Quantitative Cyber-Security

Colorado State University
Yashwant K Malaiya

CS559

L25: Project Presentations

CSU Cybersecurity Center
Computer Science Dept

Project Notes

- Each person is required to post at least two questions or comments in Canvas right after the related abstract/slides by Dec 5. The speakers should respond to these by Dec 7.
- A Peer Evaluation of Presentations of all presentations will be required to be submitted by Dec 8.
  - Novelty/Interest, Technical/ Research, Organization/Presentation, Overall
  - Scale: 10 – top 25% 9 – next 25% 8 – next 25% 7 – bottom 25%.
  - You must give 6-8 persons 10 and 6-8 persons 7
- Also note that each person will be assigned two final reports for evaluation, which will be part of Final Part A (30 pts, Dec 7-11). Final Part B (70 pt) will be on Dec 14, Th.

Notes

- CS530 Spring 2024:
  - Sections 001 and 801 will be offered
- CS599 Course Evaluation in Canvas is available
- CS 559 Final
  - Will be here for S 001 and local S 801 students.
- Reflection: What topics should be considered for addition/expansion for future CS559? Send me an email.

Mon Nov 27 Schedule

Presentations will be 11-12 minutes plus 3-4 minutes for discussions. Everyone is required to ask questions here, and on Canvas.

- A Comprehensive Analysis of Cyber Risk Management and Cyber Insurance Strategies, Mahima Chowdary Maddineni, Chaturya Katragadda
- Quantitative measurement of the impact of security breaches, Oluwatosin Falebita, Srivarshini Ksheerasagar, Sarthak Bharadwaj
- An Analysis of Smartphone Vulnerabilities and Security Models, Sushmitha Rasamalla, Jaya Veera Surendra Gupta Kurivella
- Quantitative Risk Assessment of Payment Systems/Credit Card Security, Prathamesh Chougule, Shamitha Gowra

A COMPREHENSIVE ANALYSIS OF CYBER RISK MANAGEMENT AND CYBER INSURANCE

Authors:

Chaturya Katragadda
Mahima Chowdary Maddineni

Course: CS559

Fall 2023

Note: you have max 12 minutes!

ABSTRACT

The study focuses on enhancing cyber resilience by acknowledging the dynamic nature of modern cyber threats. Key elements include an exploration of cyber risk management strategies such as risk assessments, threat intelligence, incident response plans, and staff awareness. Additionally, the paper delves into the evolution of cyber insurance plans, coverage details, and the evolving role of insurers in helping organizations mitigate cyber incidents. Noteworthy considerations like policy prices, terms, and the complexity of circumstances are examined, providing essential insights for informed cyber insurance purchases. In conclusion, the paper serves as a roadmap for organizations seeking to strengthen their defenses, respond effectively to incidents, and navigate the escalating challenges of cyber risks.

- The digital realm is besieged by a relentless surge in cyber threats, ranging from data breaches to sophisticated cyberattacks. Understanding the dynamic nature of these threats is essential for effective defense.
- Our motivation stems from the commitment to enhance the cyber resilience. By providing insights, examples, and strategies, we aim to empower entities to proactively tackle the evolving cyber risk landscape.

INTRODUCTION

- In Today's fast changing digital world, businesses are dealing with more and more security problems.
- Cyber threats are constantly changing, and it's important to understand that it's not just about following rules.
- We also focuses on different ways on how companies handle cyber risks, including risk assessments, threat intelligence, incident response plans, and staff awareness.
- The study also examines cyber insurance, including what it covers, how insurance companies help when there's a problem, and the complexities of insurance policies.

- **Continuous Education and Training**:

Offerings of training and resources to help organizations strengthen their cybersecurity defenses.

- **Customization and Hybrid Policies**:

New hybrid policies that combine cyber insurance with liability or property insurance for holistic risk management.

- **Expanded Coverage for New Threats**:

Inclusion of coverage for emerging cyber threats such as ransomware, social engineering, supply chain vulnerabilities, and regulatory compliance.

- Biswas, Baidyanath, et al. "A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks." *Decision Support Systems* (2023): 114102.
- Woods, Daniel, and Andrew Simpson. "Policy measures and cyber insurance: a framework." *Journal of Cyber Policy* 2.2 (2017): 209-226.

- **Advanced Underwriting Models**:

Development of more sophisticated underwriting models that consider factors like an organization's cybersecurity posture, incident response capabilities, and risk mitigation measures.

- **Data Breach Response Services**:

Enhanced data breach response services, including forensic investigation, legal assistance, and public relations support. Integration of incident response teams to facilitate a swift and effective response to cyber incidents.

- Malhotra, Yogesh. "Advancing cyber risk insurance underwriting model risk management beyond VaR to pre-empt and prevent the forthcoming global cyber insurance crisis." *Available at SSRN 3081492* (2017).
- Naseer, Humza. *A Framework of Dynamic Cybersecurity Incident Response to Improve Incident Response Agility*. Diss. PhD Dissertation (Melbourne: School of Computing and Information System, The University of Melbourne, 2018.

What is Cyber Risk Management?

- Identifying
- Assessing
- Mitigating

Involves: policies, procedures, controls

What is its importance for Organizations?

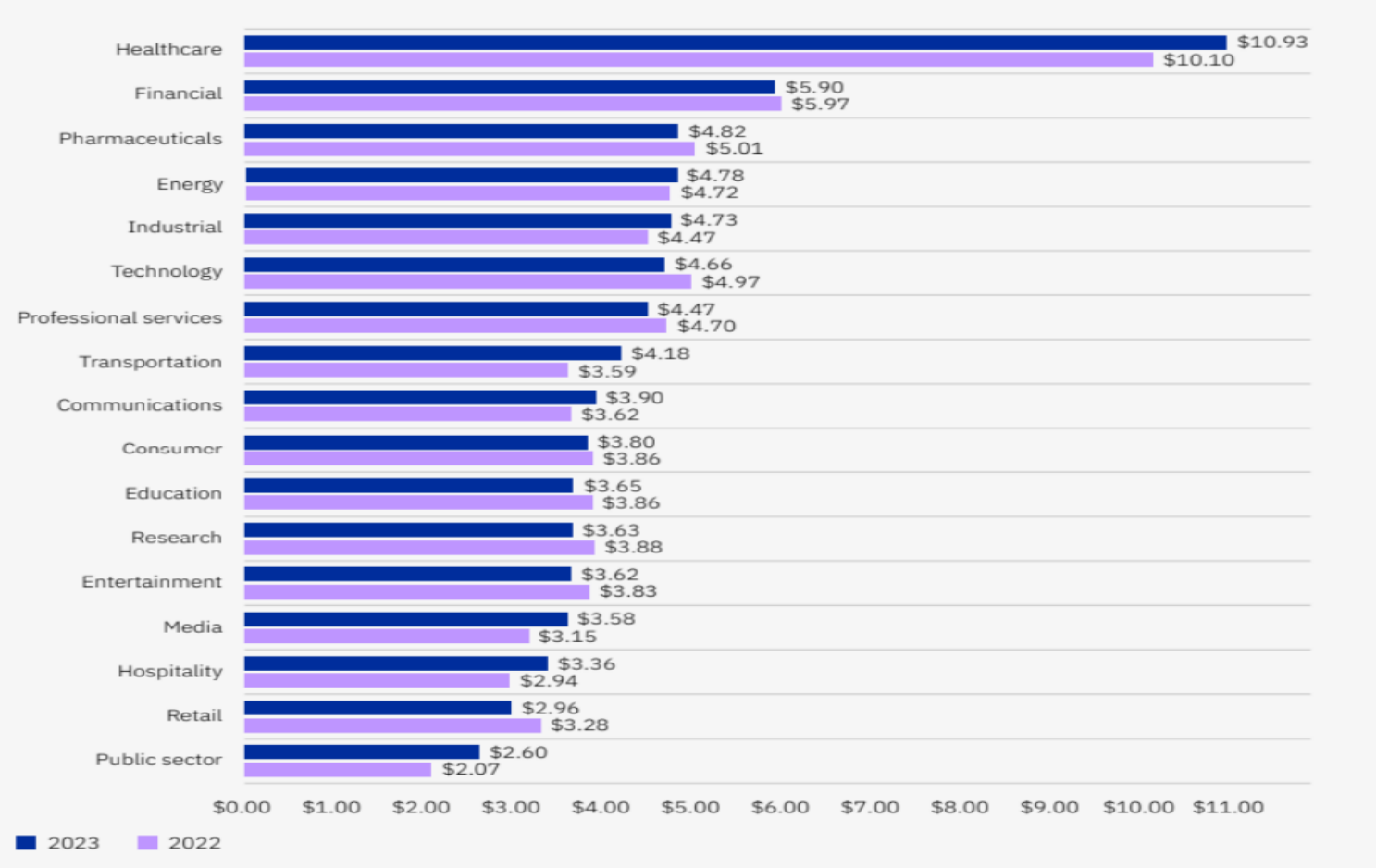
- Handle Sensitive data
- Identify and Prioritize Data.
- Detect and Respond to Cyber Incidents.
- Try to minimize the impact of Incidents that happen.

- Cyber risk is the potential negative consequences of vulnerabilities and hazards in cybersecurity, including data security breaches, malware attacks, and hacking attempts.
- Some of the most common types of cyber threats include:

  Malware

  Ransomware

- Organizations across sectors heavily rely on information technology, and any system breakdown can lead to adverse consequences, impacting an organization's ability to meet objectives.
- The evolving landscape of risk management techniques has led to various perspectives on classifying and understanding different types of cyber risk loss events.
- The Cost of a Data Breach Report 2023 by IBM Security, conducted by the Ponemon Institute, reveals an 8.2% increase in healthcare data breach expenses from 2022 to 2023.
- Over the past three years, the average data breach cost in healthcare has surged by 53.3%, emphasizing the vulnerability of the sector, especially amid the COVID-19 pandemic.



IBM Security, study conducted by Ponemon Institute, "Cost of a Data Breach Report 2023", IBM Corporation, New Orchard Road, Armonk, NY 10504. Accessed: Dec., 5, 2014. [Online]. https://www.ibm.com/downloads/cas/E3G5JMBP

ROLE OF INSURANCE IN MITIGATING CYBER RISK

- Financial Protection
- Risk Transfer
- Rapid Recovery
- Reputation Management
- Flexibility of Policies
- Regulatory Compliance

Evolution of Coverage:

- Historically, insurers have shifted coverage for cyber risks from standard liability and property insurance to specialized cyber insurance policies. Exceptionally, high-value commercial property insurance may offer limited coverage for data breaches.
- Cyber insurance policies are tailored to address specific risks and often come with comparatively lower coverage limits than general property and liability insurance.

- **Focus on Third-Party Risks:**
  - Cyber insurance primarily centers around safeguarding against third-party risks. While providing coverage for first-party concerns, a significant portion addresses expenses related to notifying and serving customers or third parties.
  - Coverage also extends to restoring services to prevent liabilities, especially in the aftermath of network security breaches like ransomware events.
- **Specific Outlined Coverages:**
  - The sale of specifically outlined coverages in cyber insurance helps insurers manage uncertainty. These policies do not cover every possible cyber-related issue but address what is explicitly stated in the contract, up to certain limits for losses.

Global Market Trends:

- The global cyber insurance market is forecasted to reach a gross written premium of $20.6 billion by 2025, indicating a thriving market post the pandemic's impact.
- Despite lower coverage limits and increasing premiums, a consistent and robust year-on-year growth in the cyber insurance market is anticipated up to 2025.

Impact of COVID-19:

- In response to the heightened threat of COVID-19 in 2020, the cyber insurance market experienced significant growth, with a 33.5 percent increase. This growth trend is expected to continue, with a projected growth rate of 27.3 percent in 2021.


Billions
$25
$20
$15
$10
$5
$-
80%
70%
60%
50%
40%
30%
20%
10%
0%
Total
Growth rate
$2.02bn
$3.53bn
$4.75bn
$5.05bn
$5.25bn
$7.01bn
$8.92bn
$11.09bn
$13.73bn
$16.86bn
$20.56bn
74.6%
34.5%
6.3%
3.9%
33.5%
27.3%
24.3%
23.8%
22.8%
22.0%
2015
2016
2017
2018
2019
2020
2021f
2022f
2023f
2024f
2025f

- **Insurability** refers to the extent to which an insurance company is willing to underwrite and offer coverage for a particular type of risk. In the context of cyber risks, several factors influence insurability:

- Data Privacy and Regulatory Complianc
- Risk Assessment
- Rapidly Evolving Threat Landscape
- Risk Aggregation
- Policy Wording and Exclusions
- Ransomware and Extortion
- Cumulative Losse
- Risk Mitigation
- Catastrophe Modeling
- Capacity and Reinsurance

- Cyber insurance originated in the late 1990s and early 2000s during the early days of the internet.
- Initially, coverage was limited to data breaches and network security issues.
- Coverage expanded in the mid-2000s and early 2010s to include business interruption, cyber extortion, and legal liability.
- The mid-2010s marked a turning point with increased demand, prompting customization of policies.
- The late 2010s and early 2020s saw a focus on customized industrial risk policies and a holistic approach to risk management.

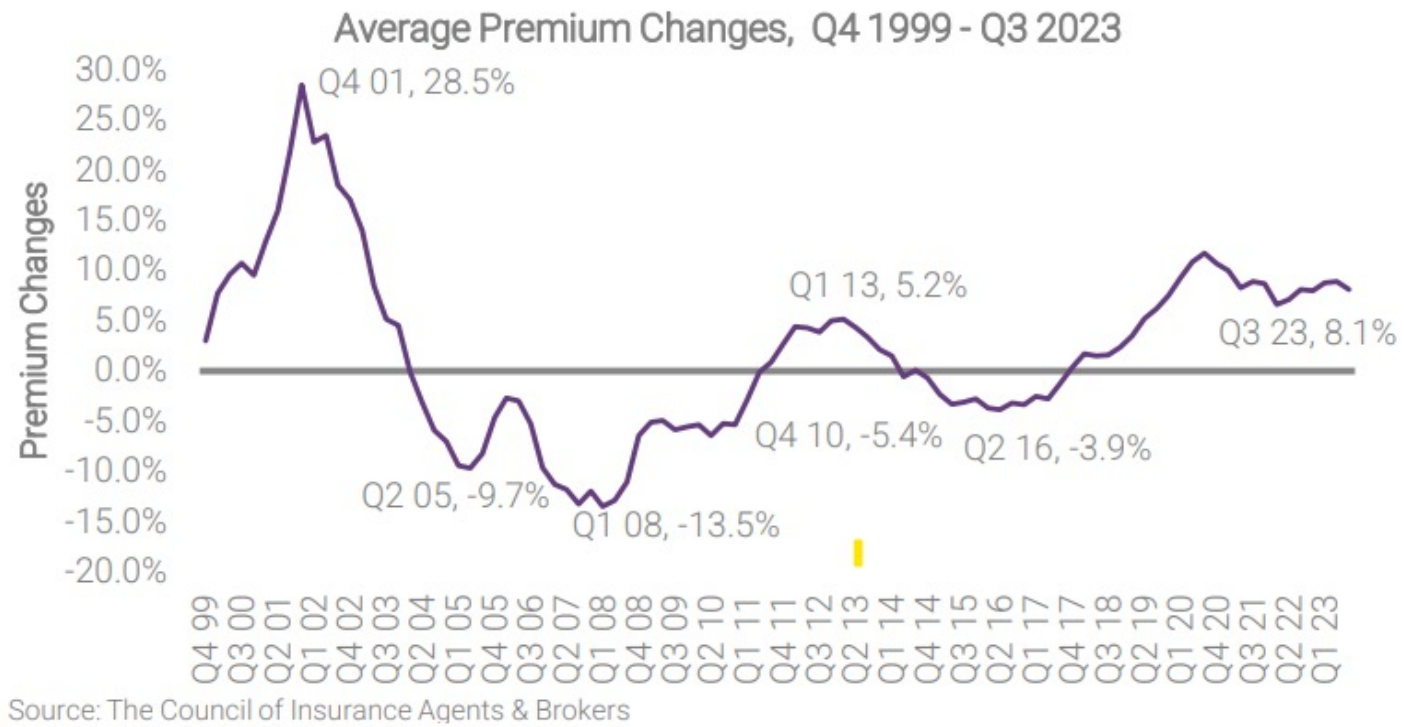
Insurability criterion	Description
Mehr and Cammack	
Incidental loss	The incident must be fortuitous and not under control of insured
Limited risk of catastrophically large losses	Catastrophically large losses must happen with very low frequency
Calculable loss	It must be possible to estimate or calculate possible losses and probability of an incident
Large number of similar exposure units	A large number of homogeneous exposure units must be available to facilitate the probability determination
Affordable premium	The premium must be reasonable for the insured
Definite loss	The loss must be difficult to forge. Its time, place and cause must be easy to determine
Large loss	The losses must be large enough for the insured to be born by himself/herself
Berliner	
Randomness of loss occurrence...	...incidents must happen independently.
Maximum possible loss...	...per incident should be manageable for insurer.
Average loss per incident...	...should be moderate.
Loss exposure...	...should be large enough.
Information asymmetry...	...should be too high.
Insurance premium...	...should be affordable for the insureds.
Cover limits...	...should be suitable for insureds.
Public limits...	...should be respected.
Legal restrictions...	...should not be violated.

Tsohou, Aggeliki, Vasiliki Diamantopoulou, Stefanos Gritzalis, and Costas Lambrinoudakis. "Cyber insurance: state of the art, trends and future directions." International Journal of Information Security (2023): 1-12.

GROWTH OF INSURANCE PREMIUMS

- Almost eight out of ten respondents (79%) said their insurance rates increased upon application or renewal
- Over two-thirds (67%) of respondents reported a 50% to 100% increase in insurance rates upon application or renewal.
- Despite increases, boards and top management teams require cyber insurance, with 81% allocating additional funding. The survey noted that investing in cybersecurity solutions to meet rising cyber insurance needs is a factor.
- Most (96%), organisations bought a security solution before their application was granted. As required by their cyber insurance plans, half of respondents purchased IAM, PAM, and MFA products.

Delinea, "Delinea's 2023 State of Cyber Insurance report", Delinea ,221 Main Street,Suite 1300,San Francisco, CA 94105. [Online]. https://www.ciab.com/resources/q3-2023-p-c-market-survey



The Council, "Commercial Property/Casualty Market Index Q3/2023", The Council of Insurance agents and Brokers, 701 Pennsylvania Avenue NW, Suite 750 Washington, DC 20004. [Online]. https://www.ciab.com/resources/q3-2023-p-c-market-survey

OBSERVATIONS

- In the early 2000s, the internet was still relatively young, and businesses were just beginning to understand the risks associated with data breaches and network security. The increased awareness of cyber risks and the novelty of the coverage are to blame for the spike in cyber insurance prices during this time.

- Businesses were increasingly adept at managing cyber risks as the market for cyber insurance grew. Insurers also improved their underwriting procedures and gained a deeper comprehension of the risks involved. This maturation may have helped stabilise or slightly lower premiums in the early 2010s, combined with shifts in risk perception and market competition.

- Due to a number of factors, including greater cyber threat sophistication, regulatory demands, customized policy offerings, integration with other insurance policies, and the growing digital world, cyber insurance premiums have grown more rapidly from the latter half of the 2010s to the present.

The increasing reliance on information technology and the escalating financial consequences of cyber incidents highlight the critical need for robust risk management strategies. Cyber insurance emerges as a key component, providing essential financial protection, supporting rapid recovery, and aiding in regulatory compliance. The historical evolution of cyber insurance reflects its adaptation to changing threats and the integration of customization and data analytics. As organizations, insurers, and regulators collaborate to navigate the dynamic cyber threat environment, cyber insurance remains a crucial tool for businesses seeking to safeguard operations and manage financial risks in the digital age.

- We started by understanding the context of cyber risk, financial loss, and insurance, reviewing the introductory paragraphs to grasp the core concepts and context.
- After establishing a foundation, I conducted forward searches by exploring specific details related to cyber risk, such as the increase in data breach expenses in healthcare and the evolving landscape of cyber insurance with the help of google scholar.
- To gain a comprehensive view, I conducted horizontal searches, examining various sections simultaneously to identify key themes, such as the vital role of insurance, the insurability of cyber risks, and the evolution of cyber insurance policies through various reports by different organizations
- Delving deeper into specific topics, I explored details about the insurability of cyber risks, including factors influencing it, the role of insurance in mitigating cyber risk, and the historical development of cyber insurance policies.

QUESTIONS?

Quantitative Measurement of the Impact of Security Breaches

Oluwatosin Falebita, Srivarshini Ksheerasagar, Sarthak Bharadwaj

COURSE: CS559 FALL 2023

COMPUTER SCIENCE DEPARTMENT

Colorado State University

Abstract

Security breaches persist in outpacing state-of-the-art preventive measures. Consequently, organizations must employ quantitative measures that offer greater efficiency in assessing the impact of cyberattacks. This paper introduces the TSS Model as a proposed framework for enhancing quantitative cost efficiency in evaluating the repercussions of security breaches.

Index Terms—Cybersecurity, cyber breaches, TSS Model

Problem Statement/ Motivation

The cost of Cybercrime is rapidly increasing, cybercrime magazine report provided an estimate for a breakdown of the cybercrime damage costs predicted in 2023:

- $8 trillion USD a Year
- $667 billion a Month.
- $154 billion a Week.
- $21.9 billion a Day.
- $913 million an Hour.
- $15.2 million a Minute.
- $255,000 a Second.

Businesses and organizations needs to measure the impact of security breaches by utilizing efficient measurement metrics in calculating the impact of cyberattacks in order to ensure business continuity.

D. Freeze, “Cybercrime To Cost The World 8 Trillion Annually In 2023,” *Cybercrime Magazine*, Jan. 11, 2023. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Introduction

- Traditional metrics like the number of breached records or stolen money often underestimate the full impact.
- Overestimations pose significant challenges for businesses in implementing effective security procedures.
- Introduction of a formal quantitative model: **The TSS Model**

S. Kaplan and B. J. Garrick, “On The Quantitative Definition of Risk,” Risk Analysis, vol. 1, no. 1, pp. 11–27, 1981

Algarni, Abdullah M., Vijey Thayananthan, and Yash- want K. Malaiya. ”Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems.” Ap- plied Sciences 11.8 (2021): 3678

Why Quantitative Measurement of Impact of Security breaches

1. Risk Assessment: Quantifying the impact of security breaches helps organizations assess the level of risk they face. By assigning numerical values to potential losses, organizations can prioritize security measures and allocate resources effectively.

2. Resource Allocation: Knowing the quantitative impact allows organizations to allocate resources proportionally. This means investing more in security measures where the potential impact is higher, thus optimizing the use of limited resources.

3. Insurance and Liability: Some organizations carry cybersecurity insurance to mitigate the financial impact of security breaches. Quantitative measurements of potential losses are essential for determining appropriate insurance coverage and negotiating premiums.

4. Cost-Benefit Analysis: Understanding the financial impact of security breaches enables organizations to conduct cost-benefit analyses for different security measures. This informs decision-making by comparing the costs of implementing security controls against potential losses.

5. Compliance Requirements: Many regulatory frameworks require organizations to assess and quantify the potential impact of security breaches. Demonstrating compliance often involves providing evidence of risk assessments and mitigation efforts based on quantitative measurements.

6. Incident Response Planning: Understanding the quantitative impact of security breaches is essential for developing effective incident response plans. It allows organizations to prioritize actions based on the severity of potential consequences.

Carfora, Maria Francesca, and Albina Orlando. ”Quantile based risk measures in cyber security.” 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA). IEEE, 2019

Cyberattack trend from 2018 - 2022

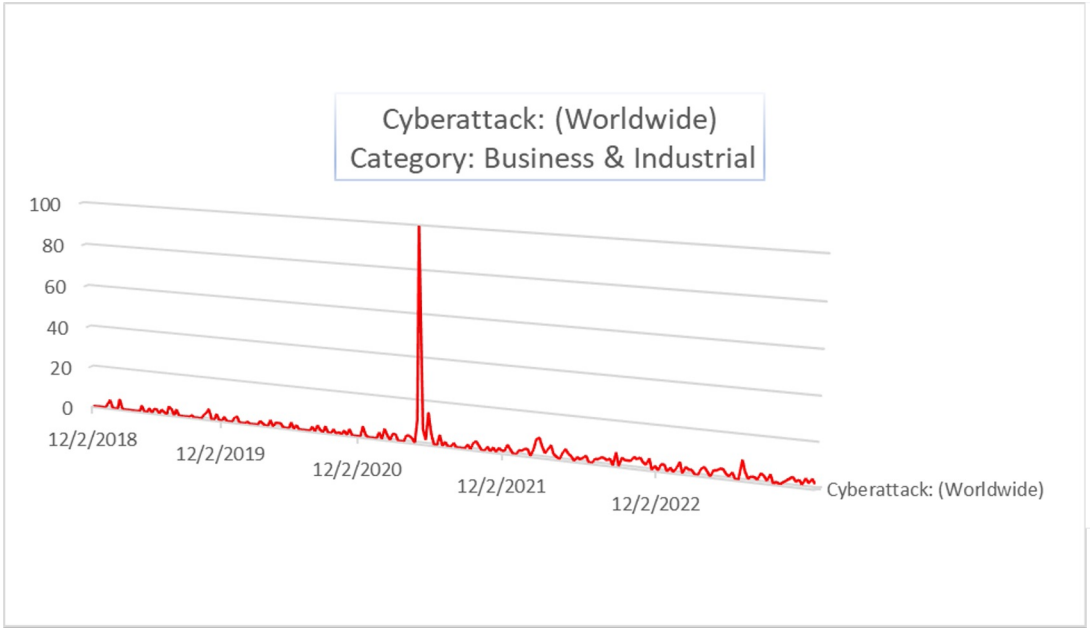


Figure 1. Cyber Attacks trends from google trend from Dec 2,2018 to June 18, 2023

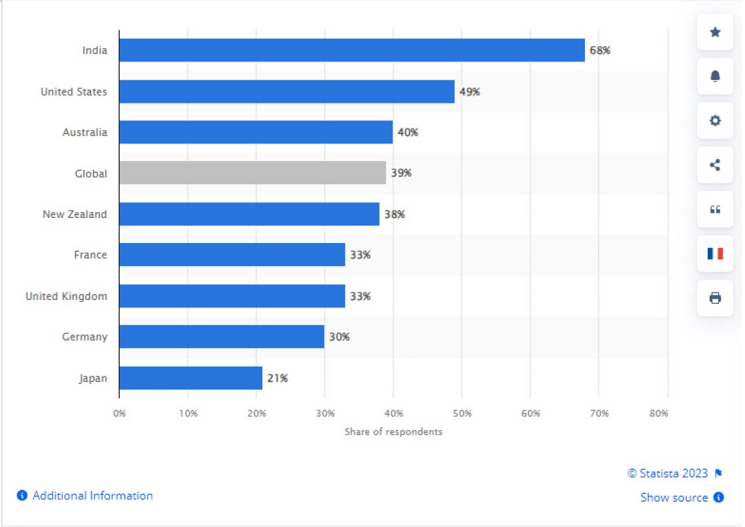


Figure 2. Cybercrime encounter rate in selected countries 2022

Google Trends," *Google*. https://trends.google.com/trends/explore?q=Cyberattack&hl=worldwide (accessed Nov. 26, 2023)

Cybercrime encounter rate in selected countries 2022," *Statista*, Jun. 08, 2023. https://www.statista.com/statistics/194133/cybercrime-rate-in-selected-countries

Cyberattack trend from Nov 2022 - Nov 2023

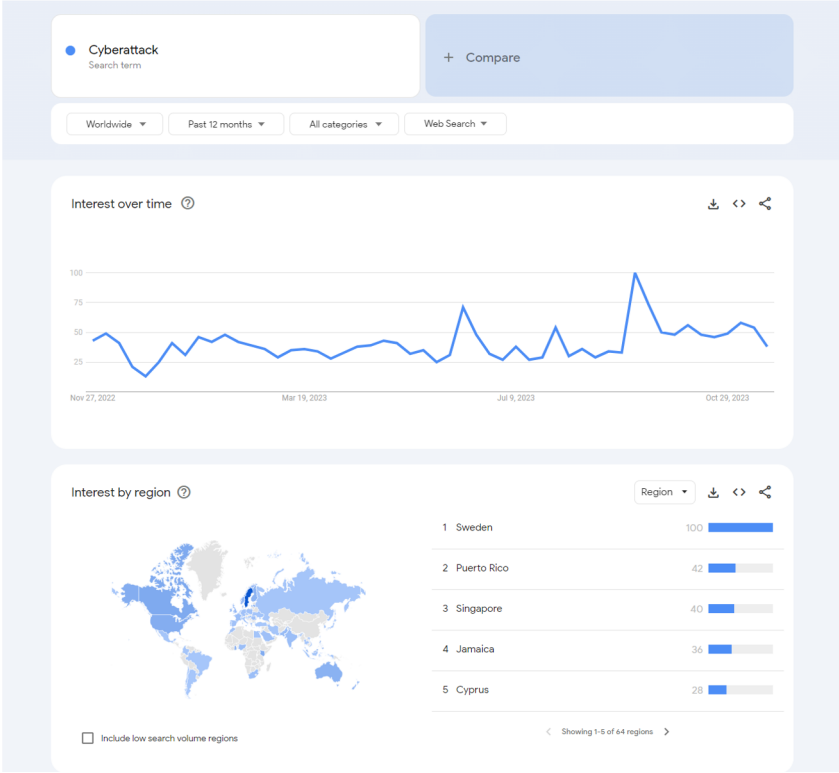


Figure 3: Data from Google Trend: Cyberattack trend worldwide on all categories

Google Trends," *Google*. https://trends.google.com/trends/explore?q=Cyberattack&hl=en-US (accessed Nov. 26, 2023).

Related works

1. Gordon et. al in their work proposed that breaches significantly affect stock market returns. Secondly, when breaches are categorized based on their primary effects (confidentiality, availability, integrity), attacks on availability have the most substantial negative impact on stock market returns. Thirdly, there is a notable decrease in the impact of security breaches in the period following the 9/11 attacks compared to the pre-9/11 period.

1. Caefora et al. proposed an estimation of Value at Risk (VaR), referred to as Cyber Value at Risk in cyber security domain, and Tail Value at risk (TVaR). The VaR at a fixed confidence level $\alpha \in [0, 1]$, is defined as the smallest number l such that the probability that the loss L exceeds l is not greater than $(1 - \alpha)$

   $$V\,aR\alpha(L) = \inf[l \in R | P(L > l) \leq 1 - \alpha].$$

   $V\,aR\alpha(L)$ corresponds to the α-quantile $q\alpha$ of the distribution function of the losses L. In the context of risk management, usual values for α are $\alpha = 0.95$, $\alpha = 0.99$ and $\alpha = 0.995$.

   A risk measure that overcomes VaR shortcomings, is the Tail Value at Risk (TVaR). It is sub-additive and quantifies the expected losses that occur beyond the VaR breakpoint. Given some confidence level α, TVaR is the conditional expectation of the loss L, given that $L \geq V\,aR\alpha$:

   $$T\,V\,aR\alpha(L) = E[L|L \geq V\,aR\alpha].$$

   TVaR represents that shape through a single number, that is the expected value of the losses higher than VaR.

[1] L. A. Gordon, M. P. Loeb, and L. Zhou, “The impact of information security breaches: Has there been a downward shift in costs?,” *Journal of Computer Security*, vol. 19, no. 1, pp. 33–56, Feb. 2011, doi: 10.3233/jcs-2009-0398.

[2] M. Francesca Carfora and A. Orlando, "Quantile based risk measures in cyber security," 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), Oxford, UK, 2019, pp. 1-4, doi: 10.1109/CyberSA.2019.8899431.

- Related works

3. Malaiya et.al develops a comprehensive, formal model that estimates the two components of security risks: breach cost and the likelihood of a data breach within 12 months using combination of formulars that evaluates costs such investigation costs, Crisis management cost per record(CMCPR), Regulatory and Industry Sanctions Cost(SCPR), Class Action Lawsuit Cost per Record(CALCPR), Computation of Data Breach Cost(CDBC), and Security Costs Regardless of Data Breach(SCRDB)

The probability of a breach of data type i (Pi) calculates the data breach probability for the organization in the next 12 months:

$$P_i = F_C \times F_{BCM} \times F_I \times F_{BC} \times F_E \times F_P \times \alpha e^{(-\beta x)}$$

where = 0.4405, = 4 × 10-5, x is the breach size, and the F factors are the six factors that impact the data breach probability.

[3] Algarni, Abdullah M., Vijey Thayananthan, and Yashwant K. Malaiya. "Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems." *Applied Sciences* 11.8 (2021): 3678.

- Related works

4. Albina et al expands on Cyber Value at Risk which is based on the concept of VaR which is a risk measure proposed by JP Morgan in 1995 as the "predicted worst-case loss at a specific confidence level". in the cyber context, takes the name of cyber value at risk (Cy-VaR).The author identified the main features and challenging issues of Cy-Var (Cyber Value at Risk) which are as follows:

a. In order to obtain a reliable estimate of Cy-VaR, these 3 factors must be considered (vulnerability, assets, and the profile of potential attackers). This listed element cannot be easily estimated for example, the vulnerability assessment of an organization depends on its previous ability to front successful attacks and on the maturity level of its security system. The identification of assets and classification of these assets into discrete categories of security risk is difficult, and the estimation of the probability of successful attacks is also not an easy task.
b. In order to estimate risk exposure using Cy-VaR, it is essential to take into account the dependencies among the three components (vulnerability, assets, and attacker profile).

Solution:

The author proposed a risk-adjusted ROSI (RaROSI), which takes into account worst cases. The idea is to consider the difference between the expected loss without mitigation effect of the investment E[L] and the worst case loss, at a given confidence level α, mitigated by the investment.

$$RaROSI_{\alpha} = \frac{\Delta U[L] - I_0}{I_0}$$

[4] A. Orlando, “Cyber Risk Quantification: Investigating the Role of Cyber Value at Risk,” *Risks*, vol. 9, no. 10, p. 184, Oct. 2021, doi: 10.3390/risks9100184.

- Related works

5. Song et al. used the loss distribution approach (LDA) and the time series model to describe cyber losses of financial and non-financial business sectors.

LDA is one of the most common risk-quantification methods to model operational losses. LDA expresses the aggregated loss L for a given time period as

$$L = N \sum i=1 Xi$$

Where N is the frequency of losses and X1, X2, . . . , XN are independent individual losses. In the operational risk context, Xi's are positive continuous random variables that represent the severity of each loss.

Due to the lack of information in the dataset, the author could not analyze the patterns of individual cyber loss observations. Future work should include the distributional properties of individual observations.

[5] S. Kim and S. Song, "Cyber risk measurement via loss distribution approach and GARCH model," *Communications for Statistical Applications and Methods*, vol. 30, no. 1, pp. 75–94, Jan. 2023, doi: 10.29220/csam.2023.30.1.075

- # Related works

6. Franco et. al introduces the Real Cyber Value at Risk (RCVaR), an economical approach for estimating cybersecurity costs using real world information from public cybersecurity reports.

The RCVaR determines the economic loss of a company with a certain degree of confidence. Thus, the costs and associated risks (i.e., probability of achieving higher costs than the expected value) are predicted using a model that reflects current quantitative cyber loss behavior related to industry reports. The RCVar model includes two submodels Data Layer and Model layer.

$$cv\_ratio_{\ year} = \frac{total\_avg\_cost_{\ year}}{avg\_market\_cap_{\ year}}$$

$$parameter\_ratio = \frac{1}{n}\sum_{i=1}^{n}\frac{cost\_param_i - avg\_factor_i}{avg\_report_i}$$

$$company\_cost_{year} = \frac{valuation_{\ ReportYear+t}}{discount^{t}_{valuation}} \times cv\_ratio \times discount^{t-ReportYear}_{cost} \times \prod_{i=1}^{11}(1 + param\_ratio_i) \qquad (1)$$

[6] Franco, M. F., Künzler, F., von der Assen, J., Feng, C., & Stiller, B. (2023). Rcvar: an economic approach to estimate cyberattacks costs using data from industry reports. *arXiv preprint arXiv:2307.11140*.

.

Key Findings on Cost Metrics until now

- Crisis Management Cost per Record (CMCPR)
- Regulatory and Industry Sanctions Cost (SCPR)
- Class Action Lawsuit Cost per Record (CALCPR)
- Computation of Data Breach Cost (CDBC)
- Security Costs Regardless of Data Breach (SCRDB)

Our contributions

We introduce the TSS Model by expanding the scope of Malaiya et al works by adding the following variable.

- Factors to consider for Financial Impact – Direct Cost + Indirect Cost
- Factors to consider for Data Impact – Data impact = volume of compromised data * sensitivity
- Factors to consider for Operational Impact (O)= Downtime * remedial cost
- Factors to consider for Reputational Impact (R)= customer trust + media coverage
- Factors to consider for Regulatory and Legal Impact (RL) = Penalties + Legal Cost
- Supply Chain Impact, Employee and Stakeholder Impact, Long-Term Consequences (LC)

Proposed Model

TSS Model = Financial Impact (FI) + Data Impact (DI) + Operational Impact (OI) + Reputational Impact (RI) + Regulatory and Legal Impact (RL) + Supply Chain Impact (SC) + Employee and Stakeholder Impact (ES) + Long-Term Consequences (LC)

$$TSS = FI + DI + OI + RI + RL + SC + ES + LC$$

Limitations

The viability of our model has been demonstrated through its construction using established metrics. Regrettably, we encountered challenges in acquiring real-life data to assess the actual performance of the method. While the model's feasibility is affirmed based on existing metrics, the absence of real-world testing data poses a limitation in validating its practical effectiveness.

“Questions.”

Thank you

Colorado State University

An Analysis of Smartphone Vulnerabilities and Security Models

Term Project - CS 559

Sushmitha Rasamalla

Surendra Kurivella

Abstract

- Mobile devices worldwide, including smartphones, PDAs, and tablets, are crucial for daily life, with operating systems like Android, iOS, and Blackberry providing platforms for these smart devices.
- A broad range of security risks have been made possible by the widespread use of various applications.
- This study aims to analyze and understand vulnerabilities in the Android operating system, focusing on the importance of maintaining smartphone security.
- The research expands on previous mobile device security research projects to improve our understanding of vulnerabilities and security models, addressing issues such as phishing, malware, botnets, spyware, permission control, privacy leakage, improper app authorization, and compromised data confidentiality.

Introduction

- Smartphone usage has increased significantly, but it also increases risks due to increased malware and security vulnerabilities.
- Apple released a critical security update in 2021 to address a "zero-click vulnerability" in iPhones, emphasizing the importance of regular operating system updates to keep phones secure.
- Apple and other businesses have experienced significant security breaches, including ransomware and data breaches, with global smartphone users reaching 6.648 billion in 2022, highlighting the need for improved security models.

Android smartphone vulnerabilities: A survey. (2016, April 1). IEEE Conference Publication — IEEE Xplore. https://ieeexplore.ieee.org/document/7578857

Related Work And Background

- Android is the dominant mobile platform, serving over 2 billion active users and hosting over 3 million apps, surpassing desktop software in digital tasks like leisure activities, communication, and commerce.
- The Android system has been criticized for its permission model, message passing system, and data protection, with concerns about potential attack points, vulnerabilities in third-party apps, and increasing threats against sensitive data stored in these devices.
- The lack of clear indicators for secure or insecure connections between apps and the Internet increases the risk of potential man-in-the-middle (MITM) attacks on user communication.

M. La Polla, F. Martinelli and D. Sgandurra, ”A survey on security for mobile devices”, IEEE Commun. Surveys Tuts., vol. 15, no. 1, pp. 446-471, 1st Quart. 2013.

Y. Desmedt, ”Man-in-the-middle attack” in Encyclopedia of Cryptography and Security, Boston, MA, USA:Springer, pp. 759, 2011.

Motivation

- Mobile apps and smartphones have become integral to our lives, providing communication, data sharing, entertainment, and gaming services. However, increased smartphone usage exposes us to security and privacy challenges.
- This work delves into the intricate realm of smartphone security, examining mobile operating systems to identify potential security vulnerabilities and potential entry points for malicious attacks.
- The study aims to identify and tackle security issues in smartphones, particularly software-based attacks like malware, to protect personal data, financial information, and device integrity, empowering users with practical solutions.

Research Questions

Considering our keen focus on resolving existing problems, the following research questions delve into various aspects of mobile application security:

1) How have threats to the safety of mobile applications altered over time, and what new dangers have emerged?
2) To what extent can mobile applications be protected, and what kinds of security solutions and technologies are most effective?
3) How do user habits and perspectives on mobile app security affect the adoption of security best practices?

Proposed Approach

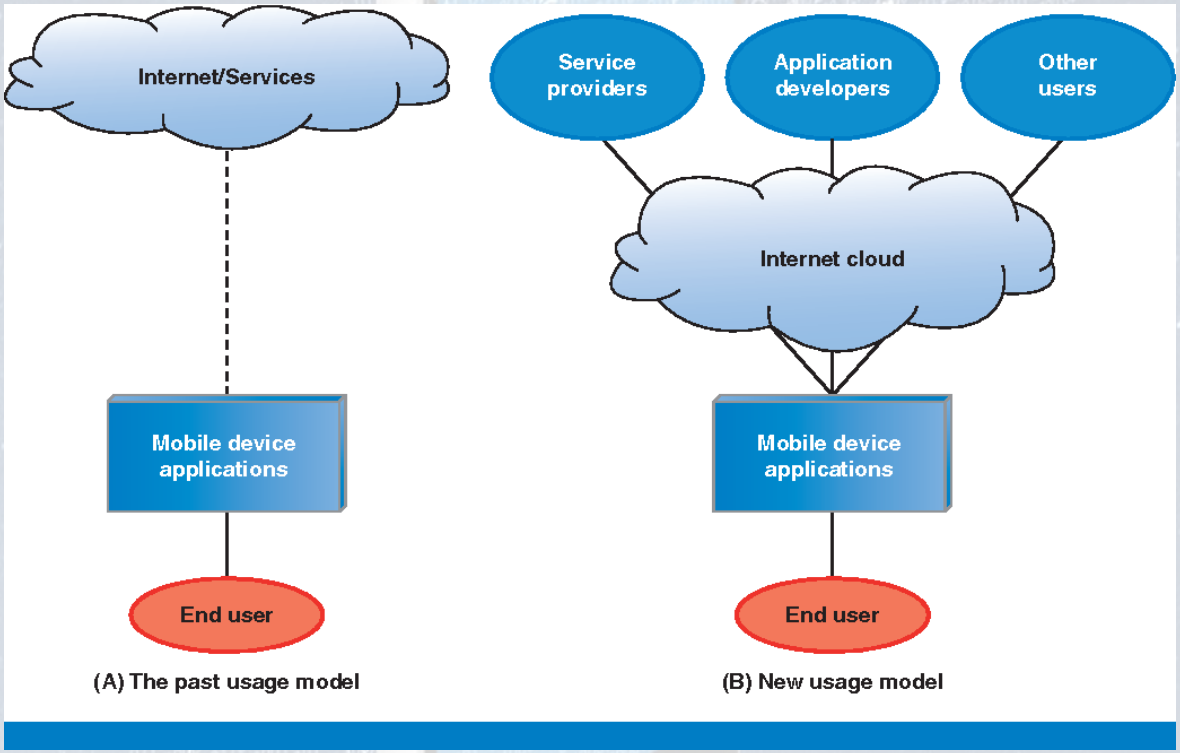
- This research focuses on smartphone security, analyzing operating systems, architecture, and security mechanisms.
- It aims to identify vulnerabilities, malicious attack entry points, and threats to user privacy, highlighting software-based threats, and providing practical security methods.
- The goal is to provide a comprehensive understanding of the dynamic threat landscape and offer practical, realistic security methods.

Mobile Operating System

- Smartphones, which run on their own specialized operating systems (mobile OS), have given us the ability to do more complex things on the go than were previously feasible solely on our desktop computers.
- In addition, it serves as a platform for developer to create apps (software programs developed for smart phones that performs specific functions) .
- There are a few main mobile device operating systems that the majority of smartphones run on, including Apple iOS, Google Android and Microsoft's Windows Phone OS.

Li, X. F. (2012). MObIle OS ArChITeCTure TrendS. https://www.semanticscholar.org/paper/MObIle-OS-ArChITeCTure TrendS-Li/140380307a91846d2226ccf6e53aefd0443344b5

Mobile Operating System Architecture Model



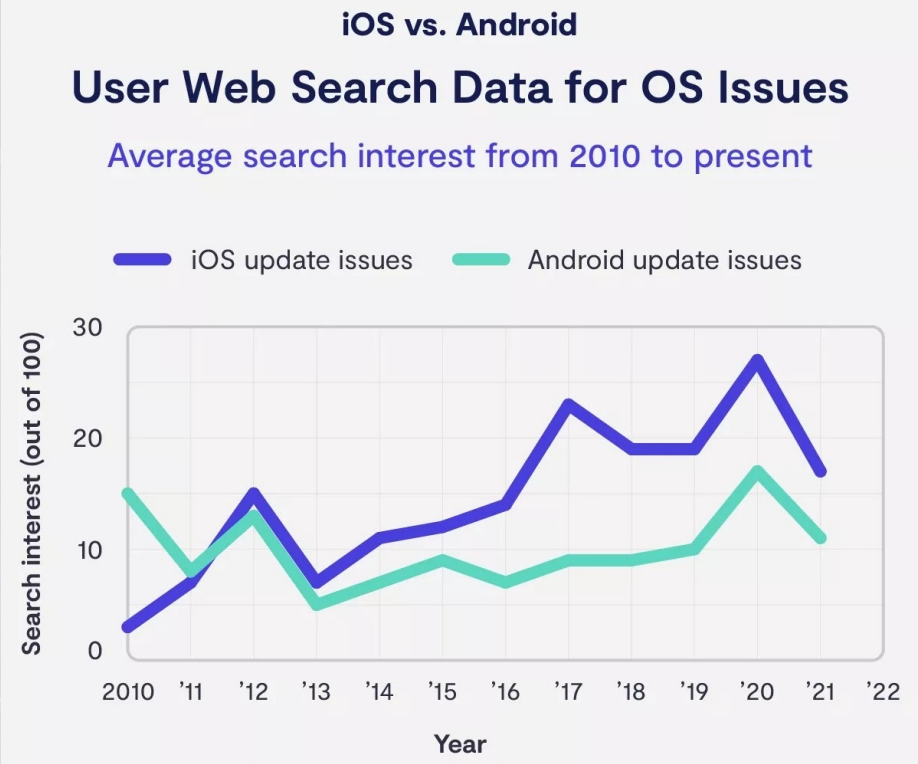
Li, X. F. (2012). MObIle OS ArChITeCTure TrendS. https://www.semanticscholar.org/paper/MObIle-OS-ArChITeCTure TrendS-Li/140380307a91846d2226ccf6e53aefd0443344b5

Mobile Operating System Features

- Smartphones use technology like cameras, fingerprints, sensors, and NFC for various functions.
- Operating systems (OS) provide control, with five major groups: Android, Apple iOS, Microsoft Windows Phone, and BlackBerry. OS comes with pre-installed programs like web browser, email client, text messaging app, navigation, and app stores.
- Most malicious applications are online, but consumers cannot distinguish between malicious and legitimate software.

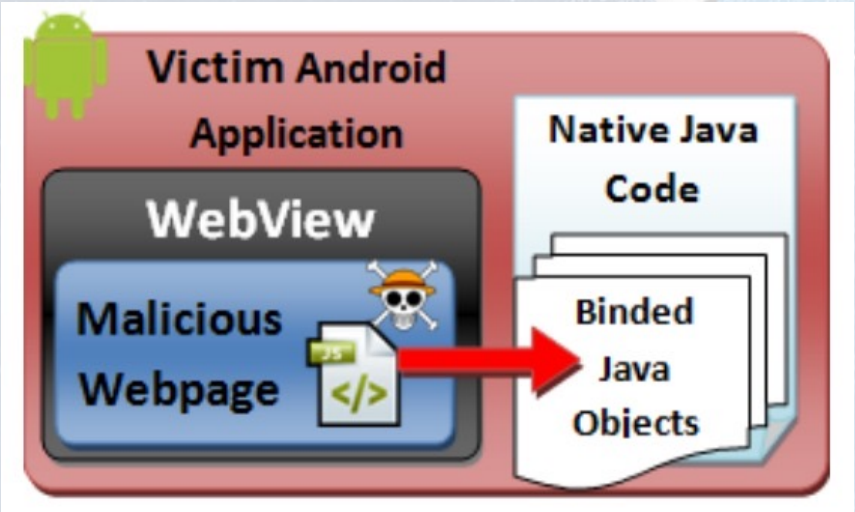
Li, X. F. (2012). MObIle OS ArChITeCTure TrendS. https://www.semanticscholar.org/paper/MObIle-OS-ArChITeCTure TrendS-Li/140380307a91846d2226ccf6e53aefd0443344b5

Analyzing a Decade of Smartphone Security: A Google Trends Comparison of iOS and Android

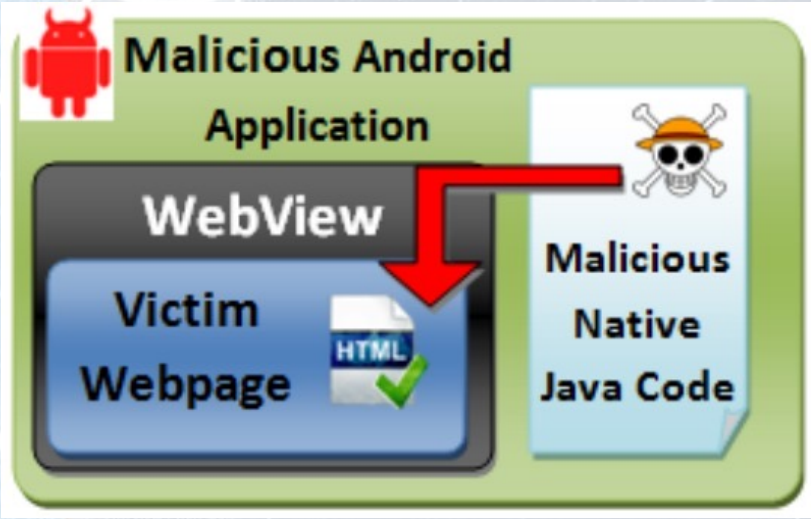


Hanko, Kateryna . “IOS vs. Android: Which OS Is More Secure in 2022?” Clario.co, 21 Feb. 2022, clario.co/blog/ios-vs-android-security/. Accessed 6 Nov. 2023

BASIC ANDROID SECURITY MECHANISM : Threat Models



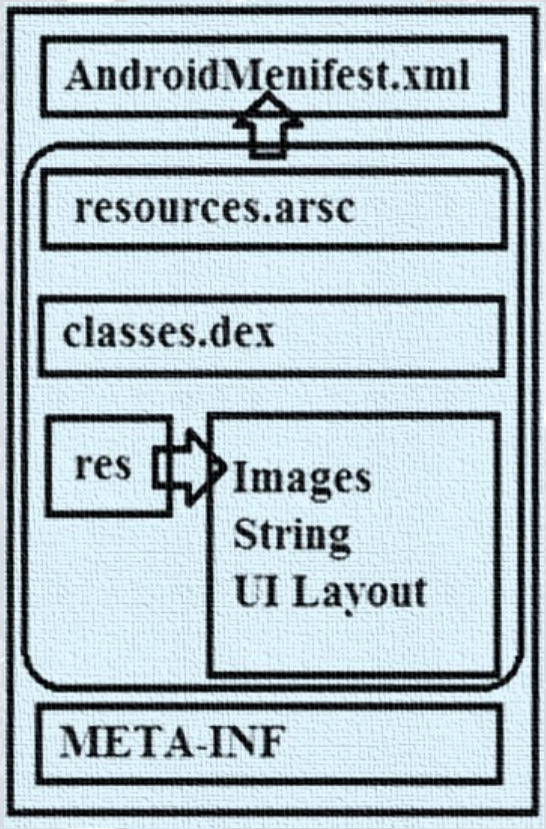
Malicious Web-Pages



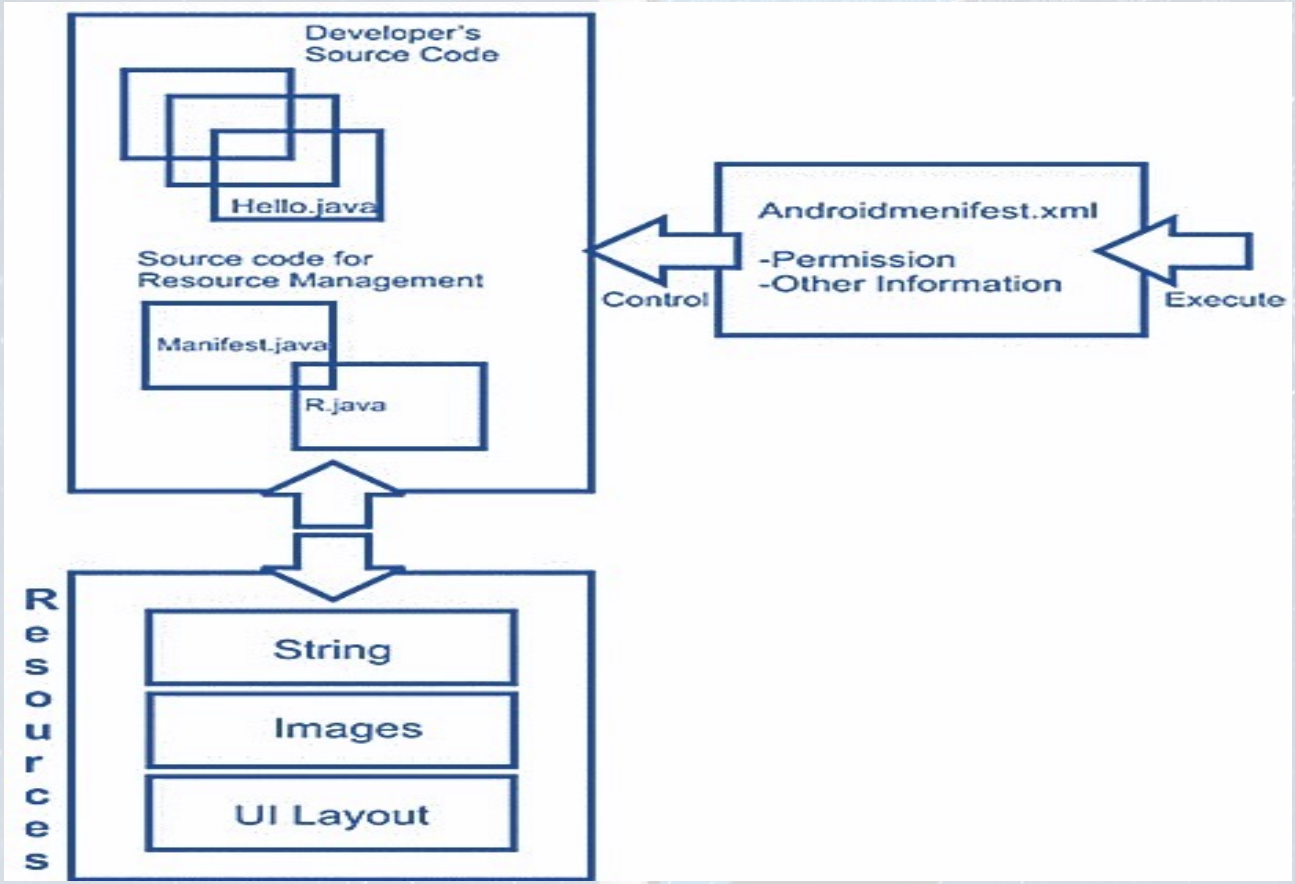
Malicious-Apps

A. Ankur and S. Patel, ”Finding Vulnerabilities in E-Governance Apps of Android Platform,” 2022 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2022, pp. 185-191, doi: 10.1109/ICTACS56270.2022.9988647.

BASIC ANDROID SECURITY MECHANISM : Android Application Structure



Apps and user permission: their relationship



T. Luo, H. Hao, W. Du, Y. Wang and H. Yin, "Attacks on Webview in the android system", Proceedings of the 27th Annual Computer Security Applications Conference, pp. 343-352.

Findings

- As per the CVEs published in NVD Database, the number of vulnerabilities related to applications used on Android platforms is increasing and its a growing concern.
- Most of them are addressed in the android updates and app updates.

Year	# Vulnerabilities found
2016	880
2017	1195
2018	461
2019	775
2020	700
2021	800
2022	670
2023	473

No. of Android vulnerabilities vs year

"Android CVE - Search Results." Cve.mitre.org, cve.mitre.org/cgi-bin/cvekey.cgi?keyword=android. Accessed 1 Nov. 2023.

Findings

- According to the survey all over world there are different kinds of vulnerabilities with which one can exploit the android devices.
- **Denial of Service :** 95% of Android devices are vulnerable to Denial-of-Service (DoS) vulnerabilities, exploited by malicious apps or crafted websites. This looping service depletes system resources and can also occur during Wi-Fi scanning.
- **Overflow :** This type of vulnerability in android can make the phone apparently dead- unable to make calls, silent, with a lifeless screen
- **SQL Injection** : SQL Injection attack is a prevalent and prevalent attack on Android devices, where malicious code is inserted into strings and executed on an SQLite instance.
- **Gain Information/ Privilege :** The Android device's inability to properly check user-supplied data creates a vulnerability for attackers to execute arbitrary code, posing a significant security risk.

Future Work

- The research project is now currently focused on detecting smartphone vulnerabilities, with the next phase dedicated for creating and evaluating solutions.
- This involves patching, user education, and security best practices.
- The final report should include realistic methods to improve smartphone security and preserve user data and privacy.


THANK YOU

COLORADO STATE UNIVERSITY

Quantitative Risk Assessment of Payment Systems/Credit Card Security

Prathamesh Chougule, Electrical Engineering.

Shamitha Gowra, Computer Science.

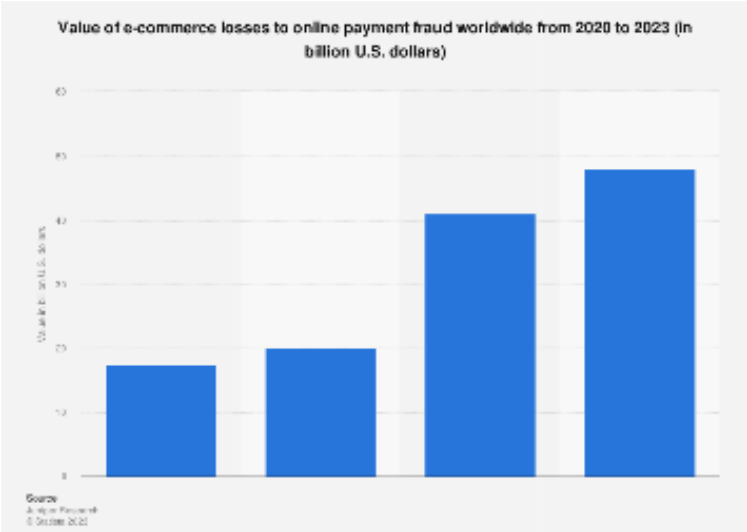
CS559 - Quantitative Security.

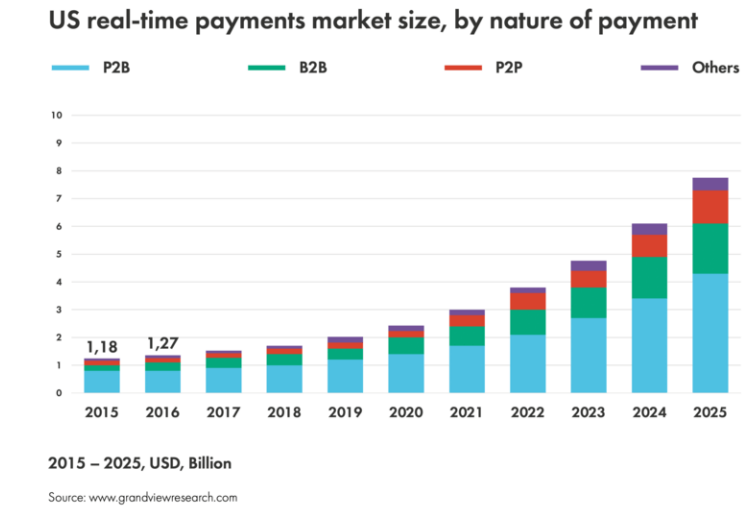
Table of Contents

- Background
- Overview of Payment Systems and Credit Card Security
- Risk Management Framework
- Methodology for Quantitative Risk Assessment
- Threats and Vulnerabilities in Payment Systems
- Quantitative Risk Matrices
- Data Analysis and Modeling
- Credit Card Security Measures
- Case studies
- Quantitative Risk Assessment results
- Risk Mitigation Strategies
- Challenges and Future trends
- Conclusion

Background

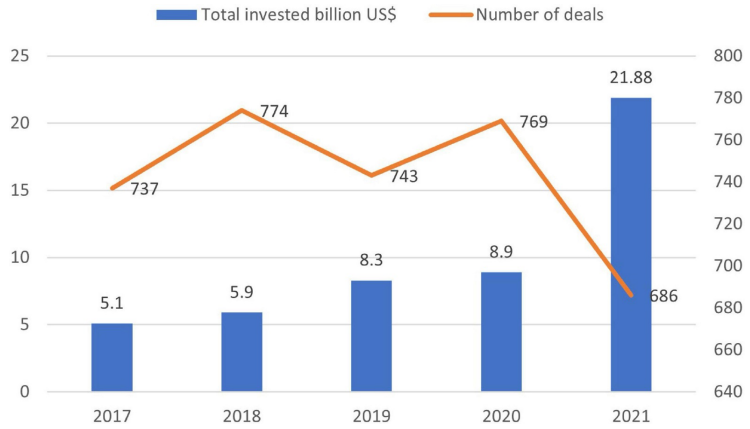
- Payment Market size is increasing day by day and it is expected to grow exponentially.
- But the number of e-commerce frauds are also increasing rapidly.
- Risk assessment can help to reduce such frauds.

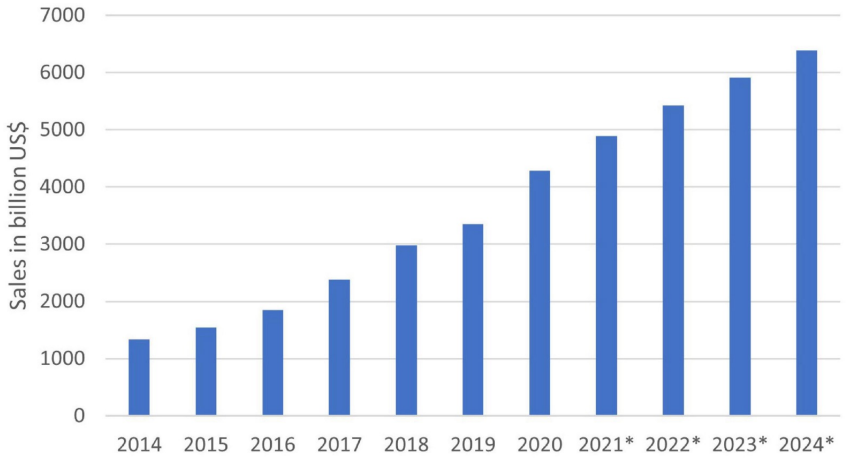




https://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally/
https://www.dataart.com/blog/what-to-expect-from-payment-trends-in-2021-and-beyond

Trends in Sales and Investments in the Cybersecurity domain





Xiang Liu, Sayed Fayaz Ahmad, Muhammad Khalid Ansar, Jingying ke, Muhammad Irshad, Jabbar Ul-Haq , Shujat Abbas ,
"Cyber security threats: A never-ending challenge for e-commerce" , CONCEPTUAL ANALYSIS article Front. Psychol., 19 October 2022
https://doi.org/10.3389/fpsyg.2022.927398

Overview of Payment Systems and Credit Card Security

- Earlier, It started with Electronic Fund Transfer (EFT), Wire Transfer etc.
- Currently the online transactions consist

1. Credit Cards
2. Net Banking
3. Mobile Wallets
4. UPI

- There are various payment gateways as well like razorpay, payubills etc.

Types of Payment Securities

1. **Tokenization** - Tokenization secures transactions by replacing payment information with randomly generated strings of characters. These tokens allow businesses to provision customer accounts, set up scheduled payments, and manage payment settings without handling sensitive cardholder information each time.
2. **Address Verification Service (AVS) -** AVS compares the address provided at checkout with the known address of the cardholder. The tool verifies whether or not the addresses match via a response code sent by the credit card company. While this is useful when paired with other methods of fraud prevention, by itself AVS is quite limited.
3. **Authentication** – SFA, 2FA, MFA , OTP etc.
4. **SSL protocol** - Secure Socket Layer (SSL) is an internet protocol that encrypts all communications on a website and is especially important for securing web pages that process customer payment information.
5. **3D secure(3DS)** -The power of 3DS comes from the data-rich information collected during and before checkout. Information such as IP address, transaction history, and purchase amount are all factored in and analyzed for risk. In total there are over 100 data points collected regarding the cardholder, their device, and the nature of the transaction.

Risk Management Frameworks

1. **Risk Identification** - In order to identify risks, possible threats and weaknesses that might compromise the security and operation of payment systems must be methodically investigated. This encompasses factors that are both internal and external, like malicious activities, human error, and technological shortcomings.
2. **Risk Analysis** - Risk analysis comprises a thorough investigation of the hazards that have been identified in order to ascertain their likelihood and possible impact. We will examine the approaches used to evaluate the risks' seriousness in this section, taking into account things like monetary loss, business interruption, and reputational harm.
3. **Risk Evaluation** - The next stage after risk analysis is to assess the risk's importance in light of stakeholder interests and organizational goals.
4. **Risk Treatment** - Creating and implementing plans to reduce, transfer, or accept hazards that have been identified is known as risk treatment. Security control implementation, risk transfer via insurance, and emergency preparation are a few examples of strategies.

https://www.tripwire.com/state-of-security/applying-risk-management-framework

Possible Threats in Payment Systems

1. **Phishing Attack** - These attacks user by phishing emails. It is an attempt to trap a user to disclose the information
2. **Social Engineering** - In social engineering, user data available in the public domain and the attackers can steal it from there. This information monetized or sold in underground market forums or used for fraudulent payments.
3. **Payment Authorization Process Compromise** – An internal attacker can gain access to critical servers may attempt to bypass fraud controls.
4. **DDOS attacks** - DDoS attacks by threat actors seeking to interrupt mobile payment services. These might affect transactions relates services hosted in the cloud.
5. **Mobile Operating System Access Permissions –** Users give certain permission to OS access, which can be use by attackers to access sensitive data and harm the mobile application.
6. **Man-in-the-Middle -** Attackers can also attempt to exploit network security weaknesses such as lack of firewalls.
7. **Relay attacks against NFC enabled POS contactless terminal** - Relay software installed on the mobile can relay commands and responses between the Secure Element and a card emulator that is installed as proxy on the mobile POS across a wireless network.

https://www.researchgate.net/publication/332113623_Wallet_Payments_Recent_Potential_Threats_and_Vulnerabilities_with_its_possible_security_Measures

Possible vulnerabilities in Payment Systems

1. Lack of user's due carefulness of validating content in emails, messages, SMS being truthful before selecting URLs, downloading attachments.
2. Use public Wi-Fi connections for mobile payments.
3. Use of fake access point with same network
4. No PIN lock set or PINs set to weak PINs.
5. No remote devices lock set and no remote data wipe set.
6. Not up-to-date OS to connect and use entrusted device.
7. Weaknesses in enforcing strong authentication for access to critical systems and databases where cardholder data is stored for validation and payment authorization to acquirer.
8. Non-effective malware detection and prevention measures.
9. Misconfiguration of fraud detection systems including rules such as positive payment checks, max limit amount per transaction, daily limits, velocity tagging.
10. Weaknesses and vulnerabilities on digital wallet servers and applications hosted at the mobile payment application provider.
11. Absence of malware detection and prevention on critical servers that provide access servers where cardholder data and user profiles are stored

https://www.researchgate.net/publication/332113623_Wallet_Payments_Recent_Potential_Threats_and_Vulnerabilities_with_its_possible_security_Measures

Quantitative Risk Matrices

Steps of Assessing Risk -

1. Determine the type of risk-

- **Strategic Risk**: risks associated with failed business decisions.
- **Operational Risk**: risks associated with breakdowns in internal processes/procedures.
- **Financial Risk** : risks associated with financial loss.
- **External Risk**: risks associated with uncontrollable sources.

2. Determine the Likelihood and Impact

- **Likelihood**: the level of *probability* the risk will occur or be realized.
- **Impact**: the level of *severity* the risk will have if the risk is realized.

3. Asses the Risks

- **High risk**
- **Moderate/Medium risk**
- **Low risk**

Likelihood/ Impact	Negligible Impact (1)	Low Impact (2)	Moderate Impact (3)	High Impact (4)	Catastrophic Impact (5)
Highly Unlikely (1)	Negligible Risk (1)				
Unlikely (2)		Low Risk (4)			
Possible (3)			Moderate Risk (9)		
Likely (4)				High Risk (16)	
Highly Likely (5)					Major Risk (25)

https://www.auditboard.com/blog/what-is-a-risk-assessment-matrix/

Probabilistic Distributions

1. Monte Carlo Simulations:

- Useful for modeling complex systems with many uncertainties.
- Determine likelihood of rare events and tail risks.
- Generate random variables for model parameters based on probability distributions.
- Calculate model outcomes many times using Monte Carlo sampling.

2. Markov Chains:

- Well-suited for modeling fraud detection states.
- Calculate long-term, steady-state probabilities.
- Model system transitions between discrete risk states.
- Define transition probability matrices between states.

Probabilistic Distributions (Contd)

3. Bayesian Networks:

- Allows combining qualitative and quantitative information.
- Update probabilities as new data becomes available.
- Represent interdependencies between risks via directed acyclic graphs.
- Incorporate expert knowledge into prior probabilities.

4. Poisson Process Models:

- Used when risk events are independent and rare.
- Estimate event frequency over time via Poisson distribution.
- Key application in modeling arrival rate of threats.

5. Survival Analysis:

- Used to model time to an adverse event.
- Quantify the probability of the system surviving without failure.
- Useful for analyzing the lifespans of critical infrastructure.

Case Studies

1. **Ripple:**

- Offers a payment service that uses the blockchain to make valuable transactions as quickly as possible and at low cost.
- Ripple Protocol Consensus Algorithm.
- This algorithm is based on nodes, and once the nodes in the network are in agreement, the transaction is validated.
- It is through this algorithm that Ripple avoids validating hostile or dangerous transactions.
- XRP is the token of the Ripple project. It is open source.
- It facilitates payments between countries, making transactions cheaper, faster, and potentially more secure via RippleNet.

Ripple - The payment service revolutionizing cross-border payments and its global influence by Kurious Society
https://www.linkedin.com/pulse/ripple-payment-service-revolutionizing-cross-border-payments

Case Studies (Contd)

2. Machine Learning for Credit Card Fraud Detection & Anti-Money Laundering in Payments :

- Western Union and Visa use ML to prevent Fraud.
- Western Union has implemented a robust machine learning system, operating on a substantial Hadoop cluster, to combat fraud in money transfers.
- Upon initiation of a money transfer order, Western Union's Hadoop cluster processes the request and returns a simple "yes/no" determination.
- Despite an increase in false positives, where legitimate transactions are incorrectly flagged as fraud, the company has achieved a significantly reduced fraud rate, surpassing the industry standard of 1.2%.
- Visa has reported that its Visa Advanced Authorization (VAA) system, utilizing artificial intelligence (AI), played a crucial role in preventing an estimated $25 billion in annual fraud.
- VAA is a comprehensive risk management tool that monitors transaction authorizations on the Visa global payment network in real time
- By employing AI to assess each transaction in about one millisecond, the system identifies and responds to emerging fraud patterns, allowing financial institutions to approve legitimate purchases while swiftly preventing fraudulent ones.
- Visa's multi-layered approach, incorporating AI, has maintained global fraud rates at historic lows, below 0.1%.

Western Union Clamps Down on Fraud with ML
https://www.datanami.com/2018/12/03/western-union-clamps-down-on-fraud-with-ml/
Visa Prevents Approximately $25 Billion in Fraud Using Artificial Intelligence
https://usa.visa.com/about-visa/newsroom/press-releases.releaseId.16421.html

Recent Developments

Online payment fraud anomaly detection:

- To detect fraudulent activities in e-banking systems while keeping false alarms at an acceptable level.
- Three main steps - pre-filtering, feature extraction, and machine learning.
- Pre-filters remove obvious normal and fraudulent transactions early on to reduce false positives. The remaining transactions are passed to the machine learning model.
- 147 features are extracted and categorized as behavioral features (based on customer's click sequences), transactional features (payment amounts, account balances, etc), and customer features (demographics, etc).
- The machine learning model consists of three unsupervised outlier detection base learners - Local Outlier Factor (LOF), Isolation Forest (IF), and Bagged Decision Trees (BDT). BDT is also used for feature selection.
- On real banking data with 0.0012% fraud rate, the model achieved 45% true positive rate at 1% false positive rate, outperforming prior benchmarks. Adding optimization further reduced fraud losses.
- The model was able to detect online payment fraud effectively on highly imbalanced real data.

Paolo Vanini, Sebastiano Rossi, Ermin Zvizdic and Thomas Domenig, ”Online payment fraud: from anomaly detection to risk management”, https://doi.org/10.1186/s40854-023-00470-w

Recent Developments (Contd)

New Machine Learning Approach:

- A new hybrid machine learning approach called FFSVM for credit card fraud detection by combining firefly optimization and support vector machines (SVM) is developed.
- Firefly optimization is used to select an optimal subset of features from the high-dimensional credit card dataset, reducing dimensionality. This improved SVM classification performance.
- The approach is evaluated on a real-world Australian credit card fraud dataset and achieves 85.65% accuracy, outperforming benchmarks. Key metrics like true positive rate, false positive rate, etc. are better.
- Provides a more accurate and computationally efficient fraud detection system.
- Firefly optimization enables both explorative and exploitative search for better feature selection.

Ajeet Singh, Anurag Jain,and Seblewongel Esseynew Biable, ”Financial Fraud Detection Approach Based on Firefly Optimization Algorithm and Support Vector Machine”. https://doi.org/10.1155/2022/1468015

Recent Developments (Contd)

Problems Associated with Using Machine Learning for Credit Card Fraud Detection:

- Data challenges like extreme class imbalance and lack of publicly available datasets remain key issues. Varied solutions proposed like SMOTE oversampling.
- Performance metrics used across papers differ significantly. Classification performance metrics like accuracy are not appropriate for highly skewed datasets.
- Proposed enhancements include distributed implementations leveraging big data platforms to handle large volumes of transactions. Usage of IoT data sources for improved fraud analytics.
- Security and privacy aspects around fraud detection systems need more attention regarding factors like data sensitivity.

Asma Cherif, Arwa Badhib, Heyfa Ammar, Suhair Alshehri, Manal Kalkatawi, Abdessamad Imine, Credit card fraud detection in the era of disruptive technologies
https://doi.org/10.1016/j.jksuci.2022.11.008

Results

- Multiple machine learning algorithms to identify Fraudulent Transactions.
- Performed comparative analysis of various algorithms for credit card fraud detection.
- The decision tree classifier worked the best with an accuracy of 99%.

Algorithm	Accuracy
Logistic Regression	94%
KNN	93.75%
Decision Tree	99%
Random Forest	93.80%
SGD classifier	96.30%

Questions
?

Wed Nov 29 Schedule

- Using fuzzing to detect zero-day vulnerabilities, Ruturaj Dhakate
- SmartPhone Security Models and Vulnerabilities, Prajith Reddy P, Sai Charan Vishwanatha,
- Enhancing Cybersecurity Resilience: A Multifaceted Approach through Security Breach Analysis and Prevention Strategies, Avyakta Chelle, Navya Yadlapalli
- Quantitative Resiliency for Cyber-physical Systems, Mahmoud Abdelgawad
- Economics of Ransomware (online), Aashray Boddu, Mudasir Attar