Zertifikatsprogramm - Z802

Cloud-Sicherheit und Cloud-Forensik

- Grundlagen von Virtualisierungstechnik und Cloud Computing
- Grundlagen von Cloud-Forensik
- Cloud-Sicherheit und Bedrohungsmodelle
- Virtual Machine Introspection
- Einbruchserkennung und Honeypots in der Cloud

Prof. Dr. Hans P. Reiser
Noëlle Rakotondravony
Johannes Köstler

Open C³S
Open Competence Center for Cyber Security

UNIVERSITÄT PASSAU

Modul 116

Cloud-Sicherheit und Cloud-Forensik

Autoren:

Prof. Dr. Hans P. Reiser

Noëlle Rakotondravony

Johannes Köstler

---

2. Auflage

Universität Passau

Universität Passau
Fakultät für Informatik und Mathematik
Innstraße 43
94034 Passau

2. Auflage (2018-09-05)

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

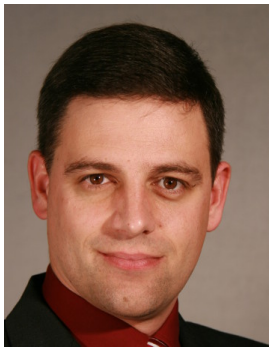
Inhaltsverzeichnis

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Quelltext	Q
Übung	Ü

II. Zu den Autoren



Hans P. Reiser ist Juniorprofessor für Sicherheit in Informationssystemen an der Universität Passau. Schwerpunkte seiner Arbeitsgruppe sind die Weiterentwicklung von Konzepten und Systemen aus dem Bereich der fehler- und einbruchstoleranten Replikation, die frühzeitliche und umfassende Erkennung von Sicherheitsproblemen und Sicherheitsvorfällen in Cloud-Umgebungen sowie die Erforschung neuartiger Sicherheitskonzepte auf Hypervisorebene.

Noëlle Rakotondravony ist seit September 2015 wissenschaftliche Mitarbeiterin in der Arbeitsgruppe von Prof. Hans P. Reiser an der Universität Passau.

Johannes Köstler ist seit Mai 2015 wissenschaftlicher Mitarbeiter in der Arbeitsgruppe von Prof. Hans P. Reiser an der Universität Passau.

III. Modullehrziele

Dieses Modul widmet sich den Themen Cloud-Sicherheit und Cloud-Forensik mit einem besonderen Fokus auf Angriffsanalyse. Der erste Studienbrief behandelt die Grundlagen von Virtualisierungstechnik und Cloud-Computing-Modellen. Dazu zählen die unterschiedlichen Konzepte von Virtualisierung im Allgemeinen, sowie die Konzepte und Architekturen von Rechnervirtualisierung im Besonderen. Darüber hinaus erlernen Sie die verschiedenen Definitionen des Begriffs „Cloud Computing“ und erlangen ein vertieftes Verständnis über die wesentlichen Service- und Verarbeitungsmodelle, nicht zuletzt im Hinblick auf Sicherheitsfragen.

Der darauffolgende Studienbrief beschäftigt sich mit den Grundlagen von Techniken der IT-Forensik sowie den dazugehörigen Vorgehensmodellen. Dabei werden die aktuellen Herausforderungen und Möglichkeiten der forensischen Untersuchung bei cloudbasierter Datenspeicherung sowie bei virtuellen Maschinen besonders herausgearbeitet. Zusätzlich werden Sie mit dem aktuellen Stand der Forschung zu forensikunterstützenden Cloud-Diensten und zur „Forensic Readiness“ vertraut.

Im dritten Studienbrief „Cloud-Sicherheit und Bedrohungsmodelle“ erlernen Sie die Grundlagen von Bedrohungsmodellierung und Risikomanagement in Cloud-Infrastrukturen, so dass Sie später in der Lage sind die Sicherheitsherausforderungen von Cloud-Systemen zu beurteilen. Sie sind vertraut mit technischen Ansätzen zur sicheren Speicherung sowie Verarbeitung von Daten in der Cloud und haben ein grundlegendes Verständnis für die Gefahr durch Seitenkanalangriffe in der Cloud.

Um die Theorie und Praxis von Virtual Maschine Introspection (VMI) geht es im darauffolgenden Studienbrief. Neben den grundlegenden Funktionsweisen und den Anwendungsmöglichkeiten von VMI gehört dazu insbesondere das Problem der so genannten semantischen Lücke (semantic gap). Des Weiteren werden Sie mit dem Werkzeug Volatility vertraut gemacht, um laufende virtuelle Maschinen mit existierenden Plug-Ins zu untersuchen und einfache Plug-Ins selbst zu entwickeln bzw. zu erweitern.

Der letzte Studienbrief schließt das Modul mit den Grundbegriffen und Funktionsweisen von Einbrucherkennungssystemen und von Honeypots. Sie erlernen die Vor-und Nachteile des Betriebs solcher Systeme in Cloudumgebungen und sind später selber in der Lage diese eigenständig zu betreiben.

Welche Lehrinhalte werden bearbeitet?

- Virtualisierungstechnik und Cloud-Computing
  - Geschichtliche Hintergründe von Virtualisierungstechnik
  - Virtualisierungsarten
  - Details von Rechnervirtualisierung (Intel/ARM)
  - Service- und Verarbeitungsmodelle von Cloud Computing (NIST)
- Grundlagen von Cloud-Forensik
  - Historische Entwicklung von IT-Forensik
  - Aktuelle Modelle der IT-Forensik
  - Datenträger-Forensik in der Cloud
  - Live-Forensik in der Cloud
  - Forensik-Dienste und Forensik-Readiness-Modelle in der Cloud
- Cloud-Sicherheit und Bedrohungsmodelle
  - Bedrohungsmodellierung und Risikomanagement
  - Sicherheitsherausforderungen in der Cloud
  - Sichere Datenspeicherung und –verarbeitung in der Cloud
  - Koresidenz und Seitenkanalangriffe
- Virtual Machine Introspection (VMI)
  - Grundlagen, Herausforderungen und Anwendungen von VMI

  - Funktionsweise der Analysebibliothek LibVMI
  - Untersuchung von Linux-Kernel-Datenstrukturen mit Volatility
  - Untersuchung aktiver virtueller Maschinen mit Volatility/LibVMI
- Cloud-Einbruchserkennungssysteme und Honey Pots
  - Grundlagen von Einbruchserkennungssystemen
  - Grundlagen von Honeypots
  - Einbruchserkennungssysteme in der Cloud
  - Honeypots in der Cloud

Was können Sie nach erfolgreichem Abschluss des Moduls?

Nach Abschluss dieses Moduls verfügen Sie über fundierte Kenntnisse im Bereich von Cloud-Sicherheit und Cloud-Forensik. Neben den Konzepten und Architekturen von Virtualisierung umfassen diese Kenntnisse das Wissen über Sicherheitsherausforderungen und Bedrohungsmodellen in Cloud-Infrastrukturen sowie einen Überblick über aktuelle Forensikmethoden und entsprechende Werkzeuge. Darüber hinaus haben Sie weiterführende Kompetenzen in der Verwendung von Virtual Machine Introspection, Honeypots und Einbruchserkennungssystemen als Werkzeuge zur Angriffsanalyse erworben.

Studienbrief 1 Grundlagen von Virtualisierungstechnik und Cloud Computing

1.1 Lernziele

Virtualisierungstechnik bildet die Grundlage von allen Cloud-Infrastrukturen. In diesem Mikromodul erhalten Sie zunächst einen Überblick über die geschichtlichen Hintergründe und die unterschiedlichen Arten von *Virtualisierungstechnik*. Darauf aufbauend entwickeln Sie ein vertieftes Verständnis für die Konzepte und Architekturen von *Rechnervirtualisierung*. Des Weiteren kennen Sie nach Abschluss dieses Mikromoduls die wichtigsten Aspekte der Entstehungsgeschichte von *Cloud Computing* und sind mit der Definition dieses Begriffes vertraut. Sie verfügen über ein vertieftes Verständnis über die wesentlichen Service- und Verarbeitungs-Modelle.

1.2 Virtualisierung: Geschichtliche Hintergründe

Die Ursprünge von Virtualisierungstechnik gehen zurück in die 60er-Jahre. Als erstes System, das es im Sinne von Rechnervirtualisierung ermöglichte, dass mehrere Benutzer auf einer physischen Hardware mehrere unabhängige Betriebssysteme ausführen, gilt das unter Leitung von Creasy entwickelte IBM CP-40 auf Basis eines Mainframe-Rechners IBM System/360 Model 40 mit modifizierter Speicherverwaltung (**?**). Hierbei stellt ein *Control Program* (was man heute üblicherweise als Virtual Machine Monitor oder Hypervisor bezeichnen würde) mehrere Ausführungsumgebungen (*virtuelle Maschinen*) bereit, die sich jeweils wie ein isolierter physischer Rechner verhalten. Diese zum damaligen Zeitpunkt bahnbrechende Architektur beeinflusste maßgeblich nachfolgende Systeme, insbesondere CP-67 für IBM System/360 Model 67 und ab 1972 VM/370 für IBM System/370.

Ermöglicht wurde die Implementierung dieser ersten Virtualisierungsarchitektur vor allem durch zwei Komponenten: Zum einen entstanden ab den späten 50er-Jahren erstmals Konzepte von virtuellem Speicher. Getrieben durch die Motivation, teuren Hauptspeicher durch preiswerteren Trommelspeicher zu erweitern, kamen nun Architekturen auf, die eine Abbildung von virtuellen Adressen auf echte (physische) Speicheradressen in Hardware unterstützten. Zum anderen wurde im System/360 zwischen den CPU-Ausführungszuständen „*privileged*“ und „*problem*“ unterschieden. Im *problem*-Zustand sind nur solche Instruktionen verfügbar, die gewöhnliche Anwendungsprogramme normalerweise verwenden und die keine Nebenwirkungen auf andere virtuelle Maschinen haben. Im *privileged*-Zustand sind darüber hinaus *sensitive* Instruktionen verfügbar, die sich auf den gesamten Rechner auswirken und daher auch andere virtuelle Maschinen beeinflussen können oder Zustandsinformationen zu anderen virtuellen Maschinen lesen können. Wird eine solche privilegierte Operation im nichtprivilegierten Zustand ausgeführt, so wird die Ausführung unterbrochen und die Kontrolle an eine dedizierte Behandlungsroutine im *Control Program* übergeben. Diese kann dann die Wirkung dieser privilegierten Instruktion innerhalb der virtuellen Maschine simulieren (**?**).

Bereits aus dieser kurzen Darstellung lässt sich erkennen, dass ein Rechner gewisse Anforderungen erfüllen muss, um die Ausführung mehrerer virtueller Maschinen zu ermöglichen. Es zeigte sich, dass eine derartige Virtualisierung auf manchen damals üblichen Rechnerarchitekturen nicht möglich war. Beispielsweise gab es bei einer DEC PDP-10 nichtprivilegierte Instruktionen, die aber dennoch sensitiv im Sinne von Auswirkungen auf den ganzen Rechner sind (**?**). Eine systematische, formalisierte Untersuchung dieser Voraussetzungen, welche ein System erfüllen muss um Hardware virtualisieren zu können, wurde erstmals von **?** durchgeführt.

Studienbrief 2 Grundlagen von Cloud-Forensik

2.1 Lernziele

Nach Bearbeitung dieses Mikromoduls sind Sie mit den grundlegenden Modellen und Vorgehensweisen der IT-Forensik vertraut. Sie haben ein tieferes Verständnis für die Herausforderungen hinsichtlich IT-Forensik in Cloud-Umgebungen entwickelt. Neben organisatorischen und juristischen Aspekten sind Sie hierbei insbesondere mit den technischen Problemstellungen und dem Stand der Forschung zu Lösungsansätzen vertraut. Sie haben einen Einblick in aktuelle Entwicklungen hinsichtlich Forensics as a Service und Forensic-Readiness-Modellen.

2.2 Grundlagen von IT-Forensik

2.2.1 Historische Entwicklung

Die unmittelbare Aufgabe von Forensik im Allgemeinen besteht in der Beantwortung der Fragen nach dem *Was*, *Wo*, *Wann* und *Wie* eines konkreten Vorfalls. Grundsätzlich verfolgt werden dabei mehrere Ziele: Neben der eigentlichen detaillierten Analyse eines Vorfalls (welche Vorgänge haben während des Vorfalls stattgefunden?) geht es einerseits um die Identifikation des Verursachers bzw. Täters und die Sammlung von verwertbaren Beweismitteln, andererseits um die Prävention gleichartiger Vorfälle in der Zukunft.

Erste Fälle zu IT-basierten kriminellen Aktivitäten gehen zurück bis in die 60er-Jahre. Nennenswert ist ein Bericht aus dem Buch „Fighting Computer Crime“ von **?**, das einen Vorfall aus dem Jahr 1966 beschreibt. Dabei manipulierte ein für die Programmierung und Wartung der IT-Systeme einer Bank Beauftragter diese so, dass er sein eigenes Bankkonto unbemerkt überziehen und sich so einen finanziellen Vorteil verschaffen konnte.

Die Ursprünge der systematischen *IT-Forensik* gehen zurück auf die früher 80er-Jahre und die Anfangszeit der Personal Computer. Erst durch die massiv wachsende Verbreitung von PCs wurde die Herausforderung, digitale Spuren auf einem IT-System als Beweismittel zu sichern, zu einem häufigen, praxisrelevanten Problem. Als „Vater der IT-Forensik“ gilt hier Michael Anderson, der als Mitarbeiter des Internal Revenue Service – Criminal Investigation Division (IRS-CID) in den USA eine tragende Rolle bei der Entwicklung von Ausbildungskursen und von Software-Werkzeugen zur Beweissicherung von IT-Hardware innehatte. Im Jahr 1988 wurde in den USA die IACIS (International Association of Computer Investigative Specialists) gegründet. Aus dieser Organisation ging bald darauf ein Ausbildungskonzept für *SCERS* (Seized Computer Evidence Recovery Specialists) hervor. Bereits im Jahr 1993 fand die erste wissenschaftliche Konferenz zu diesem Thema statt.

In Deutschland wurde später das Thema IT-Forensik vom Bundesamt für Sicherheit in der Informationstechnik aufgegriffen. 2010 erschien erstmals der *Leitfaden „IT-Forensik“* des BSI, der das Ziel verfolgt, ein praxistaugliches Modell für die IT-Forensik zu definieren. Auf dieses und andere Modelle gehen wir detaillierter in den nächsten Unterkapiteln ein.

2.5.4 Bewertung dieser Möglichkeiten

Alle diese Erweiterungen zeigen auf, dass es durchaus technische Möglichkeiten gibt, das Problem der Identifikation und Sammlung forensischer Informationen in Cloud-Infrastrukturen zu verbessern. Derzeit sind dem Autor aber keine nennenswerten Bestrebungen größerer Cloud-Anbieter bekannt, derartige Techniken in ihren Infrastrukturen anzubieten.

Diese Bewertung ist jedoch auch hinsichtlich der Cloud-Servicemodelle zu differenzieren. Alle beschriebenen Ansätze sind jeweils für das IaaS-Modell entworfen, und nur dort können sie uneingeschränkt als geeignet angesehen werden. Eine Erweiterung auf das PaaS ist insofern denkbar, wenn eine Platform für einen PaaS-Cloud-Kunden isoliert innerhalb einer virtuellen Maschine bereitgestellt wird. In allen anderen Fälle sind die beschriebenen Methoden ungeeignet, weil bisher keine Ansätze existieren, auf diesem Weg gezielt die relevanten Daten eines Kunden zu identifizieren oder die Zugriffsmöglichkeiten gezielt auf einen Kunden einzuschränken.

2.6 Übungaufgaben

Übung 2.1

Welche Bedeutung haben Vorgehensmodelle für eine forensische Untersuchung?

Ü

Übung 2.2

Erläutern Sie das Vorgehensmodell des BSI für den forensischen Prozess und vergleichen Sie dieses mit anderen bekannten Vorgehensmodellen.

Ü

Übung 2.3

Beschreiben Sie wesentliche Herausforderungen, die sich bei einer forensischen Untersuchung von cloudbasierten Diensten in den Phasen der Datenidentifikation, Datensammlung und Datenanalyse ergeben.

Ü

Übung 2.4

Ein Cloud-Nutzer einer öffentlichen Cloud ist mit einem Missbrauch seiner Dienste konfrontiert. Welche wesentlichen Unterschiede gibt es bei einer von ihm durchgeführten forensischen Untersuchung zwischen den Servicemodellen IaaS, PaaS und SaaS?

Ü

Übung 2.5

Eine Organisation nutzt eine private Cloud-Infrastruktur zur Speicherung von Daten, die auf Geräten von Mitarbeitern genutzt werden. Beschreiben und vergleichen Sie unterschiedliche Möglichkeiten der Sammlung forensischer Informationen.

Ü

Ü

Übung 2.6

Beschreiben Sie den Unterschied zwischen Rekonstruktion aktiver Abbildungen und Rekonstruktion der letzten gelöschten Abbildung im abstrakten Modell von **?**.

Ü

Übung 2.7

Beschreiben Sie die technischen Herausforderungen und Lösungsansätze einer Live-Analyse von Hauptspeicherinhalten bei Verwendung einer privaten Cloud im IaaS-Modell.

Studienbrief 3 Cloud-Sicherheit und Bedrohungsmodelle

3.1 Lernziele

Nach Abschluss dieses Mikromoduls sind Sie mit den Grundlagen von Bedrohungsmodellierung und Risikomanagement in IT-Systemen vertraut. Auf dieser Grundlage können Sie Sicherheitsrisiken in Cloud-Infrastrukturen beurteilen. Sie sind vertraut mit theoretischen und praktischen Ansätzen zur sicheren Speicherung und Verarbeitung von Daten in der Cloud. Sie können cloudspezifische Angriffe wie Koresidenz und Seitenkanalangriffe bewerten.

3.2 Grundlagen der Bedrohungsmodellierung

Die Entwicklung sicherer Softwaresysteme stellt eine große Herausforderung dar. Werden im Entwicklungsprozess Sicherheitslücken frühzeitig erkannt, können die Kosten zur Behebung dieser Lücken gering gehalten werden. Eine Voraussetzung für die Entwicklung sicherer Softwaresysteme ist die systematische Analyse von Bedrohungsmodellen und daraus abgeleiteten Sicherheitsanforderungen.

Bedrohungsmodellierung (threat modelling) ermöglicht es, einen Systementwurf methodisch zu überprüfen, um potentielle Schwachstellen zu identifizieren und zu beheben. Am größten ist der Nutzen dann, wenn damit Sicherheitslücken bereits in einer frühen Phase des Entwicklungsprozesses identifiziert werden. Dieser Aspekt ist nach **?** exemplarisch in Tabelle 3.1 illustriert. Dargestellt sind Schätzwerte für die relativen Kosten zur Behebung von Schwachstellen abhängig davon, in welcher Phase des Entwicklungszyklus diese erkannt werden.

Anforderungs-analyse	Implementierung/Unit-Tests	System-integration	Beta-Tests	Nach dem Release
1x	5x	10x	15x	30x

Tabelle 3.1: Relative Kosten der Schwachstellen-Reparatur, abhängig von der Phase des Entwicklungszyklus

Bei der Bedrohungsmodellierung werden auf Grundlage einer Bewertung von Sicherheitslücken mögliche Schutzmechanismen abgeleitet, mit denen das *Risiko* reduziert werden kann. Im Folgenden wollen wir nun diesen und weitere relevante Begriffe näher definieren.

Nach ISO/IEC 21827, einem internationalen Standard basierend auf dem *Systems Security Engineering Capability Maturity Model*, ist der zentrale Begriff *Risiko* wie folgt definiert:

Definition 3.1: Risiko nach ISO/IEC 21827

„The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets."

D

Aus dieser Definition lassen sich die drei Faktoren ablesen, die das Risiko beeinflussen: *Bedrohungen (threats)*, *Schwachstellen (vulnerabilities)* und *Auswirkungen (loss or damage to the assets)*.

Bedrohungen

Für den Begriff *Bedrohung* finden sich in der Literatur viele verschiedene Definitionen. Wir greifen in Definition 3.2 eine ausführliche Definition auf, die aus

Studienbrief 4 Virtual Machine Introspection

4.1 Lernziele

Nach Bearbeitung dieses Mikromoduls sind Sie mit Theorie und Praxis von Virtual Machine Introspection (VMI) vertraut. Sie kennen die grundlegende Funktionsweise und die verschiedenen Anwendungsmöglichkeiten von VMI. Sie kennen den aktuellen Stand der Forschung zu den zwei Ausprägungen des Problems der semantischen Lücke (weak semantic gap, strong semantic gap) und können auf dieser Grundlage die Grenzen und Risiken einer Fehlinterpretation bei Virtual Machine Introspection einschätzen. Darüber hinaus sind Sie mit den wesentlichen Datenstrukturen eines Betriebssystemkerns am Beispiel von Linux vertraut. Sie können das Werkzeug Volatility zusammen mit VMI einsetzen, um laufende Systeme in virtuellen Maschinen mit existierenden Analyse-Plugins zu untersuchen.

4.2 Virtual Machine Introspection

4.2.1 Begriff

Der Begriff der Introspektion virtueller Maschinen (Virtual Machine Introspection – VMI) geht zurück auf einen Artikel (**?**), der VMI als sehr vorteilhafte Technik zur Einbruchserkennung (Intrusion Detection) vorschlägt. Bei VMI greift ein untersuchendes System (das *Analysesystem*) von außen auf den internen Zustand eines untersuchten Systems (das *Zielsystem*) zu.

VMI-basierte Einbruchserkennung verbindet die Vorteile von netzbasierter Einbruchserkennung und hostbasierter Einbruchserkennung. Während erstere zwar eine starke Isolation zwischen Analysesystem und Zielsystem gewährleistet, bietet die Beobachtung des Netzverkehrs nur eingeschränkten Einblick in interne Vorgänge im Zielsystem. Auf der anderen Seite bieten hostbasierte Systeme potentiell sehr guten Einblick in den internen Systemzustand, sind aber als Teil des Zielsystems nicht von diesem isoliert und können dementsprechend leicht von einem Angreifer manipuliert werden.

Diese Vorteile werden durch Ausnutzung von drei grundlegenden Eigenschaften von virtuellen Maschinen ermöglicht: Isolation, Inspektion und Interposition.

Isolation bedeutet, dass das Analysesystem im Idealfall vollständig vom Zielsystem getrennt ist. Dies wird dadurch erreicht, dass das Zielsystem in einer virtuellen Maschine ausgeführt wird. Das Analysesystem befindet sich außerhalb dieser virtuellen Maschine. Eine mögliche Variante ist es, das Analysesystem direkt in den Hypervisor zu integrieren. In der Praxis oft üblich ist bei einem Bare-Metal-Hypervisor die Ausführung in einer privilegierten virtuellen Maschine wie *Dom0* beim Hypervisor Xen und bei einem Hosted-Hypervisor als Prozess des Host-Betriebssystems. Eine weitere vorteilhafte Variante ist die Verwendung einer separaten virtuellen Maschine (*Monitoring Virtual Machine*), die sowohl vom Zielsystem als auch von allen anderen Systemkomponenten isoliert ist.

Diese Isolation muss nicht immer perfekt sein. Unwahrscheinlich, aber nicht undenkbar ist, dass ein Angreifer, der das Zielsystem kontrolliert, von diesem aus Schwachstellen in der Schnittstelle zum Hypervisor ausnutzt und so zunächst die Kontrolle über den Hypervisor und in der Folge auch über das Analysesystem erlangt. Häufiger sind in der Praxis Auswirkungen auf die Performance des Gastsystems, die von diesem bemerkt werden können. Auf mögliche Wechselwirkungen zwischen virtuellen Maschinen geht das Mikromodul Seitenkanäle genauer ein.

Inspektion bedeutet, dass das Analysesystem mit Hilfe des Hypervisors Zugriff auf den Zustand des Zielsystems hat. Den wichtigsten Teil dieses Zustands stellt der virtuelle Arbeitsspeicher des Zielsystems dar. Er umfasst aber auch den Zustand der CPU-Register sowie der I/O-Geräte. Trotz Isolation kann so das untersuchende System ein sehr detailliertes Bild des Zielsystems erlangen.

Interposition bedeutet, dass der Hypervisor in der Lage ist, zahlreiche Operationen innerhalb des Zielsystems (wie das Ausführen von privilegierten CPU-Operationen und den Zugriff auf I/O-Geräte) abzufangen. Hier lässt sich ein Hypervisor leicht so erweitern, dass ein Analysesystem über derartige Ereignisse automatisch informiert wird.

Bei der VMI-basierten Untersuchung eines Zielsystems lassen sich *aktive* und *passive* Methoden unterscheiden:

- Bei *aktiver VMI* erzeugt der Hypervisor selbst Benachrichtigungen über Ereignisse, die dem Analysesystem zugestellt werden; hierzu kann beispielsweise der Zugriff auf eine bestimmte Speicherseite oder die Ausführung einer privilegierten CPU-Instruktion gezählt werden.
- Bei *passiver VMI* stellt der Hypervisor lediglich eine Schnittstelle bereit, über die das Analysesystem z. B. periodisch den Zustand des Zielsystems überprüfen kann.

Viele Anwendungen von VMI beschränken sich, wie die ursprüngliche Arbeit von **?**, auf das Lesen des Zustands (also Hauptspeicher, CPU-Register, I/O-Geräte) der virtuellen Maschine. In ähnlicher Form ist es aber auch möglich, das Zielsystem zu verändern. Während dies einerseits als Missbrauchsmöglichkeit betrachtet werden kann, lassen sich durchaus auch nützliche Vorteile aus dieser Technik erzielen. So kann beispielsweise das gezielte Injizieren von Haltepunkten verwendet werden, um dadurch aktive Benachrichtigung zu bestimmten Vorgängen im Zielsystem (beispielsweise das Ausführen von Systemaufrufen (*system calls*) oder bestimmten Funktionen) zu erzeugen (**?**). Es ist auch denkbar, dadurch gezielt bestimmte Fehler oder Schwachstellen von außen zu beheben oder sogar einzelne Prozesse z. B. mit Monitoringaufgaben in das Zielsystem von außen einzubringen (**?**).

4.2.2 Anwendungsbeispiele

Seitdem VMI erstmals als nützliche Technik beschrieben wurde, haben Forschungsarbeiten und praktische Systeme gezeigt, dass sich diese grundlegende Technik für viele unterschiedliche Anwendungszwecke einsetzen lässt.

Intrusion Detection ist dabei der ursprüngliche Zweck, der von **?** betrachtet wurde. Hierbei besteht der Vorteil gegenüber bereits etablierten hostbasierten Verfahren in der Isolation zwischen Zielsystem und Analysesystem.

Ein damit verwandter Anwendungszweck sind *Virus-Scanner*, die ebenfalls ein Zielsystem detailliert analysieren können, ohne dass die Analysesoftware durch die Schadsoftware manipuliert oder deaktiviert werden kann (**?**).

Im Bereich der *digitalen Forensik* ergeben sich ähnliche Vorteile. Für eine statische Untersuchung von Speicherabbildern werden herkömmlich Werkzeuge verwendet, die auf dem Zielsystem ausgeführt werden und daher immer eine Interaktion und folglich eine mögliche Veränderung des Zielsystems bedeuten. Diese Speicherabbilder lassen sich aber auch extern über VMI erzeugen. Darüber hinaus ermöglicht VMI eine dynamische Analyse eines laufenden Systems (**?**). Hierbei wird statt

Studienbrief 5 Einbruchserkennung und Honeypots in der Cloud

5.1 Lernziele

Nach Bearbeitung dieses Mikromoduls kennen Sie die Grundbegriffe und Funktionsweisen von Einbruchserkennungssystemen (Intrusion Detection System – IDS). Neben den beiden grundlegenden Varianten der netzbasierten und der hostbasierten Einbruchserkennung sind Sie vertraut mit den Möglichkeiten, die Virtualisierungstechnik zur Einbruchserkennung bietet (Einbruchserkennung auf Basis der Introspektion virtueller Maschinen). Auf dieser Basis sind Sie in der Lage eigenständig eine Strategie zur Einbruchserkennung in Cloud-Umgebungen zu definieren. Des Weiteren kennen Sie die wesentlichen Arten von Honeypots und haben einen Einblick in die ausgewählten Beispielsysteme. Auch sind Sie mit der der Verwendung von VMI in „High-Interaction Honeypots“ vertraut. Sie sind in der Lage, Honeypots zu betreiben, Erkenntnisse daraus abzuleiten sowie Vor- und Nachteile zu beurteilen.

5.2 Motivation

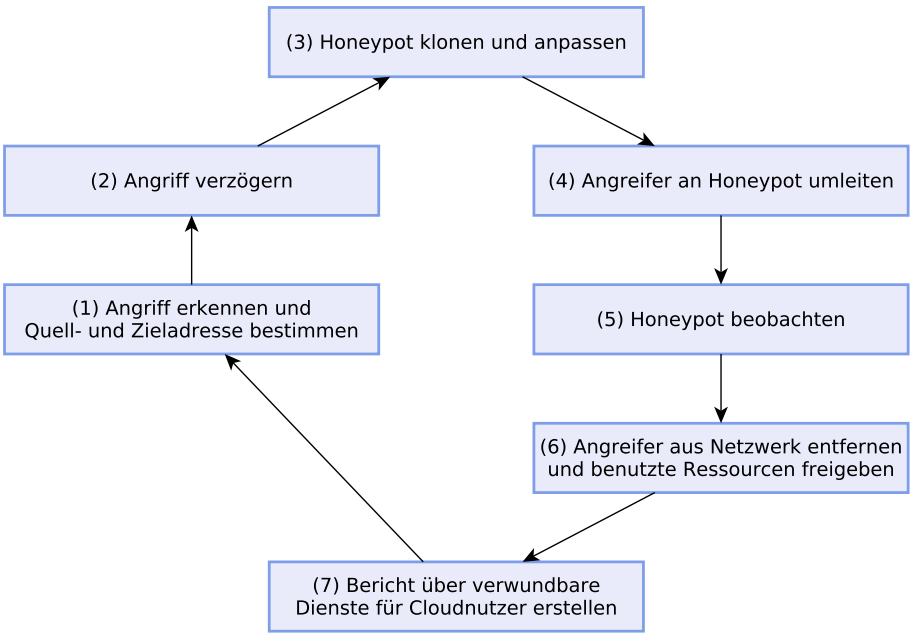
Auch wenn die Bestrebungen zum Entwurf und der Umsetzung von sicherer Software und IT-Systemen hoch sind, können diese niemals eine perfekte Sicherheit bieten. Trotz stetiger Fortschritte im Bereich der IT-Sicherheit kann keinesfalls von einer Entspannung der Gefahrenlage die Rede sein. So kommt das Bundesamt für Sicherheit in Informationstechnik in ihrem jährlichen Sicherheitsbericht zu dem Fazit, „dass die Komplexität der Bedrohungslage ebenso wie die damit einhergehenden Gefahren für die fortschreitende Digitalisierung zunimmt“ (**?**). Vor allem beim Auftreten von Sicherheitslücken und bei der Verbreitung von Schadsoftware seien deutliche Anstiege zu verzeichnen.

Im Folgenden wollen wir der Frage nachgehen, wie man mit dieser Situation in der Praxis umgehen kann. Während dieses Problem grundsätzlich für alle IT-Systeme von großer akuter Bedeutung ist, stellt sich auch die Frage, welche Auswirkungen hierbei der wachsende Einsatz von Cloud-Infrastrukturen hat. Gerade bei öffentlichen Cloud-Infrastrukturen im IaaS- und PaaS-Modell ist man diesen Herausforderungen im gleichen Maße ausgeliefert, hat als Cloud-Nutzer aber – im Vergleich zum Nutzer einer dedizierten Inhouse-Infrastruktur – nur einen beschränkten Handlungsspielraum.

Dieser Studienbrief betrachtet zwei Konzepte: Einbruchserkennung und Honeypots. Systeme zur Einbruchserkennung versuchen sich den in der Realität unvermeidbaren Angriffen entgegenzustellen, um deren Auswirkungen auf ein Minimum zu reduzieren. Dafür beobachten sie entweder zu bestimmten Zeitpunkten oder kontinuierlich die Ausführung des Systems und die durchlaufenen Zustände. Die Erkennung der Angriffe erfolgt entweder durch die Analyse des Systemverhaltens oder durch den Abgleich mit bereits bekannten Angriffsmustern. Zur Gewinnung solcher Muster können sogenannte Honeypots eingesetzt werden. Das Konzept bedient sich dabei der Metapher des Honigtopfs, welcher in vielen Geschichten als Lockmittel die Aufmerksamkeit von Bären erregen soll. Analog dazu geben sich digitale Honeypots als begehrenswerte und zumeist auch simple Ziele aus. Diese beiden Konzepte werden in diesem Abschnitt näher erläutert, bevor sich die folgenden Abschnitte genauer mit Implementierungen solcher Systeme in der Praxis beschäftigen.

so eine einfache und bedarfsgesteuerte Bereitstellung einer Vielzahl von Honeypots in Cloud-Umgebungen und unterstützt die Analyse durch weitreichende Visualisierungen.

Abb. 5.9: Dynamische Honeypot-Erzeugung (**?**)



Honeypots werden außerdem häufig als Teil von größeren Systemen zur Einbruchserkennung- und verhinderung eingesetzt. Ein Beispiel ist das von **?** vorgeschlagene dynamische Honeypot-System, welches in Cloud-Umgebungen eingesetzt wird, um Attacken gegen produktive virtuelle Maschinen (VM) auf dynamisch erzeugte Honeypots umzuleiten. Dazu werden – wie in Abbildung 5.9 dargestellt – nach der Detektion eines Angriffes die IP-Adressen vom Angreifer und dessen Ziel extrahiert. Daraufhin wird zunächst der Angriff an sich verzögert, um Zeit für die folgenden Schritte zu gewinnen. Diese Schritte beginnen mit dem Klonen des Angriffsziels in eine neue VM mittels Live-Migration. Danach werden sensible Daten von der neuen VM entfernt oder durch unbedenkliche Daten ersetzt. Anschließend wird der Angreifer an die neue Honeypot-VM umgeleitet. Die Maschine wird währenddessen umfassend beobachtet, um den Angriff genau nachvollziehen zu können. Wenn die Analyse abgeschlossen ist, wird der Angreifer aus dem Netzwerk entfernt und die zusätzlichen Cloud-Ressourcen wieder freigegeben. Im letzten Schritt erfolgt die Information des Betreibers der betroffenen VM über den erfolgten Angriff und die Verwundbarkeit des Dienstes. Dieser kann dann geeignete Maßnahmen einleiten, um ein solches Verhalten in der Zukunft vermeiden zu können.

5.5 Übungsaufgaben

Ü

Übung 5.1: Einbruchserkennung und Honeypots

Erläutern Sie die Begriffe Intrusion Detection System und Intrusion Prevention System sowie Honeypot und Honeynet. Inwiefern kann ein Honeypot ein System zur Einbruchserkennung unterstützen?

Übung 5.2: Platzierung von Einbruchserkennungssystemen

Diskutieren Sie die Vor- und Nachteile von hostbasierten, netzwerkbasierten sowie Hypervisor-basierten Systemen zur Einbruchserkennung hinsichtlich der folgenden Merkmale:

(a) Wahrscheinlichkeit, dass der Angreifer die Überwachung erkennt;

(b) Menge der Daten, die zur Erkennung herangezogen werden können.

Ü

Übung 5.3: Detektionsmechanismen von Einbruchserkennungssystemen

Erläutern Sie die Funktionsweise der folgenden generellen Detektionsmechanismen eines Systems zur Einbruchserkennung.

(a) Signaturbasierte Einbruchserkennung

(b) Verhaltens-/Anomaliebasierte Einbruchserkennung

Ü

Übung 5.4: Hostbasierte Einbruchserkennung

Nennen Sie mindestens drei Methoden, anhand derer hostbasierte Systeme zur Einbruchserkennung versuchen, Angriffe zu detektieren.

Ü

Übung 5.5: Netzwerkbasierte Einbruchserkennung

Erörtern Sie Herausforderungen bei der Erfassung von Netzwerkdaten, welche bei der Installation von Systemen zur Einbruchserkennung im Netzwerk entstehen können.

Ü

Übung 5.6: Hpyervisor-basierte Einbruchserkennung

Nennen Sie mindestens drei Methoden, mit denen Einbruchserkennungssysteme auf dem Hypervisor virtuelle Maschinen zum Ziele der Einbruchserkennung analysieren.

Ü

Ü

Übung 5.7: Snort

Informieren Sie sich zur Funktionsweise von Snort und über die Definiton von Snort-Regeln – beispielsweise anhand der offiziellen Dokumentation[16].

(a) Definieren Sie eine Snort-Regel, welche den gesamten Netzwerkverkehr (also sowohl eingehende als auch ausgehende Verbindungen) zu dem Dienst auf Port 1234 protokolliert.

(b) Definieren Sie eine Snort-Regel, welche für jeden Verbindungsaufbau zum SSH-Dienst einen Alarm auslöst.

(c) Modifizieren Sie die Snort-Regel von (b) so, dass nur noch Alarme ausgelöst werden, wenn die Verbindungen nicht von Hosts mit der IP-Adresse 10.0.0.201 aus erfolgen.

(d) Definieren Sie eine Snort-Regel, welche einen Alarm auslöst, wenn innerhalb von 30 Sekunden mehr als fünf Verbindungsaufbauten zu dem Dienst auf Port 1234 festzustellen sind.

(e) Definieren Sie eine Snort-Regel, welche einen Alarm auslöst, wenn die Zeichenkette „rotten“ (UTF8-kodiert) innerhalb von Nachrichten an den Dienst auf Port 1234 gefunden wird.

Ü

Übung 5.8: Honeypots

Klassifizieren Sie Honeypots hinsichtlich...

(a) ... der Interaktion mit dem Angreifer.

(b) ... der Art der Implementierung.

(c) ... dem verfolgten Zweck ihres Einsatzes.

Benennen Sie dabei die Vor- und Nachteile der jeweiligen Gruppen.

Ü

Übung 5.9: Anwendungsgebiete von Honeypots

Nennen Sie mindestens drei Anwendungsgebiete von Honeypots.

Ü

Übung 5.10: Hybride Honeypots

Diskutieren Sie die Chancen in der Kombination von Honeypots mit unterschiedlicher Angreiferinteraktion.

Ü

Übung 5.11: Honeypots in der Cloud

Welche Eigenschaften von Cloud-Umgebungen können sich Honeypots zu Nutze machen?

[16] `https://www.snort.org/documents` – [abgerufen am 2015-03-01]

Verzeichnisse

I. Abbildungen

II. Beispiele

III. Definitionen

IV. Exkurse

V. Kontrollaufgaben

VI. Tabellen

Open C³S
Open Competence Center for Cyber Security

Fort- und Weiterbildung

Neue Bedrohungszenarien stellen Sicherheitsexperten und IT-Verantwortliche in Unternehmen und einschlägigen Behörden vor immer größere Herausforderungen. Neue Technologien und Anwendungen erfordern zusätzliches Know-how und personelle Ressourcen.

Zur Erhöhung des Fachkräftepools und um neues Forschungswissen schnell in die Praxis zu integrieren, haben sich die im Bereich lehrenden und forschenden Verbundpartner zum Ziel gesetzt, ein hochschuloffenes transdisziplinäres Weiterbildungsprogramm im Sektor Cyber Security zu entwickeln. Auf der Grundlage kooperativer Strukturen werden wissenschaftliche Weiterbildungsmodule im Verbund zu hochschulübergreifenden Modulpaketen und abschlussorientierten Ausbildungslinien konzipiert und im laufenden Studienbetrieb empirisch getestet.

Die Initiative soll High Potentials mit und ohne formale Hochschulzugangsberechtigung über innovative Weiterbildungsangebote (vom Zertifikat bis zum Masterprogramm) zu Sicherheitsexperten aus- und fortbilden. Hierzu werden innovative sektorale Lösungen zur Optimierung der Durchlässigkeit von berulicher und hoch- schulischer Bildung entwickelt und für eine erfolgreiche Implementierung vorbereitet. Unter prominenter Beteiligung einschlägiger Verbände, der Industrie sowie Sicherheits und Ermittlungsbehörden verfolgt die Initiative das Ziel, im deutschsprachigen Raum eine Generation von Fachkräften wissenschaftlich aus- und weiterzubilden, die unser Internet schützen kann.

Open Competence Center for Cyber Security

Open C³S ist aus dem Verbundvorhabens Open Competence Center for Cyber Security entstanden. Das Gesamtziel des Programms war die Entwicklung eines hochschuloffenen transdisziplinären Programms wissenschaftlicher Weiterbildung im Sektor Cyber Security. Das Bundesministerium für Bildung und Forschung (BMBF) fördert das Großprojekt im Rahmen des Wettbewerbs „Aufstieg durch Bildung: offene Hochschulen“, der aus BMBF-Mitteln und dem Europäischen Sozialfonds finanziert wird.

Neun in Forschung und Lehre renommierte Hochschulen und Universitäten aus dem gesamten Bundesgebiet haben sich zum Ziel gesetzt, Online-Studiengänge auf dem Gebiet der Cybersicherheit zu entwickeln. Dieses Konzept soll den Studierenden ermöglichen, sich berufsbegleitend auf hohem Niveau wissenschaftliche Qualifikationen anzueignen und akademische Abschlüsse zu erlangen. Beruflich erworbene Kompetenzen können eingebracht werden. Die Bezeichnung „Open“ steht auch für die Öffnung des Zugangs zu akademischer Bildung ohne klassischen Hochschulzugang.

Mission der Initiative ist es, dringend benötigte Sicherheitsexperten aus- und fortzubilden, um mit einer sicheren IT-Infrastruktur die Informationsgesellschaft in Deutschland und darüber hinaus zu stärken.

Umsetzungsnahes Wissen ist ein wesentlicher Schlüssel um der wachsenden digitalen Bedrohung zu begegnen. Solange wir nicht in der Lage sind, Systeme hinreichend zu härten, Netzwerke sicher zu designen und Software sicher zu entwickeln, bleiben wir anfällig für kriminelle Aktivitäten. Unser Ziel ist es, die Mitarbeiter von heute zu Sicherheitsexperten und Führungskräften von morgen auszubilden und dafür zu sorgen, dass sich die Zahl und die Fertigkeiten dieser Experten nachhaltig erhöht.

Weitere Informationen zu Open C³S: https://open-c3s.de

Z802 Cloud-Sicherheit und Cloud-Forensik

Dieses Modul widmet sich den Themen Cloud-Sicherheit und Cloud-Forensik mit einem besonderen Fokus auf Angriffsanalyse. Der erste Studienbrief behandelt die Grundlagen von Virtualisierungstechnik und Cloud-Computing-Modellen. Dazu zählen die unterschiedlichen Konzepte von Virtualisierung im Allgemeinen, sowie die Konzepte und Architekturen von Rechnervirtualisierung im Besonderen. Darüber hinaus erlernen Sie die verschiedenen Definitionen des Begriffs „Cloud Computing“ und erlangen ein vertieftes Verständnis über die wesentlichen Service- und Verarbeitungsmodelle, nicht zuletzt im Hinblick auf Sicherheitsfragen.

Der darauffolgende Studienbrief beschäftigt sich mit den Grundlagen von Techniken der IT-Forensik sowie den dazugehörigen Vorgehensmodellen. Dabei werden die aktuellen Herausforderungen und Möglichkeiten der forensischen Untersuchung bei cloudbasierter Datenspeicherung sowie bei virtuellen Maschinen besonders herausgearbeitet. Zusätzlich werden Sie mit dem aktuellen Stand der Forschung zu forensikunterstützenden Cloud-Diensten und zur „Forensic Readiness“ vertraut.

Im dritten Studienbrief „Cloud-Sicherheit und Bedrohungsmodelle“ erlernen Sie die Grundlagen von Bedrohungsmodellierung und Risikomanagement in Cloud-Infrastrukturen, so dass Sie später in der Lage sind die Sicherheitsherausforderungen von Cloud-Systemen zu beurteilen. Sie sind vertraut mit technischen Ansätzen zur sicheren Speicherung sowie Verarbeitung von Daten in der Cloud und haben ein grundlegendes Verständnis für die Gefahr durch Seitenkanalangriffe in der Cloud.

Umdie Theorie und Praxis von Virtual Maschine Introspection (VMI) geht es im darauffolgenden Studienbrief. Neben den grundlegenden Funktionsweisen und den Anwendungsmöglichkeiten von VMI gehört dazu insbesondere das Problem der so genannten semantischen Lücke (semantic gap). DesWeiteren werden Sie mit dem Werkzeug Volatility vertraut gemacht, um laufende virtuelle Maschinen mit existierenden Plug-Ins zu untersuchen und einfache Plug-Ins selbst zu entwickeln bzw. zu erweitern.

Der letzte Studienbrief schließt das Modul mit den Grundbegriffen und Funktionsweisen von Einbrucherkennungssystemen und von Honeypots. Sie erlernen die Vor-und Nachteile des Betriebs solcher Systeme in Cloudumgebungen und sind später selber in der Lage diese eigenständig zu betreiben.

Nach Abschluss dieses Moduls verfügen Sie über fundierte Kenntnisse im Bereich von Cloud-Sicherheit und Cloud-Forensik. Neben den Konzepten und Architekturen von Virtualisierung umfassen diese Kenntnisse das Wissen über Sicherheitsherausforderungen und Bedrohungsmodellen in Cloud-Infrastrukturen sowie einen Überblick über aktuelle Forensikmethoden und entsprechende Werkzeuge. Darüber hinaus haben Sie weiterführende Kompetenzen in der Verwendung von Virtual Machine Introspection, Honeypots und Einbruchserkennungssystemen alsWerkzeuge zur Angriffsanalyse erworben.

Zertifikatsprogramm

Die Zertifikatsmodule auf wissenschaftlichem Niveau und mit hohem Praxisbezug bilden ein passgenaues Angebot an Qualifikation und Spezialisierung in der nebenberuflichen Weiterbildung. Damit können einzelne Module nebenberuflich studiert werden. Durch die Vergabe von ECTS-Punkten können sie auf ein Studium angerechnet werden.

https://zertifikatsprogramm.de