem sind, desto größer ist die Testmatrix und desto schwieriger wird es, die entsprechen-de Testvariation im Produktionsmaßstab zu erreichen. Wenn die Tests nicht in vollem Umfang durchgeführt werden, kann das Produktionssystem gefährdet werden, und dieses Risiko wird durch die unerbittliche Forderung nach schnelleren Implementierungen noch verschärft. Leider bestand die Lösung oft darin, auf eine vollständige Testabdeckung zu verzichten und nur für die kritischsten Anwendungsfälle auf verfügbaren Plattformen zu testen. Cyber-Angreifer werden die Stellen finden, die nicht vollständig getestet wurden.

Fuzz-Tests sind eine Methode, die zur Bewertung der Sicherheit vor dem Einsatz angewendet werden kann. Ingenieure können beispielsweise die Eingaben in ein Gerät nach dem Zufallsprinzip variieren, eine zufällige Kommunikation einführen, Protokollvariationen anwenden, Reichweiten- und Grenzüberprüfungen durchführen oder auf Puffer- und Registerüberläufe prüfen. Zufallsgesteuerte Tests erfordern jedoch Bandbreite, was wiederum die Frage der Skalierbarkeit aufwirft.

## LÖSUNG DER HERAUSFORDERUNG DER SKALIERBARKEIT

Sicherheitstests erfordern Skalierbarkeit. Kompromisse bei der Testvariation und der Testabdeckung müssen beseitigt werden. Die Lösung dieses Problems erfordert zwei wichtige Fähigkeiten: Automatisierung und Parallelisierung. Es ist von entscheidender Bedeutung, über ein Höchstmaß an Automatisierung zu verfügen, nicht nur, um den Testprozess zu beschleunigen, sondern auch, um Wiederholbarkeit zu erreichen und die Ergebnisse automatisch zu berichten und zu protokollieren. Das parallele Ausführen von Tests hilft auch, Zeit zu sparen, aber die Parallelisierung ist schwierig. Nicht alle Arten von Testsoftware können parallel ausgeführt werden; einige sind von Natur aus seriell. Und die Testparallelisierung erfordert die Existenz mehrerer Instanzen derselben Hardware, was nicht immer praktikabel oder erschwinglich ist.

## SOFORTIGE REPLIKATION VON TEST-ASSETS

Simulation und virtuelle Hardware lösen sowohl das Automatisierungs- als auch das Parallelisierungsproblem. Wenn die Hardware virtuell ist, kann jede Menge Zielhardware in jeder Systemkonfiguration sofort instanziiert werden. Ein virtuelles Hardware-Labor kann ein physisches Hardware-Labor ergänzen und es Ingenieuren ermöglichen, die Zielsysteme nach Bedarf zu erstellen. Ein automatisiertes Testsystem kann auch so programmiert werden, dass neue Hardware-Instanzen und System-Setups (sowohl von Hardware als auch von Software) automatisch erstellt werden.

Simics kann auch die Testgeschwindigkeit durch eine „Snapshot- und Wiederherstellungsfunktion" erheblich beschleunigen, d.h. es kann ein System bis zu einem bestimmten Punkt ausführen, einen Snapshot erstellen und dann abgeleitete Testfälle aus dem Snapshot ausführen, ohne dass das System jedes Mal bis zum Snapshot-Punkt neu ausgeführt werden muss.

Simics ermöglicht die sofortige und unbegrenzte Replikation von Test-Assets. Parallele Tests, die mehrere Hardware-Instanzen erfordern, können mit Simics einfach ausgeführt werden. Es können alternative Systemkonfigurationen erstellt werden, so dass Karten und Software-Kombinationen je nach den spezifischen Anforderungen variiert werden können, und die gesamte Testmatrix mit einer beliebigen Anzahl oder Kombination von Hardware-Varianten, Betriebssystem-Konfigurationen, Kommunikationsprotokollen und Geräten vervollständigt werden kann.

## AUTOMATISIERUNG DES UNMÖGLICHEN

Da in Simics alles skriptfähig ist, die Zeit kontrolliert und das System in jeder Hinsicht verändert werden kann, wird es möglich, zu automatisieren, was sonst nicht möglich wäre. Beispielsweise kann Hardware gezwungen werden, wiederholt und deterministisch zu stoppen. Fuzz-Tests können auf neue Art und Weise automatisiert werden. Testprogramme können so eingerichtet werden, dass automatisch eine beliebige Anzahl neuer Platinen erstellt wird, die mit vordefinierten Software-Stacks geladen werden und von jedem beliebigen Punkt aus in jedem beliebigen Zustand ausgeführt werden können. In Kombination mit der Fähigkeit, die Software auf einem gegebenen Satz virtueller Boards programmatisch zu ändern, ermöglichen diese Fähigkeiten die vollständige Automatisierung verschiedener Testkombinationen.

Ein wichtiger und oft übersehener Aspekt der virtuellen Hardware ist, dass sie stabiler und zuverlässiger ist als physische Hardware. Hardware-Labore sind tendenziell ausfallgefährdet und störungsempfindlich. Je größer das Labor, desto empfindlicher kann es mit zunehmender Komplexität werden. Bei der Überprüfung der Ergebnisse eines automatisierten Testsystems nach einem Test über Nacht kann man feststellen, dass Tests unterbrochen wurden, was mehrere Stunden oder Tage an Verzögerungen kostet. Ingenieure müssen möglicherweise auch Zeit aufwenden, um ein gemeldetes Problem zu analysieren und festzustellen, ob das Problem mit dem zu entwickelnden System oder dem Testsystem selbst zusammenhängt, was die Produktivität beeinträchtigt. Mit virtueller Hardware, die auf stabilen Servern läuft, wird das Testsystem vertrauenswürdiger, und alle Testteams können unabhängig von ihrem Standort Zeit sparen, die sonst verloren gehen könnte, wenn die Testautomatisierung nur auf physischer Hardware durchgeführt wird.

## SCHLUSSFOLGERUNG

Die zunehmende Automatisierung, digitale Informationen und die Vernetzung kritischer Systeme erhöhen die Komplexität der Entwicklung und Wartung sicherer Systeme. Die Entwickler kritischer Systeme benötigen Werkzeuge, die ihnen helfen, den immer raffinierteren Angreifern einen Schritt voraus zu sein. Die Systemsimulationstechnologie bietet ein effizientes und wirksames Mittel zur Erforschung, Analyse und Prüfung einer Vielzahl von Angriffsmethoden und Sicherheitsgegenmaßnahmen in einer flexiblen und skalierbaren Umgebung, und zwar auf eine Weise, die mit physischen Systemen einfach nicht machbar wäre. In einer Welt, die immer mehr von der sicheren und zuverlässigen Leistung miteinander verbundener Systeme abhängig ist, bietet die Simulation Cyberprofis eine Möglichkeit, die Oberhand zu gewinnen.

WNDRVR

Wind River is a global leader of software for the intelligent edge. Its technology has been powering the safest, most secure devices since 1981 and is in billions of products. Wind River is accelerating the digital transformation of mission-critical intelligent systems that demand the highest levels of security, safety, and reliability.