



ReMIND

Maschinelles Lernen für Echtzeit-Intrusion-Detection

Mit Techniken des Maschinellen Lernens sollen unbekannte Hackerangriffe und die neueste Schadsoftware in Netzwerken mit hohen Datenübertragungsraten zuverlässig identifiziert werden.



**SICHERHEIT UND
ZUVERLÄSSIGKEIT**

01000001001000011011001
10010001000111100100001
00100100100110010001010
00011001101000111010011

Innovation durch Intelligenz
Software macht's!

10001100101110
11000001010100

IKT 2020
Softwaresysteme

10001100100110
110000101010000
1011
1100

Vision: Abwehr von Hackerangriffen durch selbst-lernende Intrusion-Detection-Systeme

Vernetzte IT-Infrastrukturen sind einer wachsenden Zahl von Angriffen ausgesetzt. Internetworkwürmer können in kurzer Zeit tausende von Rechnern lahmlegen. „Trojanische Pferde“ werden regelmäßig von Straftätern eingesetzt, um hochsensible Daten auszuspionieren.

Klassische Sicherheitsinstrumente sind den vielfältigen, ständig neu entstehenden Gefahren aus dem Netz kaum gewachsen, denn sie müssen über Existenz und Vorgehensweise eines Schädling informiert werden, bevor sie ihn abwehren können. Die meisten Sicherheitsinstrumente erkennen Angriffe anhand bekannter Muster, den sogenannten Signaturen. Solange ihnen jedoch die Signatur eines Schädling fehlt, kann dieser an ihnen vorbei in das System gelangen und großen Schaden anrichten, ohne als Gefahr erkannt zu werden.



Im Code der Pakete einer Netzwerkverbindung können sich Hackerangriffe und Schadsoftware verstecken

Wirkungsvolle Sicherheitsmechanismen sollten dagegen Eindringlinge selbständig identifizieren. Im Projekt ReMIND entwickelt Fraunhofer FIRST Intrusion Detection Technologien, die ohne vorherige Kenntnis einer Angriffsstrategie unbekannte Angriffe in Netzwerken mit hohem

Datenverkehrsaufkommen enttarnen. So können die neuesten Schädlinge nicht nur viel schneller und effektiver bekämpft werden, sondern auch die Pflege vorhandener Sicherheitsinfrastrukturen weitgehend automatisiert werden.

Systementwicklung

Intrusion Detection Systeme (IDS) sind ein wesentlicher Teil der modernen IT-Sicherheitsinfrastruktur. Sie überwachen den Netzwerkverkehr von und zu Computern auf potenzielle Angriffe. Während sich dabei die meisten aktuellen IDS auf Signaturen stützen, analysiert das in ReMIND entwickelte IDS die Datenströme mit modernen Anomalieerkennungsalgorithmen. Diese Algorithmen bauen darauf auf, dass Angriffe semantische Eigenschaften besitzen, die sich von denen normaler Daten wesentlich unterscheiden. Pakete einer Netzwerkverbindung, die solche Eigenschaften aufweisen, werden aus den Datenströmen herausgefiltert und von den „unbelasteten“ Paketen getrennt.

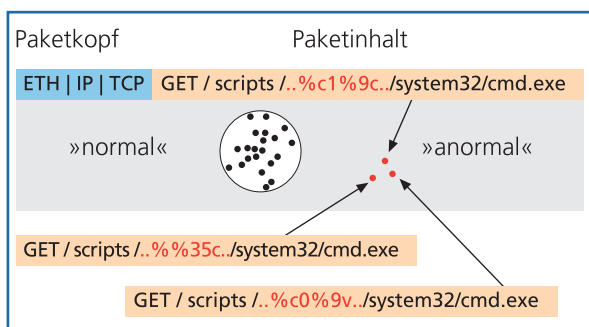
Um die Netzwerkverbindungen schnell und dennoch zuverlässig zu untersuchen, nutzt ReMIND die sogenannte progressive Angriffserkennung. Bisherige IDS betrachten entweder einzelne Pakete einer Netzwerkverbindung oder komplette Verbindungen. Im ersten Fall können komplexe Angriffe nicht zuverlässig erkannt werden. Andererseits geht wertvolle Zeit verloren, wenn gewartet wird, bis eine Verbindung abgeschlossen ist. Progressive Techniken dagegen betrachten Verbindungen, während sie sich aufbauen, und entscheiden mit zunehmender Sicherheit, ob sie Anomalien enthalten.

Wird eine Anomalie entdeckt und als Angriff enttarnt, sollen vorhandene Sicherheitsinstrumente in kürzester Zeit über den neuen Angreifer und seine Vorgehensweise informiert werden. Bisher muss zu jedem Angriff zunächst eine Signatur manuell erzeugt und per Update in das System geladen werden. Das ist zeit- und

arbeitsintensiv. Um den Vorgang zu beschleunigen, werden in ReMIND Methoden untersucht, Signaturen automatisch zu generieren und unmittelbar danach in die Erkennungskomponente einzupflegen. So können Informationen über einen neuen Angreifer im gleichen Moment, in dem er in einem Teil eines Netzwerks identifiziert wurde, bereits an alle anderen Zugangspunkte weitergegeben werden.

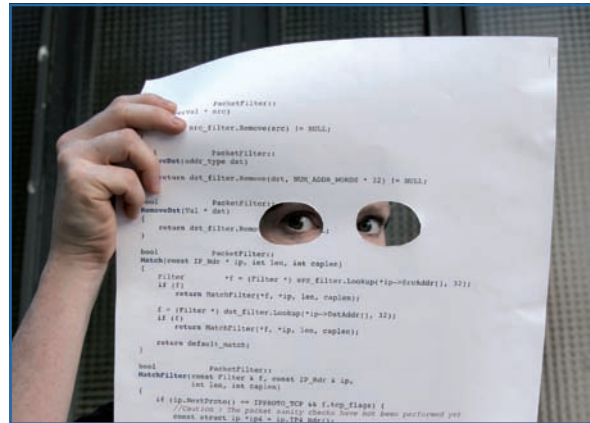
Anwendungsfelder

Die Intrusion Detection Technologien von Fraunhofer FIRST können auf vielfältige Art verwendet werden. Sie lassen sich einerseits in vorhandene IT-Sicherheitsprodukte integrieren, insbesondere in Intrusion Detection bzw. Intrusion Prevention-Systeme. So können die Systeme schneller und zuverlässiger mit Informationen über die neueste Schadsoftware versorgt werden als bisher. Andererseits können Telekommunikationsanlagen und VoIP-Anlagen sowie Internet-Frühwarnsysteme mit den ReMIND-Technologien ausgestattet werden.



ReMIND erkennt Anomalien im Inhalt von Paketen, die beim Netzverkehr ausgetauscht werden, und trennt sie von »normalen« Daten

Ein besonderes Augenmerk von ReMIND gilt der Sicherheit von Industrieautomatisierungssystemen. Solche Systeme basierten früher auf proprietären Protokollen, die Hackern kaum bekannt waren, daher nur selten angegriffen



Man kann nie wissen, was sich im Code versteckt...

wurden und allgemein als sicher galten. Da sie jedoch sehr teuer waren, werden heute in Industrieanlagen zunehmend Standard-Internetprotokolle eingesetzt, wie HTTP, TCP und IP. Damit werden die Anlagen jedoch den Risiken des Internet-Datenverkehrs ausgesetzt – selbst dann, wenn sie nicht an das Internet angeschlossen werden. Hat z.B. ein Techniker unwissentlich einen Wurm auf einem Laptop, den er zur Wartung an das System anschließt, so wird er in kurzer Zeit in alle Teile der Anlage übertragen. Mit den in ReMIND entwickelten Techniken werden Industriesysteme effizient gegen solche Risiken abgeschirmt.

Projektdaten:

- Förderprogramm: IKT 2020 / Forschung für Innovation
- Förderschwerpunkt: Sicherheit/Zuverlässigkeit
- Förderkennzeichen: 01IS07007
- Fördervolumen: 3,3 Mio. Euro
- Laufzeit: 03.2007 - 02.2010

Projektkoordinator:

Pavel Laskov, Ph.D.
Fraunhofer-Institut für Rechnerarchitektur
und Softwaretechnik FIRST
Kekuléstr. 7
12489 Berlin

Tel.: 030/6392-1879
Fax: 030/6392-1805
E-Mail: pavel.laskov@first.fraunhofer.de
Internet: www.first.fraunhofer.de/remind

Projektpartner:

Fraunhofer FIRST, Berlin
Idalab GmbH, Berlin
IT Service Omikron GmbH, Berlin
Siemens AG, München
Technische Universität Berlin

Weitere Informationen:

Projektträger des BMBF
Softwaresysteme und Wissenstechnologien
im Deutschen Zentrum
für Luft- und Raumfahrt e.V (DLR)
Rutherfordstr. 2
12489 Berlin

Telefon: (030) 67055 741
Internet: www.pt-it.pt-dlr.de

Herausgeber:

Bundesministerium für Bildung
und Forschung (BMBF)
Referat Öffentlichkeitsarbeit
11055 Berlin

10001100100110000010100110
01001111011011011001110001100100011
1100011001101000111010011110
0111010010110110101010111010010110010110

Stand Februar 2008