Intrusion Detection

Mohammad Sayad
University of Tehran

Introduction

Intruders – نفوذگران

- A significant issue for networked systems is hostile or unwanted access (either via network or local)
- Intruder attacks range from the benign (simply exploring net to see what is there); to the serious (who attempt to read privileged data, perform unauthorized modifications, or disrupt system).

Intruders – نفوذگران

- clearly a growing publicized problem
  - from "Wily Hacker" in 1986/87
  - to clearly escalating CERT stats
- range
  - benign: explore, still costs resources
  - serious: access/modify data, disrupt system
- led to the development of CERTs
- intruders techniques & behavior patterns constantly shifting, but have common features

Examples of Intrusion – مثالهای نفوذ

- remote root access compromise (to e.g. an email server)
- web server defacement
- guessing / cracking passwords
- copying viewing sensitive data / databases
- Launching a packet sniffer
- Distributing pirated software → botnet
- Taking advantage of an unsecured modem to access the net
- Impersonating a user to reset password
- Using an unattended workstation

Hackers – هکر ها

- Motivated by thrill of access and status محرک اصلی آنها هیجان و مرتبه طلبی است
  - hacking community a strong meritocracy تشکیلات آنها معمولا بر اساس شایسته سالاری است
  - status is determined by level of competence مرتبه بر اساس قابلیت در آن تعیین میشود
- Benign intruders might be tolerable نفوذگر ها غیر مخرب ممکن است قابل تحمل باشند
  - do consume resources and may slow performance
  - can't know in advance whether benign or malicious
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) along with VPNs can help counter
- Awareness led to establishment of CERTs
  - collect / disseminate vulnerability info / responses

Hacker Behavior Example – مثالی از رفتار یک هکر

1. select target using IP lookup tools
2. search target for accessible services
3. identify potentially vulnerable services
4. brute force (guess) passwords
5. use password sniffing tools on the victim's network
6. wait for admin to log on and capture password
7. use password to access the remainder of network

Hacker Behavior Example – مثالی از رفتار هکرها

- Beside brute-forcing, many hackers take advantage of client's software vulnerabilities.
  - Firefox, Snail mail, Adobe products, … have vulnerabilities
  - the hacker deliberately causes errors (e.g. by making an engineered web page or pdf file) to divert the instruction pointer to his program. These codes that take advantage of software vulnerabilities are called Exploits.
- Updates usually patch the vulnerabilities.

Example : DLL Hijacking

9

Criminal Enterprise – سازمانهای مجرمانه

- Organized groups of hackers now a threat
  - corporation / government / loosely affiliated gangs
  - typically young
  - often Eastern European or Russian hackers
  - often target credit cards on e-commerce server
- Criminal hackers usually have specific targets
- Once penetrated act quickly and get out
- IDS / IPS helps but is less effective

10

Criminal Enterprise Behavior – رفتار سازمانهای مجرمانه

1. act quickly and precisely to make their activities harder to detect
2. exploit perimeter via vulnerable ports
3. use trojan horses (hidden software) to leave back doors for re-entry
4. use sniffers to capture passwords
5. make few or no mistakes.

Insider Attacks – حملات داخلی

- Among most difficult to detect and prevent
- Employees have access & systems knowledge
- May be motivated by revenge / entitlement
  - when employment terminated
  - taking customer data when move to competitor
- IDS / IPS may help but also need:
  - (Mandatory) Access Control Mechanisms, least privilege, monitor logs, strong authentication, termination process to block access, mirror data

Intrusion Techniques - روشهای نفوذ

- aim to gain access and/or increase privileges on a system
- often use system / software vulnerabilities
- key goal often is to acquire passwords
  - so then exercise access rights of owner
- basic attack methodology
  - target acquisition and information gathering
  - initial access
  - privilege escalation
  - covering tracks

Password Guessing

- one of the most common attacks
- attacker knows a login (from email/web page etc)
- then attempts to guess password for it
  - defaults, short passwords, common word searches
  - user info (variations on names, birthday, phone, common words/interests)
  - exhaustively searching all possible passwords
- success depends on password chosen by user
- surveys show that many users choose poor passwords

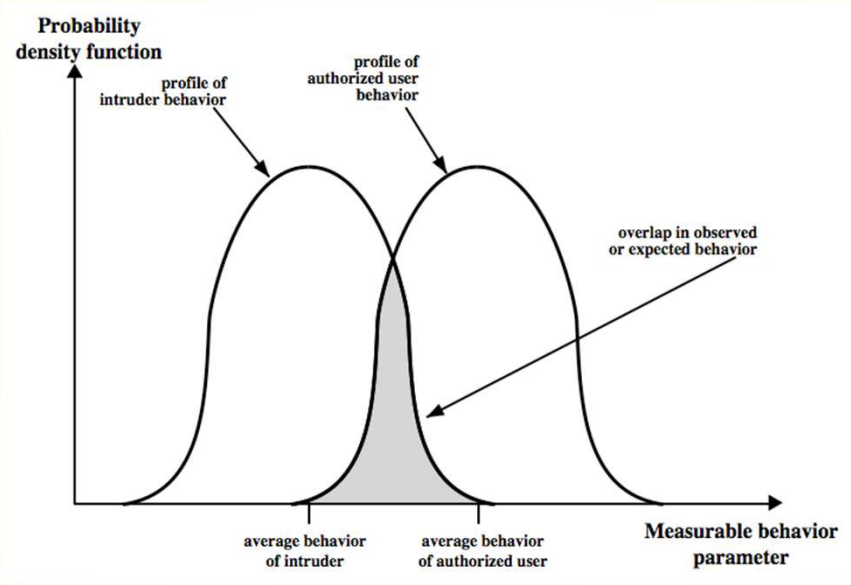
Password Capture

- another attack involves **password capture**
  - watching over shoulder as password is entered
  - using a trojan horse program to collect
  - monitoring an insecure network login
    - eg. telnet, FTP, web, email
- users need to be educated to use suitable precautions/countermeasures

Intrusion Detection Systems – سیستمهای تشخیص نفوذ

- inevitably there will be security failures
- so we also need to detect intrusions to
  - block if detected quickly
  - act as deterrent
  - collect info to improve security later on
- IDSs assume intruder will behave differently to a legitimate user
  - But there's an imperfect distinction between them

Intrusion Detection – طیف رفتاری نرمال و غیر نرمال

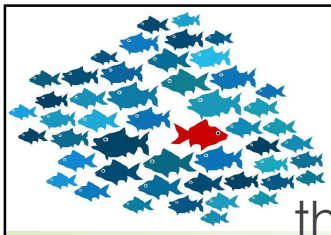


17

Approaches to Intrusion Detection

- Anomaly detection تشخیص رفتار نامتعارف
  - attempts to define normal/expected behavior
  - threshold
  - profile based
- Signature-based detection تشخیص امضای حملات
  - penetration identification
  - Knows the signatures of known attacks

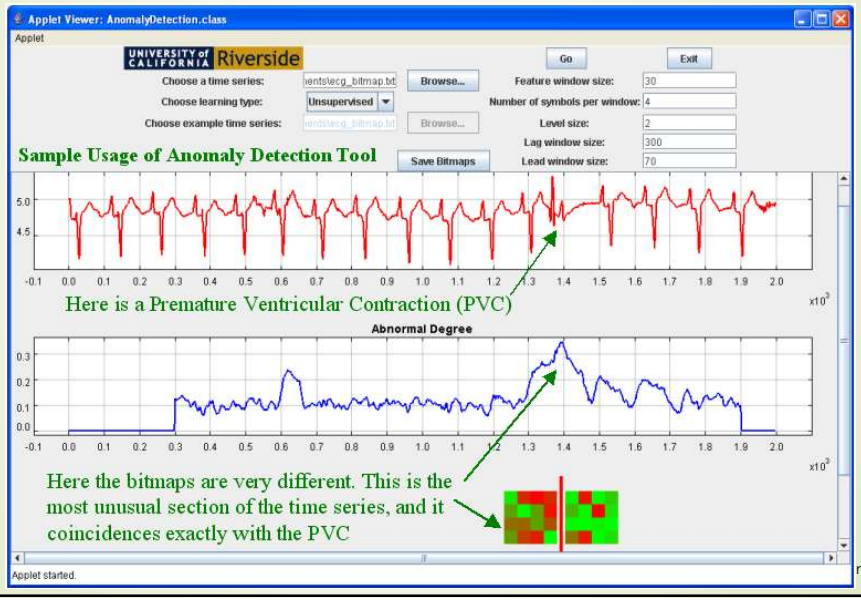
18



(Statistical) Anomaly Detection
تشخیص رفتار نامتعارف (آماری)

- threshold detection - تشخیص عبور از یک آستانه
  - count occurrences of specific event over time
  - if exceed reasonable value assume intrusion
  - alone is a crude & ineffective detector
- profile based - مبتنی بر پروفایل
  - characterize past behavior of users
  - detect significant deviations from this
  - profile consists of multiple parameters

نمونه کاربرد Anomaly Detection در حوزه پزشکی



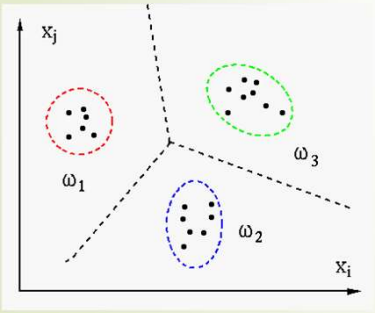
Audit Record Analysis

تحلیل اسناد ممیزی

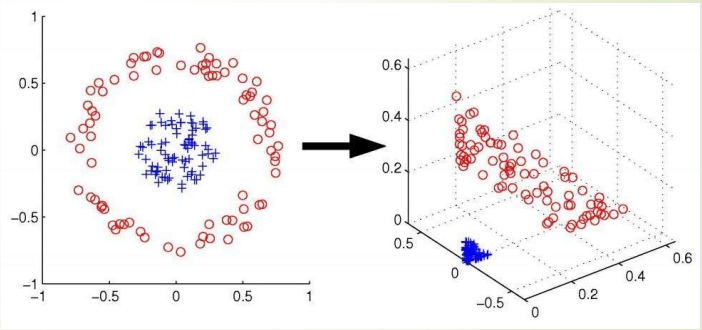
- foundation of statistical approaches
- analyze records to get metrics over time
  - counter, gauge, interval timer, resource use
- use various tests on these to determine if current behavior is acceptable
  - mean & standard deviation, multivariate, markov process, time series, operational
- An advantage of the use of statistical profiles is that no prior knowledge used.

A Classic Method for Intrusion Detection (Classification)

Define Features That help differentiate between normal and abnormal behavior → Build up a classifier → Train Test



Example 1



Example 2

Signature-based Intrusion Detection

تشخیص نفوذ از روی امضاء

- observe events on system & match them with the pre-known patterns to decide if activity is suspicious or not
- It requires a database of known attacks.
- It might miss an attack if it does not have its signature (e.g. zero-day attacks)

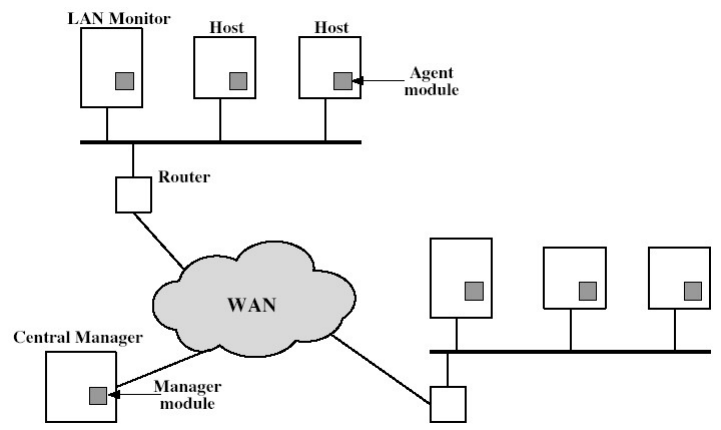
False Detections – تشخیص غلط

- practically an intrusion detection system needs to detect a substantial percentage of intrusions with few false alarms
  - if an intrusion is not detected by mistake -> false negative
  - if an intrusion is falsely detected -> false positive
  - this is very hard to make a perfect IDS which minimizes both

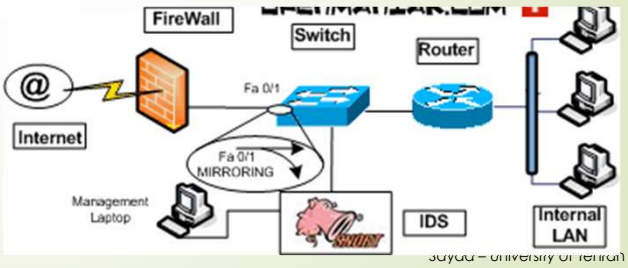
Distributed Intrusion Detection
تشخیص نفوذ توزیع یافته

- traditional focus is on single systems
- but typically have networked systems
- more effective defense has these working together to detect intrusions
- issues
  - dealing with varying audit record formats
  - integrity & confidentiality of networked data
  - centralized or decentralized architecture

Distributed Intrusion Detection – Architecture
تشخیص نفوذ توزیع یافته – معماری



- An open-source IDS
- Network-based
- Has a signature database of many attacks
- Can sniff packets



27

Intrusion Prevention System (IPS)

سیستم جلوگیری از نفوذ

- IDS ها ماجولهای Passive ای هستند به این معنی که پس از آنکه حمله اتفاق افتاد، تازه آن را تشخیص و گزارش میدهد. مقابله با حمله وظیفه آنها نیست. مقابله یا بصورت دستی انجام میشود و یا ماجول دیگری آنرا انجام میدهد.

- نمونه ماجولهای Active (Proactive) سیستمهای IPS است که جلوی نفوذ را از ابتدا با تمهیداتی که می اندیشد میگیرد. مثلا دائما با اسکن سیستم پورتهای غیر لازو م راههای نفوذ را میبندد.

28

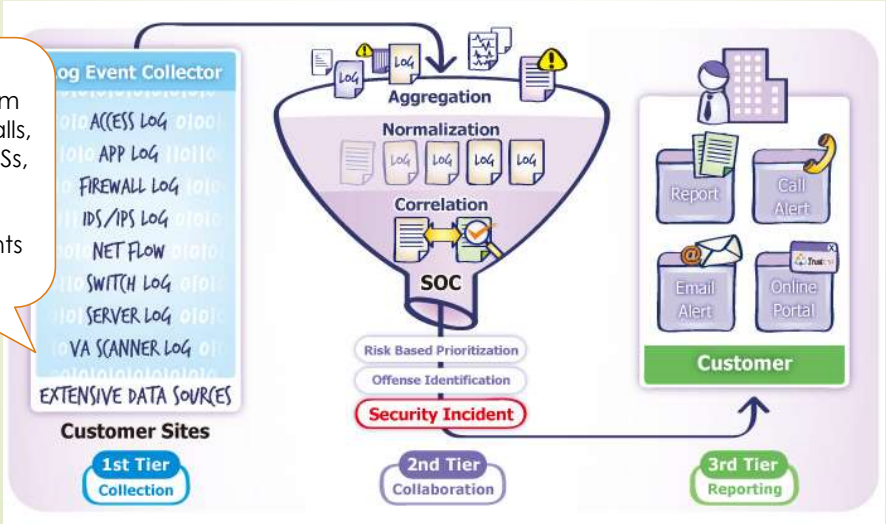
Honeypots – ظرف عسل

- decoy systems to lure attackers
  - away from accessing critical systems
  - to collect information of their activities
  - to encourage attacker to stay on system so administrator can respond
- are filled with fabricated information
- instrumented to collect detailed information on attackers activities
- single or multiple networked systems

Security Operation Center (SOC)

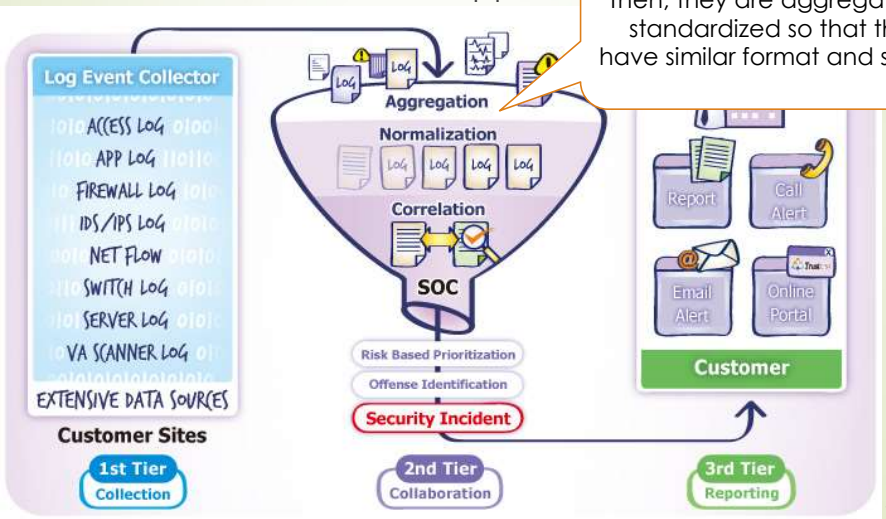
- It's a combination of multiple technologies to detect intrusions. It's a passive center. When an attack happens, it detects and reports.

Logs are collected from sensors (Firewalls, IDSs, Clients OSs, Antiviruses, Honeypots, Routers, Agents installed,…)



Security Operation Center (SOC)

- It's a combination of multiple technologies to detect intrusions. It's a passive center. When an attack happens,

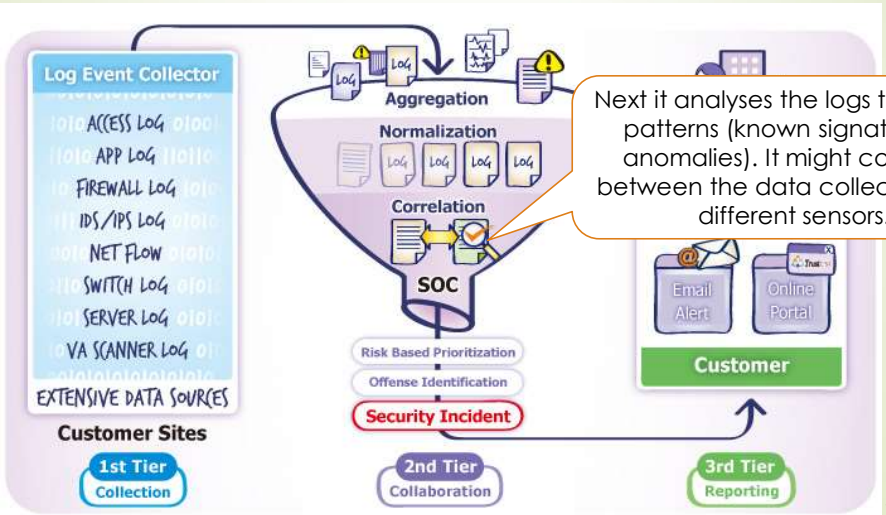


31

– University of Tehran

Security Operation Center (SOC)

- It's a combination of multiple technologies to detect intrusions. It's a passive center. When an attack happens, it detects and reports.

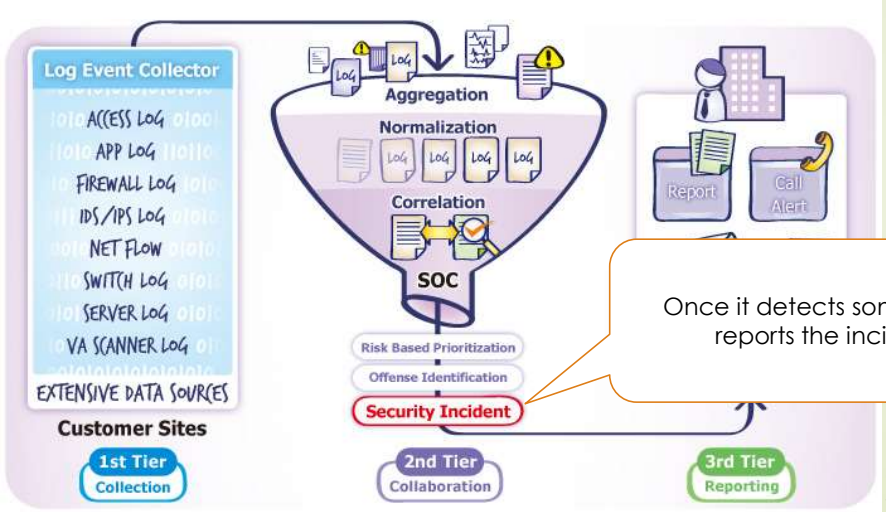


32

– University of Tehran

Security Operation Center (SOC)

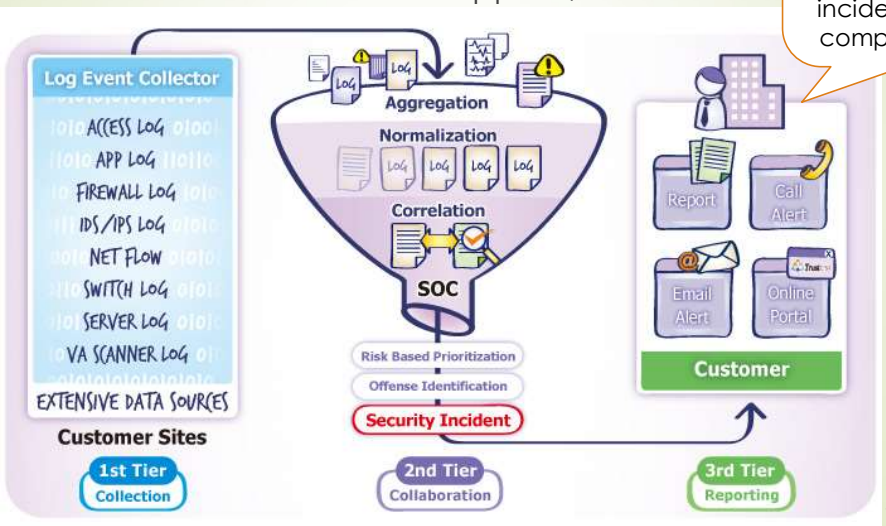
- It's a combination of multiple technologies to detect intrusions. It's a passive center. When an attack happens, it detects and reports.



Security Operation Center (SOC)

- It's a combination of multiple technologies to detect in
  passive center. When an attack happens, it detects an

SOC issues alerts for proper reaction. SOC is passive and does not react by itself. You need an incident handler to complement SOC.



Password Management – مدیریت پسورد

- front-line defense against intruders
- users supply both:
  - login – determines privileges of that user
  - password – to identify them
- passwords often stored encrypted
  - Unix uses multiple DES (variant with salt)
  - more recent systems use crypto hash function
- should protect password file on system

Password Studies

مطالعاتی در مورد پسورد ها

- Purdue 1992 - many short passwords (3% are 3 chars only)
- A study by Klein in1990 -> many guessable passwords (25% in 14000 UNIX password files)
- conclusion is that users choose poor passwords too often
- need some approach to counter this

Managing Passwords

1. Educate people for choosing good passwords
   - minimum length (>6) , not dictionary words, a mix of upper & lower case letters, numbers, punctuation, etc.
   - But users ignore guidelines
2. Let computer create passwords
   - FIPS PUB 181 one of best generators
   - But poor user acceptance
3. Proactive Checking (most common)
   - allow users to select own password
   - But have system verify if it is acceptable
4. Reactive Checking
   - Let users choose their own passwords but reactively run password guessing tools and report the bad ones.
   - But it's resource-consuming

Where can I do research?

- Don't worry, there's plenty of room:
  - Profiling (e.g. behavioral feature selection)
  - Pattern Recognition & Data Mining
  - Feature Selection & Classification
  - Optimization
  - Modelling (Hybrid Automata, Petri Networks, Markov Models, etc.).
  - Cross correlating data (Evidence theory, (Bayesian) inference, …)
  - and many more ….

It's easy!

Future Generation Computer Systems

Volume 37, July 2014, Pages 127–140

Special Section: Innovative Methods and Algorithms for Advanced Data-Intensive Computing

Special Section: Semantics, Intelligent processing and services for big data

Special Section: Advances in Data-Intensive Modelling and Simulation

Special Section: Hybrid Intelligence for Growing Internet and its Applications

Mining network data for intrusion detection through combinir
SVMs with ant colony networks

Wenying Feng

Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication

Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song

Constructing important features from massive network traffic for lightweight intrusion detection

Intrusion Detection for MANET to Detect Unknown Attacks Using Genetic Algorithm

M. Lalli
Department of Computer Science
Bharathidasan University
Trichy, India
Lalli_bdu@yahoo.co.in

A Cooperative Botnet Profiling and Detection in Virtualized Environment

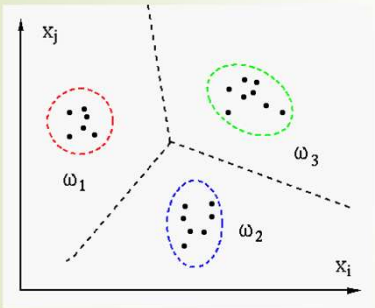
Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems

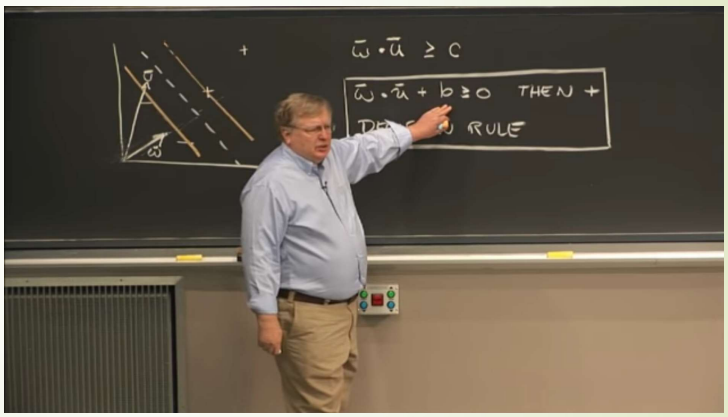
Robert Mitchell and Ing-Ray Chen, *Member, IEEE*

39

Sayad – University of Tehran

Must See: MIT AI Course, Lecture 16, SVMs





40

Sayad – University of Tehran

The End of Intrusion Detection

Scheduling
Presentations