

Subject: Civil Eng
Date: 4/4/11

to fit

Webcast

Text Books:

- Fundamentals of Computer Security Technology, Edward Amoroso (Engineering), Prentice-Hall, 1994
- Computer Security: Art and Science, Matt Bishop, 2002
- Security In Computing, Pfleeger and Shari Pfleeger, 2002

Contents:

1. Basic Concepts
2. Threat Modeling
3. Penetration Testing
4. Malicious Logic (Trojan, Horse, worm, ...) (Malware) Malice → object
5. Risk Analysis
6. Security Policies and Models (label, Information Model, ...)
7. Availability
8. Security Mechanisms (Auth, Cryptography, Access Control, ...)

Grading:

- Homework 2
- Midterm Exam 6
- Final Exam 8
- Penetration Test Lab. 4

PqPCO

Subject

Date

9/4/21

Threat:

A threat to a computer system will be defined as any

Potential occurrence, malicious or otherwise, that can have an undesirable effect on the assets and resources associated

with a computer system.

Non-Malicious intentional

Malicious intentional

Vulnerability:

A vulnerability of a computer system is some unfortunate characteristics that makes it possible for a threat to potentially occur.

Attack:

An attack to a computer system is some action taken by a malicious intruder that involves the exploitation

of certain vulnerability in order to cause an existing threat to occur.

Exploit the vulnerability

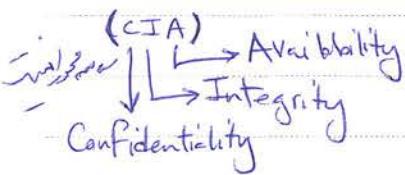
Attack
intruder
exploit
vulnerability

Subject

Date

9/4/21

Types of Threats:



Threat to Confidentiality
Unauthorized disclosure

Disclosure: Confidentiality → unauthorized disclosure

Dissemination of information to an individual for whom
the information should not be seen.

unauthorized disclosure

Threat to Integrity: Integrity → unauthorized modification

Unauthorized change to information stored on a computer
system or in transit between computer systems.

DoS

Denial of Service: Availability →
(DoS)

The denial of service threat arises whenever access to
some computer system resource is intentionally blocked
as a result of a malicious action taken by another user.

Threat to Availability → Unauthorized modification → Denial of Service

Threat to Integrity → Denial of Service

Subject

Page _____

98,4,11

(~~is~~ unauthorized no (05/11/20))

Confidentiality :

Confidentiality : concealment of information or resources

Security mechanism: Enforce policy / User enforces security policies

- Confidentiality & Data Policy

• Col Access Control (with optional Ctrls, Ctrls, Confidentiality)

• End-to-End Encryption • Access Control • Privacy & Security

(مختصر) مختصر مختصر مختصر مختصر

\rightarrow جیسا کوئی بھائی نہیں تو اس کو اپنے بھائی کا سمجھو

لوران - مرزا خاں

(رخصی ملک، و دارایی ملکی در این مورد ممکن است از این نظر از این دو نوع *existences* محسوب شود.)

لـمـكـ تـعـلـمـنـي رـزـقـ عـلـمـهـ اـسـمـهـ، نـزـلـ سـلـمـهـ لـرـزـحـهـ

خود سلیمانی در زن باره محفله سه کتاب مجموعه از سه نوشته

حرب جوہر کی سارے محرکات اور

۲۰

Subject

Date

٩٤, ٩, ٢٠

TCB: Trusted Computing Base

trust \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$ \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$ \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$

جِنَاحَةُ الْمُؤْمِنَاتِ \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$ \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$

Achievement \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$ \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$

Work \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$ \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$

Integrity:

Trustworthiness \rightarrow

\rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$

Unauthorized \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$

Data Integrity \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$

Integrity

Origin Integrity \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$

(Authentication)

\rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$

trustworthy, attacker

Integrity \rightarrow $\text{جِنَاحَةُ الْمُؤْمِنَاتِ}$

Integrity is Authentication *

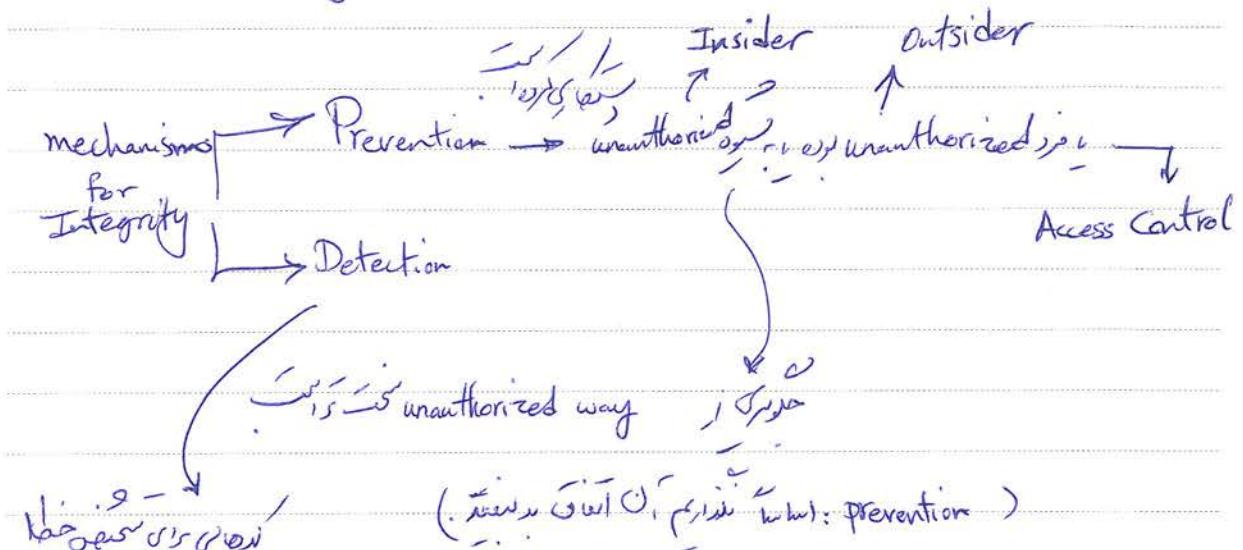
Integrity is Authentication, attacker intention (دَرْجَاتِ الْمُؤْمِنَاتِ)

Subject

Date

١٤٣٧

البيانات متسقة مع مصدرها



m	$H(m)$
Hash	

m	$H_p(m)$
Hash	

in this way the attacker

will detect the modification

(أصل البيانات متسقة مع مصدرها . الملاحظات المعاينة : (أصل البيانات متسقة مع مصدرها . الملاحظات المعاينة :

Subject

Date

٢٤ / ٧ / ٢٣

Availability:

از خواسته است که سرور می تواند طبقه ای داشته باشد که در آن می تواند خود را بخوبی نشاند. اما ممکن است این خواسته را نتوانند از خواسته داشت.

دلایلی که از این خواسته برخوردار نباشد این زمانی خواهد بود که خواسته داشت

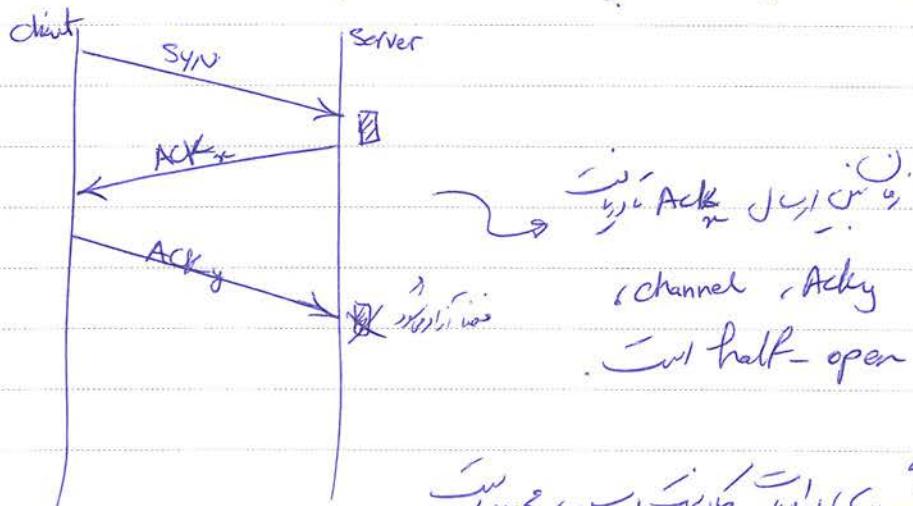
SYN Flooding

از خواسته است که سرور این خواسته را پذیرفته باشد

از خواسته است که سرور این خواسته را پذیرفته باشد. اگر این خواسته را پذیرفته باشد این خواسته را نمی شناسد و این خواسته را نمی شناسد. اگر این خواسته را پذیرفته باشد این خواسته را نمی شناسد و این خواسته را نمی شناسد.

و اگر این خواسته را پذیرفته باشد این خواسته را نمی شناسد و این خواسته را نمی شناسد.

Tcp three way handshake, TCP چهار مرحله ای است (SYN Flooding)



نهایتی که این خواسته را در درون خود دارد

سیمبل ها که نمی شناسد خود را نمی شناسد

Subject

Date

٩٤/٧/٢٠

میکسین SYN چیزی که جاسوس اتکر جا



میکسین جاسوس اتکر جا

میکسین (attacker) \rightarrow میکسین IP

(SYN-cookie) . میکسین کوکی را بفرست

میکسین Bandwidth را
↓

میکسین از این طریق از این طریق از این طریق

Shreyas:

(میکسین)

- disclosure \rightarrow unauthorized access to information
- deception \rightarrow acceptance of false data
- disruption \rightarrow interruption or prevention of correct operation.
- usurpation \rightarrow unauthorized control of some part of a system.

میکسین (میکسین) میکسین

Snooping \rightarrow unauthorized interception of information. (Disclosure)

Passive wiretapping

میکسین

میکسین

میکسین

R4PCC

Subject Computer Security
Date 9/1/2021

- modification or alteration → Deception

↳ Active wiretapping and usurpation

.Deception (msg. of its effect)

.Deception (msg. Buffer overflow)

- masquerading or spoofing → Impersonation

(false data) deception

phishing

Dos → IP spoofing

SSL, integrity (Integrity)
Digital Signature

SSL Back tracking

- Repudiation of Origin

Original

Repudiation of Origin

Digital Signature : Receipt
(receipt)

- Delay → Disruption → disruption

- Denial of Service

Subject

Date

ape, 4, YR

Policy:

الـ ~~statement~~ statement



Security Policy

بيان خطة محددة لتنفيذ المعايير وتحقيقها

(requirement, معايير)

Mechanism: policy enforcement

Impediments:

عوائق وصعوبات

- Attacker Intent → المقصود من المهاجم

Do 20 I = 1.100 (American Viking Venus
Probe)
Fortran:

D020I = 1.100

Do 20 I = 1.100

- Security and Usability

جودة البيانات، جودة الاستخدام، الأمان، سلامة، Usability، Security
+ معلمات راسخة، Strong Password

- Retrofit

تعديل، تغيير، إدخال معايير

بيان خطة لتحقيقها

patch, Update

Security Provable → Secure → Retrofit

Assumption about TCB (Trusted Computer Base) / Axiomatic view

پس از این راه است میتوان بگویی که سیستم امن است.

- Assurance → جعیت از این دلایل

راهکار: مراحل امنیتی

- Security Requirements → Policy

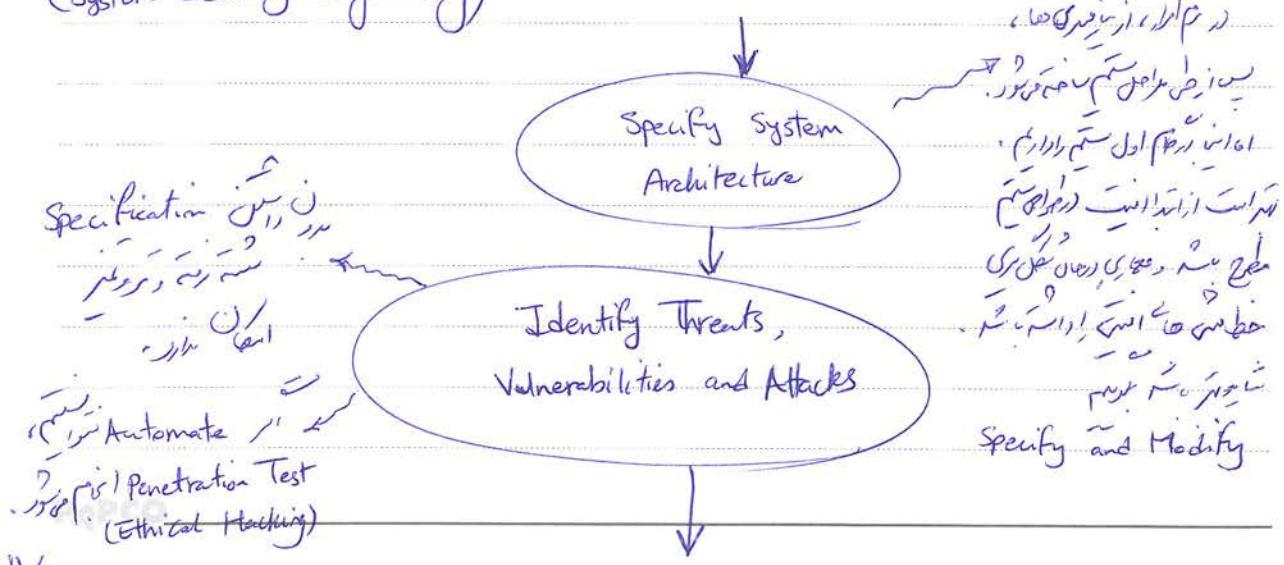
: این مرحله ایجاد مدل امنیتی برای life cycle

A security life cycle: Process model

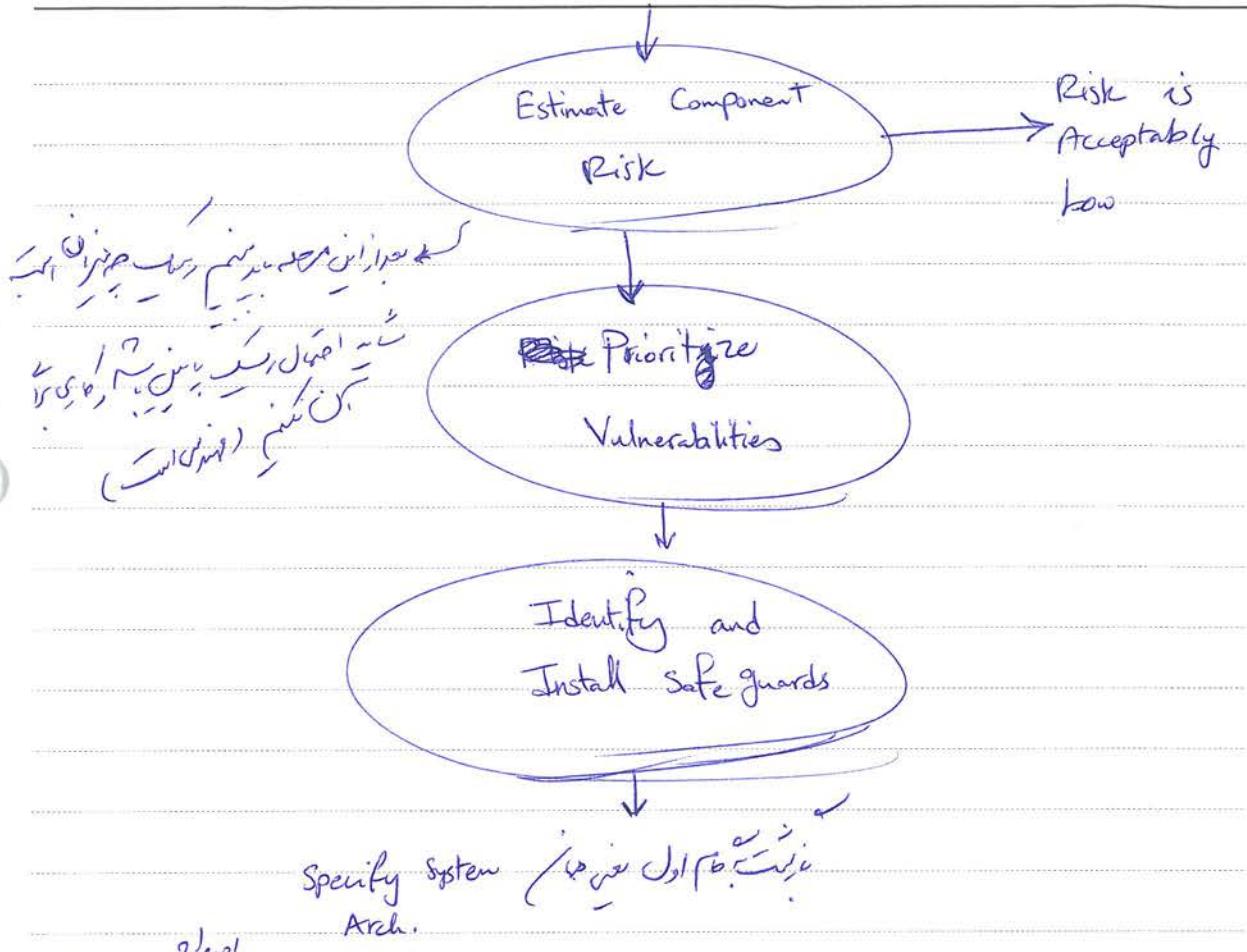
UML-Sec: نمودار زمانی ایجاد نیازهای امنیتی

Functional, Non-functional Requirements, Security Requirements

(System Security Engineering)



Subject _____
Date _____



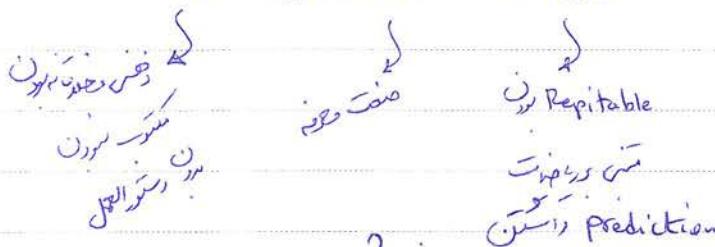
Wael
(Arms Race)

built-in security - Risk is acceptable
Requirement Eng. Springer (مقدمة إلى تصميم متطلبات)
Bishop (Introduction) /
Algebraic
Algebraic
PAPCO

Journal (Magazine) IEEE Security and Policy
Special Issue
Science of Computer Security

: علم علوم

art → craft → science



(علم علوم تكنولوجيا) Civil Science, craft و science Civil

Civil Science, craft و science life cycle is

Tool, approach, process of

Threats:

Violence, Review, inspection

In) Hospital's patient and medical information

- Patient's medical information is corrupted.
- Billing information is corrupted.
- Confidential patient information is disclosed.
- Intern schedules are compromised.

Subject _____
Date _____

(OCTAVE 3rd): پرو

بررسی امنیت سیستم، ناکامی

- Dubious Completeness → *مشهودی میزان*
(Unstructured vs.). *بررسی امنیت، Brainstorming*

- Lack of Rationale → *براساس این*
(Rational vs. Rationale)

↓
wise

↓
base

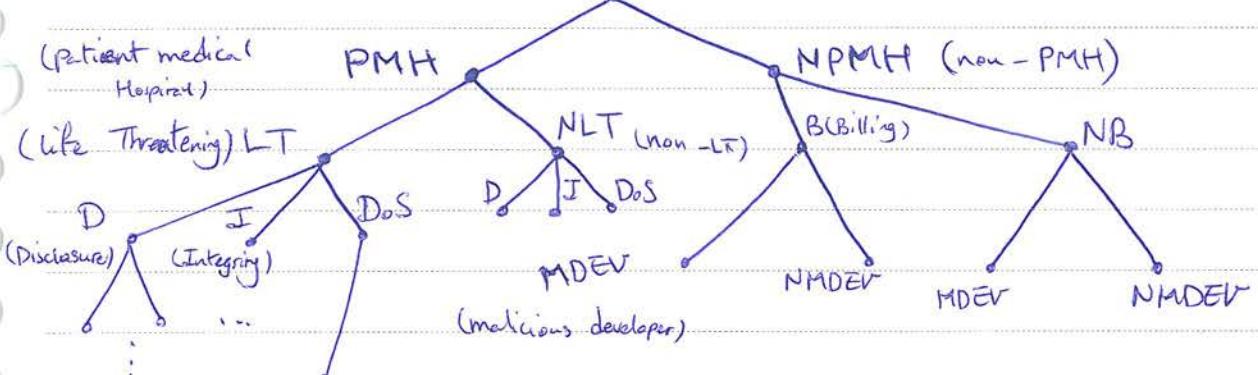
- Possible inconsistencies → *پیشگیری از خطا*

Brainstorming *بررسی امنیت، پیشگیری از خطا* در *WIS, 6+2* و *OWASP*

Threat Trees: (RN (Security))

پیشگیری از خطا

HCST (Hospital Computer System Threat)



Confidential patient
information is not
available

بررسی امنیت، Brainstorming

Subject: English
Date: 9/14/10

پریولیتیزیشن (Prioritization) (or "and all") in Cryptool شناساندن

(کلیجیات) (Priority)

(Cryptool) جس شنیشتر؟ (همه کارهای را در این مدت زمان پنهان نمایند)

Threat Scenario:

..... در مورد اینجا

- A series of events through which a natural or intelligent adversary could cause harm.

- how
- why
- who

who?

How?

What? (چی)

An employee uses a laptop running a packet sniffer in

order to eavesdrop on data sent over the LAN connected

to his office. He reads confidential management documents

attached to emails as they are in transit between managers, and then sells these documents to a competitor.

10) chain of events

why?

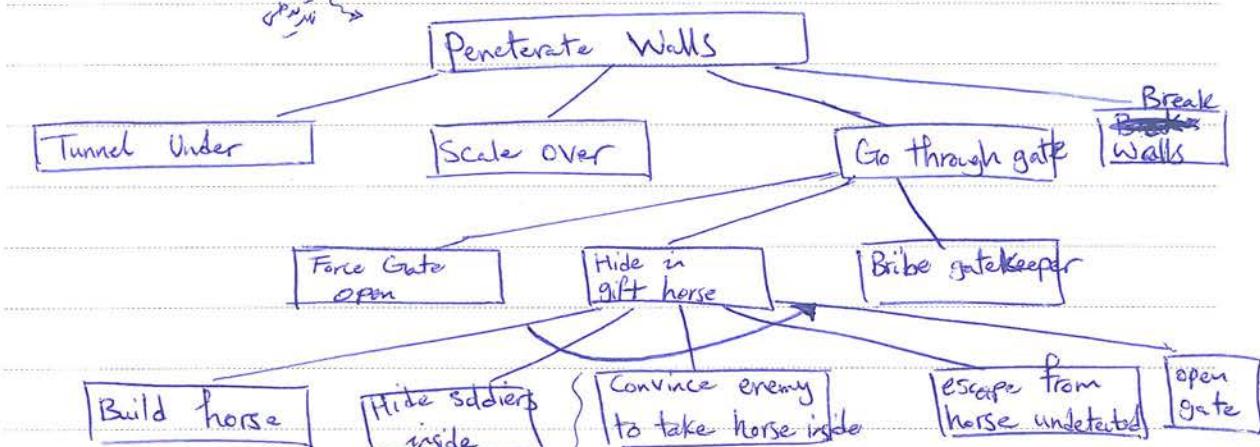
Subject
Date

میکرو پر سیگنالز برباد کسٹنگ - Micro wave Broad Casting -

(plain text) محظوظاً! هو البريد الإلكتروني -

- وقت در استفاده از طیور در حفاظت از محیط زیست می‌تواند بسیار مفید باشد (مثلاً برای این پروژه).

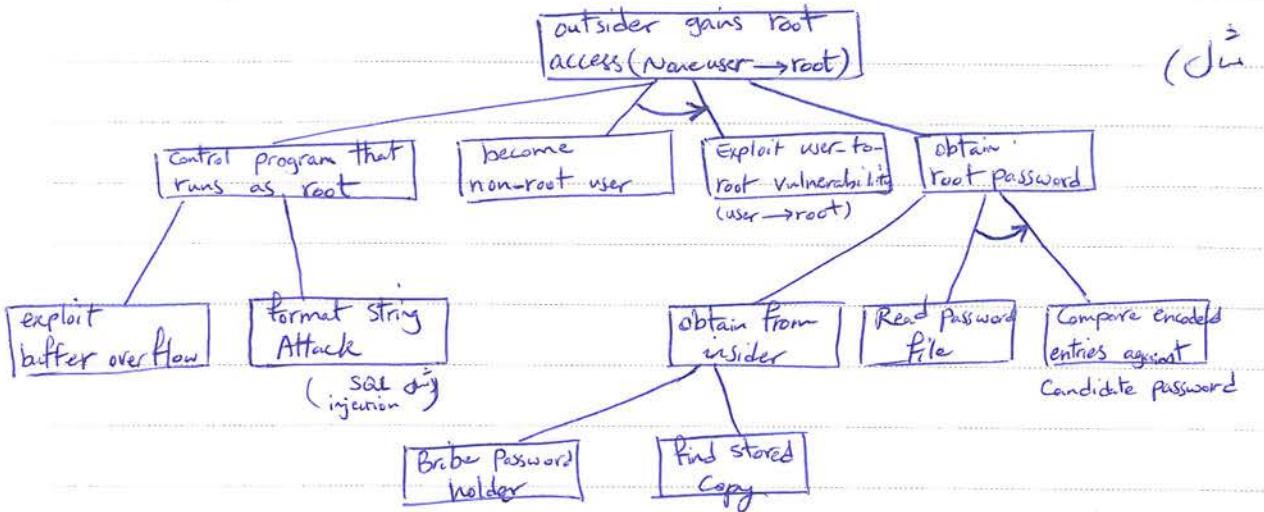
کے دراصل کدم رفتہ رسم
یہ کہتے ہوئے عقیدہ ہے!



وَالْمُؤْمِنُونَ هُمُ الْأَوَّلُونَ

دیگر سایر اینها را می‌توان باز کردن چنین چیزی که در آنها می‌باشد، از آنها جدا کرد.

Subject جغرافیا
Date ۹۷/۴/۱۰



لـ رسـم لـ نـصـاـتـاـ، دـورـهـ زـارـيـ الـلـهـ مـعـذـرـرـ:

وَيُمْسِكُ بِهِ الْمُؤْمِنُونَ (۱۰) وَمَا يَرَى مِنْ هَذِهِ الْأَفْوَاتِ فَلَا يُنَبِّهُ عَنْهَا إِنَّ اللَّهَ لَغَنِيٌّ عَنِ الْمُحْشَدِينَ

(inter-leaving) $\text{N}^{+}\text{O}^{+}\text{P}^{+}\text{S}^{+}\text{Cl}^{-}\text{Br}^{-}$

Oval arms race

Greens, Greens, we're never green again.

مکانیزم ایجاد پیشگیری

Directed Acyclic

Graph (DAG)

وَالْمُكَبَّلُونَ إِنَّمَا يُعَذَّبُونَ أَنفُسَهُمْ وَلَا يُعَذَّبُونَ مَنْ يَرِيدُ
أَنْ يَعْذَبَهُمْ وَلَا يُؤْتَى لِلْمُجْرِمِ حُكْمُ الْمُحْكَمِ

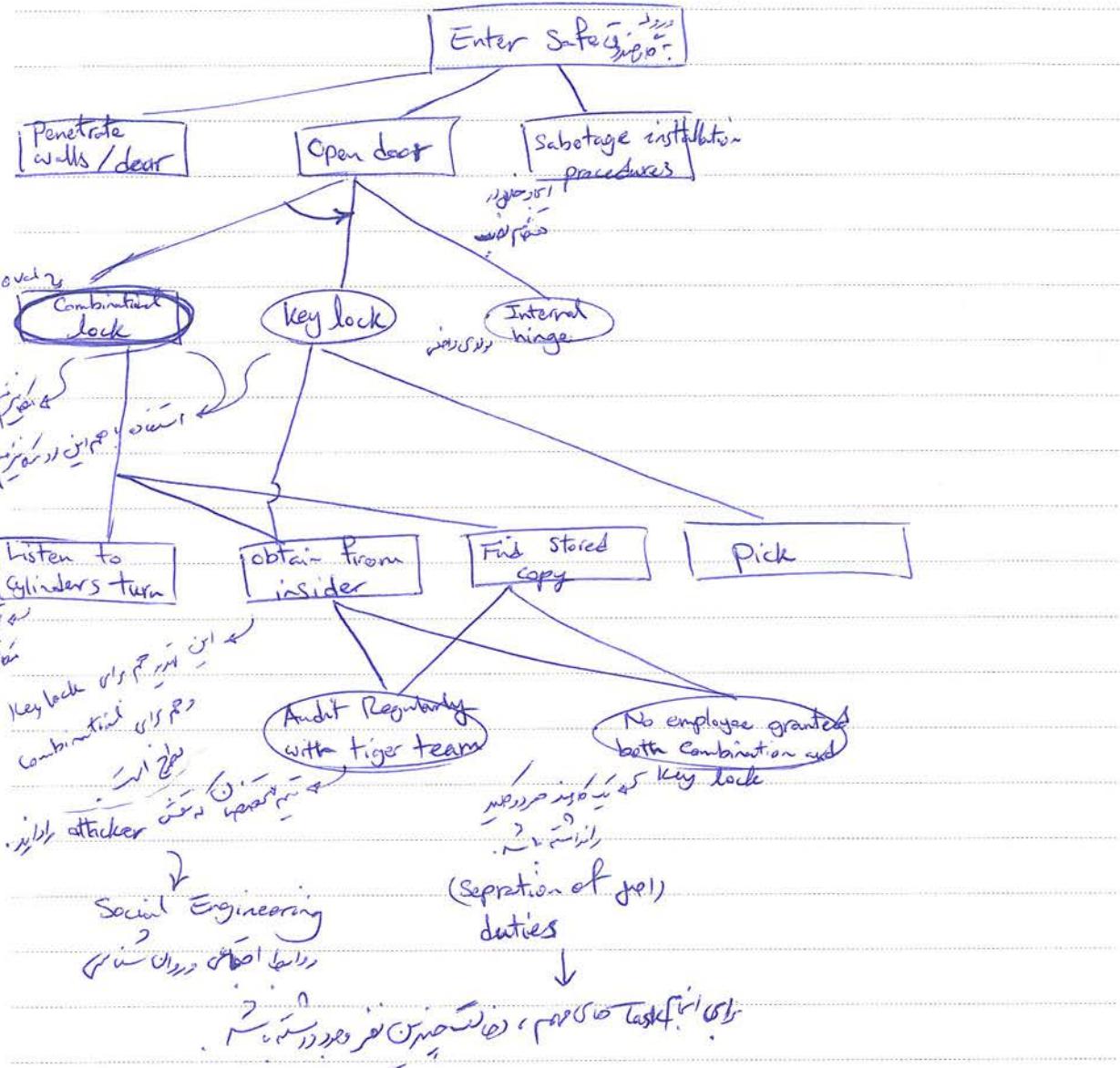
Subject

Date

9/15/2023

• چند پرسنل ایجاد کردن و اینها را برای ایجاد آسیب در سیستم استفاده می‌کنند.

• اینها را برای ایجاد آسیب در سیستم استفاده می‌کنند.



Subject

Date

qc, v, k

جیئن تیسٹنگ اسے بڑی طور پر سے کہا جاتا ہے

Penetration Testing (study):

جو ایک اچھا اور امیدوار فارماں کی طرف سے انجام دیا جائے تو Penetration Testing ہے۔

وہ ایک اتکر ایسا ہے جو اسے لئے Civil Testing ہے۔

Ethical Hackers or Tiger Team

* Criminal Hacker

Ethical Hacking

Definition - A penetration testing (study) is a test for

evaluating the strength of all security controls on the computer system. The goal of the test is to violate the site security policy.

جیئن تیسٹنگ اسے کہا جاتا ہے۔ اسے متن سوراہیں

literature کے طبق موجود ہے۔

Threat Tree ہے۔

اسے تیز و سریع ریٹریویو کہا جاتا ہے۔

Subject	Date	Anderson's Threat Matrix	Penetrator not Authorized to use Data/Program Resource	Penetrator Authorized to use Data/Program Resource
			CASE A: External Penetration	X
	9/2, V, F	Penetrator Authorized to use Computer	CASE B: Internal penetration	CASE C: Misfeasance

Layers:

- | | |
|---|---|
| 1 | <p>As an internal attacker
(misfeasance) → [Bypassing authorization mechanism, ...]</p> |
| 2 | <p>As an external attacker with access to the system
(How to access an account?)
[Guessing Passwords, Looking for unprotected accounts, attacking network servers, ...]</p> |
| 3 | <p>As an external attacker with no knowledge of the system
(How to access the system?)
[Social Engineering and/or persistence]</p> |

external attacker →
 - account, web service
 - no account
 - Technical problem

account, web service
 - no account
 - Technical problem

internal problem
 - privilege (user, administrator)

internal problem
 - user, administrator, root, root password

Subject Civilization
Date 9/11/2014

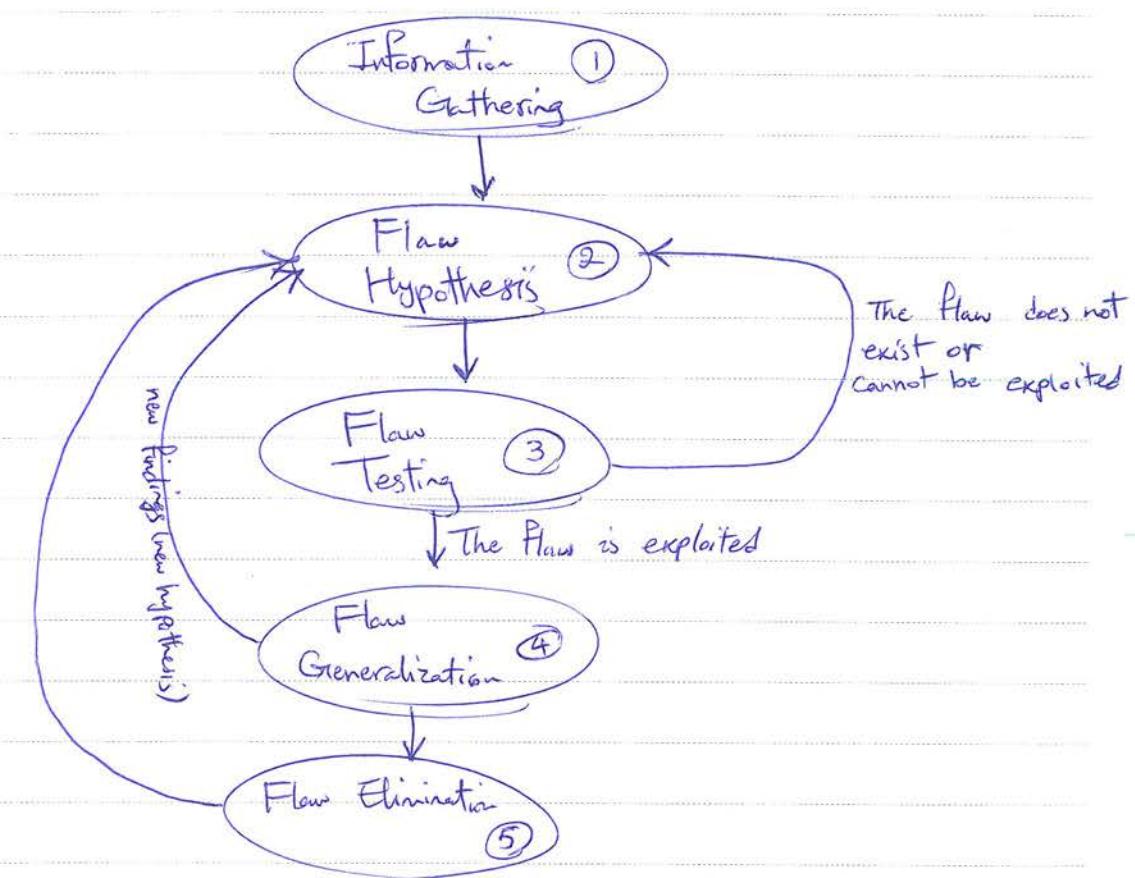
• Repetitive documentation وهي تكرار في الوثائق

مشكلة اجتماعية

FHM (Flow Hypothesis Methodology):

• cycle life cycle

• new hypothesis framework



Subject

Date

94 ✓, K

- (1) **buffer overflow** *برگشتن از حاشیه*
 - **Root user** *کاربر روت*
 - **privileged user** *کاربر با صفت خاص*
 - **installation** *نصب*
 - **incomplete input validation** *تایید ورودی ناکامل*
- (2) **race condition** *وضعیت مغایر*
 - **deadlock** *کلیچ گیری*
 - **deadlock avoidance** *کلیچ گیری پنهان*
- (3) **race condition** *وضعیت مغایر*
 - **deadlock** *کلیچ گیری*
 - **deadlock avoidance** *کلیچ گیری پنهان*
- (4) **race condition** *وضعیت مغایر*
 - **deadlock** *کلیچ گیری*
 - **deadlock avoidance** *کلیچ گیری پنهان*

Penetration of the Michigan Terminal System (Jin)

⇒ سے ملے جائیں

Goal: To acquire access to the terminal control system.

ووچهارمین نسل میانی دعا خود را در درجه ۵۰ دراین مجموعه داشت، در این درجات از

Layer: Attacker has access to an authorized account (Layer 1).
(CASE C in Anderson's Penetration Matrix)

Subject

Date

AF, VP

for IT

IT

الى امن المعلومات وتقنيات الحاسوب

Anderson PenTest

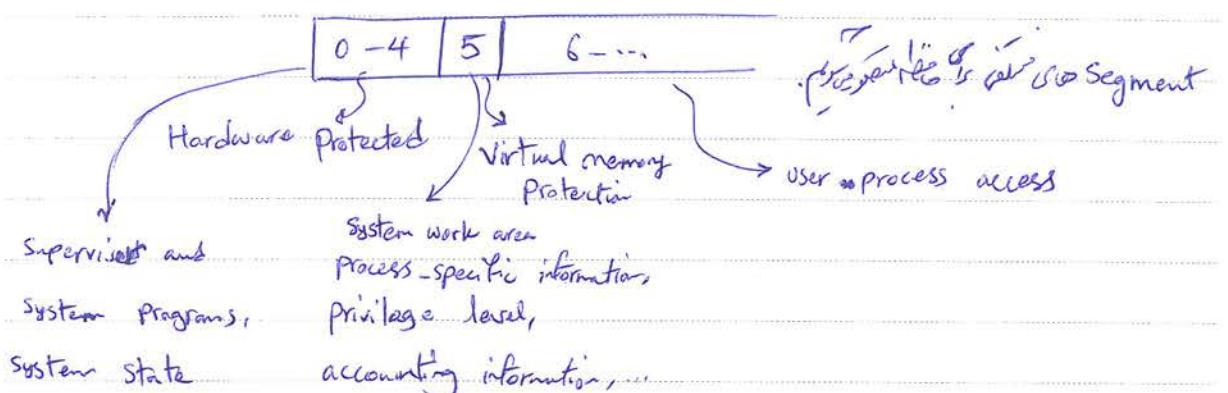
الى امن المعلومات وتقنيات الحاسوب
 (Anderson PenTest)

insider → Compromise principle

Information Gathering PDF

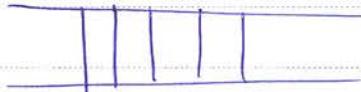
goal: control system

memory protection & overview



virtual memory protection

0-6 →



address list

protected

Pen Tester

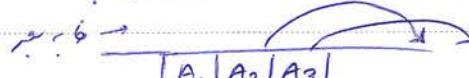
Subject

بيانات

Date

٩٨/٧/٤

نحوه فحص فجوات في Flaw Hypothesis (F)



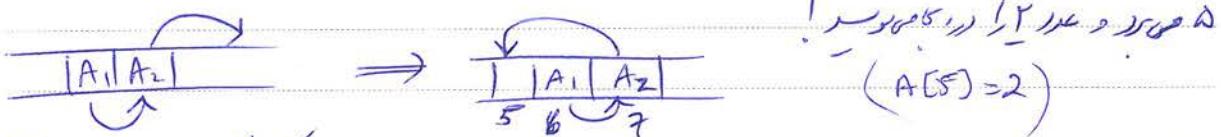
$|A_1|A_2|A_3|$

$A_1 \oplus A_2 \oplus A_3$

نحوه فحص فجوات في خوارزمية Procedural System Procedure

فريضم! بحسب خوارزمية F، $A_1 \oplus A_2 \oplus A_3 = 0$.

ما هي المكونات التي تدخل في $A_1 \oplus A_2 \oplus A_3$ ؟



ما هي المكونات التي تدخل في $A_1 \oplus A_2 \oplus A_3$ ؟

للحيلولة دون ذلك، Line Input Routine في System Routine

تحتاج إلى خطأ في line number.

ما هي المكونات التي تدخل في $A_1 \oplus A_2 \oplus A_3$ ؟

accounting information

لتحقيق ذلك، نحتاج إلى خطأ في Flow Generation (غير F)

PAPCO (Time-of-check to Time-of-use) لتحقق ذلك.

Subject

Date

9/1, V, 4

(Programmatic) for generalization, abstract behaviors

General abstraction of functionality Inappropriate Parameter Validation
(Incomplete)

Penetrating a UNIX system: Unix penetration (JW)

Goal: To gain access to the system. The target is a system connected to the Internet.

Information Gathering

Ports, services, ghost

Use of NMAP nmap

Ports used for communication, common ports

NMAP uses port scanning

1. ftp 21/tcp

telnet 23/tcp

smtp 25/tcp

finger 79/tcp

2.

Many UNIX systems use Sendmail as SMTP server.

mail server

Subject _____
Date _____

3. Sendmail version 3.1.

فیلم Sendmail یا پست دهنده در یک سرور SMTP است
ویژگی root shell wiz می باشد

920 222.com Sendmail 3.1 / 222.3.9

hello xxx

250 222.com -

wiz

250 Enter, o mighty wizard!

shell

root!

#

(User privilege authorization)

رسانیده ای از این داده های اطلاعاتی است

برخواهی اول تمثیل کرد و مخصوصاً نیاز به تغییر رمز عبور داشت. سه شنبه سعی کرده بود از این روز

که این فرآیند را برای این همچنان ساخته بود. از این طریق این همچنان ساخته شد

من یک تحریری داشتم که این فرآیند را برای این همچنان ساخته شد. این تحریر را در آن لاین دارم

و این تحریر را با عنوان Tester خواسته داشتم. این تحریر را با عنوان Tester خواسته داشتم

از سری این فرآیند این است. این فرآیند دو گزینه دارد. یکی از گزینه های این فرآیند این است

جهت رسیدن این فرآیند از این طریق است

Subject: Vuln.
Date: 9/1, V, 9

(Taxonomy)

Vulnerability Classification:

According to

- The techniques used to exploit vulnerabilities
- The software and hardware components and interfaces that make up the vulnerability.
- Their nature

Using Taxonomy

Ontology -

ontology < regular & complete

WS and XTerm, JBoss UNIT, JBoss Seam, Xterm (Java)

output, input (E.g. Root C:\)

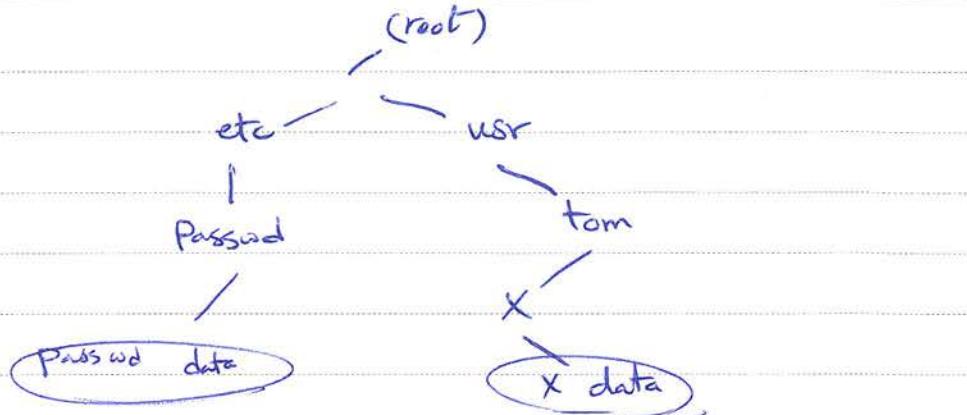
Ownership of XTerm, JBoss log file & .java log file

Who has access over JBoss XTerm? What is the user?

Subject

Date

9. V. 11



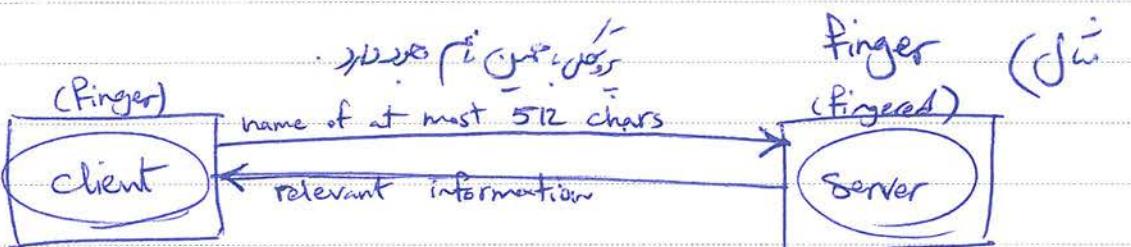
```
if (access ("usr/tom/x", w_OK) == 0) {  
    if (fd = open ("usr/tom/x", o_WRONGLY | o_APPEND))  
        /* handle error: can not open file */  
    }  
}
```

7

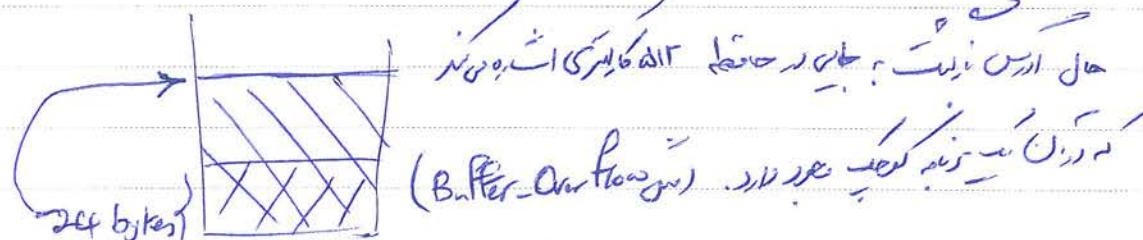
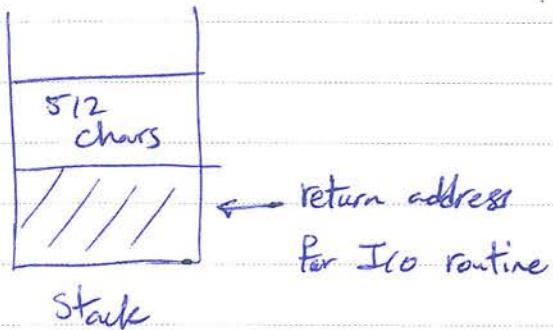
atomic finger

./
nail passwd data: & X(S) i alias & 'IP nijij
(Terminal Michigan System) . nijij

finger atomicity specific?



RPC



First Taxonomy

The RIOS study:

(Research Into Secure Operating Systems)

1. Incomplete Parameter Validation
2. Inconsistent Parameter Validation
3. Implicit Sharing of Privileged/Confidential data

Subject

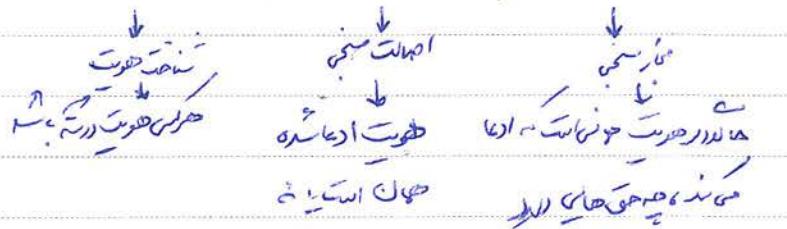
بی اسپی

Date

- ۹۶/۷/۱۱

۴. Asynchronous Validation / Inadequate Serialization

۵. Inadequate Identification / Authentication / Authorization



۶. Viable Prohibition / Limits.

۷. Exploitable Logic Error (others)

Incomplete Parameter Validation

buffer-overflow, finger (جی ای جی ای اس ند / جی ای جی ای اس ند) (جی ای جی ای اس ند / جی ای جی ای اس ند)

Inconsistent Parameter Validation

برای مثال در فرمت فایل میتوانم هر دو فرمت را در یک فایل داشتم

نحوی: هر کدامیکی که کار کند: مثلاً این کار کند

نحوی: طبق کنفرانسی میگیرد: new line, to colon

نحوی: فرمات فایل را درست نمایند: این فرمات را درست نمایند

XSS چیزی است Executable & SQL Hijack & Format String Attack

Subject
Date

بیل اسٹر
۹/۷/۱۱

Timing Attacks on RSA

Implicit Sharing of ...

cipher keys (جیسے دو RSA Keys)

بے وحیم مہردار زان سوت فاصلہ خوبی کی

Side channel Attack (JW)

لمسیات بروزگرد

TENEX (JW)
Paging (اردو)

سرد مالریم ملکریم



$$2^6 + 2^6 + \dots = 6 * 2^6$$

لکھنؤ
پورہ

پھر Travel Share

جن کارہ ارجمند بنت

نئی حفاظتیں

Subject _____
Date _____

: Asynchronous Validation ..

Time-to-check To Time-of-Use

Michigan Terminal System Xterm (Ji)

Specified \leftarrow overt \rightarrow Inadequate Identification ..

undocumented \rightarrow Covert \rightarrow -

Specified \leftarrow overt \rightarrow to Trojan Horse ..

undocumented \rightarrow Covert \rightarrow

process \rightarrow Sys\$ * DLOC\$ \rightarrow Univac Naming ..

. / . Is Privileged

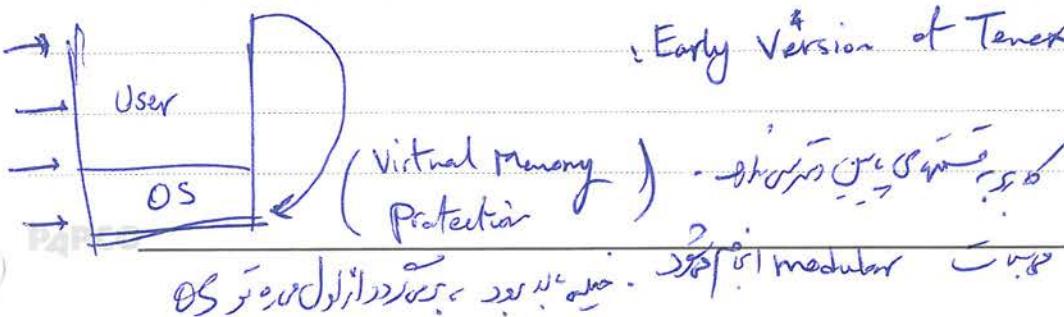
Privileged \rightarrow Sys\$ * DLOC\$

Ordinary \rightarrow

privilege \rightarrow DLOC, sys ..

: Violable Prohibition / ..

: Early Version of Tenex (Ji)



Subject : CSE 304
Date : 9th VIII

Penetration Analysis Model (PA) :

1. Improper Protection Domain Initialization and Enforcement

Subclasses:

- a. Improper choice of initial protection domain
- b. Improper Isolation of implementation detail
- c. Improper change
- d. Improper Naming
- e. Improper Deallocation/deletion

2. Improper Validation (Validation of Operands, Queue management dependencies, ...)

3. Improper Synchronization

- a. Improper Indivisibility (Interrupted Atomic operations)
- b. Improper Sequencing (Serialization)

4. Improper Choice of Operand or Operation

Subject _____
Date _____

(log)

1) Trojans (Initialization flaw enforcement)

1.a) assign → protection → boot issue

1.b) new implementation abstraction →
Timing Attack RSA

جربة برمجيّة لـ RSA

1.c) Xterm
privileged program

1.d) Trojan Horses (Aliasing)

1.e) بـ درون (Drone) كـ مـاـجـيـكـاـلـ (Magical)
Magic shell

2) finger

3)

3.a) Xterm

3.b) concurrency → race

4) others!

غير معروفة

(غير معروفة)

Subject Cryptography
Date 9/7/2018

(Reflection on Trusting Trust - Thompson - Turing Award Lecture)

جسٹریٹ / ڈیفنڈنگ سینٹر
Stage I

Stage I - A self-reproducing Program

"print out this sentence"

پڑھ لیں گے اس کا محتوا ہے کہ

کوئی " " کو نہیں پڑھ لیں گے اس کا محتوا ہے کہ

Stage II -

سچائی میں میں کوئی خطا نہیں کر رہا تھا Thompson

کوئی " " کو نہیں پڑھ لیں گے اس کا محتوا ہے کہ

character escape sequence → \n

کوئی " " کو نہیں پڑھ لیں گے اس کا محتوا ہے کہ

c = next();

if (c != '\n')

return(c);

c = next();

if (c == '\n')

return ('\n');

if (c == '\n')

return ('\n');

...

Subject _____
Date _____

نحوه افقی و عمودی تعریف شده است، این عبارت دارای دو حالت است.

\equiv
if ($c == 'n'$)

return ('\\n');

if ($c == 'v'$)

return ('\\v'); \rightarrow این حالت مخصوصاً برای نمایش اسکرین است.

$\left. \begin{array}{c} c \\ \downarrow \end{array} \right\}$

نمایش اسکرین از هر دو حالت

return ('\\');

حالات افقی و عمودی تعریف شده اند که از این دو حالت بسته به نوع پردازنده متفاوت است.

return ('\\v');

Stage III:

برای این مرحله از اوروری خود را در یک string می‌دانیم.

Compile(s)

char *s;

{

\equiv

2

فعلاً اینجا است:

~~می‌بینید~~ /

حال می‌بینید این سه عبارت را

Subject

Date

٩٤/٧/٢٠

Compile(S)

char *S;

{

if (match (S, "pattern")) {
 compile ("bug");
 return;

✓ bug -> UNIT => set user id
(جودة الأداء)

ابن لادن يعود للحياة امام مدرس سوري اثنين

متحف العجمي

Compile(S)

=

if (match (S, "pattern")) {
 compile ("bug");
 return;

if (match (S, "pattern-2")) {
 compile ("bug2");
 return; } ابراهيم
جعفر

Convert S

overwriting =

new Compile

العنوان يغير الى العنوان المكتوب

العنوان يغير الى العنوان المكتوب

٣٧

Subject

Date

٢٠١٨/٧/٢٤

البرمجيات المُسيّبة (Malware) هي البرمجيات التي تؤدي إلى إتلاف أو ضرر للمعلومات.

مُنذّر

Malware (Malicious Logic):

البرمجيات المُسيّبة التي تؤدي إلى إتلاف أو ضرر للمعلومات.

Malware Type:

(SR)

1. Self-replicating →

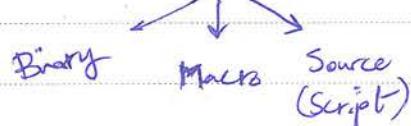
(PG)

2. Population Growth →

(بروتوكول تضليلي، يُعرف بـ "Self-Replicating logic")

3. Parasitic →

Executable Code



: مُنذّر (Conscript)

- Logic bomb (المفاجأة)، $\rightarrow SR = No$

$PG = zero$

جهاز التحكم في الملفات / Parasitic = Possibly

Trigger → Payload

Subject

Date

٢٠٢٣/١١/٢٤

Payload + Trigger

امثلة على تفعيل الاكتشاف
بروتوكول

التي ت activates the detection
trigger payload

(Remotely triggered)
(Locally triggered)

Legitimate Code = $\text{crash_computer}()$

if date is Friday the 13th \rightarrow Trigger

$\text{crash_computer}() \rightarrow \text{Payload}$

Legitimate Code =

- Trojan Horse : \rightarrow SR: No

PG: Zero

parasitic: Yes

infectious

password grabbing

password

~~Backdoor~~ (Trapdoor)

- Back Door : bypasses normal security check

A back door is any mechanisms which bypasses a
normal security checks.

Subject _____
Date _____

? (john Jack? ~~✓~~ ✘)

→ SR: No

PG: Zero

Parasitic = Possibly

(Ja)

Username = read_username();

Password = read_password();

BackDoor! } if username is "1337 h4cker"
return allow_login;

if username and password are valid

return allow_login;

else

return deny_login;

- Virus:

A virus is a malware that, when executed, tries to replicate itself into other executable code.

(Infects asset) into valid process -> (No integrity)

→ SR: Yes

PG: Positive

Parasitic = Yes

o_o (Viruses = virii)

(Viruses = virii)

(worm or virus, virus, worm)
infects victim's system

PAPCO

Subject
Date

Computer
14/7/12

(Gene Spafford)
گین سپفورد

is infected \rightarrow ای دوسرے کی حوصلہ رکھیں \rightarrow executable code

~~SR~~ \rightarrow دوسرے کی حوصلہ رکھیں \rightarrow مل اجرا \rightarrow germ

گرم \downarrow
دھنیا کی طرح
اول

self-replicating \rightarrow ویروسیں \leftarrow intended

ویرس میں دار میں ہتھیار کا کوئی نہیں ایسا \rightarrow dormant

- Worm :

\rightarrow SR: Yes

PG: Positive \rightarrow پیغام

Parasitic: No

ویرس میں دوسرے کی حوصلہ رکھیں نہیں \rightarrow (ویرس کا ویرس کی حوصلہ رکھنے والا ہے)

1) Standalone \rightarrow نیز بھائی ترینہ میں باری

2) Spreads across network \rightarrow ویرس کی دوسری باری

Worm	Virus
Standalone	Parasitic

Process U.S.A

Spreads across Network \rightarrow Spread across network
Does not

Internet Worm \leftarrow اون یا worm

(1988, Robert Morris)

CodeRed (2001)

Subject

Date

٢٤/٨/٢٠

(Bacteria)

- Rabbit:

→ SR = Yes

PG: Zero

Parasitic: No

Pork bomb (Jin)

Pork bomb جن يُطلق على البرامج التي تؤدي إلى احتراق الموارك (memories) بسبب إفراط في إستهلاك الذاكرة، مما يؤدي إلى توقف العمل في المركبات.

while (true) do

 mkdir x ↗ حفظ الملفات في المجلد

 chdir x

done

جذب الملفات raro → Rabbit

- Spyware:

→ SR: No

PG: Zero

Parasitic: No

جذب الملفات للكشف عن المعلومات الشخصية مثل البريد الإلكتروني والكلمات المرفقة بالملفات.

- Usernames and Passwords

↳ Key-Logger

- Email Addresses

- Bank Account ^{and} Credit Number

- Software License Keys

Subject: Computer Viruses
Date: 27/11/2010

- Adware:

→ ER: No

PG: Zero

Parasitic: No

marketing Successful Vir Spyware? ?

- Trojan Horse : Thompson
- Back Door
- Self-Replicating

- Zombie:

ذئب مبرمج يسكن في جهاز الكمبيوتر ويتحكم في الأجهزة الأخرى ويعمل بأمره وآثاره سلبية

(unwitting) accomplice

DOS (Denial of Service) ، DDOS (Distributed Denial of Service)

Command and Control (سرور تحكم). IRC channel (لكل باتن)، botnet (شبكة روبوتات)

، رد على IP trace back

ـ مسار الرسائل

Subject

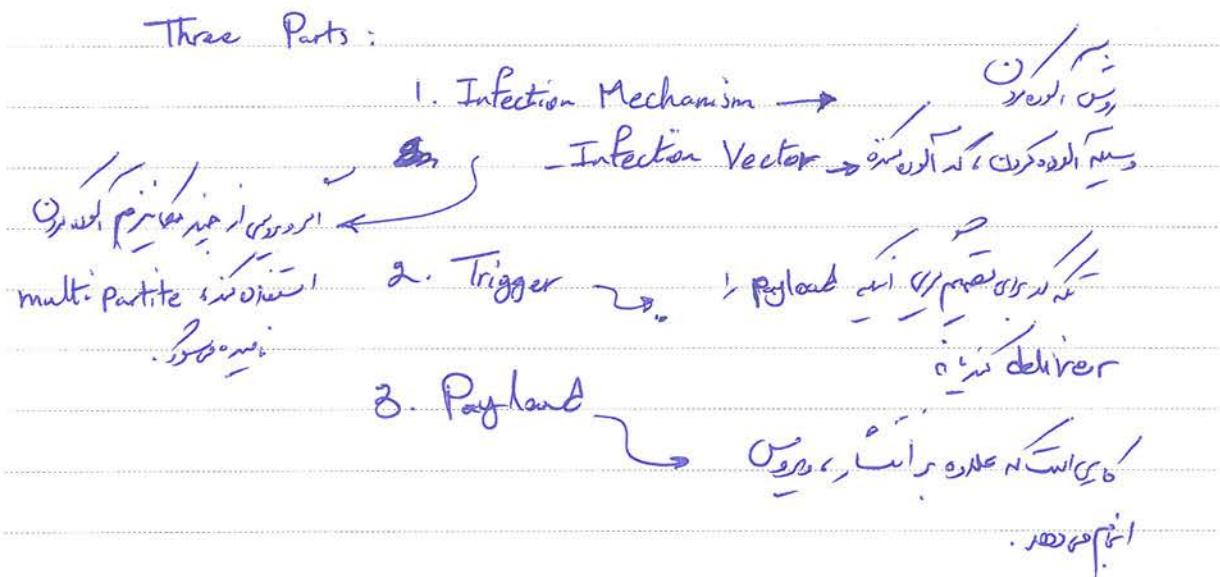
Date

٩٤.٠٧.٢٠

Virus Replication (Naming for Malware)
وَيُمْكِنُ لِلْفِيروسِ أَنْ يُسْتَعْظِمَ لِلْمُخْرَجِ (Exit)
وَيُمْكِنُ لِلْفِيروسِ أَنْ يُسْتَعْظِمَ لِلْمُخْرَجِ (Exit)

Viruses:

Three Parts:



Pseudo Code For a virus.

```
def virus():
    infect() → مُخْرِج
    if trigger() is true
        payload()
```

الفيروس يُخْرِج بحسب ما يُحدِّد بـ trigger

Subject: IT
Date: ٢٤/٩/٢٠

def infect():

repeat k times:

target = select_target()

if no target:

return

infect_code(target);

(
 mark ←
 دایرکٹریوں کا مارک →
 برائے اینہا، مارک کیلئے ایسا دھمکھ دیکھ دیجیا۔

classification:

روزگاری و موسیقی

1. The type of target the virus tries to infect.

2. The method the virus uses to conceal itself.

Classification by the target's type:

1. Boot-Sector Infectors

کمپیوٹر کے ہڈی پر ورنریز ہڈی اور اسی پر گن ایس۔ ورنریز کیلئے ایس، جن سکر بوت فائلز کیلئے ایس۔ اسی دلیل پر ایس کے نام۔

2. File Infectors → word, shell, os, javascript

فایل ایس کے نام۔ Executable ≡ infect

Subject

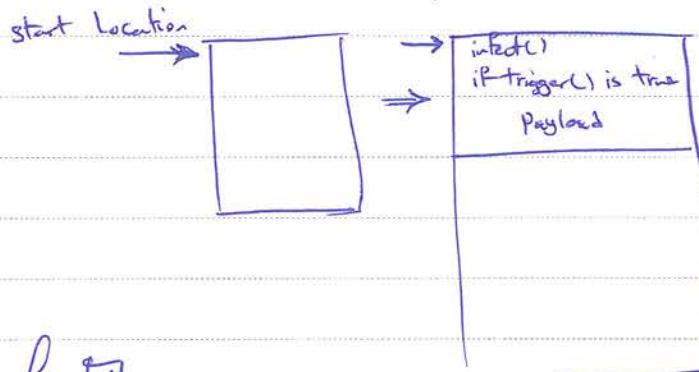
Date

94. 07.20

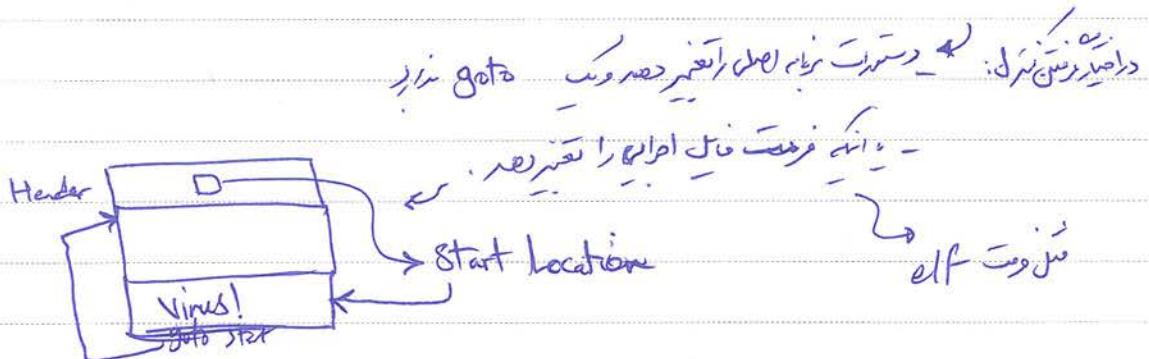
vir/wi/virus File Infector

- where is the virus placed?
- How is the virus executed when the infected file is run?

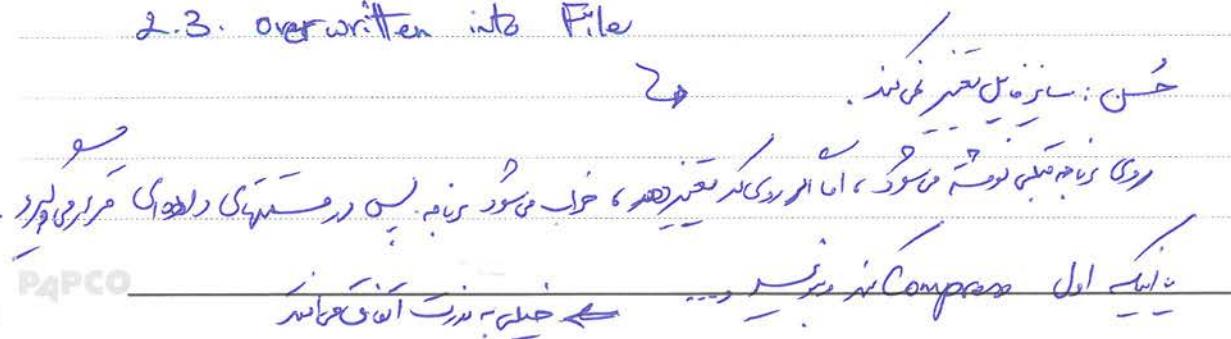
2.1. Beginning of File (Prepending Viruses)



2.2. End of File (Appending Viruses)

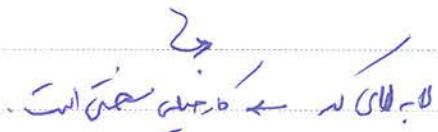


2.3. overwritten into File



Subject: In
Date: ٢٤/٧/٢٠

2.4. Inserted into File



2.5. Not in File

→ Companion Virus

حربیک از ویروس‌هایی که در فایل‌ها نصب شده باشند و در صورت اجرا برای دسترسی به فایل می‌رسند.

آنچهم infect می‌شود به عین معنی دارد که فایل اجرا شده از ویروس مبتلا شده است.

و همچنان که می‌دانید این ویروس‌ها را Trojan Horse نیز می‌نامند.

ویروس‌های Trojan Horse معمولاً در فایل‌های Executable (exe), Com (com) و DLL (dll) قرار دارند.

? . Foo.exe, ? . Foo.com, ? . Foo.dll, ? . Foo.exe از اینها اجرا شده است.

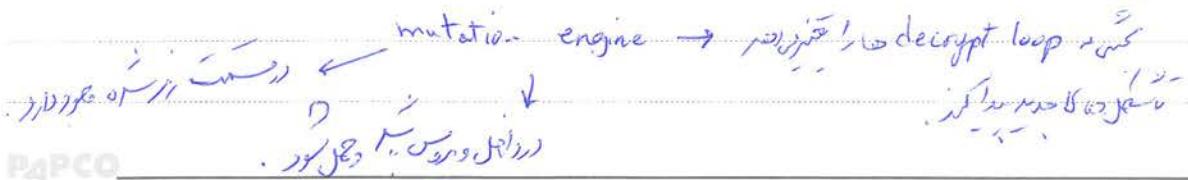
3. Macro Viruses

→ از خودها برای اجرا برخاسته و در فایل‌ها پنهان شده است.

(Data File Infectors)

Polymorphism

mutation engine → تجزیه‌گر، decrypt loop



Subject _____
Date _____

Instruction Function \approx Register

- Instruction Equivalence:

For two instructions, if they produce the same results CSE (SCE)

Clear r_1 { Binary representation of r_1
Xor r_1, r_1 → $00000000000000000000000000000000$
and $0, r_1$ → $11111111111111111111111111111111$
move c, r_1 → $00000000000000000000000000000000$

- Instruction Sequence Equivalence:

$$j = 1, \rightarrow y = 21$$

$y = j - 20$
Mutate trick of mutation engine

- Instruction Reordering:

$$\begin{array}{ll} r_1 = l_2 & r_2 = r_3 + r_2 \\ r_2 = r_3 + r_2 & \Leftrightarrow r_1 = l_2 \\ r_4 = r_1 + r_2 & r_4 = r_1 + r_2 \end{array}$$

Swapable

- Register Renaming:

$$\begin{array}{ll} r_1 = l_2 & r_3 = l_2 \\ r_2 = 34 & \Leftrightarrow r_1 = 34 \\ r_3 = r_1 + r_2 & r_2 = r_3 + r_1 \end{array}$$

(Variable renaming)

Swap

Subject CS
Date 26/V/XV

- Reordering data

order of execution

- Making Spaghetti

(مُؤْخِدَةِ دُرُجَّتِيَّة)

WTF! Code Readability

Start:

$$r_1 = l_2$$

$$r_2 = 34 \Leftrightarrow$$

$$r_3 = r_1 + r_2$$

L1:

$$r_2 = 34$$

goto L2

Start:

$$r_1 = l_2$$

goto L1

L2:

$$r_3 = r_1 + 5$$

- Inserting Junk Code

$$r_1 = l_2$$

$$r_2 = 34 \Leftrightarrow \text{inc } r_1$$

$$r_3 = r_1 + r_2 \quad \text{inc } r_1$$

$$r_1 = r_1 - 2$$

$$r_2 = 34$$

$$r_3 = r_1 + r_2$$

$$r_5 = 42$$

$$r_1 = l_2$$

X:

$$r_2 = 34$$

dec r5

bne X

$$r_3 = r_1 + r_2$$

Subject

Date

98, V, V

- Runtime Code Generation

$$r_1 = l_2 \quad r_1 = l_2$$

$$r_2 = 34 \Rightarrow r_2 = 34$$

$$r_3 = r_1 + r_2 \quad \text{generate } r_3 = r_1 + r_2$$

call generated_code

2 2 /
f i n i s h b o d y

- Interpretive dance

cpu (stack, user, ...)

Fetch \rightarrow Decode \rightarrow Execute

→ interpreter program counter

$$r_1 = l_2 \quad \text{ipc} = 0$$

$$r_2 = 34 \Rightarrow \text{loop}$$

$$r_3 = r_1 + r_2 \quad \text{switch CODE [ipc]}:$$

Case 0:

exit loop

Case 1:

$$r_2 = 34$$

Case 2:

$$r_1 = l_2$$

inc ipc

$$r_3 = r_1 + r_2$$

CODE :

2

1

0

Subject 3w
Date 9/11/2018

- Concurrency:

start thread T

$$r_1 = l_2 \\ r_2 = 34 \Rightarrow$$

$$r_3 = r_1 + r_2$$

$$r_1 = l_2 \\ \text{wait for signal}$$

$$r_3 = r_1 + r_2$$

~~return~~ ..

T:

$$r_2 = 34$$

Send Signal

exit thread T

- Inlining and outlining

↓
 $\cup_{j=1}^k \cup_{i=1}^{l_j} \cup_{s=1}^{m_{ij}}$

Call S1

$$r_1 = l_2$$

Call S2

$$r_2 = r_3 + r_2$$

S1:

$$r_1 = l_2$$

$$r_4 = r_1 + r_2$$

$$r_2 = r_3 + r_2$$

$$r_1 = l_2$$

$$r_4 = r_1 + r_2$$

$$r_2 = 34$$

$$r_1 = l_2$$

$$r_3 = r_1 + r_2$$

return

S2:

$$r_1 = l_2$$

$$r_2 = 34$$

$$r_3 = r_1 + r_2$$

return

Subject

Date 28/11/14

↳ multi-threading
↳ C++

- Threaded Code

$$r_1 = l_2$$

next = &CODE

$$r_2 = r_3 + r_2$$

goto [next]

$$r_4 = r_1 + r_2$$

CODE:

$$r_1 = l_2 \Rightarrow$$

&I₁

$$l_2 = 34$$

&I₂

$$r_3 = r_1 + r_2$$

&X

...

X:

$$r_1 = l_2$$

$$r_2 = 34$$

$$r_3 = r_1 + r_2$$

I₁:

$$r_1 = l_2$$

inc next

goto [next]

I₂:

$$r_2 = r_3 + r_2$$

$$r_4 = r_1 + r_2$$

inc next

goto [next]

- Subroutine Interleaving

with reentrant vs invisible, local vs outside, inline

Subject CS
Date 26/11/2023

call S1

call S2

call S12

S12:

$$r_5 = l_2$$

$$S1: \quad r_1 = l_2$$

$$r_2 = r_1 + r_3$$

$$r_4 = r_1 + r_2 \Rightarrow$$

return

$$r_6 = r_3 + r_5$$

$$r_2 = 34$$

$$r_4 = r_5 + r_6$$

$$r_3 = r_1 + r_2$$

return

S2:

$$\boxed{r_1 = l_2}$$

$$r_2 = 34$$

$$r_3 = r_1 + r_2$$

return

(obfuscation using)

(Reverse Engineering) $\xrightarrow{\text{Code Optimization}}$ (Obfuscation)

Super optimization, finest level

mutation $(x, p, j) \leftarrow \text{zellemer } \sigma$

Subject

J

Date

9/1/14

2014

Metamorphism, Polymorphism, Oligomorphism

Polymeric antibody \rightarrow works

virus \rightarrow mutation, deryptolog of virus body
(infection decryption)

Antivirus Techniques:

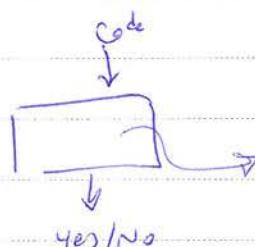
{ Detection
Identification
Disinfection

responsible for viruses

no full detection \rightarrow false alarm

not successful

undetectable virus detection by Eli Kohen



detect \rightarrow general

reduction \rightarrow undetectable work

(Self-contradiction) diagonalization

never stops \rightarrow halting

halting \rightarrow

Subject

U.

Date

4/5/14

فیروس کا ایڈنٹی فیکیشن۔ ایک فایل کا ایڈنٹی فیکیشن۔

فیروس کا ایڈنٹی فیکیشن۔ ایک فایل کا ایڈنٹی فیکیشن۔

ایڈنٹی فیکیشن سے اسی فایل کا ایڈنٹی فیکیشن۔

ایڈنٹی فیکیشن۔ یا اسی ایڈنٹی فیکیشن۔

ایڈنٹی فیکیشن۔ ایڈنٹی فیکیشن۔

Virus Present

		Yes	No	
Virus detected	Yes	True Positive ✓	False Positive X	(Positive: تیکا)
	No	False Negative X	True Negative ✓	(FN, TN, FP)

جیسے: ghost positive →

تیکا ایڈنٹی فیکیشن۔

Detection

→ Static →

موقوفہ ایڈنٹی فیکیشن۔

→ Dynamic →

موقوفہ ایڈنٹی فیکیشن۔

(Behavioral) ↓

موقوفہ ایڈنٹی فیکیشن۔

(Sandbox)

Static : Scanning, Heuristics, Integrity checkers

P4PCO

33

Subject
Date

١٢-١٩

٩-١٢) (PenTest)

(penetration testing)

Countering Trusting Trust through Diverse Double-Compiling

David A. Wheeler



static → صيغة ثابتة / static

} Dynamic → ديناميكية / dynamic
رسالة تغير درجة اطمئنانها

Runtime → وقت التشغيل / runtime

static:

- Scanning → مسح / scanning

بنية المعرفة / knowledge base

Scanner / on-demand → طلب / on-demand

on-access → على الاتصال / on-access

critical areas / مناطق حساسة

write / writing

signature pattern / نمط التوقيع

Scan strings

Signature

Signature or scan strings

wildcards

جذور / roots

• The wild card is used to scan string

Subject CS
Date 9/1/14

The process of searching for viruses by looking through a file

for signatures is called scanning, and code that does the

search is called a scanner.

الخطوة الأولى في عملية التفتيش هي مقارنة كل حرف في الملف

مع عبارات المرضي، فإذا وجدت أي حرف يتطابق مع أحد المرضي،

فهذا يعني أن

(will give us the scan string)

أول حرف في المرضي

: Scanning الملف للوصول إلى المرضي

Algorithm: Aho-Corasick

1975

مايكيل أهوكاراسيك

Parallelization

دكتور رانيل سيمونست

- A finite automaton \rightarrow will search for
- A failure function

أولاً نختار المرضي، ثم نقوم بـ state selection، أي اختيار المترافق

signature

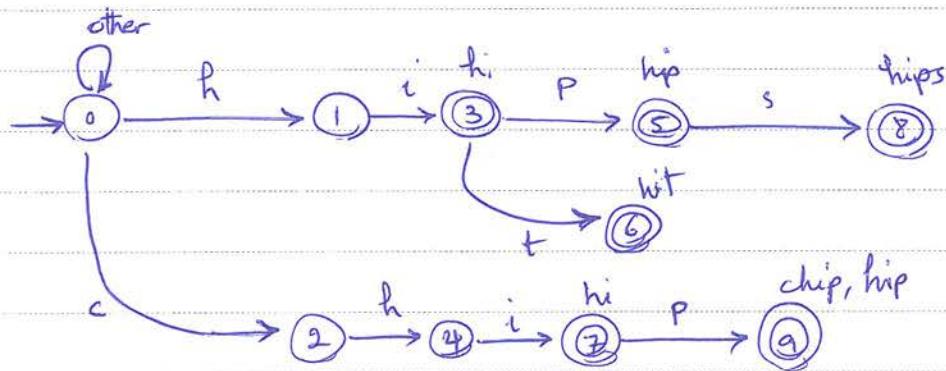
ثانياً نقوم بـ suffix linking، أي إنشاء failure function

Subject _____
Date _____

(Implementation of KMP algorithm to Scan String)

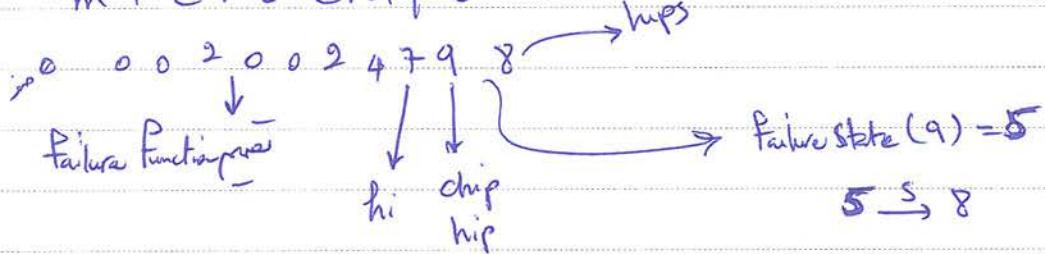
Q1)

Signatures: hi, hips, hip, hit, chip



State	1	2	3	4	5	6	7	8	9
Failure (state)	0	0	0	1	0	0	3	0	5

microchips



Time complexity of signature is $O(n) + O(m)$ in KMP

Ex:

state = START_STATE

while not end of input

ch = next input character

while no edges state $\xrightarrow{ch} t$ exists:

state = Failure(state)

state = t

if state is Final:

output matches

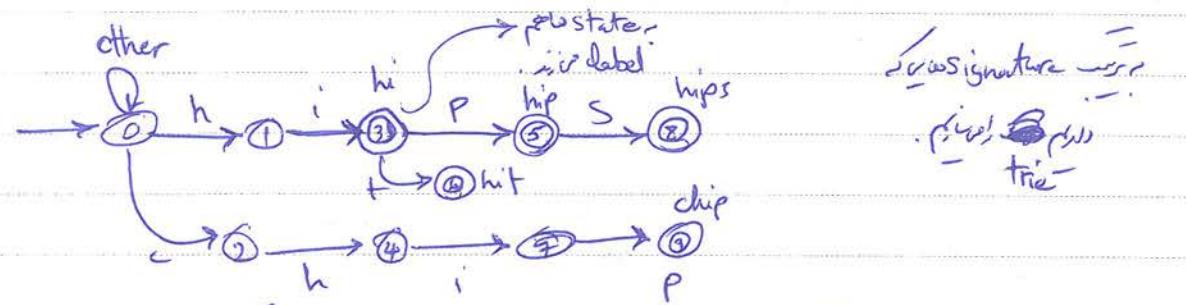
Subject JW
Date 9/17/14

: Subfailure Function, automaton construction

Build a trie

is leaf : root is unique \rightarrow signature \rightarrow

Common Prefix \rightarrow signature



Fail automaton \rightarrow

: Failure Function \rightarrow

for each state s where $\text{depth}(s) = 1$

$\text{Failure}(s) = \text{START_STATE}$

for each state s where $\text{depth}(s) > 1$, in breath order

Find the edge $r \xrightarrow{a} s$

state = $\text{Failure}(r)$

while no edge $\text{state} \xrightarrow{a} t$ exists:

state = $\text{Failure}(\text{state})$

$\text{Failure}(s) = t$

$\text{output}(s) \cup \text{output}(t) \rightarrow$

Output state

Subject _____
Date _____

Algorithm: Veldman

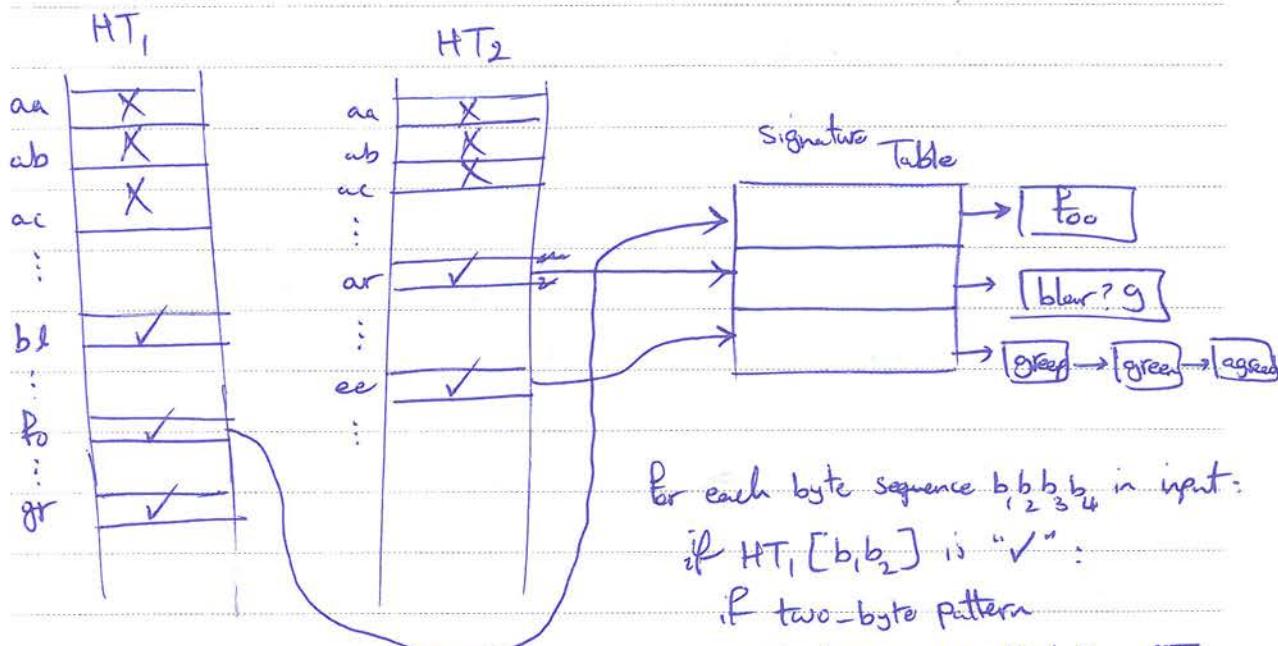
in Sequential Search $O(n)$ (search space) \rightarrow inefficient

in Hash Table $O(1)$ (signature) \rightarrow efficient

Signatures: blar?g, foo, green, agreed

Hash Table is preprocessed

foo green blar?g green green green Pattern does not occur



مودودي و مصطفى حمودي و زين حمودي خط

دمردري و ابراهيم جعفر و احمد عزيز و لطيف عزيز
جعفر و ابراهيم جعفر و احمد عزيز و لطيف عزيز

Algorithm: Wu-Manber

Subject CS
Date 9/1, 19

Improving Performance of Scanners:

- Reduce amount scanned → مساحت اسکن کرد



False Positives ایجاد شده ای

- o Top and Tail Scanning

محدوده ای اسکن کرد اینها خوب نیستند

- o Entry Point →

محدوده ای اینها خوب نیستند

- o Fixed Point Scanning →

محدوده ای اینها خوب نیستند

- Reduce amount of scans → مساحت اسکن کرد

- o Certain file types → محدوده ای اینها خوب نیستند

اینها خوب نیستند

- o Store State Information

اینها خوب نیستند

(.inf, .ico Attribute)

- Lower Resource Requirements

- o Using less precise set of signatures

6

اگرچه اینها خوب نیستند

برای FP

میتوانند اینها خوب نیستند

میتوانند اینها خوب نیستند

Subject _____
Date _____

- Change the algorithm →

غير البرمجة

ج

- Change the algorithm implementation →

غير برمجية

- Static Heuristics →

الهجاءات الستاتيك

الهجاءات الستاتيك هي طرق معرفة الأكواد المضللة من خلال التحليل الشمولي (Static Analysis) ، حيث يتم تقييم الكود بناءً على خصائصه المعرفية.

(. في Ad-hoc)

الهجاءات الستاتيك هي طرق معرفة الأكواد المضللة من خلال التحليل الشمولي (Static Analysis) ، حيث يتم تقييم الكود بناءً على خصائصه المعرفية.

الهجاءات الستاتيك هي طرق معرفة الأكواد المضللة من خلال التحليل الشمولي (Static Analysis) ، حيث يتم تقييم الكود بناءً على خصائصه المعرفية.

الهجاءات الستاتيك هي طرق معرفة الأكواد المضللة من خلال التحليل الشمولي (Static Analysis) ، حيث يتم تقييم الكود بناءً على خصائصه المعرفية.

وBooster:

وBooster هو جهاز يزيد من قدرة الكمبيوتر على إنتاج الكود المضلل.

- Junk Code →

الكود المفروم (Junk Code) هو كود غير مفهوم أو غير مطلوب في البرنامج.

الكود المفروم (Junk Code) هو كود غير مفهوم أو غير مطلوب في البرنامج.

(Signature وBooster)

- Decryption Loop

الكود المفروم (Junk Code) هو كود غير مفهوم أو غير مطلوب في البرنامج.

- Self-modifying Code →

الكود المفروم (Junk Code) هو كود غير مفهوم أو غير مطلوب في البرنامج.

الكود المفروم (Junk Code) هو كود غير مفهوم أو غير مطلوب في البرنامج.

الكود المفروم (Junk Code) هو كود غير مفهوم أو غير مطلوب في البرنامج.

Subject :
Date : ٢٠١٩

- Manipulation of interrupt vectors

- Use of unusual instructions

- Strings containing obscenities

فتن و مزدور

ـ User (Negative Heuristic) to Stopper

ـ Pop-up dialog box

ـ Text Scanning

ـ Entry Point

ـ Spectral Analysis

ـ Signature detection

ـ Anti-virus (detecting and removing viruses)

(boot sector, IBM interator, Trigram, 4-cover)

30

Subject

Date

٤٩ / ٨ / ٩

- Integrity Checkers → حفاظ (Companion) (Guardian)

فایل متنی، فایل نوشته، فایل صوتی، فایل تصویری و فایل دیگرها را در یک فایل اصلی ذخیره می‌کنند.

از همین حفاظ درست یک فایل اخراجی می‌شود، که مطابق با فایل اصلی باشد.

این حفاظ کمتر از ۱٪ تغییر خواهد داشت.

Integrity
Checkers

- Offline → حفاظ (Guardian)

خطای جمله ایجاد کننده

- Self-checking → حفاظ خودکار

خطای این فایل از خود فایل ایجاد می‌شود

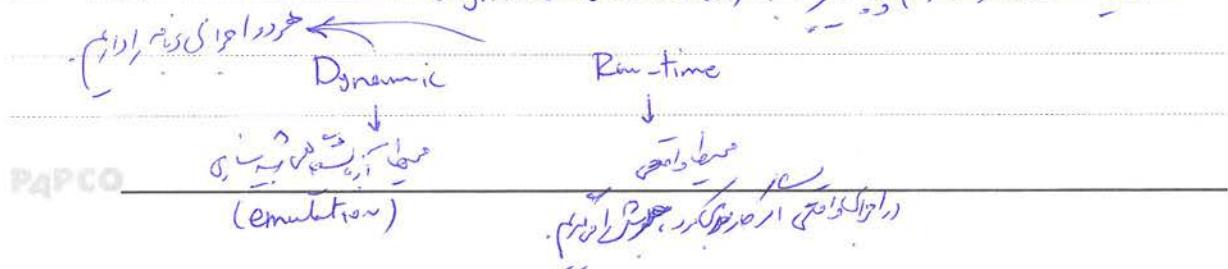
- Integrity Shell → حفاظ اجرایی

(Static shield)

Dynamic Methods:

این روش برای مخفی کردن این فایل است. آن فایل را که نباید مشاهده شود.

خدوش (dynamic obfuscation)، این روش را خود کنندگ



Subject JV
Date 25.11.9

Dynamic → Signature into action into CPU

- The actions are permitted (Positive detection)
- The actions are not permitted (Negative detection)
- Some combination of the two

(Viruses can't be detected)

for i in 1...4
 print(i)

print(i)

Print(i)

Print(i)

Print(i)

I/O to system call
open file

Appending virus

dynamic signature

1 - Opening an executable, with both read and write permission.

2 - Reading the portion of the file header containing the executable's start address

3 - Writing the same portion of the same header

4 - Seeking to the end of file

P4P5C - Appending to the file

Subject (Chapter 22 (Art and Science))
Date 2003

جتنی حملہ (Appending virus) ایک لارسی پتھر (Run-time) جنہیں جو

(Behavior Monitors or Blockers)

(Run-time (JIT))

Emulation → Dynamic method → سے باہر کرنے کی طرف

new Suspicious ہے اور Virtual Emulator

Virtual OS کا Emulator ہے

Dynamic heuristic → metamorphic

is polymorphic syscall

Generic designation

Polymorphic

honey-pot
honey-net

Covert Channels:

unspecified
undocumented

documented

A covert channel is an extraordinary path through which a program communicates information to people who should not receive it.

Subject Ju
Date 9/1/14

: multiple choice exam

ordinary communication → (a, b, c, d)

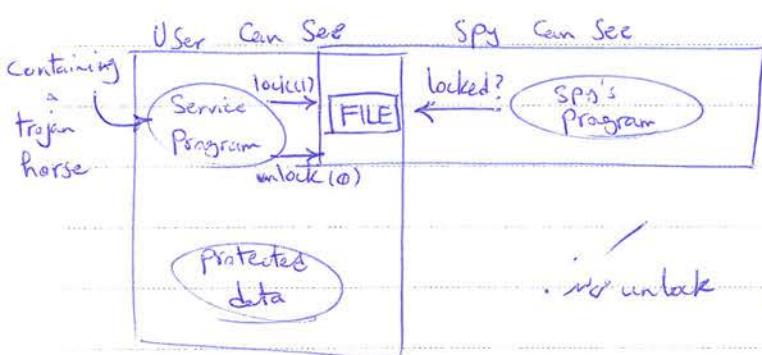
extraordinary communication Coughing Sighing once

Types of covert channel

Storage, Timing

Storage, timing
Timing, timing

Storage covert channel (original with User & Spy's program)



is unlock & lock the service program

is ! no where Trojan is locked? yes -> user

Trojan Horse by unlock, lock job. → protected data

user

for user

(is ! no where Trojan is locked job. → protected data)

P4PCO

Subject _____
Date _____

Timing covert channel

ایجاد کردن یک کانال مخفی با استفاده از timing بین CPU و پرینتر

برای این کار، اینکه CPU و پرینتر چه کاری دارند

input CPU و خروج Round Robin

پس زیر میگذرد که این کار چه کاری میکند

نحوی ساده و ساده

: Covert channel, چگونه

$h \rightarrow$ high, private $l \rightarrow$ low, public

- An implicit flow

(low observable)

$h := h \bmod 2$

↓
لیکن l را بخواه

$l := 0$

if $h=1$ then $l:=1$ else skip

: Covert channel چگونه

پس از یک - ۱

پس از یک - ۲

پس از یک - ۳

Subject Ju

Date 28.11.14

- External timing channels (Rosso Ufficio)

b := 0;

while b < 32 do

if not ($b \bmod 2 = 0$) then sleep(2) else skip;

b := b + 1;

b := b div 2;

Sleep(1);

Print("•");

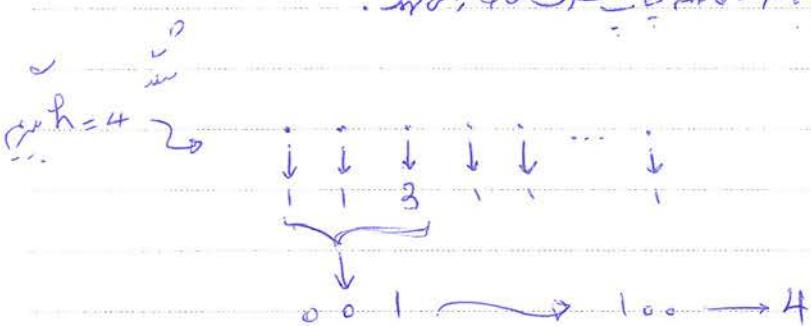
↑ dot ← follow previous implicit → explicit ;

initialization ← Sleep(n)

internal timing

multiple concurrent threads

(Coda)



- Internal timing

multiple concurrent, multi-thread

Subject

Date

thread

$c_1 : h := 0; l := h$

$c_2 : h := \text{secret}$

with sleep initial step to secure c_2

initial thread $\rightarrow c_1$

is sleep thread $\rightarrow c_2$

Round Robin

$c_1 \rightarrow c_2 \rightarrow c_1$

$h := 0 \rightarrow h := \text{secret} \rightarrow l := h$

$\text{secret} = 1$

$c_1 : (\text{if } h > 0 \text{ then sleep(100); } l := 1)$

$c_2 : \text{sleep(50); } l := 0$

c_1, c_2 initial step, then switch Round Robin

$l = 0$ or $l = 1$, $2 \leq h \leq 100$ or $0 \leq l \leq 100$ then switch



switch l direction

Non-determinism

Scheduler

non-deterministic

PAPCO

Subject
Date

in
16/1/14

? Deterministic vs Non-deterministic Refinement

non-deterministic
امثلة

الحالات

Refinement Attack

CSPL loscheduler

: Reading Assignment

Ant. Antivirus ← (جامعة) John Aycock

Vulnerabilities } Format string attack
virus } Buffer overflow → SQL injection

Attacks on Web Applications → (e.g.: XSS)

Cross-site scripting

Program Analysis ← تحليل البرامج

diagnostics

(Vulnerability), Attack , malicious logic

Security Mechanisms:

security labels:

الروابط الموصى بها

(Multi-level Security)

رسائل وقواعد المعايير

Engineering process

Subject

19 Introduction P, P, V, A, I, O, II

Date

٢٠١٨/١٢/٢٤

ج

، و پنداشتن و تحلیل -

Multi-level Security:

منطقی علیحده (منطقی) -

(Security Engineering, Anderson).

این سیستم top down می باشد

Threat Model



Security Policy



Security Mechanisms

این سیستم bottom up می باشد

نحوه ایجاد Security Policy, Threat Model

نحوه ایجاد Security Policy, Security Mechanisms

Security Policy (چیزی که

1. This policy is approved by management. → is Security Policy
2. All staff shall obey this security policy.
3. Data shall be available only to those with need-to-know. → درجه ای
4. All breaches of this policy shall be reported at once to security.

این (وافله، راپید) یعنی چیزی که Statement است

این نیست، این یعنی این (ولفر) Requirement یعنی Security Policy
(System Specification)

چیزی که

Subject U
Date AF, IN, 18

Statement (جذب)

سیاست امنیتی (Security Policy)

Security Profile, Security Target, Security Model (گزینش)

General (گام اول) (جذب امنیتی، جذب امنیتی)

Implementation (گام دوم) (جذب امنیتی، جذب امنیتی) (Implementation → target)

UNIT, Filesystem

model is instantiation (گام سوم)

? (Implementation) (target → profile)

in government, in party (Communication)

(Common Criteria)

model, target (گام چهارم)

Formalism (Common Criteria) (گام پنجم)

(target policy) (target policy) (Amaroso) (جذب امنیتی)

model (گام ششم)

Implementation mechanism (گام هفتم)

Paper (گام هشتم) (Concrete model) (جذب امنیتی) (Policy)

Subject

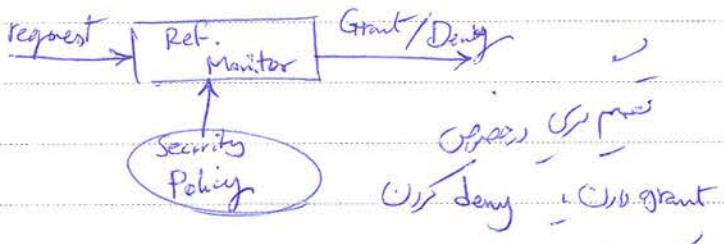
Date

Model : An abstraction of some physical phenomena.

Er. Ching's Security Model (i), Bell-LaPadula (BLP)

- Reference Monitor

↳ Immediate / Final / Upgrading
Final



Policy Outcomes

→ no grant/deny : request rejected by policy

Access Control

Classification and Clearance:

Top Secret
Secret
Confidential
Unclassified

نحوه ایجاد این سطوح

Security level نویسندگان

Totally ordered property

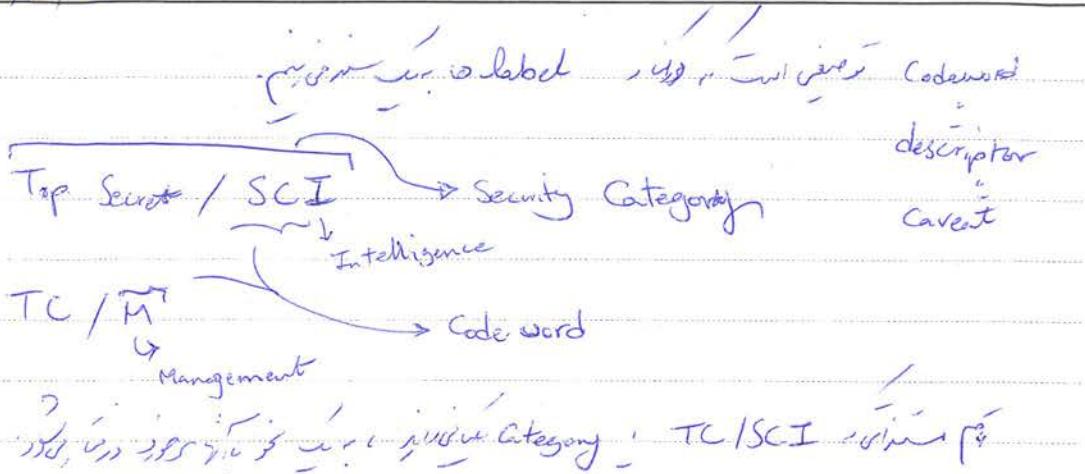
نحوه ایجاد

نحوه ایجاد این سطوح

(label نویسندگان)

codeword

Subject CS
Date 9/11/14



Sec. label / SCI, Code word

Superset \rightarrow Non-Confidential, Confidential, Superset, Codeword
AND \rightarrow Primary codeword

(also called Amoroso model) (النوع الثاني من المعايير)

Security level \rightarrow Top Secret, Secret, ...

{
- Category \rightarrow SCI #, M, ... \rightarrow سرية, مخففة, مفتوحة
- label \rightarrow TS/SCI, S/M, ...
} \rightarrow e.g. DLM (Decentralized label model), NLP/label

Active Entity \rightarrow Passive Entity \rightarrow object \rightarrow file
Subject \rightarrow Active Entity \rightarrow subject \rightarrow user
Object \rightarrow Active Entity \rightarrow object \rightarrow file
Process \rightarrow Active Entity \rightarrow process \rightarrow program, user
File \rightarrow Active Entity \rightarrow file \rightarrow user

Subject

Date

in

4, 11, 11

label

(Who is the) the object of classification is *

(Who's label is the object of classification)

To Subject of clearance

To object subset to Subject of

passive to active to form process to

levels

C categories

$$\text{Labels} = L \times P(C)$$

Power set

J.W)

$$L = \{\text{Confidential}, \text{Secret}\}$$

$$C = \{\text{NATO}, \text{CIAY}\}$$

(Confidential, {NATO})

(Secret, {NATO, CIAY})

(Secret, \emptyset)

Subject in
Date 9/1, 2022

$R \subseteq \text{Labels} \times \text{Labels}$

\rightsquigarrow policy \rightarrow صنایع

A subject s has access on o iff $s R o$.

(Amoroso \rightarrow امورو)

is bounded lattice \rightarrow no label

\rightarrow Partially Order Set (پارسیل ارڈر سٹ)

lattice:

↓ Partially Order Set (پارسیل ارڈر سٹ)

↓ Poset (پوسٹ) greatest lower bound, least upper bound \rightarrow Compartiment

meet, join
glb lub

bounded lattice \rightarrow محدود پوسٹ ایک لیٹس نامہ

↳ Order Theory

Complete lattice \rightarrow مکمل پوسٹ (meet, join)

\rightarrow bounded lattice (محدود)

Lattice \rightarrow اسے Security label کا لattice کہا جاتا ہے

$\{L, H\}$, $L \leq H$

(~~public~~)

label is

private, public



Subject _____
Date _____

$$L \times P(C)$$

$$(L, \leq) \xrightarrow{\text{lattice}} (P(C), \subseteq) \xrightarrow{\text{lattice}} (L \times P(C), \leq)$$

$\Rightarrow (L \times P(C), \leq)$ is dominated by

$(l_1, C_1) \leq (l_2, C_2) \Leftrightarrow l_1 \leq l_2 \wedge C_1 \subseteq C_2$

$l_1 \leftarrow l_2, C_1 \leftarrow C_2$

$$\begin{matrix} (l_1, C_1) \\ O_1 \\ \times \\ O_2 \\ (l_2, C_2) \end{matrix}$$

لattice policy area
نیز سیاستیں اور امنیتیں میں ایک لattice

$$E_{O_1} \downarrow$$

امانیتی information flow security flow

j)
 $L = \{\text{Confidential, Secret}\}$

$$C = \{\text{NATO, CIA}\}$$

$$(\text{Secret}, \{\text{NATO}\})$$

$$(\text{Secret}, \{\text{CIA}\})$$

$$(\text{Confidential}, \{\text{NATO}\})$$

$$(\text{Confidential}, \{\text{CIA}\})$$

$$(\text{Confidential, Secret}), (\text{NATO, CIA})$$

$$(\text{Confidential, Secret}), (\text{NATO, CIA})$$

$$(\text{Confidential, Secret}), (\text{CIA, NATO})$$

نیز loop میں، اسی طرح

P4PCO

میں بدلے کرنے کا درجہ

میں تبدیل کر دیا

کر دیا جائے گا

Subject

ج

Date

٢٤/٨/٢٣

Lattice \rightarrow $(2^2 \times 2^4)^2 = 2^8 = 256$ درجه حریق (دسته های) در لایه های

ویژگی های اطلاعاتی (information flow) در MLS، Policy محدوده های انتقال اطلاعاتی (information flow) بین object

(a, b) information flows to

Policy \rightarrow که عربی این است: چون a چیزی است که باید بـ b اطلاعاتی خواهد داشت \rightarrow A lattice-model ...

ویژگی (Consistency) \rightarrow (Jaja & Denning)

او از این لایه اولیه در لایه دیگر برای این داده را در لایه دیگر درست نمایند

Bell-LaPadula Model (BLP):

- A disclosure security model.
(Confidentiality)

کلیک آنرا در مورد این مدل بخوانید

- A Mandatory Access Control (MAC) model

واعده کردن این افراد را در محدوده های خود می کنند

DAC over
(Discretionary)

Subject

Date ٢٠١٨/٩/٢٤

(Decidable \leftarrow MAC \rightarrow Undecidable \leftarrow DAC \rightarrow Safety \rightarrow)

1. (in general) \rightarrow مفهوم انتزاع وسائل (ما يحققه الممثل)

active Passive Entity \rightarrow BLP
Subjects, objects, access rights

S O ↓
BLP (Bell-LaPadula)

alter, observe : object \leftrightarrow subject

access rights:	observe	alter	
X	X	(e) \rightarrow execute	abstraction
X	✓	(a) \rightarrow append	↓
✓	X	(r) \rightarrow read	↓ S, O, C, Covert channel
✓	✓	(w) \rightarrow write	↓ O, S, C, Covert channel faithful

$$\text{Labels} = L \times P(C)$$

function

$f_s: S \rightarrow \text{labels}$ (max label)
 \rightarrow label \rightarrow subject

$f_c: S \rightarrow \text{labels}$ (current label)

$f_o: O \rightarrow \text{labels}$
 \rightarrow history

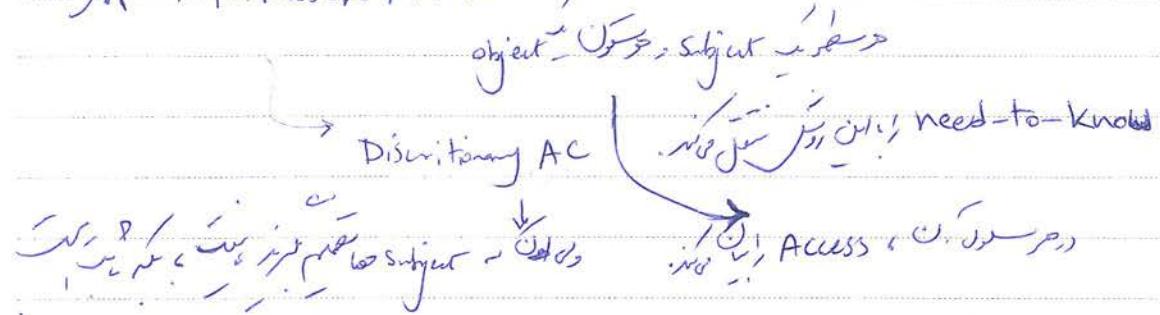
H \rightarrow hierarchy \rightarrow levels, parents, children

levels, levels

(levels, levels)

Subject CS
Date 9/11/11

$M \rightarrow$ Permission Matrix



(S, O, x) \rightarrow S \downarrow O \downarrow
 Access \rightarrow S \downarrow O \downarrow

Current Access Set \leftarrow b \cup b'

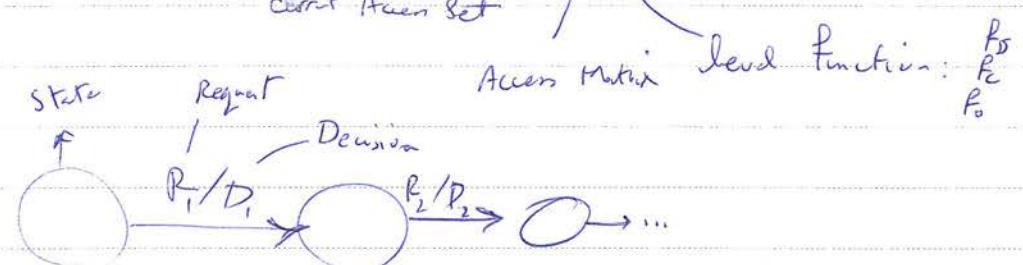
$$b = \{(S_1, O_1, x_1), (S_2, O_2, x_2), \dots\}$$

$b \in B$
 Current Access Set (b)

hierarchy

(b, M, P, h) is a state

current Access Set



make S_i Permission \rightarrow S_i in BLP \rightarrow S_i

PAPCO \rightarrow Secure state \rightarrow initial state

NY

Subject
Date

۱۴/۹/۲۳ پ.ج

: نویس، Secure State

نحوه ایجاد

1. Simple-Security Property: (no-read-up) (NRU)

(SS-Property)

که در اینجا object با subject

که no-read-up است
↓
read write

و dominate ل object label و subject label است

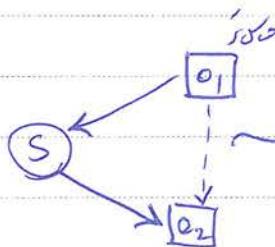
If $(s, o, r) \in b$, then $f_s(s) \succ f_o(o)$

dominates

$(l_1, C_1) \circ (l_2, C_2) \Leftrightarrow l_2 \leq l_1 \wedge C_2 \subseteq C_1$

نحوه ایجاد نویس state برای ایجاد SS-property

2. *-Property: (no-write-down) (NWD)



مخصوص این جزء بودن است
subject این جزء خارج نموده است

دارد این جزء

Subject

CS

Date

٢٠٢٣/٨/٢٠

میتوانی اگر $f_o(o)$ در $f_c(s)$ باشد، آنچه در $f_c(s)$ داشته باشید را در $f_o(o)$ نیز داشته باشید.

$$(S, o, \omega) \in b \Rightarrow f_o(o) \leq f_c(s)$$

current $\frac{1}{2}$.

این میتواند $f_s(s)$ و $f_c(s)$ را حل کند و در نتیجه $f_s(s) \leq f_c(s)$ باشد.

3. ds-property: (need-to-know)

$$(S, o, x) \in b \Rightarrow x \in M_{S, o}$$

(بررسی granuality) این باید در محدوده (range) یک object را در خانه خود (label) در نظر بگیرد.

(بررسی MAC) این باید در محدوده (discretionary) این محدوده را در نظر بگیرد.

(Basic Security Theorem) BSET $\vdash_{\text{BLS}} (\text{ds}, \text{ss}) \vdash \text{ss}$ (بررسی محدوده روی ss)

نتیجه: نظریه این است این محدوده روی ss را در نظر بگیرد.

این محدوده این است این محدوده روی ss را در نظر بگیرد.

این Safety Property $\vdash_{\text{BLP}} \text{ss}$ (بررسی محدوده روی ss)

PAPCO (Bad things never happen)

(proscribe)

Subject _____
Date _____

ـ مـوـاعـدـاتـ وـ بـاـدـ تـيـنـگـزـ bad things

ـ Safety اـنـتـرـاـنـ بـلـ بـلـ (Safety initialization policy)

something good will happen \leftarrow liveness property \wedge
(prescribe)

ـ مـوـاعـدـاتـ وـ بـلـ بـلـ (Safety initialization policy) \rightarrow termination condition

ـ مـوـاعـدـاتـ وـ بـلـ بـلـ (Safety initialization policy) \rightarrow BLP-Secure

ـ مـوـاعـدـاتـ وـ بـلـ بـلـ (Safety initialization policy) \rightarrow Computational Induction Safety property

ـ مـوـاعـدـاتـ وـ بـلـ بـلـ (Safety initialization policy) \rightarrow liveness property

ـ مـوـاعـدـاتـ وـ بـلـ بـلـ (Safety initialization policy) \rightarrow object \rightarrow subject \rightarrow \vdash $\text{BLP} \rightarrow$ BSP

(Safety Property \neq Safety Problem). \rightarrow decidable MAC \rightarrow Safety problem

ـ مـوـاعـدـاتـ وـ بـلـ بـلـ (Safety initialization policy) \rightarrow Rule \rightarrow BLP \rightarrow Liveness

ـ مـوـاعـدـاتـ وـ بـلـ بـلـ (Safety initialization policy) \rightarrow Rule \rightarrow transition (1)

(Secure-state-Preserving) \rightarrow Secure-Preserving rule \rightarrow (1)

ـ مـوـاعـدـاتـ وـ بـلـ بـلـ (Safety initialization policy) \rightarrow Rule 1 (R1) : get-read

Domain of R1: all $r_k = (g_i, s_i, o_j, r)$ in $R^{(1)}$

ـ مـوـاعـدـاتـ وـ بـلـ بـلـ (Safety initialization policy) \rightarrow Rule 1 (R1) : get-read

Subject QW
Date 9/1/15

Request to observe before alter Obj

Semantics: subject s_i requests access to object o_j in read-only mode. (r)

*-Property Function: $\star_1(r_k, v) = \text{TRUE} \Leftrightarrow p_c(s_i) \wedge p_o(o_j)$

The rule:

$$R_1(r_k, v) = \begin{cases} (? , v) & \text{if } r_k \notin \text{Domain}(R_1) \\ (\text{yes}, (b \vee (s_i, o_j, r), m, p, h)) & \text{ds-prop.} \\ & \text{if } r_k \in \text{Domain}(R_1) \wedge \text{REM}_y \\ & \text{ss-prop} \wedge p_s(s_i) \wedge p_o(o_j) \wedge \\ & (s_i \in T \vee \star_1(r_k, v)) \\ (\text{no}, v) & \text{otherwise: Trusted Subject *-prop} \end{cases}$$

وهو مفهوم Trusted Subject \rightarrow Trusted Subject \wedge *-Prop. \wedge Obj to Trusted Subject

وهو مفهوم:

: BLP (Violations)

وهو مفهوم \leftarrow Irrevocable + Safety

: MAC :-

: Compliance :-

(Security models \leftrightarrow
McLean)

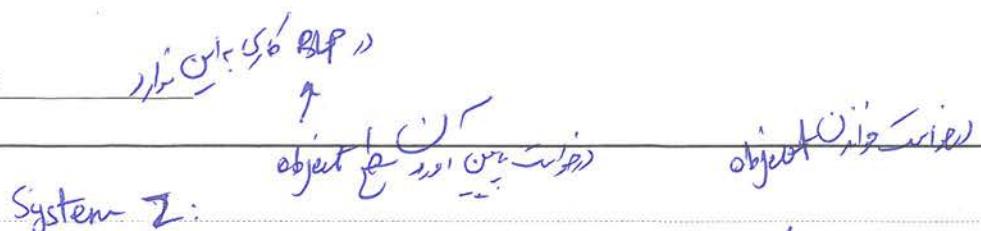
: Business Logic Formalism -

: BLP \rightarrow McLean \rightarrow System Z \rightarrow Business Logic -

P4PCO

NO

Subject _____
Date _____



وَنَفَرَ مِنْهُمْ مَنْ يَرْجُو ثَبَرَةً مُّعَذَّبَةً . (راهن نسبت)

McLean

ایرانی

object ! لیے ار stining

BLP Do بود که از این ایجاد کرد اما این کسی ایجاد کرد

object ! مل کل رئیس

ایرانی

BLP در ویسی کو درست کی ایجاد کرد ایجاد کرد

In Intensional desc. Access Control
کچھ جزویت خواہی دار کیتے تراویل، *Extensional

Subject Security
Date 4/1/10

↳ Looking back at the Bell-Lapadula Model, 2005.

↳ (Intensional vs Extensional) Bell 1973

↳ 1973 (Bell & Howell) Intensional

↳ Intensional vs Extensional Access

↳ BLP (Bell-Lapadula) Information Flow Security Denny 1973

↳ (Bell-Lapadula) Information Flow for ← (A lattice model...)

↳ dynamic BLP vs static, dynamic, static

Noninterference:

(Goguen-Messing)

↳ Extensional, noninterference

↳ (noninterfering, MLS, BLP)

One group of users using a certain set of commands is

noninterfering with another group of users if what the first

group does with those commands has no effect on what the

Second group of users can see.

P4PCO

↳ (noninterfering, MLS, BLP)

(Purge ← Insert, Insert)

NY

Subject _____
Date _____

1) noninterference assertions! (Global) (in U) Policy \rightarrow \perp

Definition - A system M consists of

- A set U of users
- A set S of states
- A set SC of commands
- A set Out of ^{state} outputs
- A set $Capt$ of capability tables
- A set CC of capability commands
- A function $out: S \times Capt \times U \rightarrow Out$
 \downarrow
initial state, user
- A function $do: S \times Capt \times U \times SC \rightarrow S$
- A function $cdo: Capt \times U \times CC \rightarrow Capt$

- s_0, t_0 : the initial machine state and the initial capability table

$$\therefore C = SC \cup CC, S = S \times Capt \quad \text{initial}$$

\downarrow
Command State

$$Ab = P(C)$$

\downarrow
Powerset

$$Capt = Ab$$

\downarrow

$$Ab = \text{U function}$$

initial output with $Capt$ initial

Subject Jc
Date 4/17/10

$$csdo : \underbrace{S \times Capt \times U \times C}_{S'} \rightarrow \underbrace{S \times Capt}_{S'}$$

$$csdo(s, t, u, c) = \begin{cases} (do(s, t, u, c), t) & \text{if } c \in SC \\ & \} \\ (s, cdo(t, u, c)) & \text{if } c \in CC \end{cases}$$

closure:

$$csdo : S \times Capt \times (U \times C)^* \rightarrow S \times Capt$$

is it, so closure is true

(closure)

$$csdo(s, t, \text{NIL}) = (s, t)$$

$$csdo(s, t, w.(u, c)) = csdo(\underbrace{csdo(s, t, w)}_{wp, state}, u, c) \quad (\text{join rule})$$

$w \in (U \times C)^*$

$$[w] = csdo(s_0, t_0, w)$$

persiste

$$w \text{ جزء من } [w]_u : \text{out}([w], u)$$

Definition - Let $G \subseteq U$, $A \subseteq C$ and $w \in (U \times C)^*$.

we let $P_G(w)$ denotes the subsequence of w obtained by
purge function \leftarrow eliminating those pairs (u, c) with $u \notin G$.

PAPCO

19

Subject: Ability to prove
Date:

$P_A(w)$ is defined similarly. Likewise $P_{G,A}(w)$ is obtained by

eliminating those pairs (u, c) with $u \in G$ and $c \in A$.

Example - $G = \{u, v\}$, $A = \{c_1, c_2\}$

$$P_{G,A}((u, c_1), (u, c_3), (u, c_2), (v, c_1)) = ((u, c_1), (u, c_2), (v, c_1))$$

Definition - Given a state machine M and sets $G, G' \subseteq V$. We say that

G does not interfere with (or is ~~not at~~ ^{noninterfering with}) G' , write $G \perp G'$,

iff $\forall w \in (V \times C)^*$, $\forall u \in G$, $[w]_u = \boxed{[P_G(w)]_u}$.

Similarly,

$A \perp G' \Leftrightarrow \forall w \in (V \times C)^*$, $\forall u \in G'$, $[w]_u = [P_A(w)]_u$.

$G, A \perp G' \Leftrightarrow \forall w \in (V \times C)^*$, $\forall u \in G'$, $[w]_u = [P_{G,A}(w)]_u$.

((()) low, high))))) high for MLS just, (())

Subject CS

Date AK, A, P

Example 1 -

$$A : | \{u\}$$

or F is given a policy in form

MP Job, A, \leq , 10

Example 2 - level: $U \rightarrow L$ (L, \leq)

$$U[-\infty, \infty] = \{u \in U \mid \text{level}(u) \leq \infty\}$$

$$U[n, +\infty] = \{u \in U \mid n \leq \text{level}(u)\}$$

n is multilevel-secure iff

$$\forall n' \exists n. U[n, +\infty] \subset U[-\infty, n'].$$

or

$$U[n, +\infty] = | \overline{U[n, +\infty]} \xrightarrow{\text{complement}}$$

Wij zijn bijna

Example 3 - $A \xrightarrow{\text{User}} \text{proj1}, \text{Cap. table}, \text{view}$

Ability with Security Officer is Seco

$$\{\text{Seco}\}, A : | U$$

P4PCO ~~There is just one designated user 'seco' who can use of commands~~
ay 'A' will have any effect.

Subject

J

Date

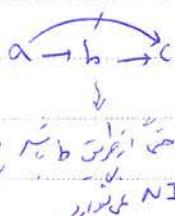
9/14, 9/15

is transitive justice and do not care

$G:1G' \wedge G:1G'' \not\Rightarrow G:1G$

is intransitive partial justice (A Policy)

Scope Policy, Credibility, non-interference, is intransitive justice



is transitive justice is intransitive
Credibility of Bob's Policy \Rightarrow non-local

Open
non-judgmental

channel = a set of commands

$A \subseteq C$. similarly in judge

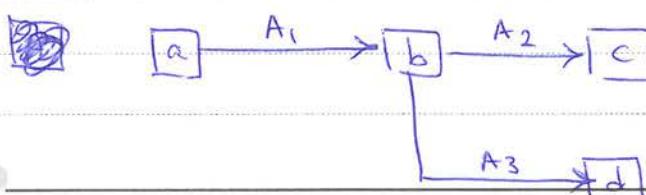
$G, G' \in U$

G and G' can communicate only through the channel A .

(private channel). instead of A it's A'

$G, \bar{A}:1G' \wedge G'\bar{A}:1G$

is intransitive justice



Subject

CS

Date

26/9/15

Fixing Assertion Errors

{b,c,d} : Kary

sat, $\bar{A}_1 : \{b,c,d\}$

{c,d} : 1 {b}

{b}, $\bar{A}_2 : \{c\}$

{c} : 1 {d}

{b}, $\bar{A}_3 : \{d\}$

{d} : 1 {c}

At Specification: $\text{sat} \vdash \text{assertion}$ \rightarrow $\text{sat} \vdash \text{assertion}$

When refining for assertion

NI = Non-Deterministic

Ex.

- مکمل پرچشل سیستم (محضی، پارهیزیت) خود حفظ کنید، پس از حذف (Purge)

- Deterministic (مطابق با مدل)

(Deterministic state, initial state)

non-deterministic approach

trace-based

Specify both concurrency & non-determinism

Implementation refinement, deterministic Policy

(non-deterministic behaviour). In non-deterministic

Security models

non-deterministic

NI (Non-Deterministic)

Subject _____

Date _____

1. چیزی که دیگر نیست، این Restrictive شناختی است

ideal cryptography می تواند این را بفرموده باشد. خوب است این را درست

برای خود

: non-deterministic trace-based model of

چیزی که در مجموعه Σ^* می تواند اتفاق بخورد

trace پس از یک trace می ورثت از input

از آن پس

Trace = A sequence of events.

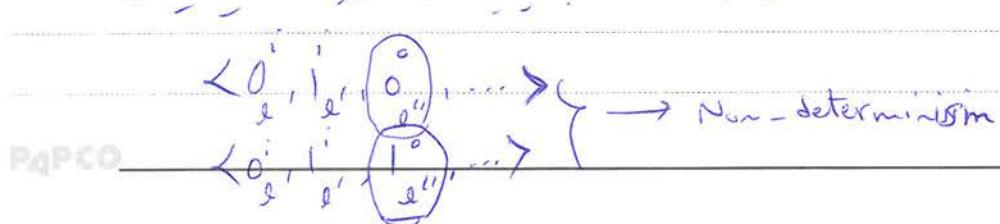
event : input, output

$$T = \{ \langle 0, 1, 0, 1, 0, 1 \rangle \rightarrow \text{Output} \}$$

$\text{Pref}(T) \subseteq T$

Trace \sqsubset Trace \sqcup prefix

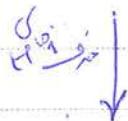
non-deterministic چیزی که در مجموعه Σ^* می تواند اتفاق بخورد



Subject JW
Date ٢٤, ٩, ١٥

: H, L جواب

$$\langle \overset{0}{H}, \overset{1}{L}, \overset{0}{L}, \overset{0}{H}, \overset{1}{H} \rangle$$



in low observation & H is input

$$\langle \overset{1}{L}, \overset{0}{L}, \overset{1}{H} \rangle \rightarrow \text{NI} \rightarrow \text{high obs: } 0^*$$

T Untraceable, and H is not traceable

(GMNI-Secure)

NI-Secure، NI

Non-deductibility:

(Sunderland 5.1)

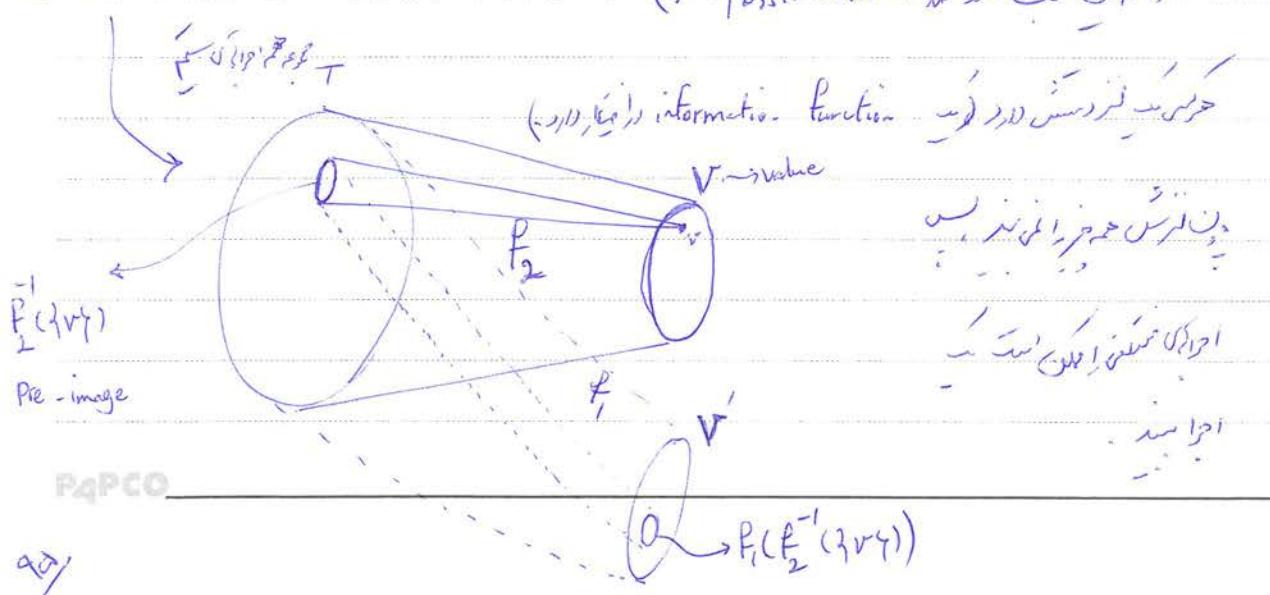
نحویات NI

نحویات ندھریتی Non-deductibility، NI

نحویات ندھریتی

a set of possible worlds

(Possibilities)



Subject _____
Date _____

$f_2^{-1}(V_f)$ is not a function from V_f to V_f . It is not surjective.

دستگاه

$f_1 \circ f_2$ is not a function from V_f to V_f .

(view)
(low $\leftarrow f_2$)
(high $\leftarrow f_1$)
(hidden):

$f_1(f_2(V_f)) \neq V_f$

Exclude first (view, high $\leftarrow f_1$, low $\leftarrow f_2$). f_1 flows to f_2 on v . f_2 on f_1 .

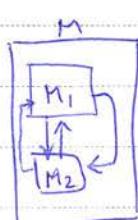
$\forall v \in V, f_1$ does not flow to f_2 on $v \Leftrightarrow f_1$ does not flow to f_2

: moto is of

(M_1, M_2, V_f). $M_1 \rightarrow f_1$ exists if f_1 exists.

interclude $M_1 \rightarrow f_1$ exists if f_1 exists.

ND \oplus : (N_1, N_2) (زیر جزوی) high \rightarrow high (زیر جزوی) high \rightarrow NI *



و زیر جزوی high \rightarrow

M_1, M_2 : Secure
so, M is Secure \rightarrow Composable, \rightarrow ND, NI

و زیر جزوی high \rightarrow high \rightarrow moduler, پنهانی، پنهانی

Subject: Ju
Date: 9/9/18

Composition:

Composition is modular. If M_1 and M_2 are secure, then $M_1 \circ M_2$ is also secure.



If M_1 is secure and M_2 is secure, then $M_1 \circ M_2$ is secure?

Ju: McCullough → chapter 25, Amoroso

Ju: Heiko Mantel

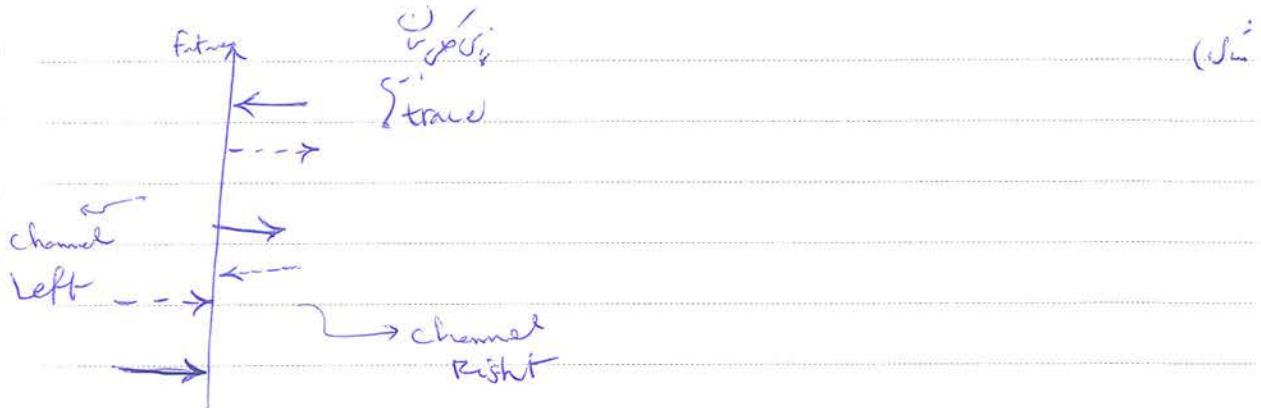
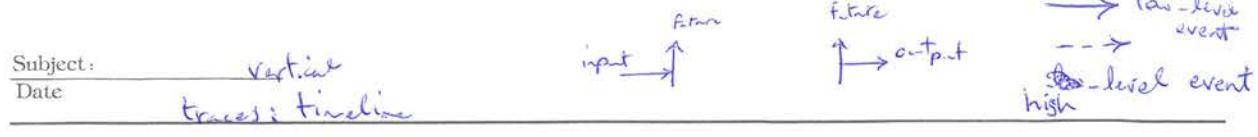
- Project Framework
- Policy
- (Assembly kit)

trace-based \vdash Non-deduplicability

For any two acceptable traces T and S , there is an acceptable trace R consisting of T 's low-level events (in their respective order), S 's high-level inputs (in their respective order) and possibly some other events that are neither low-level events from T nor high-level inputs from S .

↳ \vdash $T \circ S \vdash R$
↳ include

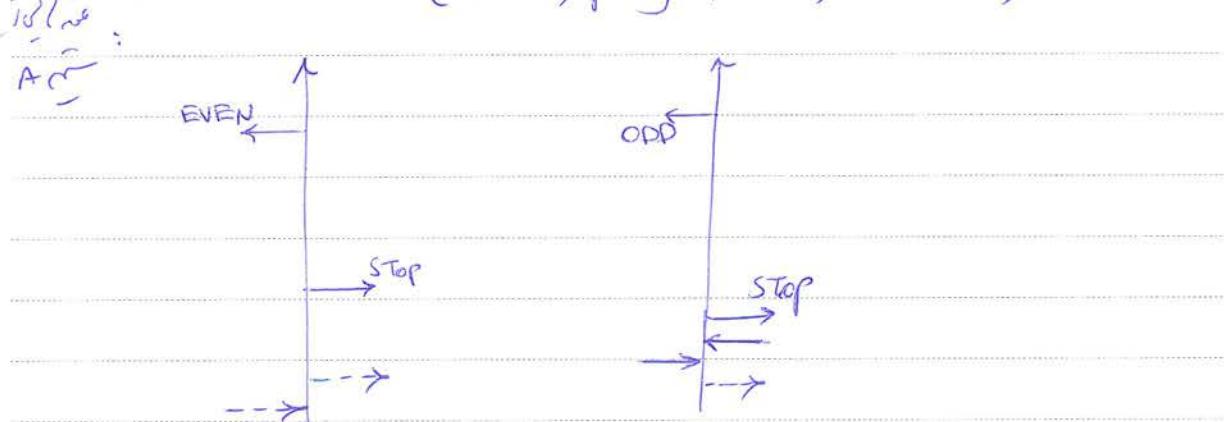
PAPCO



System A: each trace starts with some number of high-level inputs or outputs followed by the low-level output STOP followed by the low-level output ODD (if there has been an odd number of high-level events prior to STOP) or EVEN (if there has been an even number of high-level events prior to STOP).

The high-level outputs and the output STOP leave via the right channel and the events ODD and EVEN leave via the left channel.

(STOP, parity, Even & EVEN, ODD)



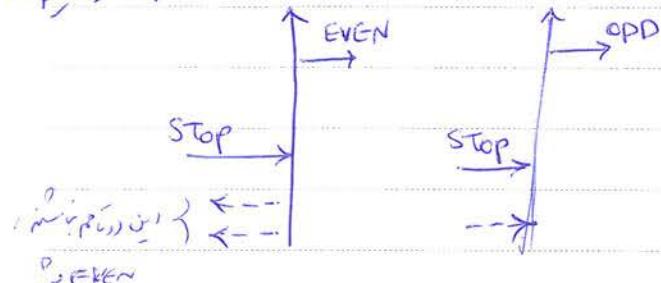
Topic: high-level input vs. low-level observation of A

System B:

: A \vdash , B \vdash does

- its high-level outputs leave via left channel.
- its EVEN and ODD outputs are output from its right channel.
- STOP is an input to its left channel.

B \vdash does:



EVEN

Is System A nondeducability secure? Yes

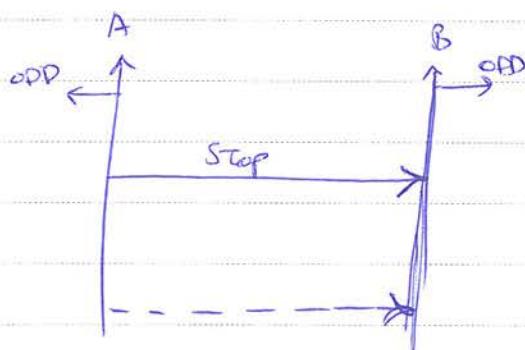
B ? Yes

/
✓ excludes no high-level input; high-level input vs. low-observability?

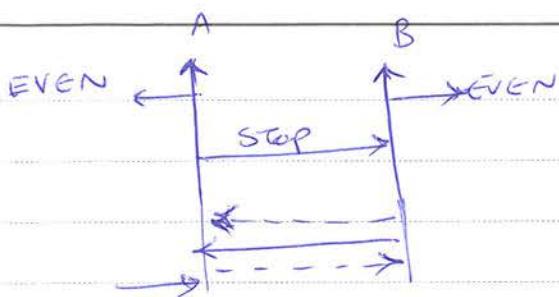
: fixing hook-ups \rightarrow fix jobs

: fix job A \rightarrow fix job B \rightarrow fix job

Connect the left channel of B to the right channel of A.



Subject: _____
Date: _____



exclude! \rightarrow high-level input, \rightarrow (odd, even) rules

Or parity \rightarrow parity \rightarrow parity \rightarrow

Ex high-level input \rightarrow (odd, even) \rightarrow interaction

(parity original)

Composable, Non-deductible

- Composable \rightarrow restrictiveness occurs if
(super event \cup_{α}) \vdash \neg α

trace \rightarrow Possibility, information flow

1. \vdash \neg α \vdash trace

محدث: \neg α \vdash \neg α \vdash trace

non-composability Possibility, not exclude

not exclude, \vdash \neg α \vdash trace

Probabilistic \leftarrow not leakage

Subject: پر

Date:

4 A.V

Probabilistic UML Approach پر میں درج کر دیا

(Probabilistic UML) این سے Refinement پر میں درج کر دیا

Refinement Specification پر میں درج کر دیا

non-determinism

non-determining non-determining اسے اپنے Refinement پر میں درج کر دیا

Refinement Specification اسے اپنے Refinement پر میں درج کر دیا

UML Probabilistic اسے اپنے Refinement پر میں درج کر دیا

Information Flow Rules اسے اپنے Refinement پر میں درج کر دیا

جنہیں بھر کر رکھ کر اسے اپنے Refinement پر میں درج کر دیا

Hyperproperty, Property اسے اپنے Refinement پر میں درج کر دیا

Refinement ← اسے اپنے Refinement پر میں درج کر دیا

Refinement-closed اسے اپنے Refinement پر میں درج کر دیا

Enforcement اسے اپنے Refinement پر میں درج کر دیا

Property اسے اپنے Refinement پر میں درج کر دیا

Hyperproperty اسے اپنے Refinement پر میں درج کر دیا

Subject: Integrity model
Date: Biba

= multi-level model

Integrity Models:

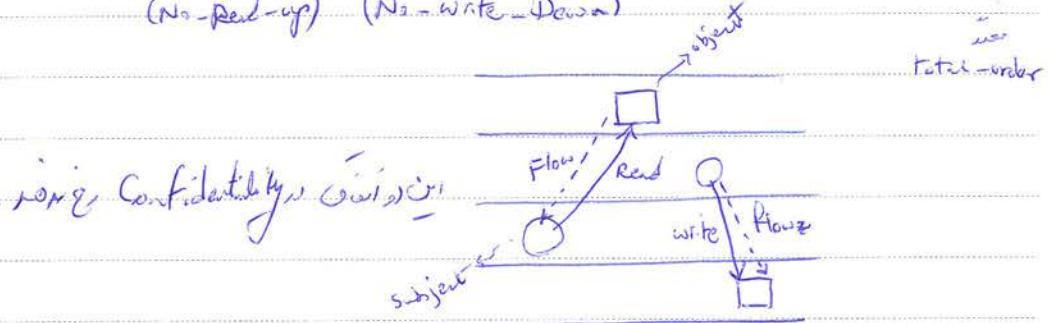
↳ Integrity \rightarrow Confidentiality \rightarrow dual
BLP \rightarrow A MAC (Confidentiality) model \rightarrow ↓ iterations
↳ P model

Biba Model:

: پروتکل امنیتی بیبا، در BLP باشدیت و

BLP \rightarrow NRU, NWP

(No-read-up) (No-write-down)



و شناسی در این Integrity، Confidentiality نیست

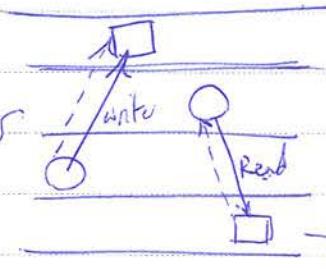
که در این سیستم این دو مفهوم را در نظر نمی‌گیرند

برای این سیستم این دو مفهوم را در نظر نمی‌گیرند

Integrity, Confidentiality, Label

Subject: بیان
Date: ۹۶/۱۰/۱۰

سیستم مخصوص امنیتی: Biba Model



NRD (No-Read-Down)

NWD (No-Write-Up)

این سیستم از اینکه کسی میتواند اطلاعات را در سطح بالاتر از خود تغییر دهد، جلوگیری میکند.

(Integrity) (Confidentiality)

Biba
NRD

NWD NWD



پس از حفظ کردن اطلاعات، این امنیتی را میتواند در توزیع اطلاعات نگهداشته باشد / Information Flow Control

In Mandatory Biba Model

Subject Low-water mark model:

Water Mark: خط کنترل - درین مرتبه

or PAPCO

(Integrity vs. watermark)

Subject:

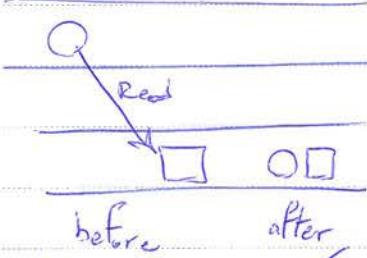
Date

دستورات محدود

NRD (نر) rigid، صریح، (بای) Mandatory (مجبو)

ویا Read Done & subject پس از بخواهند Relax، NRD نیز

اجباری subject باز رخواه

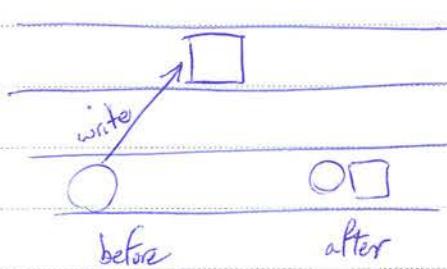


منفی: حفظ اگر کسی کسی می‌خواهد این کسی کسی نمایند

Object low-water mark model:

no relax، LWW

Object ایجاد شود و write up، object ایجاد شود و subject ایجاد شود



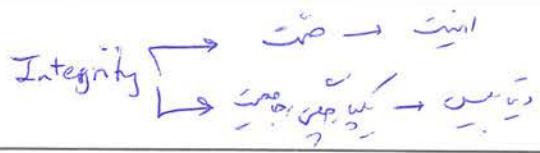
محدود، خود

لیبل یا Policy یا Rule، Biba، BLP، آنچه پس از اینها است

PAPCO

لیبل درینجا نداشته باشد

Subject: Integrity
Date: at 9/6



Object is object, subject is subject. Integrity is mandatory for all users *

(عند حفظ الملفات على القرص) ~~عند حفظ الملفات على القرص~~ *

Unmodified, Modified & Untrusted, Trusted \rightarrow Integrity Levels *

For multi-level objects? For multi-level objects?

Integrity

The Clark-Wilson Model:

Bookkeeping Accounting in Commercial Organization
(A comparison of commercial and military security policies)

Well-defined transactions

Sequence of atomic actions

order

multiple users, personal

Separation of Duties

D: A set of data items

جواب

$$D = CDI \cup UDI ; CDI \cap UDI = \emptyset$$

CDI: Constrained Data Items

UDI: Unconstrained Data Items

Unconstrained

100% user constrained process

Subject: well-defined transaction
Date:

Integrity Rule

1. Using (S), no two subjects have same rule in

transformation Procedures (TP)

$$Tp: \text{Subjects} \times D \rightarrow D$$

$$Tp(S, d) = d'$$

2. $d' \in d$: domain of Tp or S subject

$$\text{Copy}(S, d) = d$$

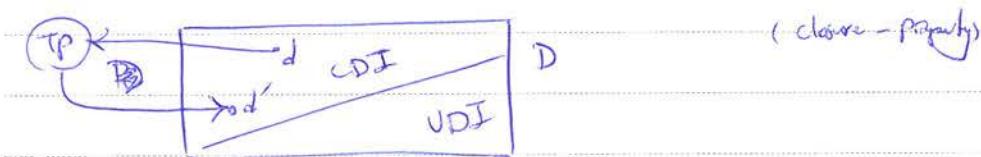
$$\text{nullify}(S, d) = \text{null}$$

Rule 1: IVPs must be available on the system for validating the integrity of any CDI.

IVP: Integrity Validation Procedure

checksum Σx_i^2

Rule 2: Application of a TP to any CDI must maintain the integrity of that CDI.



PAPCO $Tp(S, d) = d' \wedge d \in \text{CDI} \Rightarrow d' \in \text{CDI}$

جی (BIP جی کوئی)

Subject:

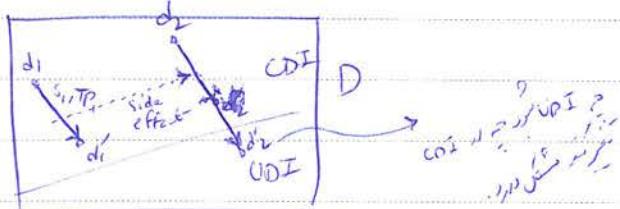
Date: ۲۰/۹/۱۶

کوئی تحریک نہیں کر سکتا جی کوئی CDI پر تحریک کر سکتے ہیں اس کا side effect ہے rule ۳

کوئی TPs کو کوئی side effect نہیں کر سکتا

Rule 3: A CDI can only be changed by a TP.

کوئی TPs کو کوئی CDI کو تحریک نہیں کر سکتا



کوئی TPs کو کوئی CDI کو تحریک نہیں کر سکتا

it f (int n) {

 it y; → یہ اپنے ڈائیکٹ اسے کرے

 y = n + 1;

 z = y;

 return y

 ایسا ڈائیکٹ اسے کرے

}

Rule 4: Subjects can only initiate certain TPs on certain CDIs.

$$R = \{ (s, t, d) | \dots \} \subseteq \text{Subjects} \times \text{TPs} \times \text{D}$$

پہلے ٹپ کی ایجاد کرنے کی اجازت

Topic: CDI تحریک کرنے والے TPs کو کوئی subject کو کہا جائے

Subject:

Date

9/9/18

Rule 5. CW-triples must enforce some appropriate separation of duty policy on subjects.

Separation of duty policy

Separation of duty policy

Separation of duty policy

Review policy

Rule 6. Certain special TPs on UDI's can produce CDI's as output.

Deserialisation

Serialisation

Rule 7. Each TP application must cause information sufficient to reconstruct the application to be written to a special append-only CPI.

Reconstruction information

Rule 8. The system must authenticate subjects attempting to initiate a TP.

Authentication

P4PCO

Subject: 5

Date:

9, 14

Rule 9. The system must only permit specific subjects (i.e. security officers) to make changes to any authorization-related lists.

(. فرمانیه ایجاد و تغییر محدود است) WR لست های امنیتی را تغییر نماید

برای این ایجاد و تغییر محدود است (Multi-level, Multi organization Security) (فروشنده ایجاد و تغییر محدود است)

و Policy, و ایجاد و تغییر محدود است (abstraction)

BLP ایجاد و تغییر محدود است (ایجاد و تغییر محدود است، ایجاد و تغییر محدود است)

Commercial Trusts ایجاد و تغییر محدود است

نحوی سیستم Biba, BLP, CW ایجاد و تغییر محدود است

CW ایجاد و تغییر محدود است (ایجاد و تغییر محدود است، Biba ایجاد و تغییر محدود است)

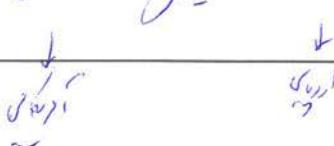
Multi lateral Security:

ایجاد و تغییر محدود است (ایجاد و تغییر محدود است، ایجاد و تغییر محدود است)

ایجاد و تغییر محدود است (ایجاد و تغییر محدود است، ایجاد و تغییر محدود است)

Compartment Security ایجاد و تغییر محدود است (ایجاد و تغییر محدود است)

PAPCO



109

Subject:
Date

lattice model:

ادن پریمیوں کا ایک جزو
→ "ultra"

(b) Compartiment no. 9. Category - 10-11
Compartment no. 9. Category - 10-11

جذب الماء من العصارة بـ Na_2SiO_3 و CaCl_2 في H_2O

Chloroform water (chloroform in water) Compartiment (in). In

Chinese Walls: (Brewer and Nash) (The Chinese wall security Policy)

Wrong sides, right side towards wall etc.

④ a partner who has worked recently for one company in a

business sector may not see the papers of any other

Company in that sector.' ↑ To what irrational is

Conflict of interest (प्रतिवाद)

Database Organization → Hierarchical Structuring of Information

There are three levels of significance:

a) at the lowest level, we consider Σ^0

individual items of information, each concerning a single corporation. (objects)

Subject: J.L.
Date: 17/9/18

b) at the intermediate level, we group all objects which concern the same corporation together into what we call a company dataset.

c) at the highest level, we group together all company datasets whose corporations are in competition. We will refer to each such group a conflict of interest class.

Corporation's Company dataset y_r

notation:

o_r
 r -th object : o_r
 y_r : o_r 's Company dataset
 x_r : o_r 's conflict of interest class

i) Bank - A

oil company - A

oil company - B

Corporation's Company dataset: y_r object o_r

y_r : Bank - A, Oil Company - A, Oil Company - B

x_r : y_r 's Conflict of Interest

x_r : Banks' ~~Company~~, Petroleum Companies

↳ Sector ↳

PAPCO

11

Subject: _____
Date: _____

نحو:

Simple Security:

نحو: ~~نحو: معاً~~ Conflict of interest (Interest) \rightarrow (Allowed access)
(Possess)

نحو: Basis of Access

نحو: Mandatory Access Control (MAC) \rightarrow (Free choice)

نحو: ~~نحو: معاً~~ A subject has access to an object.

نحو: ~~نحو: معاً~~ A subject has access to an object.

The only information already

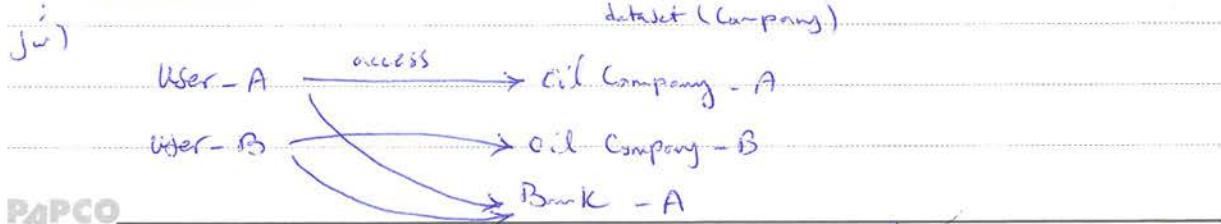
Access is only granted if the object requested:

a) is in the same company dataset as an object already accessed by that subject, i.e., within the wall

or

b) belongs to an entirely different conflict of interest class.

* - Property:



نحو: ~~نحو: معاً~~ User-B can't access Oil Company-A because User-A has it.

Subject: ISYE
Date 26/7/14

Write access is only permitted if

- ✓
Properties
a) access is permitted by the simple security rule, and
b) no object can be read which is in a different
company dataset to the one for which write access
is requested and contains unsanitized information.

✓
either sanitize or de-identify

(deidentification)

Subject Object

✓
or just use Chinese Wall rule

- The simple Security property:

a subject s has access to σ_r if and only if, for all σ_p of which s can read, either $y_p \neq x_p$ or $y_p = y_r$.

✓
if $y_p \neq x_p$ then σ_p is not in σ_r

- The π -property:

a subject s can write to σ_r only if s cannot read any $\sigma_{r'}$ with $x_{r'} \neq \emptyset$ and $y_{r'} \neq y_r$.

✓
(if latter is true then $\sigma_{r'}$ is at a lower level than σ_r)

Reading 1 - The Chinese wall security policy, Brewer and Nash.

Subject: 1 - Chinese wall security policy, Brewer and Nash.
Date 2 - Chinese wall by Foley in his book (480) -
Scand Eng.

The BMA model: (multi-lateral U.S.A.)

(British Medical Association)

1. Objectives
2. Principles
3. Policies
4. Procedures
5. Controls

Centered on principles of transparency, accountability, and trade-off between
privacy and security. It is a multi-lateral model involving multiple parties.

Access Control (الوصول)

Object → Subject → Data → Process → Data → Subject

Access will be granted to authorized users.

- DHHS → Department of Health and Human Services, U.S.A

- HIPAA → Health Insurance Portability and Accountability Act

Regulation
or legislation

Threat model:

The main threat to medical privacy is abuse of authorized access by insiders, and the most common threat vector is social engineering.

Physical Security, IT Security, Social Engineering → operational Security

PAPCO

Physical Security
IT Security
Social Engineering

Subject: in
Date: 9/6/9/14

Reading: 3 - The Requirement Analysis (Ch 3) (37)

number of people who have access to it, value

Centralized cases

The security policy:

- AIDS Databases → Secret
- Normal patient Records → Confidential
- Administrative Data → Restricted
 - e.g. drug prescriptions, bills for treatment

AZT

IPM, End data subject

No inference

EPR (Electronic Patient Record)

Project EPR

Project EPR

PAPCO

Project EPR

Subject: _____
Date: _____

(ج) ایجاد امنیتی مبنی بر داد و ستد
ج) ایجاد امنیتی مبنی بر داد و ستد

- human fertilization

- sexually transmitted diseases.

- Prison medical services

- Birth Records

سما:

اصل: کل عاجزه، بار بستر کاربرد

اصل: کل عاجزه، بار بستر کاربرد

Access Control: اصل این \leftarrow all on the floor *

Record opening: اصل \leftarrow Principle

نیز \leftarrow

Denial of Service:

(کل خدمت را ممکن نمایند)

Availibility: این

Deny & Grant

و عرض

نمایش

الله هر قسم عملی کی بزرگ

مشکل ایجاد نمایند

maximum waiting time \leftarrow (Ginger time)
(MWT)

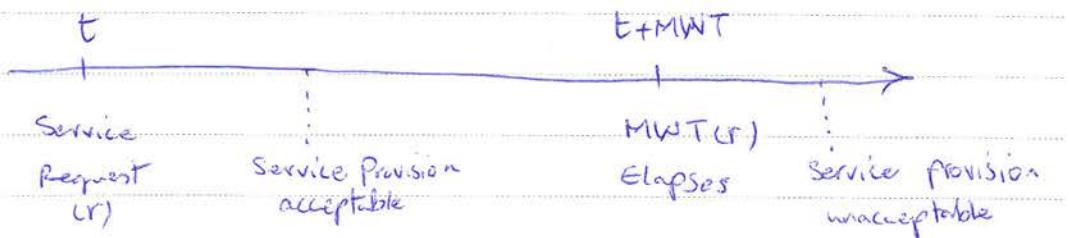
Subject: Ur
Date: 18.9.19

- The MWT for a given service is defined as the length of time after the service has been requested within which its provision is considered acceptable.

عندما يتم طلب الخدمة في وقت t، يجب أن تتم الخدمة قبل وقت t + MWT(r).

إلا إذا تم ذلك، فسيكون غير قابل للقبول.

MWT(r)



- The DoS threat is defined to occur whenever a service with associated maximum waiting time (MWT) is requested by an authorized user of time t and is not provided to that user by time $t + MWT$.

المُنْظَرُ مُنْظَرُ دَسْ بِمُنْظَرِ الْمَكْلُومِ، لِمَنْ يَأْتِي مَعَهُ الْمَكْلُومِ.

activity.

بِمُنْظَرِ دَسْ بِمُنْظَرِ الْمَكْلُومِ، لِمَنْ يَأْتِي مَعَهُ الْمَكْلُومِ.

وَلَا يَأْتِي مَعَهُ الْمَكْلُومِ، لِمَنْ يَأْتِي مَعَهُ الْمَكْلُومِ.

(Co-insider malicious J1) (Co-intend) .

از خود راهی کنید
Subject: A specification and verification method for preventing DoS,
Date: دویست و نهمین دوره مهندسی سایبری
IEEE Transaction on Software Eng. 1990, Yu and Gilster

Temporal logic

enforcement

Reasoning

which

model logic

منطق مدل

الخط

Knowledge

پیشامد، proposition

Conciseness

($\phi \wedge \psi \rightarrow \psi$) $\vdash \psi$

که از $\phi \wedge \psi$ پیشامد ψ است

و $\phi \vee \psi$ از ϕ و ψ پیشامد است

و $\phi \rightarrow \psi$ از ϕ خود ψ است

A $\phi \rightarrow \psi$ mode is ϕ made

R: obligation, time & knowledge \rightarrow mode

↓ ↓ ↓

deontic modal Epistemic

temporal

Subject: S

Date: ٢٠١٩/٩/٢٨

atom

$$\varphi ::= p \mid \neg \varphi \mid \varphi \wedge \varphi$$

: Propositional Syntax

: Derivable Syntax (مُدَرِّج)

$$\varphi \vee \varphi, \varphi \rightarrow \varphi$$

: (Box) مُعْلَم (Propositional Logic)

$$\varphi ::= p \mid \neg \varphi \mid \varphi \wedge \varphi \mid \Box \varphi$$

always \vdash (valid) hence Truth

(no map is required to interpret it - Semantics, meaning)

مُعْلَم (State)

(State Proposition)

$$\Diamond \varphi \triangleq \neg \Box \neg \varphi$$

مُعْلَم (Temporal Logic) $\varphi \rightarrow \psi \leftarrow \varphi \wedge \psi$ صيغة صحيحة (Valid Formula)

$$\Diamond \varphi$$

T

interval temporal logic \rightarrow این فضای زمانی

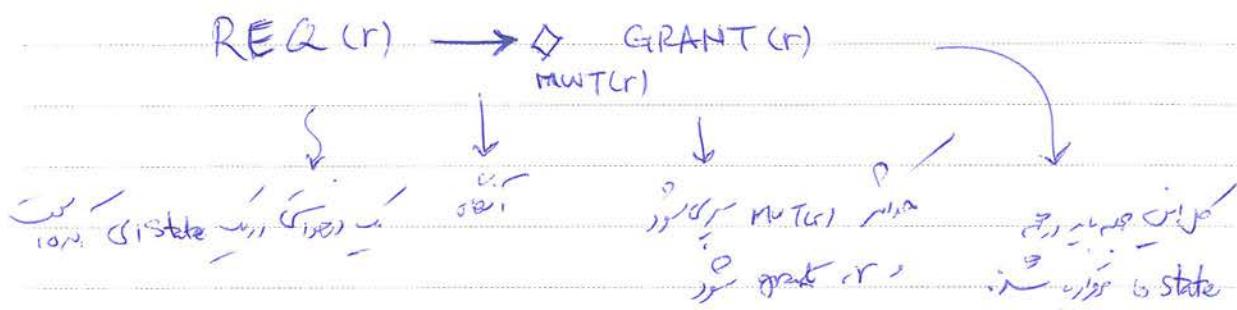
(past) $\Diamond \varphi$ صيغة صحيحة (Valid Formula)

verification (Verification) of temporal logic (Temporal Logic) \rightarrow Propositional Temporal Logic

PAPCO

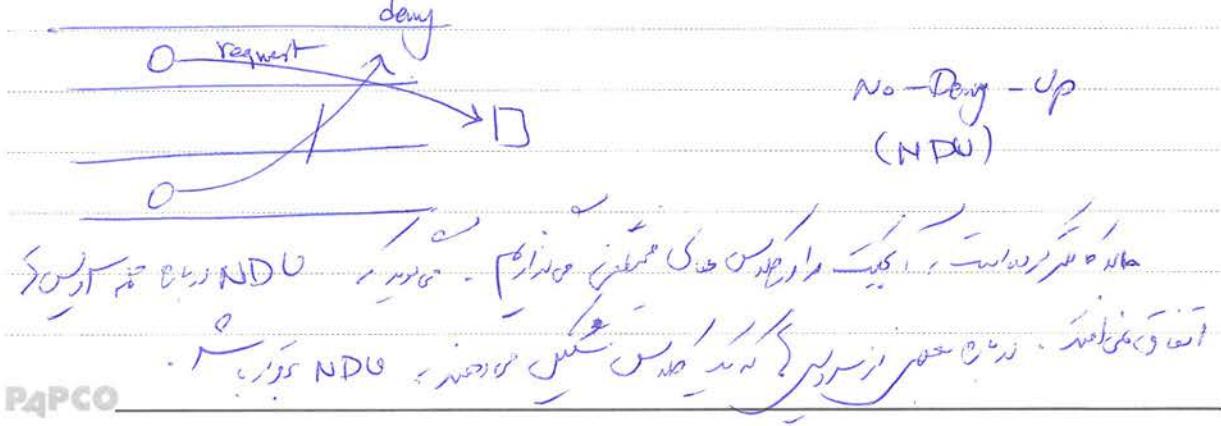
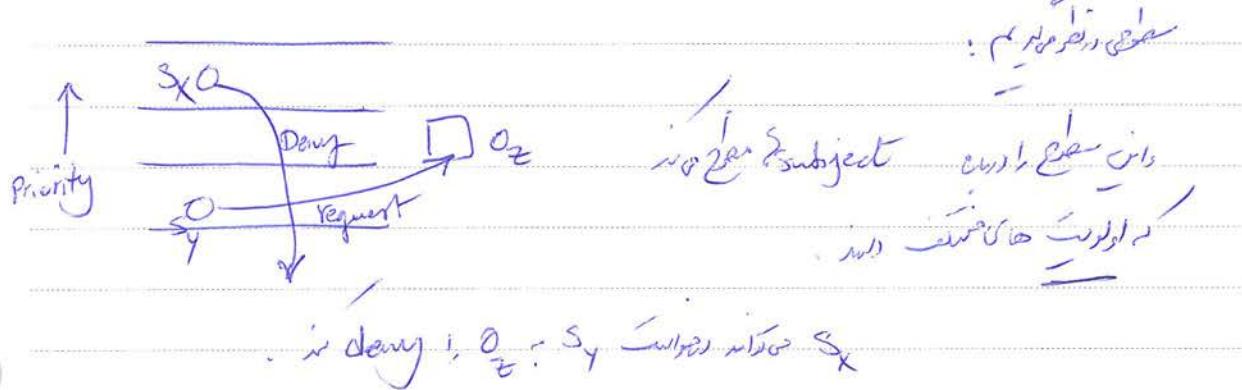
Subject: IS
Date: 20/9/18

انواع اذن و محدودیت اذن در پروتکل اینترنت



برای امتحان این ساختار را بخوبی!

Mandatory DoS Model:



Subject: یہ

Date: ۲۹/۸

ایک سیستم کا Priority ہے جس کی طبقہ
ایک سیستم کا خرچ کا ملک، بخراہ، ایک سیستم
ایک سیستم کا ملک، بخراہ، ایک سیستم

ایک سیستم کا ملک، بخراہ، ایک سیستم

Miller's RAM:

↓
Resource Allocation Model

Critical Resources، کوچک کی تعداد کی نسبت میں دیکھی جائے۔

ایک سیستم کا ملک، بخراہ، ایک سیستم

★ DPB (Denial-of-Service Protection Base)

TCB \rightarrow
MWT, FWT, AWT \rightarrow TCB
Finite average \rightarrow TCB
Worst-case \rightarrow TCB
Worst-case \rightarrow TCB

DPB \rightarrow rule, سیستم

A Resource Allocation Model for Denial of Service

John Miller, 1992

Context \rightarrow سیستم کا ملک، بخراہ، ایک سیستم

PAPCO

11A

Subject: J.
Date 9/9/2018

A Framework for the Analysis of DoS Attacks

Shavat and Falaki (2004)

Computer Journal Oxford University

Writings (جایزه) Undergraduate and PhD Analysis

Network Security vs. DoS is the DoS problem (چیزی کو کس کرنا)

Countering DoS attack

Survey of Network-based Defense Mechanisms

Peng, Leckie, Ramamurthy ACM Computing Survey 2006 Counting the DoS and DDoS problems

Survey based

new approaches to DoS countermeasures

Network layer → DoS → Application layer

(E.g., IP Traceback) → → Spoof

Network layer → DoS → Application layer

Parco
Infecting network nodes
Syn-flood

Subject: IS
Date AF, 9, 10

Safeguards and Countermeasures:



عوپلیں اور مذکورہ میں سے کوئی

سروچت ہیں جو اسی راستے پر

A safeguard is defined as any mechanism or procedure design to mitigate the effects of a threat before it can occur.

اے
عوپلیں
کوئی
مذکورہ
میں سے
کوئی

(alleviate)

عوپلیں اور مذکورہ میں سے کوئی
مذکورہ میں سے کوئی
مذکورہ میں سے کوئی
مذکورہ میں سے کوئی

(Preventive, Proactive)

سے Safeguard Use

- Integrated into design
- Avoid disastrous threats → life threatening
- possible waste of resources → Risk Analysis
- Difficult to measure to success

A countermeasure is defined as any mechanism or procedure designed to mitigate subsequent effects of same threat that has already occurred.

عوپلیں اور مذکورہ میں سے کوئی
مذکورہ میں سے کوئی
مذکورہ میں سے کوئی
مذکورہ میں سے کوئی

(Reactive)

(Postmortem) (After-deault)

Subject: _____
Date: _____

نحوه ایجاد امنیتی پس از میلادی، فوکوس Reactive است. در این دoS ها

نحوه ایجاد امنیتی پس از میلادی، فوکوس Reactive است. در این دoS ها

(Intrusion Detection and Response) - In Safeguard و زیرا

Countermeasure از Computer Emergency Response Team (CERT)

و پروتکل برای Procedures

و زیرا

: Countermeasure و زیرا

- { - Possibly avoids waste of resources
- { - Easier to measure success
- Allows threats to occur

← : Countermeasure و زیرا

: b Countermeasure و زیرا Safeguard و زیرا

- Auditing and Intrusion Detection

- Identification and Authentication

- Encryption

= Access Control (e.g. Mandatory, Discretionary - Role-based, ...)
(Authorization)

- Configuration Management

Subject: Ju
Date: 9.7.9.15

- Formal Specification and Verification →
 - Approach
 - Requirements
- Enhanced lifecycle Activities

Jeffrey S. Johnson's paper: Enhanced Lifecycle Activities, Configuration Management

(Jeffrey S. Johnson) Dines Bjørner (correlation)
Dines Bjørner (correlation)
Jeffrey S. Johnson

Lifecycle Enhanced ~~Activity~~ Activities:

- Documentation
- Reviews
- Traceability mappings →
 - Product features
 - Requirements
 - Requirements
- Tool Use
- Testing

Reading Assignment:

? 15 Jan., Vol. 15, 2010 JUC Requirements Engineering as
Special Issue

iu - Guest Editorial: Security Requirements Engineering
Past, Present, and Future

P47-48 - A comparison of security Requirements Engineering Methods.

Subject: Security
Date:

auditing & intrusion detection

→ audit, ^{اودیت}
→ security ^{سکریوٹی} ^{Dos} ^{ڈس}

Auditing and Intrusion Detection:

Audit: ^{اودیت} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل} → log ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل}

log: ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل}

Intrusion Detection vs. Auditing

log ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل} ^{log} ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل}

log: ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل}

log: ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل}

log: ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل}

log: ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل}

log: ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل}

(IDS)

log: ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل}

log: ^{لوج} ^{کام کی رجوع میں ایک مکمل بررسی کرنے کا عمل}

Subject: بی اس ای
Date: ۲۷/۱۰/۲۰

ویر

: فایل ویرجین ۱۳۵۰ - Anderson's Penetration Matrix

- Masquerader →
 - ۱. خود را با شخصیت خوبی می‌پوشاند
 - ۲. از خارج از شبکه می‌باشد
- Misfeasor →
 - ۱. خود را با شخصیت بدی می‌پوشاند
 - ۲. از خارج از شبکه می‌باشد
- Clandestine User
 - ۱. خود را با شخصیت خوبی می‌پوشاند
 - ۲. در شبکه وجود دارد
 - ۳. از خارج از شبکه می‌باشد

Audit collector, Surprise

Outsider - Insider also ← (کارکرد امنیتی، هدف امنیتی)

Masquerader, Misfeasor, Clandestine User, Masquerader

Clandestine User, Misfeasor, Misfeasor

Malicious User (intrusion serious) (bright)

Intrusion (bright)

Root

Remote (کارکرد امنیتی، هدف امنیتی)

Defacing -

(Root Cracker, Exploit Cracker) (کارکرد امنیتی، هدف امنیتی)

PAPCO

(کارکرد امنیتی، هدف امنیتی)

۱۸۰

Subject: _____
Date: _____

مسح على الملفات وتحذيف الملفات

١٢) صيغة إدخال كلمات مرور \rightarrow Password Format

١٣) Detection (察覺) \rightarrow Prevention (預防) \rightarrow انتشار براسخ

١٤) Polymorphic virus

١٥) خاصية الرؤى (Behavior) \rightarrow IDS (Intrusion Detection System)

١٦) نظر إلى البروتوكول (Protocol) حسب الرؤى (Behavior)

١٧) Intra-intrusion detection

١٨) Malicious pattern \rightarrow pattern of intruder

١٩) Nslookup (نـسـلـكـوـپ) \rightarrow IP lookup (نـسـلـكـوـپ) : انتقام من المهاجم (Hacker)

٢٠) nmap (نـمـاـپ) \rightarrow Port scanner (نـمـاـپ) \rightarrow NMAP (نـمـاـپ) \rightarrow اكتشاف الارتباط (Port Scan)

٢١) PC Anywhere (نـسـلـكـوـپ) \rightarrow انتقام من المهاجم (Hacker)

٢٢) NetworkMiner (نـسـلـكـوـپ) \rightarrow PC Anywhere (نـسـلـكـوـپ) \rightarrow BackTrack (نـسـلـكـوـپ)

٢٣) Wireshark (نـسـلـكـوـپ) \rightarrow انتقام من المهاجم (Hacker)

٢٤) Enigma (نـسـلـكـوـپ) \rightarrow انتقام من المهاجم (Hacker)

٢٥) Kali Linux (نـسـلـكـوـپ) \rightarrow انتقام من المهاجم (Hacker)

٢٦) Instant Messenger (نـسـلـكـوـپ) \rightarrow انتقام من المهاجم (Hacker)

٢٧) Spyware (نـسـلـكـوـپ) \rightarrow انتقام من المهاجم (Hacker)

Subject: ب
Date: ٢٠١٥/٦/٥

الشكل ٣: النمط المترافق مع التهديد

: Intrinsic-Detection نظام اكتشاف الداخلي

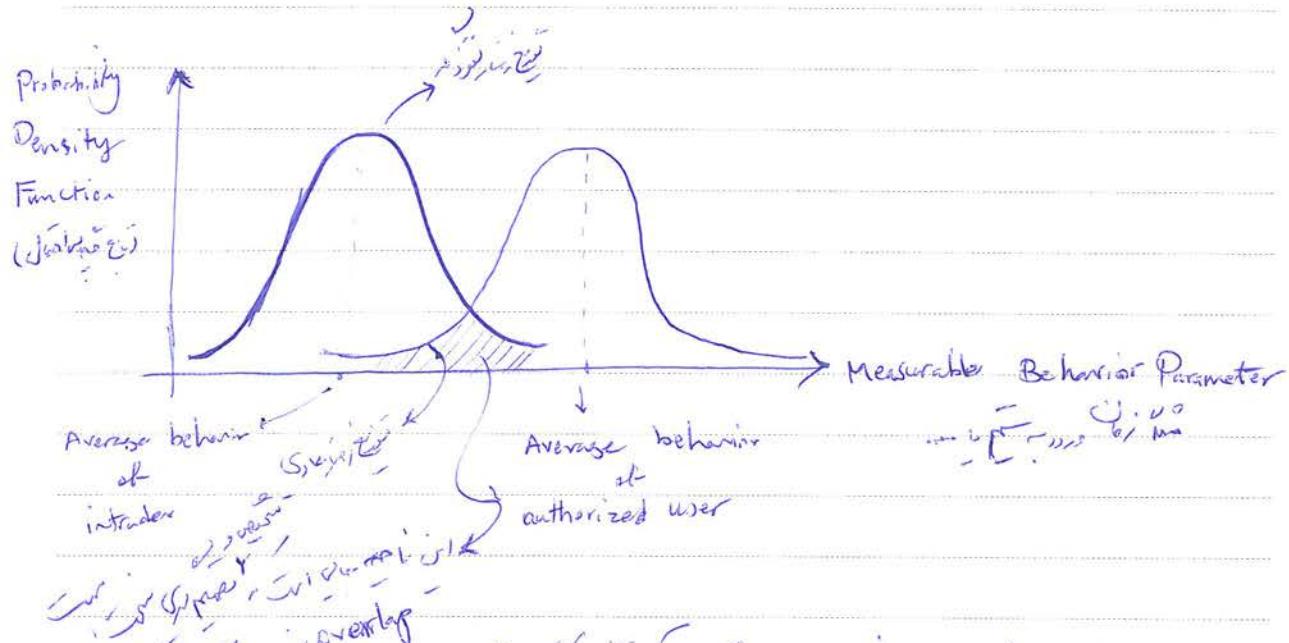
١- انتهاك خاص بـ نوع المخترق (أو نوع المخدر) أو نوع المحتوى.

يُعرف على هذا كـ معلم خاص.

٢- خروج IDS من المقدار المعتاد.

٣- التحقق (أو التحقق) أو التحقق من المخترق.

٤- القياس (quantify) أو القياس لـ نوع المخترق وـ نوع المخدر، أو نوع المحتوى).



PAPCO (False Positive) - الإيجابي الخطأ (أو الإيجابي الخطأ، الإيجابي الخطأ)
False Negative - السلبي الخطأ

Subject: IT

Date: ٢٠/١٠/٨

فیلترینگ اسپری میراست

لایت ٹائپ فائلر Legitimate Use, Masquerader الیکٹریکی

میکسیبل فائلر دار

امنیتی احمد بھری کے

Anderson ڈسکریپشن میکسیبل فائلر اسٹ

کوئی کوئی بیرونی طریقے سے

نہیں کر سکتے اور Clandestine

Approaches to Intrusion Detection:

1) Statistical Anomaly Detection

Statistical

Statistical

a. Threshold Detection

خط انتقالی

b. Profile-based Detection

خط انتقالی

2) Rule-based Detection

rules based

پہلے فایل کا نمونہ کر کر اس کا میکسیبل فایل رکھ دیا جائے اس کا تعلق نہیں (1-a)

آخر فایل کا نمونہ کر کر اس کا میکسیبل فایل رکھ دیا جائے اس کا تعلق نہیں (1-b)

PAPCO کے

اسے masquerader عیسیٰ کہا جاتا ہے (L-U) لایت ٹائپ فائلر

امنیتی اسپری

2) Rule-based Detection:

Involves an attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder.

- a. Anomaly Detection → ~~new, no regular rule~~

عمرانیں، احمدیات، نصریہ، قوام (match نسور) (جمعیتیہ ریاستہ بھر)

- ## b. Penetration Identification

نحوه (نحوه) می باشد که در آن می خواهیم بگفت که این نسبت را کجا می توانیم در میان دو عبارت مورد بررسی قرار داد.

(no abnormality)

(misuse detection) (Signature-based)

Specification-based misuse , Anomaly : patterns of

لے (ریڈر) چینہ اٹھو 2.a

$2 \cdot b$ $l-a, l-b, 2 \cdot a$

↓
1-a, 1.b, 2-a

مکرور سیکل ۴ موتور اکسیژن

Specification and history 11/2

• Rule-based AI (with stateless logic) in Pearson AI *

Subject: _____
Date: _____

Audit Records:

دокументات مراجعة

- Native audit records

جداول اداري سكريبت، نسخه وتحفظ، وسجلات

خن: شرکت اینترنت بسته خدمات

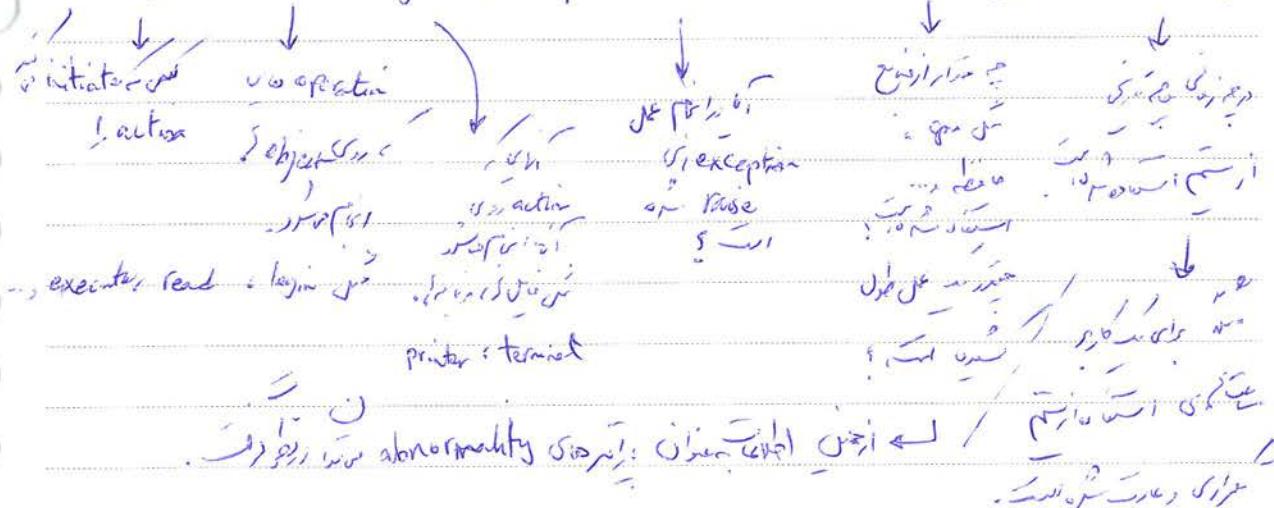
مس: شرکت اینترنت بسته خدمات

- Detection-specific audit ~~records~~ records

رسائل تحذيرية جرائم امن، تأمين، دعم كليات، معلومات امن، وسجلات

audit record من-denning

subject, action, object, exception-condition, resource usage, time-stamps



Subject:

Date

4/1/14

• It's atomic in its action. (x)

• Now, if you consider it, it will never fail.

Copy GAME.EXE To <Library> GAME.EXE (J)

→ It's an audit record for command

Smith	execute	<Library> Copy.EXE	0	CPO=00002	1105872678
↓ exception Occurred					

Smith	read	<smith> GAME.EXE	0	RECORDS=0	1105872679
-------	------	------------------	---	-----------	------------

Smith	write	execute	<Library> Copy.EXE	write-viol	RECORDS=0	1105872680
-------	-------	---------	--------------------	------------	-----------	------------

? → alert will occur if it is statistical Anomaly Detection.

: wednesday is given

Metric (for profile-based detection):

• Counter → number of logins per user

→ number of logins per session

— number of logins by a single user during an hour.

— number of times a given command is executed during a single user session.

Subject: _____
Date: _____

• Gang → *نوعی وسیلیں
entity = چیزیں
user application*

- The number of logical connections assigned to a user application.

- The number of outgoing messages queued for a user process.

• Interval Timer → *کمینسیوں کا ایجاد*

- The length of time between successive logins to an account.

• Resource Utilization → *ressources کا استفادہ*

- *کارڈ سے کارڈ کے بینے کا استفادہ*

- *کارڈ کے بینے کا استفادہ*

- *کارڈ کے بینے کا استفادہ*

- *کارڈ کے بینے کا استفادہ*

Tests:

- Mean and Standard Deviation *میانہ اور انحراف میانہ*

- *legitimate, یعنی قانونی*

Subject: ↓
Date:

9/10/14

o alert, تذكرة انتها واردة الى المراقب

- Multivariate → (correlation مترافق)

input: resource usage, process time

- Markov Process → (التحول بين الحالة)

(State Transition)

o Command to state

- Time Series → history, last n, previous step, etc.

:

o Penetration Identification, چهار نوع، Rule-based

درباره اینها

o in personal directory, ساخته شده

ویرایش شده

o with device, low-level, وب

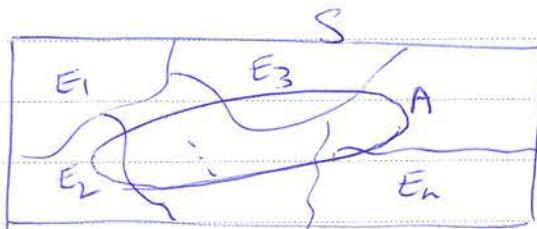
P4PCO

144

Subject: _____
Date: _____

Base-rate fallacy:

$$P(E|F) = \frac{P(E \cap F)}{P(F)}$$



$(E_1 \cup E_2 \cup \dots \cup E_n)$ is a partition of event A.

Thus, P(A) is the probability of event A.

$$A = (A \cap E_1) \cup (A \cap E_2) \cup \dots \cup (A \cap E_n)$$

$$\Rightarrow P(A) = P(A \cap E_1) + P(A \cap E_2) + \dots + P(A \cap E_n)$$

$$= P(E_1) \cdot P(A|E_1) + P(E_2) \cdot P(A|E_2) + \dots + P(E_n) \cdot P(A|E_n)$$

$$= \sum_{i=1}^n P(E_i) \cdot P(A|E_i)$$

Bayes' Theorem -

$$P(E_i|A) = \frac{P(E_i) \cdot P(A|E_i)}{\sum_{j=1}^n P(E_j) \cdot P(A|E_j)}$$

Subject: in
Date: 25/1/19

اگر ایک ایجاد کننے والے انسان میں سے ایک ایسا بھروسہ انسان ہے جو اپنے بیماری کا (جسے (Positive)۔

اے Test Accuracy = 87%۔

The incidence of the disease in the population is 1%. \rightarrow Base-rate

$$P(\text{well} \mid \text{Positive}) = \frac{p(\text{positive} \mid \text{well}) \cdot p(\text{well})}{p(\text{positive} \mid \text{well}) \cdot p(\text{well}) + p(\text{negative} \mid \text{disease}) \cdot p(\text{disease})}$$
$$= \frac{(0.13)(0.99)}{(0.13)(0.99) + (0.87)(0.01)} = 0.937$$

اے ایک ایجاد کننے والے انسان میں سے ایسا بھروسہ انسان ہے جو اپنے بیماری کا (جسے (Positive)۔

اے $p(\text{well})$ کا فارمیسیس پریمیس $p(\text{positive} \mid \text{well}) = p(\text{well})$ ۔

اے $p(\text{well} \mid \text{positive})$ کا فارمیسیس پریمیس $p(\text{positive} \mid \text{well})$ ۔

$$\therefore p(\text{well} \mid \text{positive}) = 0.09 \rightarrow \text{Test Accuracy} = 99.9\%$$

Base-rate Fallacy \leftarrow ایک ایجاد کننے والے انسان میں سے ایسا بھروسہ انسان ہے جو اپنے بیماری کا (جسے (Positive)۔

Subject: _____
Date: _____