Netzwerksicherheit

Intrusion Detection Systems

Stephen Wolthusen

Fraunhofer IGD Institut Graphische Datenverarbeitung

Kategorien für IDS

- Externe Penetration
  - Angreifer hat keinen Zugriff auf Authentisierungsdaten oder kann Revision/Zugangskontrolle umgehen
- Interne Penetration
  - Auch als „Maskerade“ bezeichnet
  - Angreifer verwendet Authentisierungsdaten anderer Nutzer
- Mißbrauch
  - Legitime Nutzer, die der Sicherheitspolitik zuwider handeln

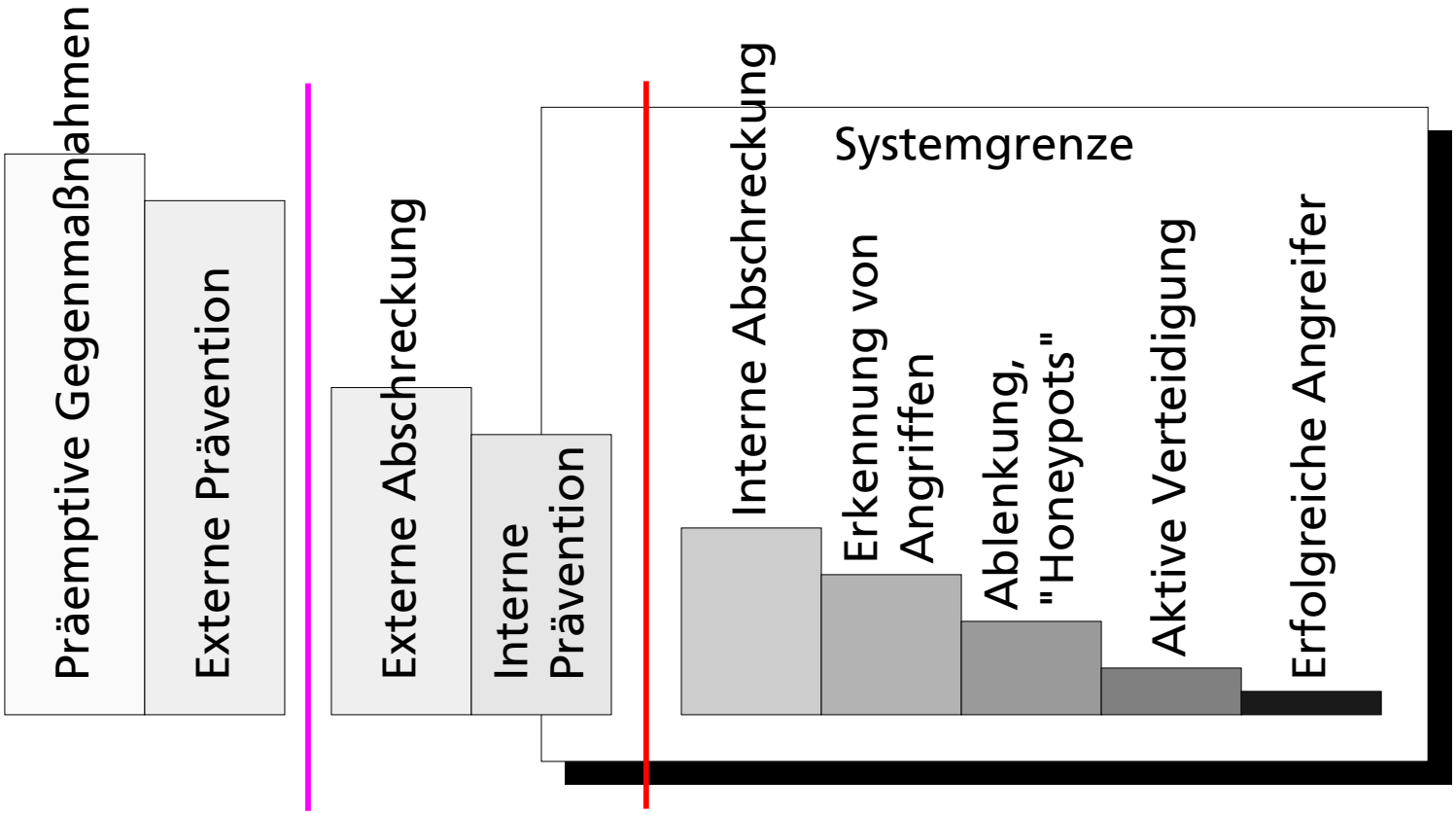
Das Maskerade-Problem

- Zuerst von Anderson (1980) beschrieben
- Maskerade kann anhand von Revisionsdaten bestimmt werden
  - Systemnutzung außerhalb „normaler“ Arbeitszeiten
  - Abnorme Nutzungshäufigkeit
  - Abnorme Anzahl von Zugriffen auf Daten
  - Abnorme Zugriffsmuster (Programme/Daten)

Begründung für automatisierte IDS

- Problem: Feststellung abnormaler Muster
  - Revisionsdatenvolumen
  - Muster können sehr umfangreich sein
  - Vorgehen a la Cliff Stoll´s „The Cuckoo´s Egg“ ist zu aufwendig
- Vorschlag von Anderson: Automatisierte Verfahren zur Reduktion von Revisionsdaten
  - Extraktion relevanter Merkmale, Anomalien
  - Qualität der Revisionsdaten ist entscheidend
  - Bestimmung der Kriterien für Angriffe problematisch

Klassifizierung von Gegenmaßnahmen



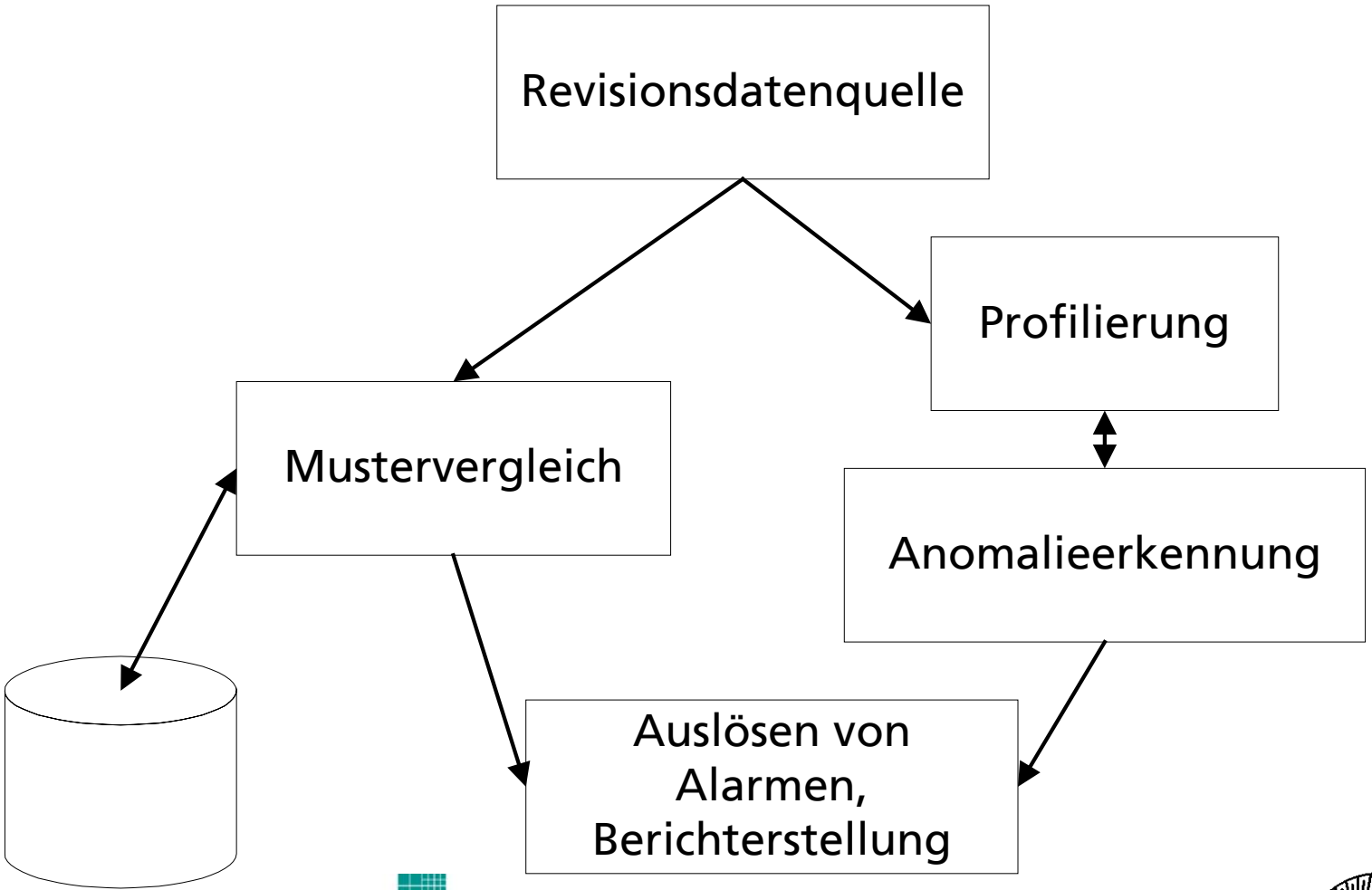
Gegenmaßnahmen (1)

- Präemptive Gegenmaßnahmen
  - Aktive Eliminierung einer Bedrohung ist i.d.R. nicht möglich, rechtliche Probleme, Feststellung der Identität des Angreifers
- Externe Prävention
  - Aufhalten von Angriffen außerhalb der eigenen Enklave: Firewall
- Externe Abschreckung
  - Androhung strafrechtlicher Verfolgung, Ankündigung von Überwachung
- Interne Prävention
  - Interne Firewalls, „Härtung“ interner Systeme, regelmäßige Aktualisierung der Systeme nach ECOs

Gegenmaßnahmen (1)

- Interne Abschreckung
  - Sanktionierung von Mitarbeitern bei Zuwiderhandlung gegen Sicherheitspolitik
- Erkennung von Angriffen
  - Hier sind IDS angesiedelt, beinhaltet auch Reaktion auf Angriffe
- Ablenkung
  - Bereitstellung „attraktiverer“ Ziele („Honeypots/-nets“)
- Aktive Verteidigung
  - Aktive / autonome Gegenmaßnahmen (Blockierung von Nutzerkonten...)

Abstraktes IDS-Modell



Fraunhofer IGD Institut Graphische Datenverarbeitung

ID-Verfahren: Anomalie-Erkennung (1)

- Vorkonfigurierung von Angriffsmustern für Erkennung nicht notwendig
  - IDS lernt anhand von Systemverhalten normales Verhalten und erkennt abnormales Verhalten
    - kann auch neue Verhaltensmuster erkennen
  - Klare Trennung in „legales“ und „illegitimes Verhalten selten möglich, meist existiert Grauzone
    - Identifikation aller möglicher verdächtiger Verhalten führt zu inakzeptabler Häufigkeit von Falschmeldungen

ID-Verfahren: Anomalie-Erkennung (2)

- Nutzerverhalten ändert sich mit der Zeit
  - neue Aufgaben, verbesserte Handhabung des Systems etc.
  - Definition von „normal“ ändert sich entsprechend: „conceptual drift“
- Anomalie-ID muß zur Vermeidung von Fehlalarmen diese Änderungen mitverfolgen und die Definition der Anomalie laufend anpassen
  - Angreifer kann gezielt Verhaltensmuster in Richtung unerwünschten Verhaltens variieren bis der eigentliche Angriff keine Anomalie mehr darstellt

ID-Verfahren: Anomalie-Erkennung (3)

- Große Anzahl von Sensoren (Revisionsdaten von Betriebssystemen, Pakete von Netzwerk-Sniffer, Logins, etc.)
- Hohe zeitliche Auflösung der Sensordaten
  - Hochdimensionale Räume für die Darstellung der Sensoren
  - Analyse erfordert erhebliche Rechenleistung
- Problem der Dejustierung von IDS bei Einführung
  - Präsenz von Angreifern/Mißbrauch läßt Kalibrierung für Anomalieerkennung ungenau werden

ID-Verfahren: Signatur-Erkennung

- Revisionsdaten werden gegen vorgegebene Muster verglichen
  - Erstellung der Muster („Signaturen“) erfolgt i.d.R. in Handarbeit: aufwendig und fehleranfällig
    - Erzeuger der Muster müssen System, Angreifer genau kennen und in der Lage sein kritische Merkmale aus Angriffen zu extrahieren
  - Ermöglicht deutliche Reduktion der Fehlalarme
  - Nur gegen bereits bekannte Angriffe wirksam
    - Wenn Signatur überspezifiziert ist genügen bereits geringe Änderungen an Angriff zur Nicht-Erkennung

ID-Verfahren: Spezifikationsbasierte Verfahren

- Invertierung des Signatur-Erkennungs-Ansatzes
  - Festlegung legitimer Verhaltensmuster
  - Alarm bei Abweichung von spezifizierten Mustern
- Verwendbarkeit für nicht triviale Anwendungsprogramme und Systemprozesse fragwürdig
  - Selbst wenn Spezifikation/Quellen von Anwendungen vorliegen würden: Komplexität ist zu hoch um Verhalten hinreichend genau zu beschreiben
  - Alternative ist zu grobe Spezifikation erlaubten Verhaltens
    - Reduktion der Erkennungsrate

Taxonomische Merkmale von IDS (1)

- Quelle der Revisionsdaten
  - Host-basierte Quellen: Sensoren sind lokal auf zu überwachendem Knoten angebracht
    - Direkte Verwendung der Revisionsdaten des Betriebssystems
    - Weitere Instrumentierung des Systems (system calls...)
    - Anwendungsspezifische Revisionsdaten
  - Netzwerk-basierte Quellen: Setzt voraus, daß relevanter Netzwerkverkehr von Sensor erfaßt werden kann (Switching)

Taxonomische Merkmale von IDS (2)

- Reaktion auf erkannte Angriffe
  - Passive Reaktion: Benachrichtigung des Administrators
  - Aktive Reaktion
    - Versuch ohne Interaktion mit Administrator Schaden zu begrenzen durch
      - Maßnahmen, die nur lokales System betreffen (z.B. Verstärken der Erfassung von Revisionsdaten)
      - Maßnahmen, die mutmaßlich angreifendes System beeinflussen

Taxonomische Merkmale von IDS (3)

- Verzögerung bis zur Angriffserkennung
  - Echtzeit (feste obere Zeitschranke von Ereignis bis Erkennung) vs. annähernd Echtzeit-Systeme
  - Post Factum-Analyse wird von fast allen Systemen beherrscht
- Granularität der Verarbeitung
  - Verarbeitung der Sensordaten direkt bei Auftreten vs. Sammlung von Gruppen von Beobachtungen
- Ort der Verarbeitung: Lokal, zentral
- Ort der Datensammlung: Einzelne Sensoren, verteilte Systeme

Analytische Verfahren

- Grundkonzepte der Anomalie-Erkennung: Anderson (1980)
- Weiterentwicklung zum ersten formalisierten Modell am SRI durch Peter Neumann und Dorothy Denning
  - Grundlage für das IDES-System des SRI und fast alle modernen IDS
- Metriken
  - Ereigniszähler
  - Zeitintervalle
  - Ressourcenmaße

Statistische Modelle für Anomalieerkennung

- Zufallsvariable x
- Reihe von Beobachtungen $x_1,\ldots,x_n$
- Aufgrund einer oder mehrerer Beobachtungen x_{n+1} muß das IDS entscheiden, ob eine Anomalie vorliegt
- Einfachste Variante: Operative Modelle
  - Vergleiche Beobachtungen gegen feste Grenzwerte
  - Bei Überschreitung von Schwellwert wird Alarm ausgelöst
  - Bestimmung der Grenzwerte durch Heuristiken aus zuvor gesammelten Beobachtungen

Momente 1.+2. Ordnung für Anomalieerkennung (1)

- Verwende Momente erster und zweiter Ordnung
  - Mittelwerte aus bisherigen Beobachtungen

$$\mu_x = \frac{1}{n}\sum_{i=1}^{n} x_i$$

  - Standardabweichung bisheriger Beobachtungen

$$\sigma_x = \sqrt{\frac{1}{n}\left\{\sum_{i=1}^{n} x_i^2 - \frac{1}{n}\left(\sum_{i=1}^{n} x_i\right)^2\right\}}$$

Momente 1.+2. Ordnung für Anomalieerkennung (2)

- Neue Beobachtungen x_{n+1} sind abnormal wenn sie außerhalb des *d* Standardabweichungen entfernten Konfidenzintervalls liegen
  - Tschebyscheff´sche Ungleichung: Wahrscheinlichkeit, daß Beobachtung außerhalb des Intervalls liegt ist $1/d^2$
- Modell ist auf sämtliche Beobachtungen anwendbar
- Wissen über Schranken muß nicht modelliert werden
- Conceptual Drift kann durch stärkere Gewichtung neuerer Beobachtungen einbezogen werden

Multivariate Methoden für Anomalieerkennung

- Erweiterung einfacher statistischer Modelle: Korrelationen zwischen zwei oder mehr Metriken
  - Stellt Relationen zwischen Variablen fest
- Faktoranalyse
  - Stellt Kovarianzen zwischen Menge von Variablen durch endliche Anzahl latenter Variable fest
  - Annahmen: Variable hängen linear zusammen, kein unkorelliertes Rauschen, gesonderte Variationen
  - Erlaubt Schätzung linearer Beziehungen, Betrag der Variationen

Multivariate Methoden: Multidimensionale Skalierung

- Erlaubt Erkennung globaler Ähnlichkeiten zwischen Beobachtungen durch Reduktion des Darstellungsraums der Ähnlichkeiten zwischen den Beobachtungen
- Definiere für je 2 Objekte *i,j* Proximitätsmaß p_{ij} (kleiner, je besser die Ähnlichkeit von *i,j*)
- Konfiguration *X* stellt Menge von *n* Punkten in *m*-dimensionalen Raum dar, *n* x *n* Matrix der n Koordinaten der Punkte auf *m* Achsen eines kartesischen Koordinatensystems. Distanz in *X*:

$$d_{ij} = \sqrt{\sum_{a=1}^{m} \left(x_{ia} - x_{ja} \right)^2}$$

MDS-Methoden

- Verschiedene MDS werden durch Wahl einer Abbildungsfunktion $f(p_{ij})$ bestimmt:
  - Absolute MDS: Distanz zwischen Punkten i,j: $f(p_{ij}) = d_{ij}$
  - Verhältnis-MDS: Verwendet multiplikative Konstante b sodaß $f(p_{ij}) = bp_{ij}$ für alle definierten p_{ij}
  - Intervall-MDS: Verwendet lineare Funktion $f()$
  - Nichtmetrische MDS: Operation findet nicht direkt auf Proximitätsmaß statt; $f()$ ist beliebige ordnungserhaltende Transformation der Proximitätswerte

Markov-Prozesse für Anomalie-Erkennung

- Zufallsprozeß, bei dem Übergangswahrscheinlichkeiten von einem Zustand zum nächsten ausschließlich vom vorhergehenden abhängen:

$$p(S) = p(s_1 \cdots s_n) = p(s_1) \prod_{i=2}^{n} p(s_i \mid s_{i-1})$$

- Als Metrik sind nur Ereigniszähler geeignet, jede einzelne Beobachtung kann Zufallsvariable sein
- Markov-Prozeß erster Ordnung: nur eine einzige vorherige Beobachtung wird berücksichtigt
  - kann als 2d-Matrix aufgefaßt werden
  - Anomalie wenn Wert in Matrix zu groß ist

Zeitreihen für Anomalie-Erkennung

- Reihenfolge und zeitliche Abstände zwischen Beobachtungen
  $x_1 \ldots x_n$ werden erfaßt
- Beobachtungen sind abnorm, wenn Wahrscheinlichkeit, daß Beobachtung zum gemessenen Zeitpunkt eintritt, zu gering ist
- Erlaubt Erfassung von Tendenzen über längere Zeit gegenüber einfachen Verfahren auf Grundlage von Momenten 1. und 2. Ordnung
  - deutlich höherer Aufwand gegenüber einfachen Verfahren

Hidden Markov Modelle für Anomalieerkennung (1)

- HMMs sind doppelt stochastische Prozesse und bestehen aus 4 Komponenten
  - Menge von k Zuständen
  - Zustandsübergangsmatrix A, die Wahrscheinlichkeiten der Übergänge zwischen den einzelnen Zuständen erfaßt. Bei Markov-Prozessen erster Ordnung ist dies
    $$a_{ij} = p(q_{t+1} = s_j \mid q_t = s_i)$$
  - Ausgangsverteilung *B* (diskretes Alphabet, diskrete Wahrscheinlichkeitsverteilung b_j auf diesem Alphabet)
  - Initiale Zustandsverteilung, die angibt, daß das System im Zustand q_i beginnt

Hidden Markov Modelle für Anomalieerkennung (2)

- Zur Anwendung von HMM müssen drei Probleme gelöst werden:
- Beobachtungswahrscheinlichkeiten
  - Gegeben eine Folge von Beobachtungen, Modell: Wahrscheinlichkeit, daß diese Folge unter dem Modell auftritt
- Zustandsfolgenauswahl
  - Bestimme Folge von Zuständen, die unter einem Optimierungskriterium höchste Wahrscheinlichkeit hat, Beobachtungsfolge zu erzeugen
- Training
  - Optimierung Parametermenge sodaß Beobachtungswahrscheinlichkeiten maximiert werden

Hidden Markov Modelle für Anomalieerkennung (3)

- Bestimmung der Beobachtungswahrscheinlichkeiten
  - Verwende Forward-Backward-Algorithmus
  - Forward-Schritt berechnet aufeinander folgende Wahr-scheinlichkeiten partieller Folgen von Beobachtungen
  - Berechnung aller Zustandsfolgen ist nicht notwendig:
    - Ausnutzung der Markov-Eigenschaft
  - Wahrscheinlichkeit einer Beobachtungsfolge ***x*** unter einem Modell kann in $O(k^2T)$ Schritten berechnet werden

Hidden Markov Modelle für Anomalieerkennung (4)

- Zustandsfolgenauswahl
  - Mehrere Zustandsfolgen haben dieselben Beobachtungsfolgen: Kriterium für Auswahl der Folge genügt, es muß nicht genau eine bestimmt werden
  - Häufig verwendetes Kriterium: Zustandsfolge die Wahrscheinlichkeit der Folge unter Präfix maximiert (Viterbi-Algorithmus)
  - Wahrscheinlichkeit entlang von Pfaden, analog zu Forward-Backward-Algorithmus
  - Kann in $O(k^2T)$ Schritten berechnet werden

Hidden Markov Modelle für Anomalieerkennung (5)

- Trainingsverfahren
  - Optimierung von Parametermenge sodaß Wahrscheinlich-keit einer gegebenen Beobachtungsfolge maximal ist
  - Generelles Optimierungsproblem, eine Möglichkeit: Baum-Welch-Verfahren
    - Gradientenbasiert, findet nur lokale Maxima
    - Ausgangswert daher von großer Bedeutung
    - Iterativer Prozeß konvergiert, aber potentiell langsam
- HMMs sind mächtiges Werkzeug,
  aber nur bedingt für Echtzeit-IDS geeignet

Genetische Algorithmen für Anomalieerkennung (1)

- Iteratives Optimierungsverfahren
- Versucht natürliche Selektion und Genetik nachzubilden
  - Variable werden als Gene auf einem Chromosom abgebildet
  - Kandidaten für Lösung des Optimierungsproblems werden als initiale Population betrachtet, Verbesserung der Population durch
    - natürliche Selektion: günstige Charakteristiken pflanzen sich fort
    - Mutation und Rekombination: Zufällige Änderung, Vermischung von „Eltern“-Chromosomen

Genetische Algorithmen für Anomalieerkennung (2)

- Grundmuster genetischer Algorithmen
  - Bestimmung initiale Population (zufällig, Modifikation bestehenden Genoms). Muß hinreichend vielfältig sein
  - Bewertung der Tauglichkeit einzelner Chromosomen: Numerische Repräsentation z.B. durch Bohachevsky-Funktion
  - Selektion der Chromosomen mit höchsten Tauglichkeits-werten, pseudozufällige Verknüpfung mit anderen hochwertigen Chromosomen, Entfernung niederwertiger C.
  - Rekombination und Mutation: Zufällige Paarung von C. führt zu 2 neuen Kind-C. Mutationen ändern lediglich Werte einzelner Gene

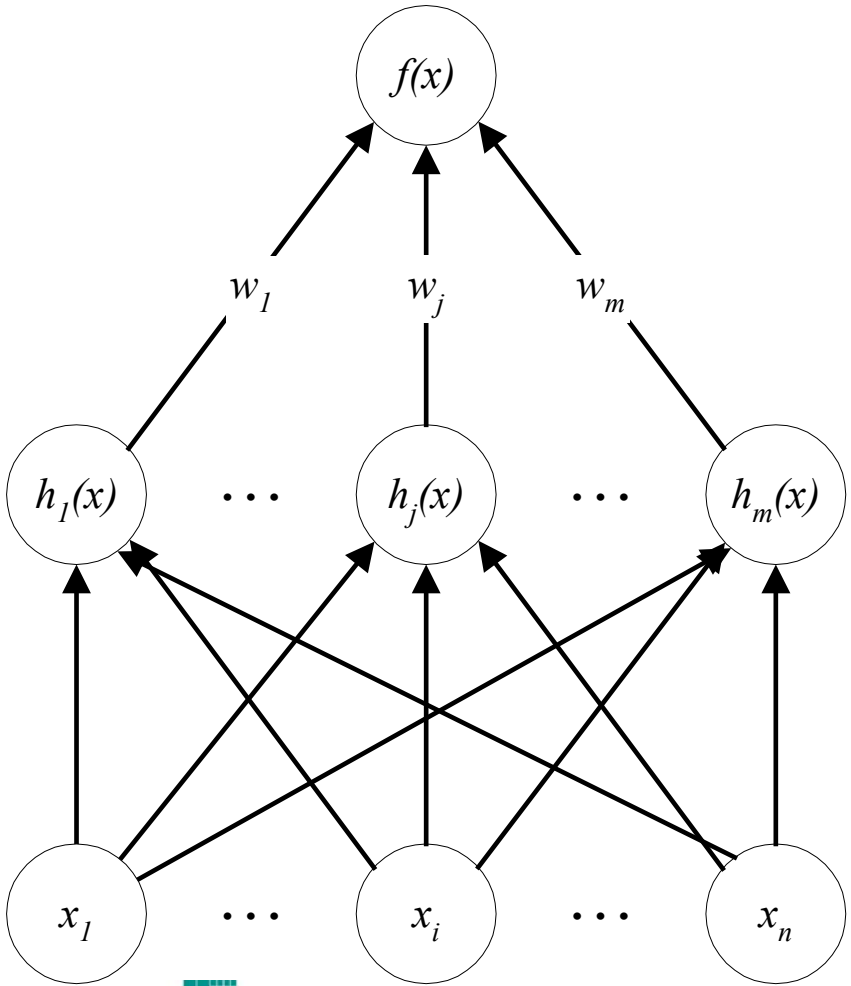
Neuronale Netze für Anomalieerkennung (1)

- Nichtlineare Regressions-/Diskriminanz-/ Datenreduktionsmodelle
- Biophysikalische Analogie: Neuronen „feuern“, wenn Eingänge Schwellwerte erreichen. Schwellwertfunktion ist dabei meist die Sigmoid-Funktion
- Neuronen werden in Ebenen angeordnet und Verarbeitung mit Richtung vorgenommen
- Summe der Klassifizierungsfehler für Trainingsdaten muß reduziert werden
  - Geeignete Auswahl der Gewichtung der Eingänge der Neuronen

Neuronale Netze für Anomalieerkennung (2)

- Geeignete Auswahl der Schwellwertfunktion erlaubt Darstellung als Differentialgleichung
  - Ermöglicht Rückrechnung der Einflüsse von Gewichten über mehrere Schichten
  - Anpassung der Gewichte realisiert Gradientenverfahren
- Andere Varianten:
  - Radial-Basis-Funktionen
    - meist nur mit einer Assoziationsebene
  - Self-Organizing Maps
    - Selbstkonfigurierende topologische Abbildungen

Einfaches Radial-Basis (analog: Perceptron) NN



Fraunhofer IGD Institut Graphische Datenverarbeitung

Immunologisches Analogon für Anomalieerkennung

- Natürliches Immunsystem von Vertebraten muß a priori unbekannte Proteine von eigenen unterscheiden, als gefährlich klassifizieren
  - Zufällige Erkennungsmuster werden in T-Helferzellen eingeprägt
  - Eliminierung von T-Zellen die Autoimmunreaktionen zeigen
- Analogon mit Strings, die Vektoren von Beobachtungen enthalten als Proteinen, Detektoren für derartige Strings
  - Eliminierung von Detektoren für bekannt harmloses Verhalten

Produktionssysteme für Signaturerkennung

- Mengen von Regeln mit Prämissenteil und mindestens einer Konsequenz, evtl. auch mit Alternativzweig
  - Charakteristika von Angriffen oder Teilen werden von Experten in derartige Regeln gefaßt
  - Meist interpretative Systeme (langsam)
  - Stark abhängig von Qualität des von Experten eingegebenen Wissens
    - Menge der Regeln muß möglichst minimal sein und dennoch alle relevanten Verhaltensmuster abdecken
    - Ansonsten „Explosion“ von feuernden Regeln

Zustandsübergangsmodelle für Signaturerkennung

- Modellierung von Angriffen/Vorfällen als Sequenz von diskreten Ereignissen
  - Zuordnung von Ereignissen zu Akteuren
  - Zeitliche Abfolge von Ereignissen
- Modellierung in Zustandsgraphen, Ereignisse sind Übergänge, Knoten repräsentieren Zustände (z.B. Erlangung von root-Rechten)
  - Effiziente Darstellung durch endliche Automaten
  - Parallele Bearbeitung mehrerer Automaten notwendig
  - Intuitive Modellierung von Expertenwissen
  - Unabhängigkeit von zeitlichen Abständen

IDES, NIDES, EMERALD

- Seit 1983 am SRI Forschung zu IDS: Folge von Projekten
  - Viele Grundlagen und theoretische Modelle stammen aus diesem Projekt (Denning, Neumann, Lunt)
  - IDES war primär Anomalieerkennung.
    - Prämisse: Legitime Nutzer verhalten sich vorhersagbar
  - Später: Signaturerkennung mit Experten-/Produktionssystem
  - NIDES ermöglichte Verwendung mehrerer Hosts als Quellen
    - Daten wurden vor Verarbeitung an zentraler Stelle in kanonische Form konvertiert
  - EMERALD ist verteilter Rahmen für Sensoren, Mechanismen

MIDAS

- Für DOCKMASTER (NCSC, Multics) entwickeltes IDS
  - Extern angeschlossene Symbolics-Maschine mit Expertensystem
  - Regelwerk bestand aus mehreren Ebenen, die Verdachtsmomente hierarchisch aufbauend konkretisierten
  - Ebenfalls vorhanden: Analytische Komponente (statistisches Modell nach Neumann, Denning)
  - DOCKMASTER wurde in mehr als 10 Jahren von 1984-1998 (öffentlich an das Internet angeschlossen, prominentes Ziel) nie kompromittiert

Network Security Monitor (NSM)

- Netzwerk-basiertes IDS
  - Jedes zu überwachende Segment erhält Sensor, sämtliche Datenpakete werden überwacht
  - Erfordert Zusammensetzung von Paketen höherer Protokollebene (IP-Fragmente, TCP-Segmente...)
    - Hoher Speicheraufwand, Rechenzeit
  - Extraktion von bidirektionalen Kommunikationspfaden zwischen einzelnen Hosts
    - Reduziertes Datenvolumen wird von Expertensystem verarbeitet

Hyperview

- Betrachtet Revisionsdaten als multivariate Zeitreihe
  - Nutzer sind „dynamische Prozesse“
- Zwei Komponenten: Expertensystem und neuronales Netzwerk
  - Zeitreihen werden auf NN abgebildet
  - Partielle Rückkopplung der Ausgaben des Netzwerkes
    - ermöglicht Speicherung innerhalb des Netzwerkes
  - Expertensystem diente ebenfalls als Eingabemechanismus für Netzwerk: Zusätzliche Information für Entscheidungsprozeß

DIDS

- Weiterentwicklung von NSM, Haystack
- Drei Komponenten:
  - Jeder Host hat lokalen IDS-Monitor der autonom agieren kann und Daten an DIDS Director weiterleitet
  - Jedes Netzwerksegment hat einen NSM-Monitor, der ebenfalls Daten an DIDS Director weiterleitet
  - DIDS Director dient als Sammelstelle, zur Administration des verteilten Systems

IDIOT und Snort

- IDIOT modelliert Angriffe durch Colored Petri Nets
  - ermöglicht parallele Betrachtung mehrerer möglicher Alternativen für Angriffe
  - Es sind beliebig viele Pfade zwischen zwei beliebigen Knoten unter Verwendung unterschiedlicher Übergänge möglich
  - Modell kann anschaulich visualisiert werden
  - Relativ effizient, tauglich für Echtzeit-IDS
- Snort ist einfaches regelbasiertes Netzwerk-IDS
  - Sensoren an konfigurierten Netzwerk-Schnittstellen
  - Frei erhältlich, Regeln werden gut gepflegt