WHITEPAPER

Convergence of Digital Security and Big Data Analytics

Behavioural Predictive Analytics for Better Cyber Security

Protecting businesses from fraud has forever been the challenge for organizations like Banks, Credit Card Companies, Online Commerce and even Enterprises. Stolen Credit Card Details, Phishing attacks, Leakage of critical client data etc result in username and passwords gradually becoming an obsolete method of protecting users from internet theft. Systems have evolved to add additional layers of authentication such as knowledge based (set of questions), picture based etc but are these enough? Predictive Analytics on Big Data platforms offer a new way of analysing customer behaviour real time to predict the likelihood of fraud. "Machine Learning" allows systems to learn customer behaviour and differentiate between whats genuine and what's not! This can be the basis of either completely blocking the transaction or prompting users additional challenges to confirm the identity of the user.

CHALLENGE

The biggest challenge in online commerce is how to continuously keep pace with ever changing cyber security landscape. On the one side, we have SMS based authentication becoming vulnerable to attacks while on the other side the ability to understand user behaviour getting more complex across a multitude of platforms and channels of customer interaction. The big questions is – as an organization, how does one device a comprehensive security programme that goes beyond traditional internet security and is able to dynamically understand user behaviour to detect risks and frauds? How does one device an authentication framework that is able to adapt to the potential risk and move from vulnerable forms of authentication to more secure ones?

Identity theft has been one of the largest causes of financial losses to Banks. While Phishing attacks, malware etc. continue to exist, newer threats such as ransomware are taking over where customer's computers and therefore data and identity are taken control of and ransom being demanded! Targeted attempts at identity theft also include social engineering where pieces of information from social media profiles help hackers put together the individual's identity and use that for monetary benefits!

Designing an appropriate Security Framework

How does one therefore design a security framework that balances security, cost (both to end customers and the organization) and ease of use? Can the proposed solution work well with the existing IT security policies, architecture and platforms? Can it keep pace with changing internet security paradigm?

If we look at the different methods of authentication, on the one end we have username/passwords while on the other we have Trusted Identities such as Digital Signatures using Public Key Infrastructure issued by Trusted Third Parties such as Governments, Certification Authorities offering highest form of security with benefits of legal non-repudiation.

This leads to the need for design of an authentication system which is simple to use for basic uses – a username/password to login into a news portal while providing the ability to scale to trusted identities or other forms of complex authentication methods for sophisticated uses – fund transfers in Internet Banking. Even within the same Banking platform based on the risk assessment of the transaction and based on customer behaviour systems should evolve from basic to advanced authentication methods.

With Mobile emerging as a significant alternate channel, identity and authentication must be designed keeping in mind the ability to authenticate the next few billion who use a mobile first to do many critical transactions on the internet including e-commerce, banking etc.

SOLUTION

Customer behavioural analytics therefore forms the basis for designing advanced security frameworks. Gone are the days where a rule based system will work to comprehensively to identify changes in user behaviour!

Machine learning tools offer easy and reliable ways to model complex user behaviour. At eMudhra, our advanced analytics frameworks are coupled with our flagship authentication platform – emAS (eMudhra authentication server).

emAS considers several parameters that are configurable to predict the likelihood of deviation which include:

Device and Client context

- Device Information – Operating System, Browser Configuration, MAC Address, Locale
- Location Information – IP Address.
- Date and Time Information
- Client Context – Keystrokes, Usage of delete, backspace and time taken between keystrokes.

User Behaviour

- Transaction Data – Ability to model transaction data as a parameter. In case of Banking, this could be value and category of transaction and the pipe through which it goes through.

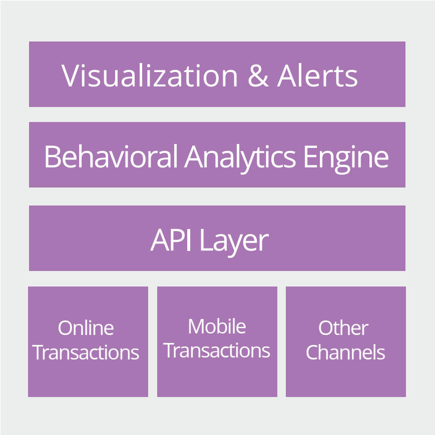
Relational Parameters

- Through a graph database, relationships between entities are modelled in a way to identity two or more people that share the same address or phone number. Using this, emAS derives the ability to model complex frauds For ex - where multiple users are acting at the same time to withdraw funds at multiple locations from an ATM.

USING MACHINE LEARNING

Machine learning allows learning of complex fraudulent patterns using all features in a Big Data scenario. The biggest benefit is that Machine Learning can quickly adapt to changing distribution as fraud evolves.

Anomaly Detection using Unsupervised Machine Learning allows continuous modelling based on purely client side parameters that can on a real time basis detect deviations in user behaviour – change in location, keystroke time for entering the password longer than usual etc. This can be used to define rules about prompting for additional layers of authentication or completely blocking the request.



Rules Engine as an overlay

While Machine Learning allows modelling complex user behaviour, a Rules Engine as an overlay to the model allows quick and effective capture of known deviations. emAS allows the usage of both Machine Learning and Rules Engine following a 3 step process to effectively reduce number of false positives.

- Rules Engine - for known deviations such as change in location within a time period.
- Supervised Machine Learning – based on existing deviations/fraud instances in transaction data.
- Unsupervised Machine Learning – Anomaly detection using client side parameters.

This allows for a completely flexible deployment of emAS authentication suite across a host of applications in Enterprise Risk Modelling or in Financial Institutions across all channels of customer interactions.

emAS as a universal plug and play server

emAS is designed as a cross-platform universal plug and play authentication server and has been quickly deployed in several large Banks and Enterprises.

Use cases

emAS can be deployed in a variety of use case scenario both in Enterprise as well as Banking advanced authentication using behavioural analytics.

Enterprise Risk Authentication – With a host of applications moving to the cloud, enterprises invariable have hybrid enterprise/cloud implementations with critical Client/IP data on the cloud. The complexity as a result of geographical spread and users traveling results in potential vulnerabilities of identity theft where a competitor can gain access to sales pipelines or IP data. emAS helps in identifying deviations in user behaviour and allows blocking of access to the data while sending real time alerts to users/administrators so that quick remediation measures can be implemented.

Risk Authentication in Financial Institutions – emAs allows creation of an integrated database of risk score across multi-channel customer communication such as Online, Mobile, Fund Transfers through Wire or NACH. emAS then uses this data to understand behaviour patterns and anomalies using machine learning and assigns a risk score for each client. This allows for creation of a multi layered security framework for each user based on their risk scores with alerts sent to users/administrators for any deviations.

ABOUT THE AUTHOR

Mr.Sai Prasad brings 14 years of experience in the information security domain & also contributed to product innovation in PKI. Sai is also working towards acceptance and adoption of digital signatures in various industries & businesses.