Twitter

MOHAMMAD IDREES

BITM-F19-096

December 7, 2022

Contents

Twitter

Twitter, a web-based social media platform presented in 2006, it was point of fact perhaps of the most well-known social medium stages currently being used, with 100 million normal dynamic clients and 500 million tweets refreshed every day. Twitter can be utilized to watch out for conspicuous hotshots, stay in contact with secondary school buddies, and get everyday news. But its popularity might be scary, Twitter is appreciatively quite easy to use. We'll see what Twitter is, who uses it, and in what way to start using it right away and its security features.

WHAT IS TWITTER

Co-founder of Twitter Jack Dorsey had an billion Dollar idea in 2006, he built an SMS-based messaging system that permitted friends to get in touch by posting statuses and uploading tweets. Twitter was originally considered as an idea very similar to texting. The concept transformed, in large part as a result of suggestive of meetings with Evan Williams, Dorsey's co-founder. Jack made the first tweet on March 21, 2006, with the message of "just setting up my twitter...". More than sixty thousands tweets were sent during the 2007 South by Southwest Interactive conference, which saw Twitter's exponential potential. The Twitter bunch involved the gathering as a chance to begin expanding their client base. The 140 person limit was first set by Portable Sim administrators, not Twitter, as Twitter started as a SMS-based site. They decided to keep up with the impediment as Twitter developed into a web stage since it means to deliver exceptionally skimmable substance for our tech-weighty, consideration shortage present day world. In the decade earlier, Twitter has acquired remarkable advancement. Its last objective is to rapidly convey data, some of which might be serious (like when Iranian nonconformists utilized Twitter to collect walks). In various viewpoints, Twitter is a product as administration with unending planned and reason. It can unite you to your kinsman as fast as it can associate you with someone in Thailand. You can choose to follow update sources, superstars, comics, business influential, or pals in your area. Twitter has efficiently established a very addictive platform by letting each user to modify their content to their distinct preferences and interests.

USE OF TWITTER?

Twitter is a social media network platform with the foremost achievement of joining users and allowing them to show their ideas to a hefty spectators. Consumers can follow people or businesses who share content they enjoy understanding, study about the greatest summary and proceedings trendy right now, or just use Twitter to join with pals. PR organizations and marketers likewise use Twitter to involve their consumers and increase brand awareness

Twitter for Marketers

Twitter may be a useful device for developing you're following and giving individuals something quick to peruse prior to becoming clients. As far as possible can assist you with composing compact and charming adverts, for example, those that notice online courses your business is facilitating or connections to free digital books. You can utilize Twitter to fabricate genuine associations with your objective socioeconomics. You can "like" or "retweet" a remark in the event that it talks about one of your items or contributions. Subsequently, in the event that a client tweets a grumbling about your administration, you might reach out to them and fix the issue immediately. Twitter is a social networking site whose major goal is to link users and give them a platform to share their opinions with a large audience. Users can follow people or industries who post content they enjoy interpretation, learn about the greatest news and proceedings trendy right now, or just use Twitter to attach with pals. PR groups and marketers can also use Twitter to involve their audiences and raise brand mindfulness.

Twitter as a News Source:

Twitter is sometimes even faster than traditional media channels at breaking news dissemination, hence it is frequently used for this purpose. For instance, before many media outlets had learned about the United states Airways plane crash-landing on the bank of Hudson River in 2009, Janis Krum's was one of the first to share the news on Twitter: As a reporter, you may shape a substantial audience by tweeting concise summaries to inform

your audience of everyday incidences. Twitter is often a good resource when looking for insider info or direct quotes to utilize for an article because numerous stars, sportspersons, and representatives choose to post on their rather than via media sources when they need to share info with their followers.

PHYSICAL SECURITY:

What is Physical Security?

Physical security is protection of persons, tools, networks, and information from physical acts and events that could outcome in noteworthy financial loss or other harm to an industry, government agency, or academic institution. This shields protection against stealing, theft, damage, terrorism, fire, flood, and other natural disasters. While many of these are protected, physical safety line up damage anticipation in order to stop the time, money, and capital lost as a consequence of these disasters. Access control, surveillance, and testing make up the physical security framework's three key components. How well each of these components is implemented, improved, and maintained consistently affects how effective a physical security program is for an organization. Physical security or digital safety are progressively interlinking, when conventionally they were two different fields. Access control and monitoring systems preserve digital logs, investigation systems are becoming supplementary with internet-connected, and use cases for artificial intelligence in physical security are becoming more and more prevalent. For instance, Video surveillance image verification can alert you to approaching people or vehicles. With more sophisticated systems, you might be able to detect an unauthorized visitor or an employee who is in a security zone by using facial or even walk identification across whole facilities. Access controls that are combined with behavior and personality can alert you to unusual behavior. Drone manufacturers are increasingly striving to incorporate automated, unmanned capabilities as businesses start using drones to monitor

their operations. Over the next five years, investments in physical security might "dominate" AI-based video analytics, according to Memoori study.

PHYSCIAL SECURITY OF TWITTER

Twitter data centers are built with security in mind. Twitter claims to never sell or distribute their custom-built servers outside of their own data centers. In addition, Twitter facilities are among the safest places for user data to reside thanks to the 24/7 worldwide efforts of industry-leading security staff. Twitter business continuity and catastrophe recovery plans are also quite strong. For instance, they instantly and easily switch data access to a different data centre in the case of a fire or any other disturbance to ensure that users can continue working without interruption. Even in the case of a power outage, data centers are kept running by emergency backup generators. Twitter data centers' ISO 22301:2019 certification serves as evidence of their continued dedication to business continuity. In its place of keeping each user's information on a lone computer or collection of computers, Twitter scatter all data, including their personal, over many computers in numerous place. The information is then divided up and simulated across numerous systems to stop a single point of failure. As an extra safety safeguard, they give these data portions random names that are incoherent to the naked eye. Twitter server's routinely backup important information while users are working. You can therefore continue using your computer right away if a coincidence happens, such as a computer failure or theft. Last but not least, twitter sensibly monitor individually hard drive's site and state in data centers. To stop illegal access to the information on hard drives that have touched the end of their valuable lives, they destroy them thoroughly or in several step. Multiple security measures are in place to protect Twitter's user's data centers and protector against unwanted entree to information. They privilege to make use of biometric verification, extensive camera coverage, secure perimeter protection systems, and a safety force on responsibility around-the-clock. At Twitter data centers, they also implement a constricted access and safety policy and make sure that each worker has conventional security awareness training. Additionally, they have local security operations centers that shelter complete fleet of information centers. These SOCs incessantly track native and universal proceedings that can have an influence on how twitter's data centers function and

display alerts at all of our sites. To make sure they're always prepared to reply to any disaster, the teams also conduct a solid enterprise danger management program in addition to routine testing to proactively classify and decrease any hazards to the data centers. Twitter started providing phishing-resistant security keys to its staff and demanding that their teams utilize them as an additional security measure. With tremendous success, Twitter two step authentication is applied to place in 2017. All new hires at Twitter were obliged to complete security, privacy, and data protection trainings. In addition, mandatory training courses on how to avoid becoming phishing targets for attackers were required for those with access to non-public data. The business added that it has been enhancing its internal detection and monitoring capabilities, which warn it of potential unwanted access.

PERSONAL SECURITY:

The methods and best practices used to safeguard your privacy, data, and gadgets against unwanted access and harmful cyberattacks called personal security. The three pillars that make up personal security may come to mind:

i. Online Privacy
ii. Data protection
iii. Device Security

Online Privacy:

You may imagine that one of the key components of the most exquisite personal cybersecurity dessert is your online privacy. Hackers may ruin the credit history you worked so hard to earn if they gained access to details like credit card and banking information stored online. They might even sell this information to other cybercriminals on the dark web. Additionally, everyone should be aware of how to safeguard themselves against these cybersecurity threats given that almost 10 million people have their identities stolen annually. Former or current workers, contractors, or business partners are the sources of insider threats. They might abuse their access

or inside information to hurt our customers, employees, property, or reputation. The goal of personnel security is to lower the risks brought on by insider threats. Any person who intentionally or unintentionally undermines the safety of their association or New Zealand by engaging in surveillance, violence, the illegal revelation of information, or the loss or depletion of a resource is considered an "insider threat" or "insider" (or capability). Common insider acts are:

Fraud or procedural corruption brought on by the unauthorized revelation of public, private, or proprietary information. Theft, assault, or physical harm to others. Unauthorized access to ICT systems. Economic or industrial espionage. Many security lapses are inadvertent and happen because people are unaware of or pay little attention to security procedures, are preoccupied, or are tricked into unintentionally helping a third party.

Personal Security of Twitter:

Protects your account from phishing:

Every day, Twitter stops more than 100 million phishing attempts. However, even the savviest users might be duped by sophisticated phishing techniques into providing their sign-in information to hackers. When using Advanced Protection, user must sign in to your Twitter Account using a security key to confirm your identity. Without your username and password, unauthorized users cannot sign in.

Provides extra protection from harmful Content:

Twitter's Safe Browsing shields 4 billion devices from dangerous links, while Advanced Protection does even more thorough checks before each Tweet. It alerts you to potentially hazardous files and may even stop you from accessing them.

Keeps your personal information secure:

You are frequently prompted to grant access to your Twitter Account data, such as your contacts, location, or Gallery, when you join up for new apps or services ,instead of giving all information Twitter ask the users which

information they want to give to particular application for signup. Twitter Accounts have built-in security features that verify more than 40 million saved passwords daily for breaches. However, some attackers have the ability to pose as an authorized third party in order to access information.

Twitter provides these services to safeguard the personal security:

- *1: **Never reveal your password to anyone!***

  No one from Twitter will ever request your password. To assist you, they don't require it.

- *2: **Please review your privacy settings.***

  To control who can send you messages, access your Stories, or view your location on Map, check your privacy settings.

- *3: **Pick a Secure Password***

  Don't use personal information in your password, such as your name, username, phone number, or birthdate, and choose a password that is at least 8 characters long. Your password should be a mixture of numbers, symbols, capital, and letters. Don't divulge your password to anyone and refrain from using it on other websites or apps.

- ***4: Verify both your email and phone number**:*

  Check the Twitter settings to make sure the email address and mobile number linked to your account are correct.

- ***5: Configure Two-Factor Authentication.***

  For added security, you can use two-factor authentication to confirm that you are the one logging into your Twitter account. This increases the security of your account.

OPERATION SECURITY:

WHAT IS OPERATION SECURITY?

Operational security is security and threat supervision method that guards against uninvited access to vital information. OPSEC can also be used as a means to catch seemingly innocent behaviors that unintentionally reveal sensitive information to a hacker. IT and safety experts are motivated by OPSEC to examine their systems and work frameworks from the perspective of a potential attacker. It is both a method and an approach. It performs the best in terms of security and protects against analytical activities and measures like social media and behavioral checking. One essential element of OPSEC is the use of risk management to identify potential hazards and faults in corporate operations, operational events, and the software and hardware that staff members use.

How OPSEC came into picture

A U.S. military outfit known as Purple Dragon was instrumental in the creation of OPSEC in during Vietnam War. The U.S.'s adversaries might anticipate the surveillance team's ideas and tactics if they are unable to decrypt their conversations or lack the intelligence assets necessary to steal their data. They concluded that the American military men were actually passing intelligence to their foe. Purple Dragon, who gave the first OPSEC definition, said it was "the capacity to keep information of our strengths and weaknesses hidden from hostile forces." Other government organizations, including the Department of Defense, have now adopted this OPSEC procedure in their initiatives to safeguard trade secrets and national security. Additionally, it aids businesses in addressing corporate espionage, information security, and risk management by helping them handle the need to protect consumer data.

OPERATION SECURITY IN TWITTER

Vulnerability management:

Twitter's vulnerability management methodology constantly scans for security risks using a variety of available commercially as well as internally created tools, vigorous automated and manual penetration efforts, quality control procedures, software security assessments, and outside audits. The vulnerability team keeps records, assigns an owner to, and prioritizes newly discovered vulnerabilities according to their severity. The team keeps track of every problem and follows up repeatedly until they can say with certainty that it has been fixed. Twitter maintains contact and engages in regular discussion with the security research community in order to track identified issues with Twitter services and open-source tools.

Malware prevention:

A malware assault that is successful may compromise accounts, steal data, and even gain additional network access. Twitter takes the dangers to its networks and users extremely seriously, thus it uses a variety of methods to prevent, detect, and remove malware. Through malicious sites or attachments, harmful software is downloaded on users' computers with the aim of stealing personal information, committing identity fraud, or attacking other networks. When visitors browse these websites, hijacking software is secretly downloaded onto their machines. Twitter examines its search index for sites that could be used as conduits for malware or phishing as the first step in its anti-malware approach. Our attachment malware scanner, which scans more than 900 million Tweets a week to block malicious content, is another one of our major defenses. The 63% of harmful documents that we block change daily. We recently incorporated a new generation of document scanners that use deep learning to enhance our detection abilities in order to keep ahead of this continuously changing danger. Twitter's protected browsing innovation safeguards in excess of 100 million gadgets consistently. Huge number of new dangerous connections are found consistently by Safe Perusing, a considerable lot of which are real sites that have been compromised. We show alarms on Twitter's Hunt and in internet browsers when we track down perilous destinations.

Monitoring

Internal network activity, user input on systems, and outside knowledge of weaknesses are the key data sources for Twitter's safety monitoring software. External traffic is inspected for unusual behavior at numerous points in Twitter global network, including the presence of information that might indicate connection to bots, utilizing a combination of open-source and the tools for traffic collection and parsing. We advance this analysis method by employing a tailored correlations method based on Twitter technologies and by scanning logs for unusual activity, such as efforts to obtain consumer data. Twitter security engineers actively examine incoming security reports, keep an eye on public mailing lists, blogs, and wikis, and establish standing search alerts on public data repositories to seek for security issues that could harm the company's infrastructure. Automated system log analysis is used in conjunction with automated network analysis to identify potential unknown threats and escalate them to twitter security staff.

Incident management:

Incident management is a key part of Twitter's complete privacy and security approach. They follow a rigid process to deal with data incidents. Occurrence the board is a vital piece of Twitter's finished protection and security approach. They follow an unbending interaction to manage information occurrences. This cycle spreads out the means that ought to be taken in case of any potential entanglements that could think twice about secrecy, exactness, or availability of client information. It additionally portrays alleviation, arrangement, and revealing measures. Twitter's occurrence reaction framework is managed by groups of gifted episode responders from an assortment of expert areas to guarantee that every response is fittingly focused on to the issues raised by every occasion. To guarantee that every response is fittingly fit to the issues presented by every event, groups of prepared occasion responders from a few expert areas screen Twitter's episode reaction plan. These groups' topic experts partake in different ways. Episode chiefs evaluate the occurrence's tendency and co - ordinate the episode the executives, which incorporates finishing up the emergency appraisal, changing the episode's seriousness as required, and actuating the important episode reaction group with the essential functional/specialized leads who

survey current realities and distinguish basic regions that require request. As a feature of the goal cycle, the PC criminology group screens for dynamic assaults and directs legal examinations. Item designs endeavor to limit the adverse consequences on clients and proposition fixes for the defective item (s). The legitimate group communicates with policing government specialists, gives lawful counsel, and works with individuals from the important security and protection group to execute Twitter's arrangement for proof gathering. Support staff individuals screen client warnings and answer client questions, concerns, and demands for additional data and backing.

Communication Security:

Communications security (COMSEC) is the act of prevention of unapproved admittance to media communications traffic or to any composed data that is sent or moved. Its objective is to protect the transfer of classified and unclassified DOD information that has not been authorized for public release while preserving its availability, secrecy, and integrity. It is utilized for analogue and digital applications, wired and wireless lines, and secures voice, video, and data transmission on military communications networks. COMSEC consists of:

- Crypto safety
- Transmission Safety
- Emission safety
- Physical safety of COMSEC

Objectives of COMSEC

1: Information sent by the DOD must be safeguarded using COMSEC procedures.

2: The techniques that have been approved must be used for the development, acquisition, operation, maintenance, and disposal of COMSEC materials.

3: It is necessary to design and maintain a program to guarantee the operational readiness of frequently used COMSEC equipment during emergencies or disasters.

4: COMSEC hardware must be interoperable with key management systems that have received DOD approval. The COMSEC Material Control System (CMCS), a comparable material control system, or a combination of the two must be used to track controlled cryptographic items (CCI) in a way that ensures responsibility and visibility.

COMSEC in Twitter:

With chat abilities, you can send messages through versatile information and Wi-Fi, share records and high-goal photographs, see when somebody is composing, and see when messages have been perused. The Rich Correspondence Administration (RCS) convention, a transporter interchanges industry standard, is utilized when you use talk highlights to communicate messages. Before messages might be communicated through RCS, talk abilities should be empowered for every member in the discussion. If not, you can send messages using SMS or MMS. Chat services could be provided by your RCS service provider, which could be Jibe Mobile from Twitter or your phone carrier.

Network Security

Network security is important for defense of client information and data, maintaining the security of collective data, promising reliable network presentation, and defensive in contradiction of online threats. An actual network security clarification drops overhead expenses and defends businesses from noteworthy losses brought on by a data crack or other security event. Safeguarding appropriate entree to systems, applications, and information eases company processes and customer facility.

How network security work?

There are numerous coats to study when managing network security throughout a company. Assaults can occur at any level due to the concept of network safety layers; as a result, your information security hardware, software,

and policies must be built to target each region. Network security frequently involves the employment of organizational, technological, and physical safeguards. Below is a brief description of the main network security methods and how each control works.

Physical Network Security:

Network hardware like routers and cable cabinets are required to be physically protected from unauthorized employees by physical security measures. Any firm must have controlled access using locks, biometric identification, and other technology.

Technical Network Security:

Technical security tools protect data that is stored on the network or that is being transferred across, into, or out of the system. Systems and data need to be secured against both unauthorized users and malicious employee behavior. Both fronts need to be protected.

Administrative Network Security:

Safety events and rules that control user behavior, such as how employers are confirmed, what level of admission they have, and how IT function members update the structure, make up managerial safety controls.

Network Security of Twitter:

Twitter Cloud has enhanced its Private Service Connect product, which connects groups, projects, and other organizations over encrypted links, on the networking front. PSC now has routing, telemetry, and security based on Layer 7 to guarantee uniform policy control throughout the service. According to Sambi, it also supports connecting on-premises sites to other PSC endpoints via Twitter Cloud's highly available, low-latency connection service, Cloud Interconnect. Confluent, Data bricks, DataStax, Grafana, and Neo4J all offer managed data and analytical services that are integrated with PSC. According to Sambi, PSC prevents customer network traffic from

accessing the open internet by routing it only through Twitter's backbone network. Customers use PSC endpoints with private IP addresses on Twitter Virtual Private Cloud (VPC) networks to connect to Twitter Cloud. Twitter has expanded its centralized Network Intelligence Center to include network management. The platform's Network Analyzer, which learns and keeps track of customer networks to find errors and alterations in network topology, firewall rules, routes, load balancers, and connectivity to services and applications, the business claimed, is now available. Performance Dashboard, one of the new features of Network Intelligence Center, offers visibility into latency measures for Twitter Cloud-to-internet traffic at the project and global levels. According to Sambi, this aids in the planning of the overall network architecture and the placement of customer Twitter Cloud resources. Cloud Firewall Essentials and Cloud Firewall Standard, two tiers of the company's Cloud Firewall service, were on display. Expanded policy objects for firewall rules are provided by Cloud Firewall Standard, which is intended to make configuration and micro-segmentation easier. The new entry-level firewall capability is called Cloud Firewall Essentials. It has built-in IAM [identification and access management] controls that can be applied across VPCs and supports batch-rule updates. It also has global and regional network firewall policies. Scalable micro-segmentation policies that follow workloads wherever they are placed are made possible by new IAM-governed Tags.

Information Security:

Information security refers to the procedures and techniques used by businesses to protect their customer's data (or InfoSec). Setting up security measures to prevent unauthorized people from accessing sensitive data is part of this. Information security is an ever-expanding and dynamic discipline that covers a wide range of problems, including network and infrastructure safety, testing, and checking (InfoSec). Information security shields delicate data from unauthorized actions like scrutiny, change, recording, disruption, or destruction. The goal is to ensure

the security and privacy of sensitive data, such as customer account information, financial information, and intellectual property. Security events can result in data loss, data manipulation, and theft of private information.. Attacks can cost money, damage a company's reputation, and hinder corporate operations. Businesses must budget for security and ensure that they are equipped to thwart threats like phishing, malware, viruses, malicious insiders, and ransomware. Attacks can hinder company operations, damage their reputation, and cost money. Businesses must budget for security and ensure that they are equipped to thwart threats like phishing, malware, viruses, malicious insiders, and ransomware.

Information Security in Twitter:

While in transit, encryption keeps data private and secure. Twitter services are more secure and private thanks to encryption. The data user generate moves between user device, Twitter services, and Twitter's data centers. When user send tweet, share videos, browse the web, or store photos. Twitter use this data is protected by numerous layers of protection, including modern encryption techniques like HTTPS and Transport Layer Security. If we notice anything that we believe you should be aware of, such as a strange login or a harmful website, file, or program, Twitter will alert you right away. They'll also provide you advice on how to improve your security. For instance, on Twitter it will alert you if someone signs into your account from a device that isn't connected to you or before you download an attachment that might compromise your security. You may secure your account with just one click by receiving a notification when we find something suspect in your account in your inbox or on your phone. Ads that include malware, obstructing the material you're trying to see, promoting fake items, or otherwise violate our advertising policy may have an adverse effect on your online experience and risk your security, we treat this issue seriously. Through a combination of real reviewers and advanced automation, we successfully block billions of undesirable ads annually - approximately 100 each second. We also provide you with the means to block certain types of adverts and report objectionable ones. And to ensure that everyone utilizes the internet safely, we appears to be growing our knowledge and best practices. We operate one of the reliable and safest cloud infrastructures in the world, complete with specialized data centers and private underwater cables

that transmit data across continents. It is regularly monitored to keep your data accessible and safe. In the event of a disruption, platform operations can also be moved automatically and instantly from one facility to another, allowing them to continue without interruption. Accounts provide helpful, personalized services, but logging in is the biggest security risk currently present. Millions of credentials are exposed every day as a result of data breaches, endangering your personal details. You may sign quickly and safely.

Security and Risk Management

To reduce misconfigurations, reduce risk, and improve security readiness, Twitter's Risk Manager Tool scans your workloads on Twitter Cloud provides preventative security advice. To help you continuously understand your security risk posture and determine where to focus your security investments, Risk Manager creates a report that acts as an indicator of your security baseline. Obtain a Risk Manager report with identified risks against the CIS Benchmark, which is the industry standard. The report can be sent directly from the UI to the insurance z companies Allianz Global Corporate & Specialty (AGCS) and Munich Re in order to ascertain their underwriting eligibility for Cloud Protection +, a cyber-insurance plan created just for users of Twitter Cloud.

How to manage risks on Twitter?

- Understand what information they have on you.
- Do not use Twitter to sign into other accounts
- Avoid the suspicious link

Security Architecture

A detailed security design known as security architecture takes into account both the needs and potential dangers of a given situation or environment. It also explains when and how to implement security controls. Often, the design process can be repeated. Clear design principles are identified by security architecture, and detailed security control specifications are frequently defined in other documents. System architecture is a term used to describe a design that addresses the connections in between components as well as its structure.

- Threat management
- Benchmarking the good practice
- Monetary
- Lawful and regulatory

Twitter uses the widely used SHA-256 secure hashing algorithm, which is a standard in fields like online banking. Twitter uses a secure way which is called Hashing, A "hashing algorithm" is a one-way mathematical operation that yields a text's non-reversible, fixed-length fingerprint. The "message digest"—basically a fingerprint of the original data—is always produced when the same hashing technique is applied to a text string. It is not possible to reverse this fingerprint back to its original value using any mathematical operation or "key."

Every Twitter user's "hash" values are already calculated by Twitter. Your list of hashes is compared to previously computed hashes when your data is sent to the servers. The Twitter user is added to a custom audience that is kept in advertisements account if a matching hash is discovered. They just disregard a specified hash if there is no match for it. Twitter is aware that you wish to target the users who have been matched with advertising, but it is unaware of your relationship with these users (such as whether they are prospects or customers).

Cryptography:

By using programs, cryptography is a method for encrypting information and communications to safeguard that only the projected spectators can read and understand it. In PC designing, the expression "cryptography" connects with safe correspondence and data moves toward that utilization determined ideas and a course of action of computations in light of directions, or "calculations," to change messages in manners that are hard to peruse. These deterministic cycles are utilized in the arrangement of cryptographic keys, advanced signature, web based perusing on the web, and individual correspondences like email and exchanges with credit cards.

Cryptography Algos:

Cryptosystems encryption and unscramble data utilizing an assortment of methods called cryptographic calculations, or codes, to encoded correspondence between PC organizations, devices, and applications. A code suite utilizes three unique calculations: one is for encryption, one for verification plan, and one for key trade. This methodology, which is done utilizing conventions that are incorporated into programming and executed by organized PC frameworks and working frameworks (OSes), involves:. This procedure, which is carried out using protocols that are built into software and executed by networked computer systems and operating systems (OSes), entails:

- Public and private key for encryption
- Digital signing and authentication for information
- Key exchange

Encryption Types:

Right now, symmetric and asymmetric encryption are the two sorts of encryption generally normally utilized. Whether a similar key is utilized for encryption and decoding gives the expression its name.

Symmetric Key:

A same key is used for encryption and decryption in symmetric encryption. Consequently, it is significant to consider a protected way while moving the critical between both the beneficiary and the source.

Asymmetric Key:

A pair of keys is used in asymmetric encryption; a distinct key is used to encrypt and decryption. Typically, one of the keys is referred to as the confidential key, and the other is known as the public key. The proprietor takes the confidential key confidential, while the endorsed collectors or general society overall approach the public key. Simply the proper confidential key can be utilized to decode information that has been encoded utilizing the beneficiary's public key. Subsequently, information moves can be made without stressing over unapproved or unlawful access.

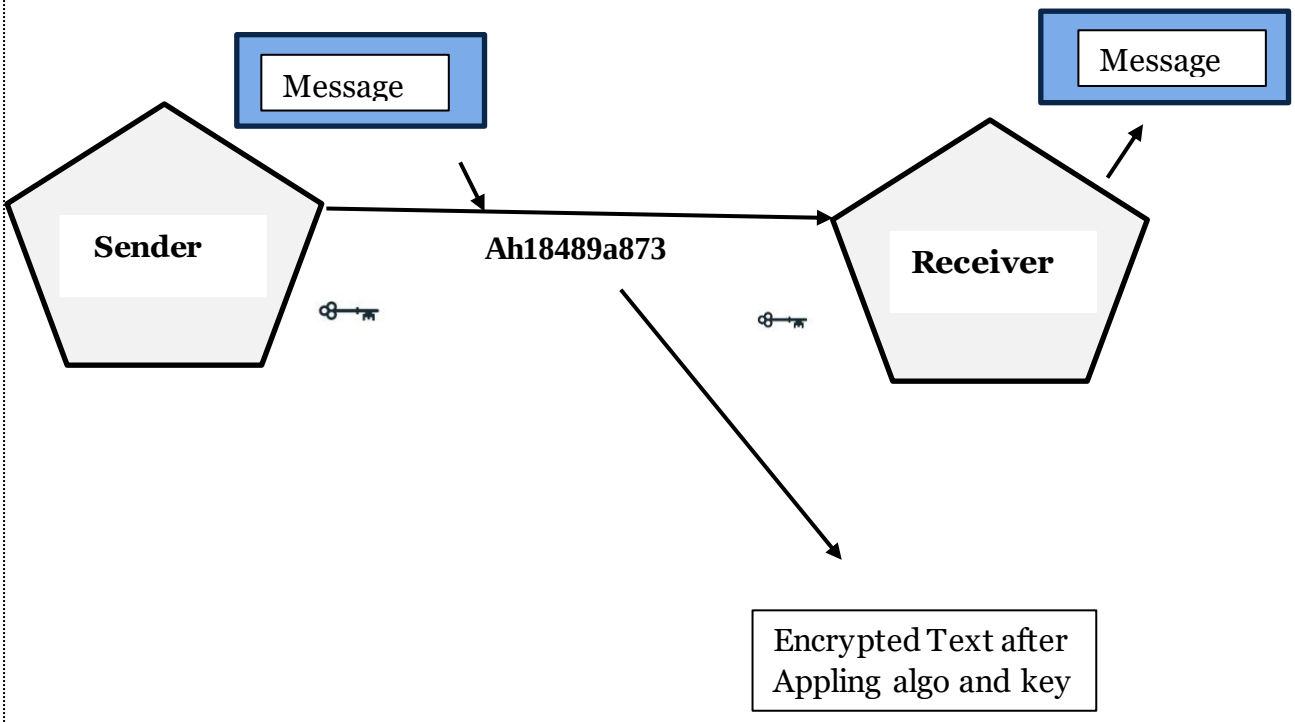
Encryption in Twitter:

End-to-end encryption wants to make sure that texts are encrypted before they end up leaving the sender and are decrypted to enable reading at the recipient end. The two or more parties must employ a cryptographic pair of keys to encrypt and decrypt the content of their messages in order for this to function. In the majority of E2EE systems, the sender encrypts their communication using their secret key and the recipient decrypts it using their cryptographically signed public key. Since Wong refers to a "conversation key" in the context of Twitter, the E2EE solution there may be "symmetric," indicating that both participants in a chat utilize the very same key for encryption and decryption. Any intermediates, such as the internet service providers, network snooping, or even Twitter themselves, will not be able to comprehend the message's contents because the sender's message is converted into unreadable cipher text and stays in this condition throughout the transmission process. Customers will be more comfortable about the privacy and security of their communications in unfortunate circumstances like platform-impacting hacks if Twitter implements E2EE on DMs.

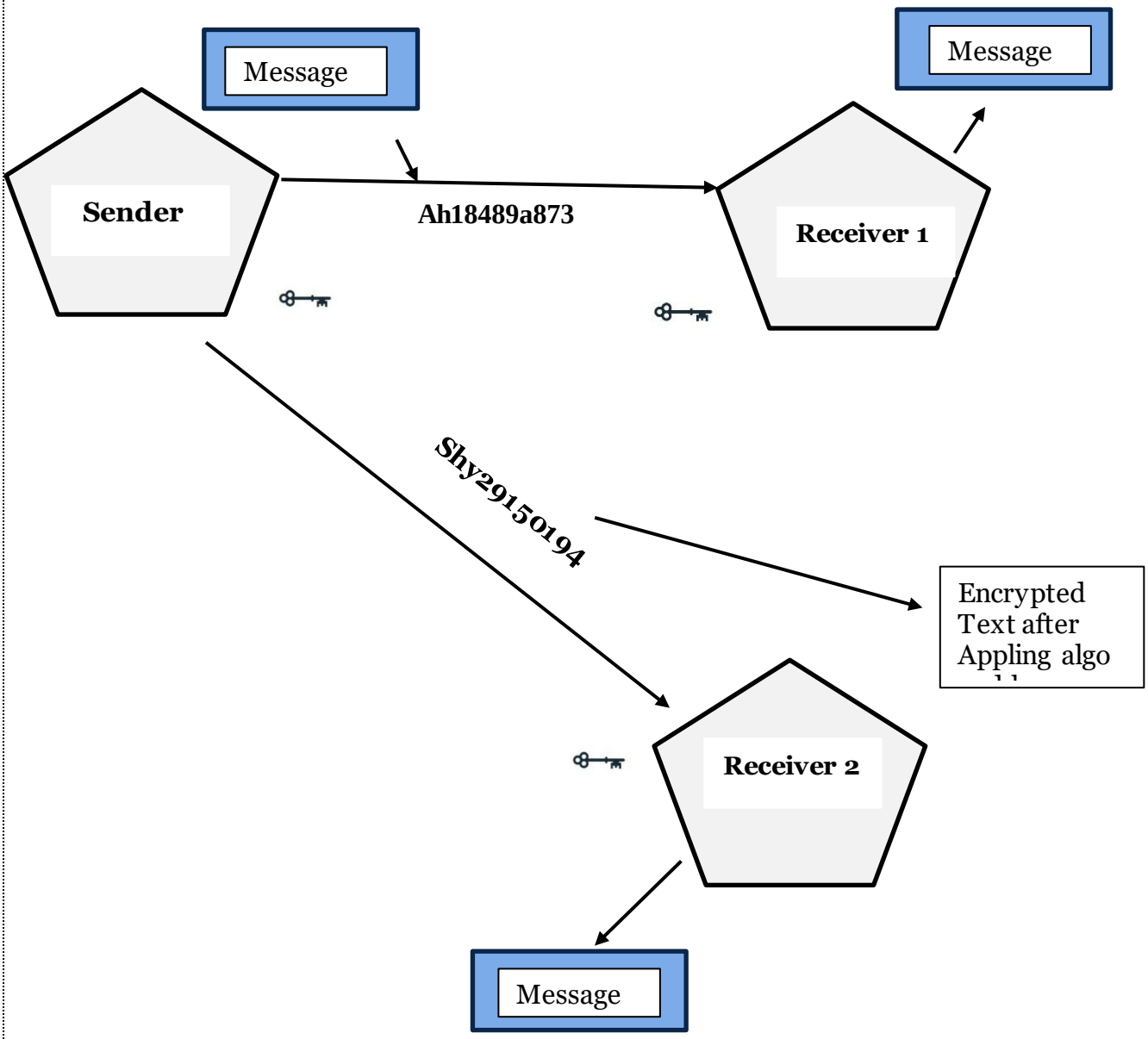
Framework Diagram

In this Framework diagram I'm using the InfoSec's domain **Cryptography**. In which when the sender send a message using Twitter it will first decrypt with the specific key and some random code will be generated in result, and when the message received by the receiver he need to apply the private key to decrypt the message and get the actual text.

ONE TO ONE MESSAGE:



Group Messages



ID	Name	Username	Text	Encryption	Receiver	Status
1	A. Donald Machin	RepMcEachin	Check this video out -- President Obama at the White House	Jsdjaksd7821s	tpryan	Success
2	Aaron Michlewitz	RepMichlewitz	I love LeBron. http://bit.ly/PdHur	Eqwvdvfg5654	vcu451	Success
3	Aaron Pekin	AaronPeskin	@Pills LeBron IS THE BOSS	Fweyfwef8wf7	chadfu	Success
4	Aaron Pea	Aaron Peña	JQuery is my new best friend.	Kjfkjasduasud	SIX15	Success
5	Aaron Schlock	Aarons chock	Reading my kindle2... Love it... Lee child's is good read.	Pfovodvu2846	yamarama	Success
6	Abby Finkenauer	Abby4Iowa	LeBron and zydrunas are such an awesome duo	Cdsjchjcuasy8	GeorgeVHulme	Success
7	Abigail Span Berger	SpanbergerVA07	In Montreal for a long weekend of Rampur. Much needed.	Eewdqwrq3rqe	Seth937	Success

8	Abigail Span Berger	Repspanberger	I'm itchy and miserable!	Vifurr9482242	Dcostalis	Success
9	Abigail Span Berger	SpanbergerVA07	is going to sleep then on a bike ride:]	Vfdvs1r13ffgup	PJ_King	Success
10	Abigail Span Berger	Repspanberger	Can't sleep... my tooth is aching.	Sfdi9ddufiuiu0	Mandanicole	Success
11	Adam Ki zinger	repkinzinger	Is in San Francisco at Bay to Breakers.	Cpqbhcuorpwo	Jpeb	Success
12	Adam Putnam	adamputnam	Shaun Woo hate's on Aug.	D2463axccfccv	Kylesellers	Success
13	Adam Schiff	RepAdamSchiff	Going to see star trek soon with my dad.	Ffdfe12efmocp	Theviewfans	Success
14	Adam Smith	RepAdamSmith	Malcolm Gladwell might be my new man crush	1ofhfocue03u2	MumsFP	Success
15	Adam Remke	adamzemke	playing with curl and the Twitter API	20ciencpmaifu	vincentx24x	Success

16	Adlai Stevenson III	AdlaiEStevenson	Hello Twitter	Ncbaehwifo02i	cameronwylie	Success
17	Adrian Fenny	adrianfenty	playing with Java and the Twitter API	2ucy2onxchxua	luv8242	Success
18	RepAdrianSmith	RepAdrianSmith	yahoo answers can be a butt sometimes	D01nc4ncXHcc	mtgillikin	Success
19	RepEspaillat	RepEspaillat	'Next time, I'll call myself Nike'	Vhw083dnckap	ursecretdezire	Success
20	John Edward	fredwilson	Class... The 50d is supposed to come today :)	Rif95930tmvmv	Native_01	Success
21	Mark Luther	JoeSchueller	@ Work tile 6pm... Let’s go Lakers!!!	Vvkjfof-069694	princezzcutz	Success
22	Martin Sob	scottabel	Why the hell is Pelosi in freak in China? And on whose dime?	Jfofjcjcjpotj432	peterlikewhat	Success
23	Dolph Zeg	JustMe_D	History exam studying ugh	Cjsos2010r8736	emceet	Success

24	Matt Walash	hiteshbagai	Zoom!!! I have a G2!!!!!!!	Idodi44991js1sb	CocoSavanna	Success
25	David genom	Annimallover	At GWT fireside chat @google	Cmfor049282re	DreambigRadio	Success
26	Alexendria	J_Holl	Lakers played great! Cannot wait for Thursday night Lakers vs.???	Cmdpqidbstqor	andrewwatson	Success
27	Andrew Tate	Vamsmack	Watching Night at The Museum. Lmao	Fjwur7qnxapjty	fredwilson	Success
28	Steven joe	Schroncd	Going to the dentist later.|	Fnspqfncncxjdhtf	JoeSchueller	Success
29	Donald luu	MarissaLeeD	Jake's going to Safeway!	1hgctqpqcalqpf,r	scottabel	Success

Vulnerabilities Report

In this Dataset which was leaked by twitter insiders are revealing the following:

- ID
- Name
- Username
- Plain Text
- Cipher Text
- Receiver Username
- Status of Encryption

Vulnerabilities:

- Identity Expose
- Data Theft
- Email/password cracking
- Vulnerable third party apps
- Phishing/MITM Attacks

In this Dataset we're applying the cryptographic algorithm of **Vigenere cipher** in which they converting the tweets text messages/ password of the user to cipher text from the plain text by doing this we can achieve the following

Keeping the Information Confidential:

By applying the cryptographic algorithm Twitter can hide the sensitive information of user like personal messages or the passwords by applying the encryption, and if any unauthorized entity tries to steal the data he need to spend lot of time to decrypt it.

Removal of Vulnerability of MITM/Phishing:

One of the major threat during sending or receiving data is Man in the Middle attack, in which Unauthorized person enters in the network of 2 device and steal the data by pretending actual user, by applying this encryption, even if the attacker tries to steal data he'll be unaware of the actual data because data (messages, passwords) are encrypted in random text and high chances are he will skip these ciphered text

Authentication

Using this algorithm we can authenticate the valid users over the network of twitter because if any unauthorized person tries to get into the network he need to have the valid auth code generated the cryptographic algorithms and only with those will be able to join the ecosystem of Twitter

Plagiarism Report

InfoSec Report

ORIGINALITY REPORT

13%	3%	0%	11%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	3%
2	Submitted to Colorado Technical University Student Paper	3%
3	www.networkworld.com Internet Source	2%
4	Submitted to American Public University System Student Paper	2%
5	Submitted to Wilmington University Student Paper	1%
6	Submitted to University of Greenwich Student Paper	1%
7	Submitted to The University of the South Pacific	<1%
9	Submitted to Universiti Malaysia Pahang Student Paper	<1%
10	Submitted to Washington State University System Student Paper	<1%
11	Submitted to Fiji National University Student Paper	<1%
12	Submitted to Embry Riddle Aeronautical University Student Paper	<1%
13	Submitted to North West University Student Paper	<1%
14	Submitted to University of the Western Cape Student Paper	<1%
15	Submitted to Anatolia College Student Paper	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

References:

- https://www.techtarget.com/searchcio/news/1359732/Twitter-security-risks-popularity-spark-regulatory-concerns
- https://www.3qdept.com/wp-content/uploads/2016/06/facebook_audiences_data_security_overview.pdf
- https://www.techopedia.com/definition/72/security-architecture
- https://commonslibrary.org/7-tips-for-facebook-risk-management/
- https://www.techtarget.com/searchcio/news/1359732/Twitter-security-risks-popularity-spark-regulatory-concerns
- https://www.forcepoint.com/symantec-dlp-migration
- https://security.googleblog.com/2017/12/securing-communications-between-google.html
- https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/
- https://www.techtarget.com/searchsecurity/definition/COMSEC-communications-security#:~:text=Communications%20security%20(COMSEC)%20is%20the,until%20the%20data%20is%20decrypted.
- https://www.fortinet.com/resources/cyberglossary/operational-security
- https://us.norton.com/blog/privacy/personal-cybersecurity#
- https://www.csoonline.com/article/3324614/what-is-physical-security-how-to-keep-your-facilities-and-devices-safe-from-on-site-attackers.html
- https://resources.infosecinstitute.com/topic/importance-physical-security-workplace/