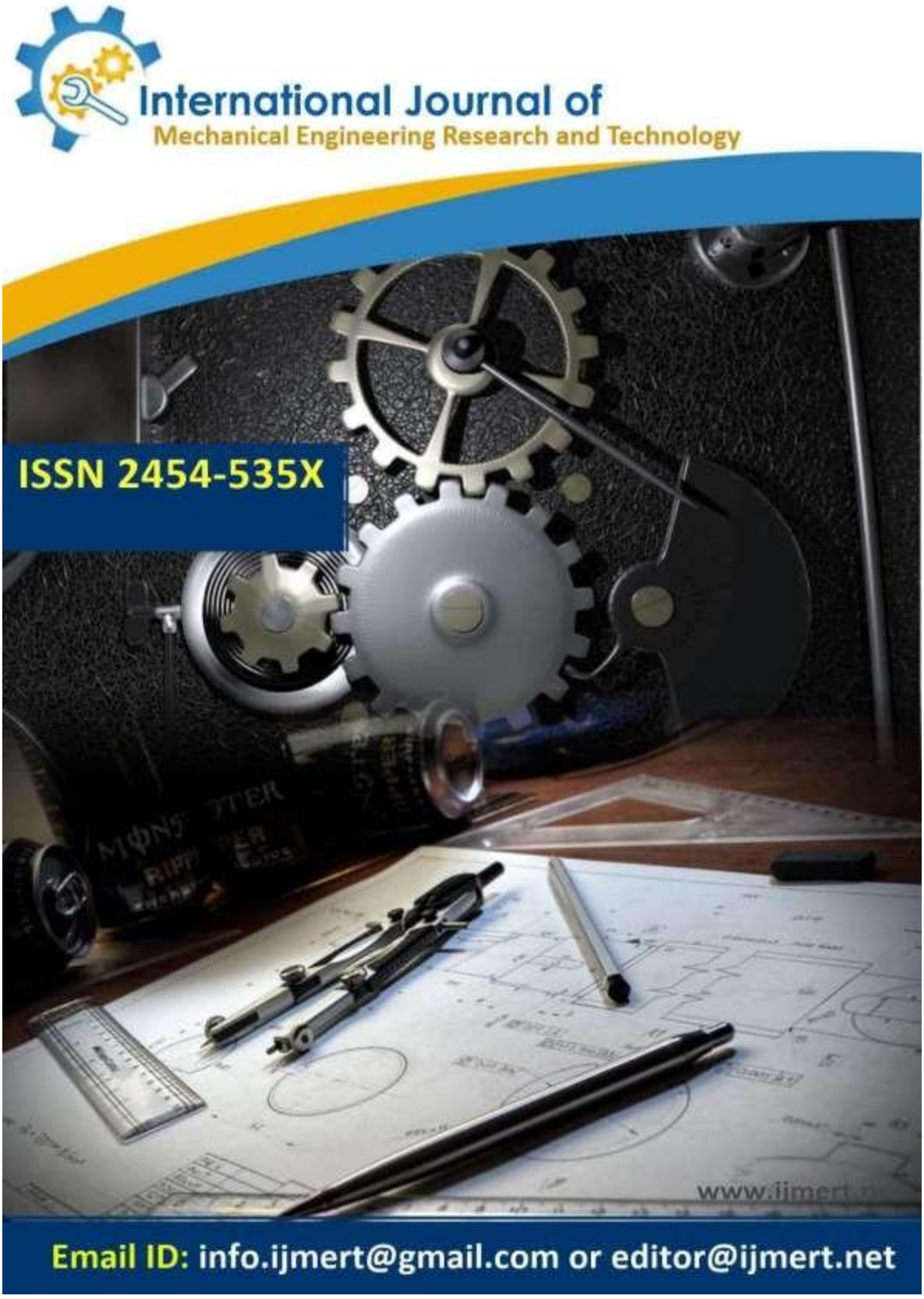

International Journal of
Mechanical Engineering Research and Technology
ISSN 2454-535X
www.ijmert
Email ID: info.ijmert@gmail.com or editor@ijmert.net

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024

DUAL SECURITY FOR SMART CARD

Project Guide
Mr.M.Lakshminarayana
Associate.Professor

GULLA DHANUSH KUMAR

SHAIK MULLA IRSHAD HUSSAIN

YERUVA ADIVI VENKAT REDDY

KELASORU MANGALI PRAVEEN

Abstract **-** In this work, we provide a Secure System development Life Cycle Approach to address software security concerns throughout the early phases of system development. Here, we examine the need for security by comparing it to the needs for functionality.Use use case, attack tree, threat modeling, and risk assessment to design a secure smart card system and architecture. Examining the smart card microcontroller via static and dynamic analysis, and then putting the different security testing methods to use. This work uses the Semi-Marchov Chain and the Steady state matrix to assess the security improvement of a smart card's SDLC for various attack levels. The Security State Diagram is a useful tool for evaluating the safety of any smart card driver. Because of the disparity in security levels between the integrated and series systems, an improvement in security may be calculated.

Keywords: Various security diagrams, threat modeling, attack trees, vulnerabilities, semi-Markov chains, generic transition matrices, and steady-state security are used.

INTRODUCTION

Smart cards include an integrated circuit, which may be a memory chip alone, a secure microcontroller, or an analogous intelligent device with internal memory. The card may be inserted into a reader by touching it directly or by using a distant contactless radio frequency interface. Smart cards can store a lot of data, perform on-card activities like encryption and mutual authentication, and communicate intelligently with a smart card reader since they feature an integrated microprocessor. As an example, contactless cards, microprocessor cards, and memory cards are all forms of smart cards.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

Guntur Engineering College

Jawaharlal Nehru Technological University, Kakinada.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024

II. Eliciting Requirements Section A:
Servers, RAM, communication lines and channels, and hardware tokens are all bits of hardware.
Operating systems, database management systems, communication and security application programs—these are the software components that make up the system. Data, especially databases housing information pertaining to customers, is the third category.
4. Staff members: include administrative, computer, clerical, and professional staff. Section B: Functional Needs for Security

Detailed functional requirements document how the system is supposed to operate. The system is expected to carry out certain services, processes, or functions in order to demonstrate its behavior. First, there is security testing, which includes things like user identification and verification before any activity is taken, the definition of user attributes, and the monitoring of stored data integrity.
2. Security Management: Managing the behavior of security functions, roles within security, static attribute initialization, complete access control, security attribute based access control, subset information flow control, simple security attributes, potential violation analysis, unobservability, notification of physical attack, resistance to physical attack, and so on.

I. SECURE DESIGN

Secure design of smart card contains following properties-

A. *Use Case Diagram*

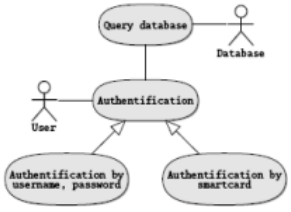


Fig.1 Use Case Diagram of Smart Card

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024

B. *Attack Tree*

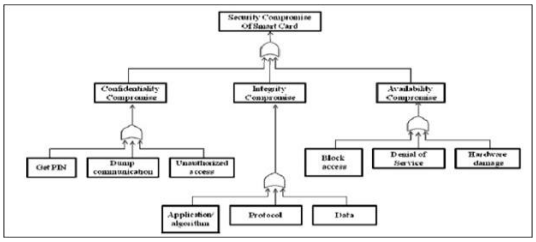


Fig.2 Attack Tree of Smart Card

As shown in the figure 3, confidentiality of the smart card is compromised by stealing its PIN, sniffing and unauthorized access. Integrity is generally violated when the attacker can exploit a badly written protocol or an unsecure application or use of inefficient cryptographic technique on the data. Similarly availability is compromised by blocking PIN access, denial of service and hardware damage.

Section C.: Risk Analysis

A security policy may be compromised in a number of ways; one of these ways is via the practice of vulnerability, which is what we mean when we talk about threats. Any entity that might compromise the security, authenticity, accessibility, or lawful usage of a system asset is considered a threat source. Unauthorized access, hacking, infiltration, theft, violation of integrity, violation of availability (such as Distributed Denial of Service), illegitimate usage, system penetration, and tampering are all potential dangers to the smart card system.

D. Smart Card Attacks

The table shows every possible attack on a smart card.

E. Finding Security Flaws

First, there are technical issues. The organization's server has guest ID enabled, the TCP/IP protocol stack is vulnerable, there is no database backup, the authentication and authorization mechanisms for users are weak, the encryption techniques are old, the firewall enables incoming telnet, and so on.
2. Non-technical Vulnerabilities: Carelessness in monitoring workers' conduct, negligence in erasing the system IDs of dismissed personnel.

F. Assessing Potential Dangers

When considering the likelihood of an attack succeeding, the cost of vulnerability is measured as risk. Assessing risks, creating a risk matrix, and implementing mitigation strategies are the three pillars of a comprehensive risk management program. The first step is to conduct a risk assessment, which includes weighing the potential dangers of each smart card type and establishing an overall risk rating. One way

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024

to indicate the degree of danger is with a risk value, which might be high, medium, or low.
2. Risk Matrix: Creating a risk matrix that displays the tolerable risk based on the attack likelihood and the impact of an attack on each smart card type. It is necessary to think about both the possibility of an attack on the smart card and its potential impact in order to create the risk matrix. It will be possible to attribute assault probabilities (Pa) and consequences (Ca) to different kinds of smart cards. Table

Weights are assigned to the smart card types to determine the risk level. The main purpose of developing the risk matrix is to show the risk tolerability level that each smart card type has.

TABLE 2 Risk Matrix

Consequences Probability	Negligible (0≤Ca≤.2)	Marginal (.3≤Ca≤.5)	Critical (.6≤Ca≤.8)	Catastrophic (.9≤a)
Frequent (.9≤Pa)			Identification Card	
Probable (.6≤Pa≤.8)		Identification Card	Banking Card	
Occasional (.3≤Pa≤.5)		Health Card		
Improbable (0≤Pa≤.2)	Loyalty Card	Prepaid Card		

1). *Risk Mitigation:* It is extremely important to mitigate or even trying to eliminate the risks. The main idea behind this part of the process is to come up with controls to eliminate the risk or reduce the level of risk to an acceptable level.

TABLE 3 Security Methods for each type of Smart Card

Banking Card	Identification Card	Health Card	Loyalty Card	Prepaid Card
PIN and Biometrics (Fingerprint or Signature)	PIN and Biometrics (Fingerprint or Signature)	PIN and Biometrics (Fingerprint or Signature)	PIN	PIN
Cryptographic Key Management (PKI)	Cryptographic Key Management (PKI)	Cryptographic Key Management (PKI)	Symmetric or Asymmetric Encryption And Digital Signature	Asymmetric Encryption And Digital Signature

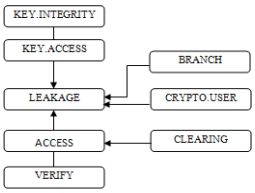
C. *Secure Design Pattern*

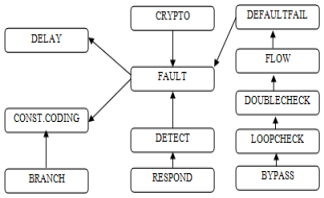
1). Patterns to defend against data leakage

The secure design patterns are used to prevent application program code from leaking sensitive information when this information is processed. Application developers can use these patterns to protect confidential data like keys and passwords.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024





(1)
(2) shows the weights and their descriptions.

TABLE 1 Probability of attack and Consequence of attack

Weights	Probability of Attack (Pa)	Consequences of Attack(Ca)
0 to .2	Improbable	Negligible
.3 to .5	Occasional	Marginal
.6 to .8	Probable	Critical
.9 and above	Frequent	Catastrophic

Fig.3 Secure Design Pattern for Smart Card

Patterns to defend against fault injection

The usage of data and code is constrained by strong typing in programming languages. For example, one cannot create a reference by casting an integer, and one cannot skip over part of a function's code. Program dependability is often improved by this discipline. Also, it's possible to use it to make a software isolation layer impenetrable. There are a plethora of other ways in which type-unsafe code might disrupt isolation and cause the virtual machine to malfunction: Stack smashing, Out-of-bounds access, pointer forgery, and illegal casting Explicit deallocation, prevention of context switches

B. Analysis without data

Ensure that all variables are assigned information levels to avoid any potential disclosure of sensitive information. Using a method call graph to abstract the control flow, Use temporal logic to express control qualities, and then use model checking to verify these properties on the abstraction.

Ch. Analyses in motion

A. Patterns to defend against fault injection

The patterns in this section assist in preventing fault injection in application

Security measures include keeping an eye on the passivation layer, voltage, frequency, bus scrambling, and the ability to permanently switch between test and user modes.

Section V: Safe Testing

One of the biggest security issues confronting the smartcard business is preventing unauthorized access to smartcard chips and other embedded microchips. In order to achieve the desired level of precision when repositioning a secure microcontroller, the development team set out to build a video-based, high-power microscope device that could deliver and image a very small, highly focused area of two wavelengths of laser energy.

Section I: Security Assessment

An attacker's actions could be completely random, unexpected, and multi-faceted. An acceptable modeling approach for illustrating attacker behavior is the semi-Markov chain process. One unique feature of semi-Markov chains is that the current state is the lone

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024

determinant of the likelihood of any event transitioning to a future state. For example, if Xt = i represents the current state, then Xt+1 = i + 1 represents the future state, and Xt-1 = i - 1 represents the previous state. If the system begins in state i at any point in time, the n-step transition probabilities pij(n) are the conditional probabilities that, after precisely n steps, it will be in state j = i + 1, the future state.

are conditional probabilities, they must be positive, and therefore must make a transition into some state where the conditions of pij(n) ≥ 0 satisfy all the values for i an

d j; and

$$\sum_{j=0}^{N} p_{ij}^{(n)} = 1,$$

Where n = 0, 1, 2 …, N.

A. *States*

0: Normal	5: Availability attacked
1: Vulnerable	6: Authentication attacked
2: Attacked	7: Non-Repudiation
3: Confidentiality attacked	8: Failure
4: Integrity attacked	

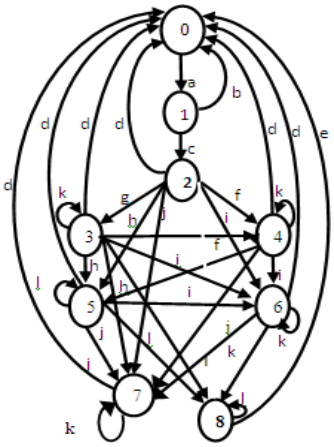


Fig.4 Security State Diagram of a driver under attack

B. *Transitions*

a: Vulnerability found	g: Attack on confidentiality
b: Vulnerability eliminated	h: Attack on availability
c: Vulnerability	i: Attack on

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024

exploited	authentication
d: Attack & recovery initiated	j:Attack on Non-Repudiation
e: System restarted	k: Attack & recovery failed
f: Attack on integrity	l: System failed

From all states, the system can return back to state (0), the normal state, with different levels of probability and degrees of loss. P in the above is a matrix formulation of the relationship between the states and their probability.

$$P = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \end{array} \begin{array}{c} \begin{array}{ccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \overline{p_1} & 0 & p_{12} & 0 & 0 & 0 & 0 & 0 & 0 \\ \overline{p_2} & 0 & 0 & p_{23} & p_{24} & p_{25} & p_{26} & p_{27} & 0 \\ \overline{p_3} & 0 & 0 & p_{33} & p_{34} & p_{35} & p_{36} & p_{37} & p_{38} \\ \overline{p_4} & 0 & 0 & 0 & p_{44} & p_{45} & p_{46} & p_{47} & p_{48} \\ \overline{p_5} & 0 & 0 & 0 & 0 & 0 & 0 & p_{57} & p_{58} \\ \overline{p_6} & 0 & 0 & 0 & 0 & 0 & p_{66} & p_{67} & p_{68} \\ \overline{p_7} & 0 & 0 & 0 & 0 & 0 & 0 & p_{77} & p_{78} \\ \overline{1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

Where

$$\overline{p_1} + p_{12} = 1$$
$$\overline{p_2} + p_{23} + p_{24} + p_{25} + p_{26} + p_{27} = 1$$
$$\overline{p_3} + p_{33} + p_{34} + p_{35} + p_{36} + p_{37} + p_{38} = 1$$
$$\overline{p_4} + p_{44} + p_{45} + p_{46} + p_{47} + p_{48} = 1$$
$$\overline{p_5} + p_{57} + p_{58} = 1$$
$$\overline{p_6} + p_{66} + p_{67} + p_{68} = 1$$
$$\overline{p_7} + p_{77} + p_{78} = 1$$

Integrity and Authentication therefore a high value of (pc = pI = pAut = 0.20) is assigned. Finally, driver 4, the people has a high confidentiality and Integrity, Availability and Authentication therefore high values (pc = pI = pA = pAut = 0.15) are assigned.

TABLE 5 CIAAN probabilities for Smart Card Drivers

Smart Card Driver	p_v	p_c	p_I	p_A	p_{Aut}	p_{Nrp}	$\overline{p_{CIAAN}}$
Hardware	.10	.25	.25	.10	.10	.05	.15
Software	.15	.20	.10	.10	.20	.05	.20
Data Transmission	.10	.20	.20	.10	.20	.10	.10
People	.15	.15	.15	.15	.15	.10	.15

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024

TABLE 4 State Transitions	
0 [a] 1	Moves to vulnerable state.
From State 1 (Vulnerable)	
1 [b] 0	Vulnerability eliminated
1 [c] 2	Vulnerability exploited
From State 2 (Attacked)	
2 [d] 0	Attack detected & recovery initiated
2 [g] 3	attack on confidentiality
2 [f] 4	attack on integrity
2 [h] 5	attack on availability
2 [i] 6	attack on authentication
2 [j] 7	attack on Non-Repudiation
From State 3 (Confidentiality attacked)	
3 d 0	Attack detected & recovery initiated
3 [k] 3	Attack detected and recovery failed
3 [f] 4	attack on integrity
3 [h] 5	attack on availability
3 [i] 6	attack on authentication
3 [j] 7	Attack on Non-Repudiation
3 [l] 8	System failed
From State 4 (Integrity attacked)	
4 [d] 0	Attack detected & recovery initiated
4 [k] 4	Attack detected and recovery failed
4 [h] 5	Attack on availability
4 [i] 6	attack on authentication
4 [j] 7	attack on Non-Repudiation
4 [l] 8	System failed
From State 5 (Availability attacked)	
5 [d] 0	Attack detected & recovery initiated
5 [i] 6	attack on authentication
5 [j] 7	attack on Non-Repudiation
5 [l] 8	System failed
From State 6 (Authentication attacked)	
6 [d] 0	Attack detected & recovery initiated
6 [k] 6	Attack detected and recovery failed
6 [j] 7	attack on Non-Repudiation
From State 7 (Non-Repudiation)	
7 [d] 0	Attack detected & recovery initiated
7 [k] 7	Attack detected and recovery failed
8 [e] 0	System restarted

C. *Security Analysis of Smart Card*

A smart card consists of four drivers as Hardware, Software, Data Transmission and people.

1) *CIAAN probabilities for Smart Card Drivers*: Drivers contains following values for Confidentiality, Integrity, Availability and Accountability. Driver 1, the Hardware, is concerned more with confidentiality and integrity, so high weights are given to both (pc = pI= 0.25). Driver 2, the software, is also concerned more with confidentiality and authentication, therefore a very high value is assigned for (pc = pAut = 0.20). Driver 3, the Data Transmission, is concerned

2) Generic transition matrix (GTM)

The generic transition matrix GTM for each driver (*i*) created
from Table 3. Table 4 presents a generic transition matrix (GTM) for a driver *i* created by substituting the parameters. (GTM) for a driver i created by substituting the parameters.

TABLE 6 Generic Transition Matrix for driver i

From To	N (0)	V (1)	Att (2)	C (3)	I (4)	A (5)	Aut (6)	Nrp (7)	F (8)
(0)	0	1	0	0	0	0	0	0	0
(1)	$\overline{p_1}$	0	p_{12}	0	0	0	0	0	0
(2)	$\overline{p_2}$	0	0	p_{23}	p_{24}	p_{25}	p_{26}	p_{27}	0
(3)	$\overline{p_3}$	0	0	p_{33}	p_{34}	p_{35}	p_{36}	p_{37}	p_{38}
(4)	$\overline{p_4}$	0	0	0	p_{44}	p_{45}	p_{46}	p_{47}	p_{48}
(5)	$\overline{p_5}$	0	0	0	0	0	0	p_{57}	p_{58}
(6)	$\overline{p_6}$	0	0	0	0	0	p_{66}	p_{67}	p_{68}
(7)	$\overline{p_7}$	0	0	0	0	0	0	p_{77}	p_{78}
(8)	1	0	0	0	0	0	0	0	0

Table 7 presents an initial transition matrix for driver 1 (P1).it is generated by substituting the values of pv,pc,pI,pA,pAut,PNrp .

TABLE 7 GTM for driver 1 Pa1 at

From \To	N (0)	V (1)	Att (2)	C (3)	I (4)	A (5)	Aut (6)	Nrp (7)	F (8)
(0)	.90	.10	0	0	0	0	0	0	0
(1)	.90	0	.10	0	0	0	0	0	0
(2)	.25	0	0	.25	.25	.10	.10	.05	0
(3)	.15	0	0	.25	.25	.10	.10	.05	.10
(4)	.40	0	0	0	.25	.10	.10	.05	.10
(5)	.85	0	0	0	0	0	0	.05	.10
(6)	.75	0	0	0	0	0	.10	.05	.10
(7)	.85	0	0	0	0	0	0	.05	.10
(8)	1	0	0	0	0	0	0	0	0

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024

more with Confidentiality,

eight attack levels, is summarized in Table 6. Hence, each row in this table represents a steady-state for corresponding attack level. Where pS = p0 + p1. Similarly steady-state security for driver 2, 3 and 4 are developed.

TABLE 8 Steady State Security for Driver 1

Attacker Level	Normal Π_0	V Π_1	Att Π_2	C Π_3	I Π_4	A Π_5	Aut Π_6	Nrp Π_7	F Π_8	Security Π_s
0.10	.8600	.0860	.0086	.0028	.0038	.0015	.0017	.0009	.0010	.9460
0.30	.8580	.0858	.0257	.0085	.0114	.0045	.0050	.0032	.0035	.9438
0.50	.8200	.0820	.0410	.0136	.0182	.0072	.0081	.0046	.0051	.9020
0.70	.7950	.0795	.0556	.0185	.0247	.0099	.0110	.0063	.0070	.8745
0.90	.7700	.0770	.0693	.0231	.0308	.0123	.0137	.0078	.0087	.8470

3) *Integrated Steady-state Security*

Table 9 represents system security when all drivers are sharing both the functional and the security information as an integrated security system.

TABLE 9 Integrated Steady-state Security for Smart Card

Attacker Level	Normal Π_0	V Π_1	Att Π_2	C Π_3	I Π_4	A Π_5	Aut Π_6	Nrp Π_7	F Π_8	Security Π_s
0.10	0.8800	0.0880	0.0044	0.0019	0.0016	0.0008	0.0008	.0025	0.0004	0.9621
0.30	0.8732	0.0873	0.0174	0.0074	0.0062	0.0031	0.0034	.0073	0.0016	0.9269
0.50	0.8481	0.0848	0.0296	0.0127	0.0106	0.0053	0.0058	.0116	0.0028	0.8887
0.70	0.8240	0.0824	0.0412	0.0176	0.0147	0.0073	0.0081	.0156	0.0039	0.8587
0.90	0.8012	0.0801	0.0520	0.0223	0.0186	0.0093	0.0103	.0190	0.0050	0.8249

D. *Discussion of Results*

To analyze the relationship between the four drivers of the Smart Card with system wide security there are two cases: CASE 1: Drivers share information without sharing security and vulnerability information. In this case, system-wide security will be very low. The total security is a multiplication of all individual driver security values; Ps(sys) = pS1 pS2 pS3 pS4 (1).

CASE 2: Drivers share functional information as well as security information. In this case, the level of vulnerability will be reduced, hence increasing the security level. The integrated system is obtained mathematically by multiplying each master transition matrix for all drivers to obtain the transition matrix for the system, Psw as Psw = Pa1. Pa2. Pa3.

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024

Pa4.

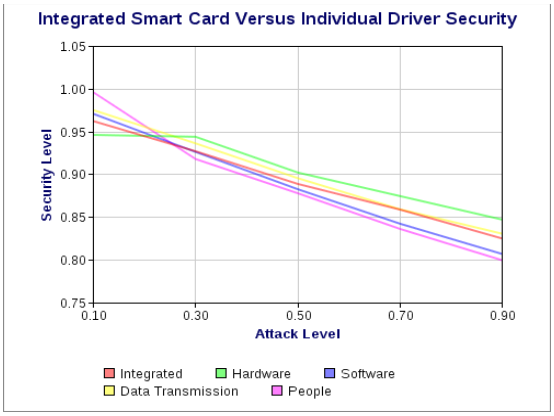


Fig.5 Integrated Smart Card versus Individual Driver

2) Comparison of System Security

Table 8 summarizes the results obtained from integrated and series system security of a Smart Card. We can clearly observe that security has improved by 37% (from 0.4537 to 0.8249 at the high attack level 90%).

Attacker Level	Type of System Security	
	Integrated	Series
0.10	0.9621	0.8914
0.30	0.9269	0.7509
0.50	0.8887	0.6256
0.70	0.8587	0.5290
0.90	0.8249	0.4537

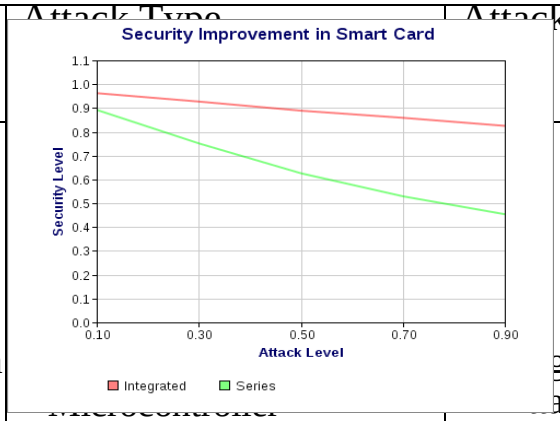
TABLE 10 Comparison of System Security

State-wide system security for Smart Card has less vulnerability, which leads to better security due to the sharing of information about attackers. An individual driver is more vulnerable than the integrated system in a Smart Card. Figure 5 compares two curves; one represents integrated security for a Smart Card, and the other represents Smart Card drivers working together but without sharing security information are much more vulnerable.

*1*Comparing Individual Driver Smart Cards with Integrated Smart Cards System wide (SW) security, as seen in Figure 4, improves performance across the board from 10% to 90% attack levels.With the exception of Hardware, these curves reveal significantly reduced security for all drivers. However, when security information is not

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024



Attack Class	Attack Type	Attack	Attack Type
Physical Attacks		gical acks	1. Hidden Commands
			2. Buffer Overflow
			3. File Access
	4. Probe Stations		4. Malicious Applets
	5. Focused Ion beam (FIB)		5. Communication Protocol
			6. Crypto-Protocol, Design ,Implementation
Side Channel Attacks	1. Timing Attack	Development	1. Development of the Smart Card Microcontroller
	2. Fault Attack		2. Development of Smart Card Operating System
	3. Power Analysis Attack	Manufacturing Process	1. Authentication in the Manufacturing Steps
	4. EM Attack	Other Attacks	1. Eavesdropping
	5. Acoustic Attack		2. Interruption of operations
	6. Visible Light Attack		3. Denial of service
	7. Error Message Attack		4. Covert transactions
	8. Cache-based Attack		5. Communication links and dual modes
	9. Frequency-based Attack		6. Data Remanence
	10. Scan-based Attack		7. Pin guessing
	11. Combination of Side Channel Attacks		8. Reverse engineering of the chipset
	12. Combination of SCA and Mathematical Attacks		

International Journal of Mechanical Engineering Research and Technology

ISSN 2454 – 535X www.ijmert.com
Vol. 16 Issue. 1, May 2024

References

[1Version 3.0 of the Security Measurement White Paper, 13.01.2006. Projected by the PSM Safety & Security Task Force Group [2]. https://www.4shared.com/office/.../John_Wiley Smart_Card_.html

[3]. A white paper published by the Smart Card Alliance's Contactless and Mobile Payments Council (CPMC-0802), available at www.smartcardalliance.org. Models for Reliability and Security [4] Joined by Kishor S. Trivedi, Dong Seong Kim, and Arpan Roy. The Duke University School of Electrical and Computer Engineering is located in Durham, North Carolina, USA.paper6.pdf can be found at www.sis.pitt.edu/~dtipper/3350.

[5]. An Evaluation of Supply Chain Management Systems' Information Security http://www.idea-group.com.

[6]. https://buildsecurityin.us- cert.gov/. Build Security in Home.

[7]. An Examination of Supply Chain Management Systems' Information Security http://www.idea-group.com.

[8]. Secure Platform Profile for Smartcard IC Version 1.0, 2001.source: www.commoncriteriaportal.org/files/ppfiles/ssvgpp 01.pdf.

(ISC)³-Experts in Information Technology Certification and Security site: www.isc2.org/.

[10] OWASP, the Open Web Application Security Project (https://www.owasp.org/), 11th January 2006 Security Measurement White Paper V3.0 Projected by the PSM Safety & Security Task Force Group [12]. This is the URL for the file: www.4shared.com/office/.../John_Wiley Smart_ca rd_.html.

The Smart Card Alliance's white paper on contactless and mobile payments (CPMC-08002) is available online at www.smartcardalliance.org (reference number: 13).