SECURITY ASSURANCE AND REPUDIATION THREATS

Srinivas Rao Doddi[1] and Akshay Krishna Kotamraju[2]

[1]Department of Information Technology, University of Los Angeles, Los Angeles, California, USA
[2]Founder Non-profit , Think Cosmos, Saratoga, California, USA

ABSTRACT

Social engineering attacks pose a serious threat to individuals through various phishing attacks and also scams. Scams also comprise wherein a very prominent type of fraud occurs wherein first party or the user is made to believe in a nefarious scheme as profitable i.e. "collusion" wherein threat actor colludes in perpetrating fraud wherein a percentage of money gets split or victim's get their money drained before they realize that they have been duped. These situations also lead to a scenario called "first party fraud" wherein the victim even after knowingly authorizing payments denies subsequently and go to court. In such scenario, it is upon the entity or financial organizations to prove that they do have "authorization" and it was indeed the same person to deal with "repudiation scenarios" , else financial institutions may have to bear the lost This paper presents a converged security framework towards a comprehensive prevention and detection controls mechanism to mitigate these threat vectors. It also explores different types of social media attributes ,leverage data mining engineering tactics. The paper also discusses associated limitations and challenges and recommends security best practices, and proposes an integrated framework. Finally, paper proposes a converged security framework that allows various parties from fraud, cyber, and physical security to collaborate.

KEYWORDS

Security, Assurance, Authentication, Information, Policy

1. INTRODUCTION

Untrusted traffic originating from decentralized identity providers presents a significant threat to financial entities impacting operations and meeting compliance obligations. This paper presents a framework that addresses attack vectors that either originate from a known and unknown entities in an uncontrolled environment or from a compromised endpoint. Automated validators generally are referred to as financial BOT's that originate in either trusted entity or untrusted. It also explores different types patterns that are then identified and data mined to enabled automatic routing of segmenting in real time a "known good" vs "unverified traffic aka known bad or deemed high risk".[1] The paper also discusses associated limitations and challenges and recommends security best practices, and proposes an integrated framework to make it difficult for high-risk traffic to operationally viable and makes it unsustainable by increasing the cost of continued ingress traffic via increased attack surface the paper proposes a cyber data devaluation framework for automated that makes the continued attack vectors expensive to maintain and resultant output to be of negligible value.

David C. Wyld et al. (Eds): NLAI, IBCOM, MLDS, GridCom, SCAI, ICCSEA, SPPR – 2024
pp. 209-219, 2024. - CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.142213

2. LAYERED SECURITY FRAMEWORK WITH ZERO TRUST

Our preventative model comprises of three key areas of security – fraud, cyber and physical security. [Figure. 1]. These form the basis of individual security domains acting as data feeds and the overarching decision engine is named as the "converged security through interdiction services". Traditional financial risk systems have been disparate and have significant data sharing limitations. These are largely due to process and compliance obligations. The ability to process and share information in real time between different security domains such as fraud, cyber and physical security have significant limitations. Each of these domains have their own signalling and alert disposition tools. Additionally , the tools have limitations at channel level and have limited view of the context thereby triggering high false positive rates.Security controls require context and often times they are limited due to legacy systems within channel. These could be due to infrastructure, applications or process fragmentation. This restricts the ability to enforcement controls that balances risk vs client experience. Threat actors take advantage of one channel and its associated processes to infiltrate and inflict financial loss in the other. [2]For example, a call centre control and procedure operating book may not be aware of a digital channel control and associated playbook. Threat actors initiate a simple non-monetary profile change at one channel such as call centre or a branch and trigger a monetary event via another such as digital.

2.1. Proposed Framework

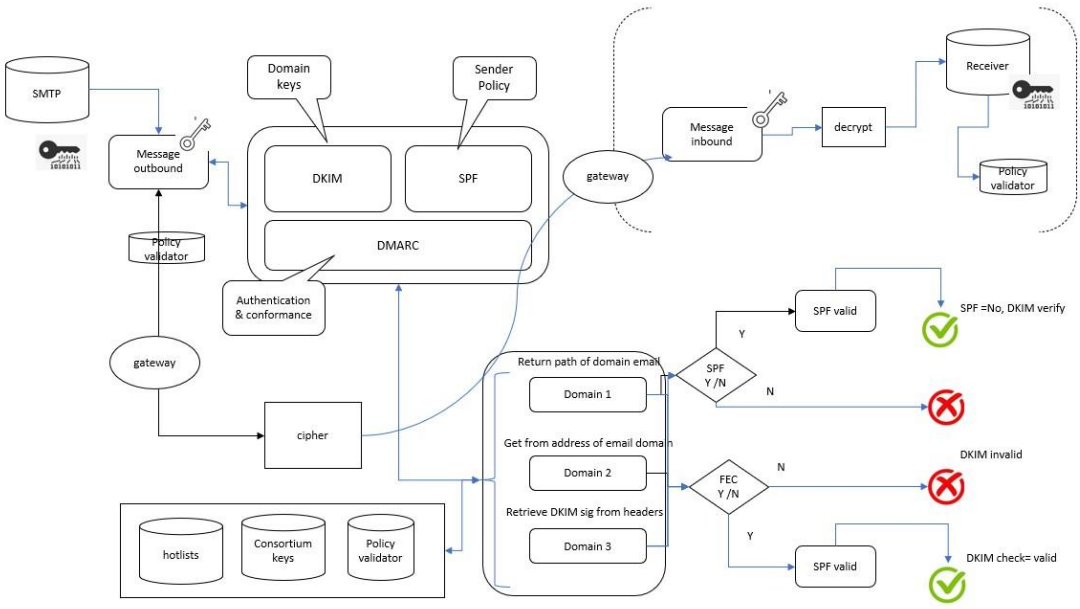


Figure 1. Overall framework to prevent Security gaps in BEC fraud

2.1.1. Ingress Header Validations

Any inbound traffic has a specific pattern when it comes to trusted identity providers. A systemic non-human traffic end point may be demarked with an allow listing framework that can help provide critical attributes at gateway for traffic signatures and associated token introspections. For example, an aggregator traffic that has established a known endpoint on source and shared a public key token can easily be identified and with appropriate routing protocols as opposed to unknown traffic originating from distributed endpoints.

2.1.2. Design Flow for Business Email Compromise Attack Vector

It is estimated that every year there are severe losses related to security gaps related to p2p email comms that have instructions for payments.[2] This is also known as "business email compromise or BEC". We present a simple framework that allows for flagging of such risk related to Bec using the DMARC protocols and process enhancements.

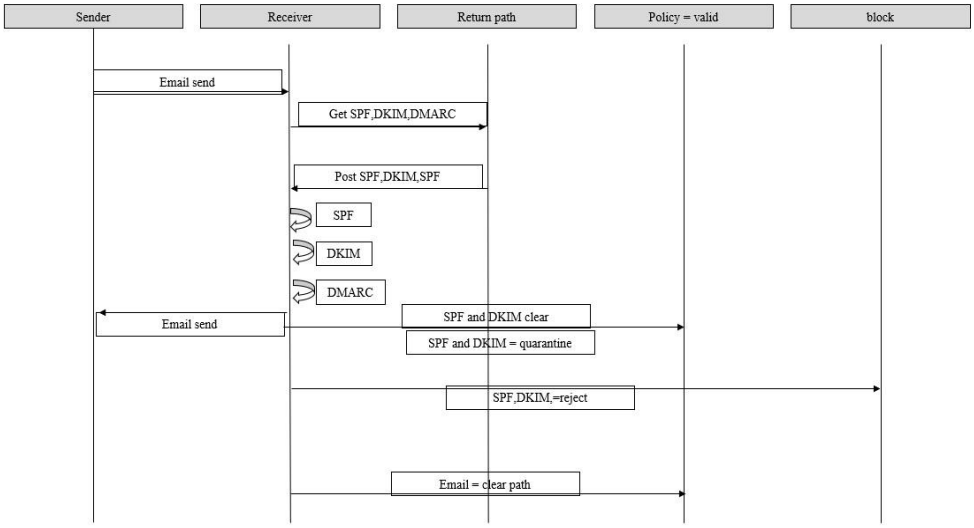


Figure 2. Sequence flow for detecting and preventing BEC security risk

Table 1. Spam traffic sample

Tag	Value	Item
P	DMARC-0	Version
Q	NA	Policy
R	1	Update Db
S	receiver	Update urls and domains

2.1.3. Malware Detection

P1- Perimeter WAF ,P2-Load Balancer, A-Ingress traffic ,A1-Appserver ,A2-Middleware ,F-Fraud Systems, Idv-Identity verification platform, AN- Authentication, AZ-Authorization ,DbDedicated in Memory database

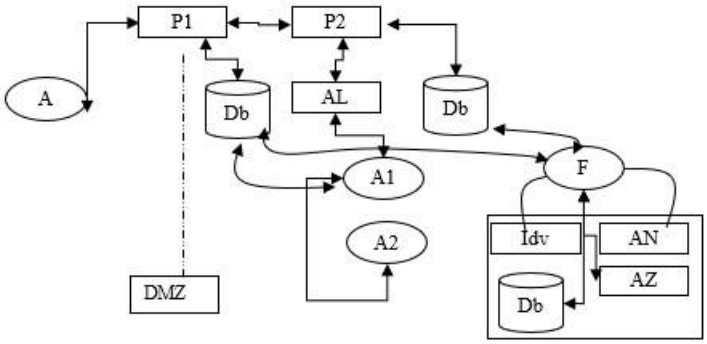


Figure 3. Malware anomalous signals

2.1.4. Operational Challenges and Mitigation

Current financial engines rely on traditional methodologies' when it comes to employing Know your customer aka KYC when it comes to originations. These methods depend on a combination of batch vs real processing or risk attributes. These attributes once aggregated and normalized present a significant pressure to process and disposition applications received for products and services due to compliance and client experience aspects at a minimum. The processing queue as a result get held up due to operational challenges in dispositioning of alerts or leads generated due to false positives.[3].Additionally , the disparate tool sets make it hard to ascertain ingress traffic patterns from a verified and trusted entity vs. traffic originating from an anonymous automated validator endpoints in a distributed eco-system of server farms affecting operational efficiencies and impacting know good clients and meting compliance obligations in maintaining service level agreements aka SLA's.

2.1.5. Data Controls and Privacy

Data that is exchanged via an automated validator needs to be systemically handled via a secure framework such as OAuth 3-legged protocol , so it has the appropriate level of tokenization applied . The data associated with decision systems although may be in one data lake , they have limited proposes to serve for analytics as opposed to real time decisioning and analytics due to governance controls and oversight required. Additionally, the data when it comes to fraud has personally identifiable information which attracts additional controls to protect privacy concerns.[4][6] The financial institutions have an obligation to safeguard users' data from a compliance and privacy standpoint with appropriate consent and disclosure management. Therefore, any such data transfer or sharing should also involve appropriate storage of users consent with provisioning of revocation of corresponding consent tokens.

2.1.6. Token Introspection and Claims Scrubbing at Gateways

The data privacy laws such as GDPR,CAPP etc. [3]. have regulatory requirements such as local vs global movement of data , access controls and also has regulatory and reputation implications in a breach or a cyber-attack. Therefore, it is imperative that organizations must ensure a framework to be able to share anonymized data but in a secured and protected way where no personally identified information is needed. The tokens need to be introspected either in batch or real time mode at multiple levels during egress and any detection of PII data need to be validated against the consent and 3'legged OAuth patterns.[5] The tokens also need to have a predefined

"time to live" definition as applicable, so a data purge can be done in the event of a GDPR /CCPA requirement being sought by the end user.

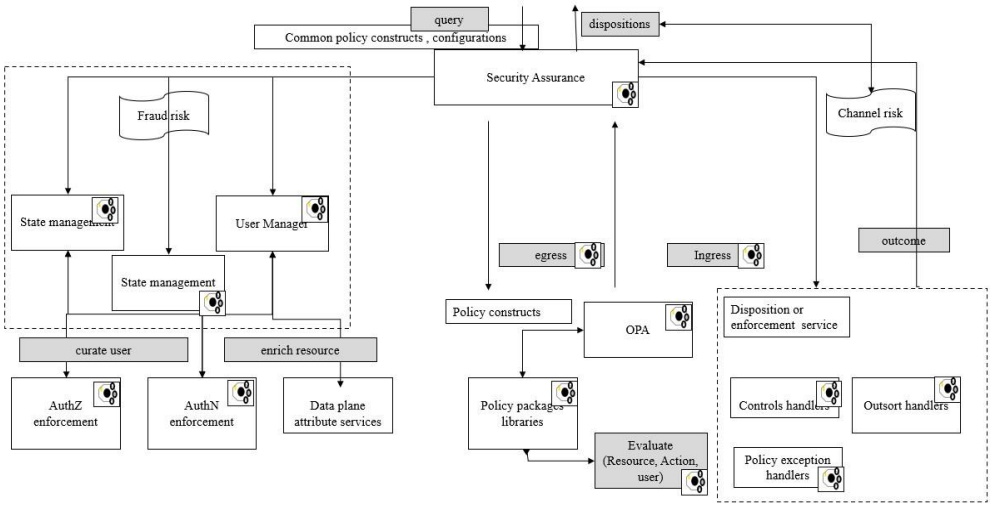


Figure 4. Token authorizations and introspections

2.1.7. Response Playbook

Each Security domain has its toolset and associated decision engines in addition to alert/signal disposition processes. We identify a control wherein a real-time feedback loop of learnings from signal/alert dispositions are factored for preventative controls for future events as a predictive capability. These responses could further be enabled as part of a standard playbook for responding to any attack patterns within the same channels or across multiple channels. Our framework proposes to data mine these variation across channels and aggregates signals to a consolidated queue which can be run through firm's policies for out sort dispositions.

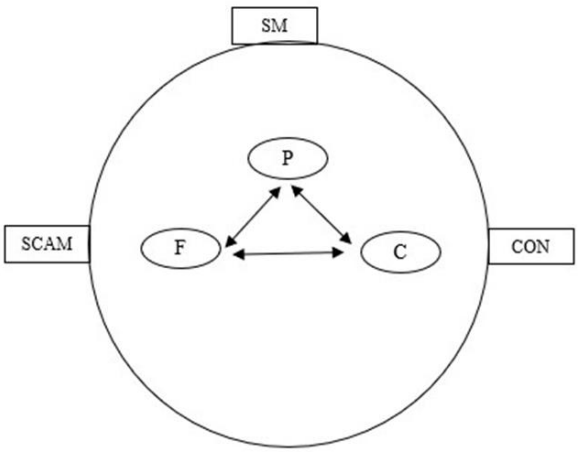


Figure 5. Spam traffic sample

2.1.8. Compliance and Regulatory Obligations

A transaction type , type of fraud or a payment category or payment rails used have corresponding regulatory requirements for institutions to adhere to when it comes to disposition

of customer concern or fraud or cyber event. For example, a Reg E,REG CC [8] or a data loss event have different set of compliance requirements. Threat actors often exploit these to their advantage. An example would be if an electronic card transaction-based fraud is identified, the requirement up to when it may be reported could be more than 60 days after the event. Threat actors file claims and continue to perpetrate fraud using compromised credentials ,account takeover (ATO) while the single of multiple set of claims are pending disposition.

2.2. Authentication

Our framework includes ingesting attribute data tokens as signals from multiple entities such as fraud, cyber, physical security. The framework requires signal inputs from social media trends by using keywords that have in the last 90 days a high frequency occurrence of scams and identified losses with similar attributes and compares to the consortium data in the following 612 months of claims data across multiple financial entities.

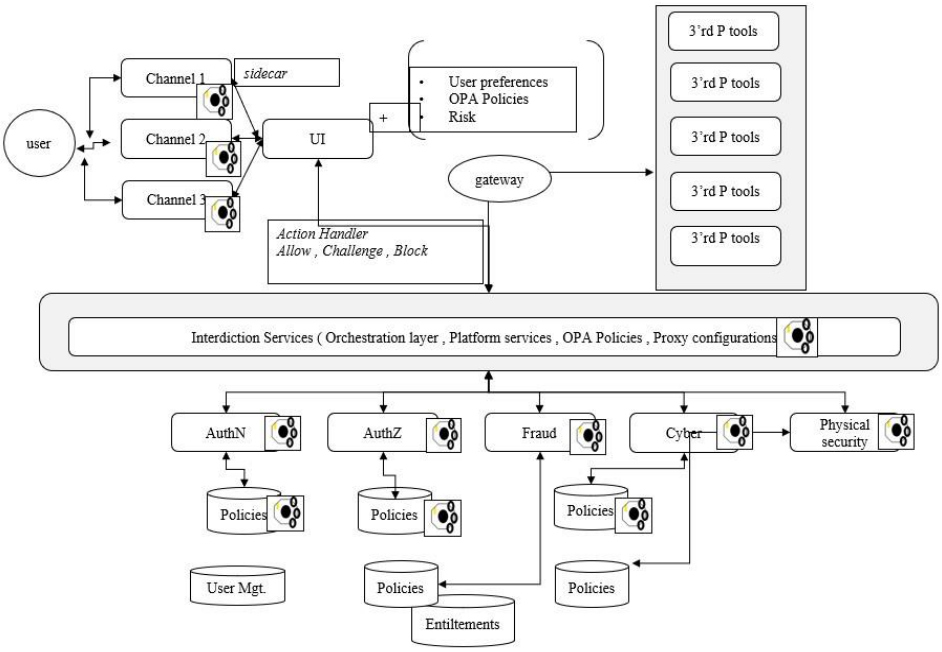


Figure 6. Spam traffic sample

2.3. Multi-Channel Signal Ingestion and Correlation

Our framework includes ingesting attribute data tokens as signals from multiple entities such as fraud, cyber, physical security. The framework requires signal inputs from social media trends by using keywords that have in the last 90 days a high frequency occurrence of scams and identified losses with similar attributes and compares to the consortium data in the following 612 months of claims data across multiple financial entities.[10] Our framework includes ingesting attribute data as signals from multiple entities such as fraud, cyber, physical security. The framework requires signal inputs from social media trends by using keywords that have in the last 90 days a high frequency occurrence of scams and identified losses with similar attributes and compares to the consortium data in the following 6-12 months of claims data across multiple financial entities.

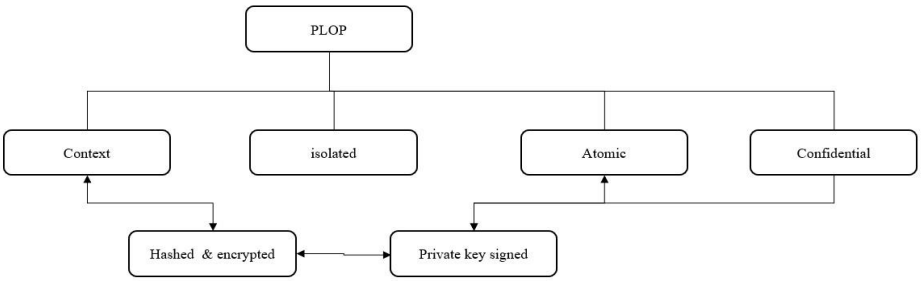


Figure 7. Spam traffic sample

2.4. Non-Human and Systemic Access Controls and Linking

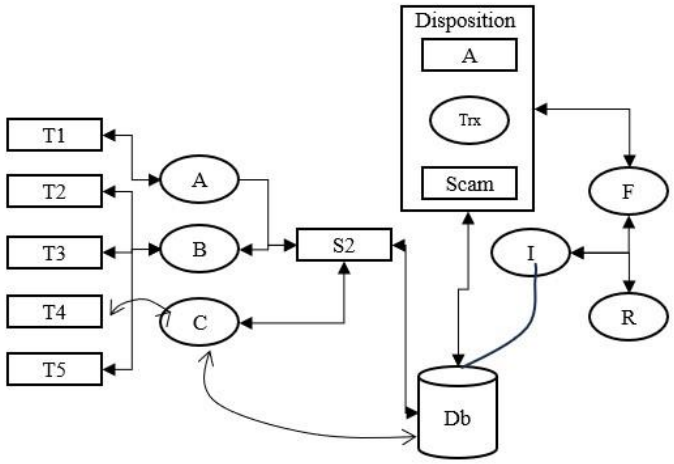
Non -human interactions are deemed to be system-system interactions in the context of our framework such as an API traffic. A common attribute occurrence of user data including meta and personally identifiable information is then mapped to the claims data from the past 12 months. [11A separate model is then created for this specific use case to identify relationship patterns. The relationship is extended recursively to beyond users, systems, applications, and external sites through social media public data mining via their approved interfaces.

2.5. Client Education

Exploits in one channel due to lack of client education and awareness of ongoing scams is considered a standard attack pattern. Therefore, regular communication of ongoing scams , social engineering methodologies, workshops between relationship managers and threat experts is recommended. Limited email communications are recommended that have action associated in the communication content as this often leads to phishing and malware exploits. Incentives for proper security hygiene are often ignored to drive adoption and this is an area where an industry driven approach helps solidify bringing awareness of vulnerabilities. Leveraging law enforcement agencies are recommended to provide legitimacy and confidence towards gaining public trust. This leads to a comprehensive effort that educates that security is best when collaboration is at best. Leveraging law enforcement agencies are recommended to provide legitimacy and confidence towards gaining public trust. This leads to a comprehensive effort that educates that security is best when collaboration is at best. Consortium data sharing control that allows instant broadcast communication through list servers is a new control being recommended. This is a control that needs to be added as must have during onboarding process of account or relationship opening.

2.6. Social Media Data Mining Signals

Our framework includes ingesting attribute data as signals from multiple entities such as fraud, cyber, physical security. The framework requires signal inputs from social media trends by using keywords that have in the last 90 days a high frequency occurrence of scams and identified losses with similar attributes and compares to the consortium data in the following 612 months of claims data across multiple financial entities.



Security domains and categorizations . T1-Social Trend,T2-Identified fraud, T3-Reported Fraud, T4- Context , T5- Reported Loss ,S – Scam, I-Account linking , A- Systems, Trx - Transaction , A- Non-Monetary event , B-Monetary event, C- Collusion , Db- Consortium Database

Figure 8. Spam traffic sample

2.7. Trusted Identity Providers and Allow Listing Techniques

Our preventative model comprises of three key areas of security – fraud, cyber and physical security. These form the basis of individual security domains acting as data feeds and the overarching decision engine is named as the “converged security through interdiction services” .An allow list ensures at the domain level and at application lever who has access to what and would act as an additional layer of fraud prevention or unauthorized access.

2.8. Automated Validators

Security assurance levels are identified based on NIST 800.63 guidelines. Each assurance level has 3 sub levels applied for domains namely- identity , authentication , authorization. The framework allows dynamic elevation of control enforcement where applicable. This allows the interdiction services framework to ascertain 4 areas of form factors . These form factors are inherence, possession ,inference and behaviour. The framework recommends application of controls related to identity assurance levels from 1 to 3 , Authentication assurance levels from 1 to 3 , and Authorization assurance levels from 1 to 3 in the increasing order of assurance. Interdiction services also reserve the right to reverse apply the enforcement via suppression of a control to maintain customer experience and manage risk. Therefore, the security model proposed allows the control enforcement in a dynamic and risk-based methodology.

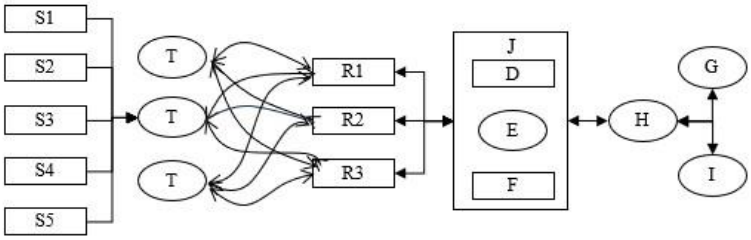


Fig – **X,** Security domains and categorizations . A-Sentiment linking ,B-Endpoint attributes, C-Behavior linking , D- Context , E- Token Introspection ,F- Channel , G – Entity linking ,H-identity , ,I-Account linking , J –Policy , S1- Systems, S2 –Authorization , S3 – Authentication , T1- Bots, T2-Egress Traffic , T3-Automated validators, T4-Ingress traffic , T5- Application traffic

Figure 9. Spam traffic sample

.

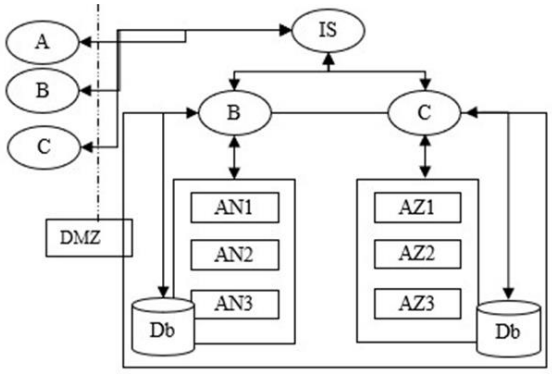


Fig – **X,** Interdiction services . AN Authentication , AN2 – Multifactor Authentication - MFA , AN3- Authenticator Assurance Level ,AZ 1- Authorization method 1 –Role based , AZ 2- Authorization method 2 –Attribute based , AZ 3- Authorization method 3 – Policy based , A – Desktop channel, B-Mobile, C- API channel

Figure 10. Interdiction /Interceptor service

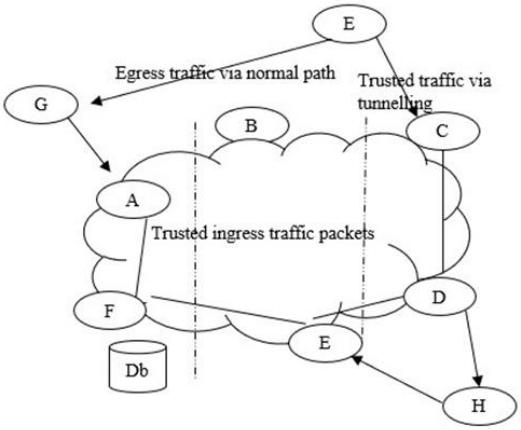


Fig. 11.Converged Security. F- Fraud domain, C- Cyber Domain , P-Physical domain, SCAM – Various scams ,CON-Consortium data ,SM – Various social media.

3. CONCLUSIONS

Proposed security framework addresses multiple areas of challenge in combatting security risks and associated threats. Our framework is unique as it proposes to combine intelligence from multiple security domains while preserving data privacy, integrity concerns. Our framework also is unique in that it allows use case specific models to be enabled that have more of the associated context , this approach allows of better client experience and enabled significant reduction in false positives for alert disposition. The framework also complies with regulatory requirements in the areas of data protection, compliance for fraud. Proposed framework i.e., “Converged security through interdiction services” spans all 3 major domains of security while preserving confidentiality, Integrity and availability.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, just everyone!

REFERENCES

[1] https://docs.sophos.com/central/customer/help/enus/ManageYourProducts/EmailSecurity/EmailSecurityPolicy/EmailImpersProtection/index.html.
[2] https://verafin.com/2024/03/business-email-compromise-a-globalmenace/#:~:text=Nasdaq's%202024%20Global%20Financial%20Crime,number%20at%20%246 .7%20billion%20globally.
[3] https://www.sacmat.org/2023/resource/slides/3_1_1_MeadowsCatherine.pdf
[4] https://www.sacmat.org/2023/resource/slides/3_1_1_MeadowsCatherine.pdf
[5] https://nordlayer.com/learn/zero-trust/benefits/
[6] X. Zhu and Y. Badr, “Identity Management Systems for the Internet of Things: A Survey Towards Blockchain Solutions,” Sensors (Basel, Switzerland), vol. 18, no. 12, pp. 1–18, 2018.
[7] R. Taylor, D. Baron, and D. Schmidt, “The world in 2025 - Predictions for the next ten years,” 2015 10th International Microsystems, Packaging, Assembly and Circuits Technology Conference, IMPACT 2015 - Proceedings, pp. 192–195, 2015.
[8] P. Handy, “Introducing Masked Authenticated Messaging,” 2017. [Online]. Available: https://blog.iota.org/introducing-maskedauthenticated-messaging-e55c1822d50e
[9] A. Gruner, A. Muhle, T. Gayvoronskaya, and C. Meinel, “A Quantifiable Trust Model for Blockchain-Based Identity Management,” in 2018 IEEE International Conference on Internet of Things (iThings), Green Computing and Communications (GreenCom), Cyber, Physical and Social Computing (CPSCom) and Smart Data (SmartData), no. September. IEEE, 7 2018, pp. 1475–1482. [Online]. Available: https://ieeexplore.ieee.org/document/8726703/
[10] Conceptual Foundations for Forming a Configuration Management Subsystem of a
[11] Telecommunications Network ;A. K. Kanaev;E. V. Login;K. A. Pudovkina; 2024 International Russian Smart Industry Conference (SmartIndustryCon) User identity and Access Management trends in IT infrastructure- an overview. Manav A. Thakur, Rahul Gaikwad. 2015 International Conference on Pervasive Computing (ICPC)

AUTHORS

Srinivas Rao is a technology professional currently at university of Los Angeles, California.

Akshay Krishna Kotamraju is founder of a nonprofit organization “think cosmos” aimed at helping students learn more about Astronomy& Programming

©2024 By AIRCC Publishing Corporation. This article is published under the Creative Commons Attribution (CC BY) license.