CTC(T&IT),CRPF

Monthly e-Newsletter

AUG - 2021

Always do your best. What you plant now, you will harvest later

ctcit@crpf.gov.in @ctctitranchi CTC(T&IT)_CRPF_RANCHI ctctitcrpfranchi

"What you get by achieving your goals is not as important as what you become by achieving your goals.."

— Zig Ziglar

Aug-2021, Published on Aug 31-2021

EDITOR'S CENTER

Published By
CTC(T&IT),CRPF,Ranchi

READER'S CENTER

WhatsApp has introduced end-to-end encryption :-

WhatsApp has announced this end-to-end encryption now in order to prepare the broader technical community with the new approach before it's available to beta testers and eventually to everyday users.

WhatsApp new feature will be released as an optional feature and in the coming weeks, the instant messaging platform will be rolling this out to iOS and Android users.

How does it work

Currently, WhatsApp's backup management relies on mobile device cloud partners, such as Apple and Google, to store backups of the WhatsApp data (chat messages, photos, etc.) in Apple iCloud or Google Drive. Prior to the introduction of end-to-end encrypted backups, backups stored on Apple iCloud and Google Drive were not protected by WhatsApp's end-to-end encryption.

Now, the instant messaging platform will offer the ability to secure backups with end-to-end encryption before they are uploaded to these cloud services. With the introduction of end-to-end encrypted backups, WhatsApp has created an HSM (Hardware Security Module) based Backup Key Vault to securely store per-user encryption keys for user backups in tamper-resistant storage, thus ensuring stronger security of users' message history.

With end-to-end encrypted backups enabled, before storing backups in the cloud, the client encrypts the chat messages and all the messaging data (i.e. text, photos, videos, etc) that is being backed up using a random key that's generated on the user's device.

Where will the key be stored

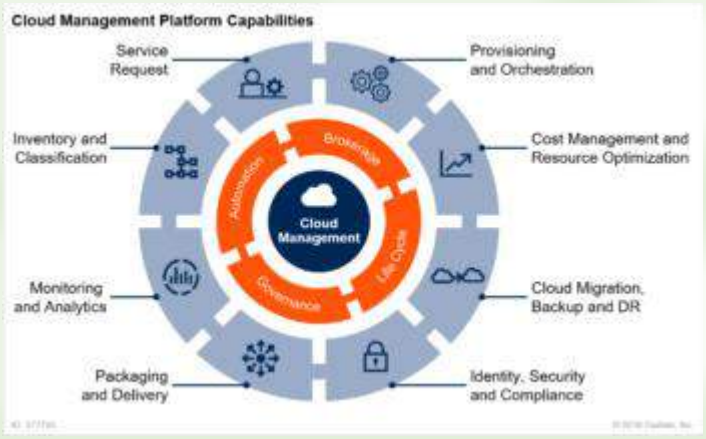
The key to encrypt the backup is secured with a user-provided password. The password is unknown to WhatsApp, the user's mobile device cloud partners, or any third party. The key is stored in the HSM Backup Key Vault to allow the user to recover the key in the event the device is lost or stolen.

The HSM Backup Key Vault is responsible for enforcing password verification attempts and rendering the key permanently inaccessible after a certain number of unsuccessful attempts to access it.

****

Cloud Security Posture Management

Cloud Security Posture Management (CSPM) is a market segment for IT security tools that are designed to identify misconfiguration issues and compliance risks in the cloud. An important purpose of CSPM programming is to continuously monitor cloud infrastructure for gaps in security policy enforcement.



Gartner, the IT research and advisory firm that coined the term, describes CSPM as a new category of security products that can help automate security and provide compliance assurance in the cloud. CSPM tools work by examining and comparing a cloud environment against a defined set of best practices and known security risks. Some CSPM tools will alert the cloud customer when there is a need to remediate a security risk, while other more sophisticated CSPM tools will use robotic process automation (RPA) to remediate issues automatically.

CSPM is typically used by organizations that have adopted a cloud-first strategy and want to extend their security best practices to hybrid cloud and multi-cloud environments. While CSPM is often associated with Infrastructure as a Service (IaaS) cloud services, the technology can also be used to minimize configuration mistakes and reduce compliance risks in Software as a Service (SaaS) and Platform as a Service (PaaS) cloud environments.

Key capabilities of CSPM

The key features of the most popular enterprise Cloud Security Posture Management tools include the ability to:

detect and perhaps automatically remediate cloud misconfigurations;

maintain an inventory of best practices for different cloud configurations and services;

Why misconfigurations occur and how to prevent them

Misconfigurations are most often caused by customer mismanagement of multiple connected resources. With cloud-based services, there can be a lot of moving pieces to keep track of and manage. Misconfigurations of the environment can be easily made, especially with API-driven approaches to integration. Misconfiguration opens an organization to the possibility of a data breach, because it only takes a few misconfigurations in the cloud to leave an organization vulnerable to attack.

Many times, a misconfiguration is created merely due to a lack of visibility. If an organization lacks an understanding of which resources interact with one another, then a misconfiguration of cloud resources becomes more likely.

One of the more common misconfigurations is accidentally granting public access to storage buckets or containers within the cloud that can be assigned individually to storage classes. When access to storage buckets is left open, the buckets are vulnerable to attack from anyone who knows where to look.

CSPM vendors

Since its conception, Cloud Security Posture Management vendors have changed from just being able to detect and notify users of misconfigurations, to now being able to automatically remediate them as well. Three examples of CSPM vendors include Zscaler CSPM, Orca Security and Trend Micro Cloud Conformity.

Zscaler CSPM is a CSPM tool that works with AWS, Azure, Google Cloud Platform, SaaS, IaaS and PaaS platforms. The tool can automatically identify and remediate misconfigurations. In 2020 the company Zscaler announced its intention to acquire Cloudneeti to add CSPM to its platform.

Orca Security is a startup and CSPM tool that works on AWS, Azure and Google Cloud services. Orca Security combines CSPM and cloud workload protection platform (CWPP) capabilities. The goal is to provide visibility and analysis in a multi-cloud environment.

Trend Micro acquired Cloud Conformity in a $70 million deal in order to be able to offer CSPM in the tool Cloud One Conformity. Cloud One Conformity works with AWS and Azure Cloud environments, with the goal of maintaining security, governance and compliance in public clouds.

map current configuration statuses to a security control framework or regulatory standard;

work with IaaS, SaaS and PaaS platforms in containerized, hybrid cloud and multi-cloud environments; and

monitor storage buckets, encryption and account permissions for misconfigurations and compliance risks.

Why using CSPM is important

CSPM tools play an important role in securing a cloud environment by reducing the possibility of data breaches.

According to Gartner, misconfiguration of the cloud environment is one of the more common mistakes in the cloud that can lead to a data breach -- and use of a CSPM tool can reduce cloud-based security incidents due to misconfigurations by 80%.

How CSPM works

Cloud Security Posture Management tools are designed to detect and remediate issues caused by cloud misconfigurations. A specific CSPM tool may only be able to use defined best practices according to a specific cloud environment or service, however, so it is important to know what tools can be used in each specific environment. For example, some tools may be limited to being able to detect misconfigurations in an AWS or Azure environment.

Some CSPM tools can automatically remediate issues by combining real-time continuous monitoring with automation features that can detect and correct issues, such as improper account permissions. Continuous compliance can also be configured according to a number of standards, including HIPAA.

Other CSPM tools can be used in tandem with Cloud Access Security Broker (CASB) tools. CASB is a software tool or service that can safeguard the flow of data between on-premises IT infrastructure and a cloud provider's infrastructure.

Additional benefits of enterprise CSPM

In addition to monitoring for compliance, CSPM tools can also make risk visualization, incident response and DevOps integration easier by providing

greater visibility across multiple cloud partners. Additional benefits of implementing CSPM in the enterprise include the ability to:

continuously monitor cloud environments in real time for threat detection;

assess data risk in real time;

detect policy violations across multiple cloud providers;

automate provisioning; and

detect and automatically remediate

source :- https://searchcloudsecurity.techtarget.com/definition/Cloud-Security-Posture-Management-CSPM

****

Robotic Process Automation (RPA)

Like AI and Machine Learning, Robotic Process Automation, or RPA, is another technology that is automating jobs. RPA is the use of software to automate business processes such as interpreting applications, processing transactions, dealing with data, and even replying to emails. RPA automates repetitive tasks that people used to do.

Although Forrester Research estimates RPA automation will threaten the livelihood of 230 million or more knowledge workers or approximately 9 percent of the global workforce, RPA is also creating new jobs while altering existing jobs. McKinsey finds that less than 5 percent of occupations can be totally automated, but about 60 percent can be partially automated.

For you as an IT professional looking to the future and trying to understand latest technology trends, RPA offers plenty of career opportunities, including developer, project manager, business analyst, solution architect and consultant. And these jobs pay well. An RPA developer can earn over ₹534K per year - making it the next technology trend you must keep a watch on!

Mastering RPA will help you secure high paying jobs like:

RPA Developer

RPA Analyst

RPA Architect

****

Privacy-enhancing computation

Privacy-enhancing technologies (PET) are technologies that embody fundamental data protection principles by minimizing personal data use, maximizing data security, and empowering individuals. PETs allow online users to protect the privacy of their personally identifiable information (PII) provided to and handled by services or applications. PETs use techniques to minimize possession of personal data without losing the functionality of an information system. Generally speaking, PETs can be categorized as hard and soft privacy technologies.

The objective of PETs is to protect personal data and ensure the users of technology that their information is confidential and management of data protection is a priority to the organizations who withhold responsibility for any PII - allowing users to take one or more of the following actions related to their personal data sent to and used by, online service providers, merchants or other users.

The goal of privacy-enhancing technologies include increasing control over personal data sent to, and used by, online service providers and merchants (or other online users) (self-determination). PETs aim to minimize personal data collected and used by service providers and merchants, use pseudonyms or anonymous data credentials to provide anonymity, and strive to achieve informed consent about giving personal data to online service providers and merchants. In Privacy Negotiations, consumers and service providers establish, maintain, and refine privacy policies as individualized agreements through the ongoing choice among service alternatives, therefore providing the possibility to negotiate the terms and conditions of giving personal data to online service providers and merchants (data handling/privacy policy negotiation). Within private negotiations, the transaction partners may additionally bundle the personal information collection and processing schemes with monetary or non-monetary rewards.

PETs provide the possibility to remotely audit the enforcement of these terms and conditions at the online service providers and merchants (assurance), allow users to log, archive and look up past transfers of their personal data, including what data has been transferred, when, to whom and under what conditions, and facilitate the use of their legal rights of data inspection, correction and deletion. PETs also provide the opportunity for consumers or people who want privacy-protection to hide their personal identities. The

process involves masking one's personal information and replace that information with a pseudo data or an anonymous identity.

Source :- https://en.wikipedia.org/wiki/Privacy-enhancing_technologies

****

QUIZ

Q1. The DOGE-1 Mission to the Moon will be launched by which company in 2022?

A. SpaceX

B. ISRO

C. NASA

D. Roscosmos

Q2. Anti COVID Drug 2-DG has been developed by which organization?

A. DRDO

B. ISRO

C. CDIR

D. DGCI

Q3. Who has launched its new Taj Mahal inspired Engineering Hub in NCR?

A. Snapdeal

B. Microsoft

C. Amazon

D. Flipkart

Q4. What is the name of the Worlds 1st Artificial Intelligence Ship?

A. Sunflower 40

B. Earth 2030

C. Mayflower 400

D. Seafarer 66

Q5. Which country is the first country in the world to control desert locusts using drones?

A. China

B. USA

C. Pakistan

D. India

Q6. The new Android version launched by Google on August 22, 2019

A. Android Pie

B. Android 10

C. Android Coco

D. Android 9A

Q7. Which of the following scheme is to promote the electric and hybrid vehicle technology to ensure the growth?

A. FAME

B. RISE

C. NPRT

D. EAHV

Q8. Name of the virus that hit 1.5 crore android devices across the country recently.

A. Black Horse

B. Agent Smith

C. Target John

D. Super Bug

Q9. Facebook launches cryptocurrency which allows users to make financial transactions across the globe. It's named as;

A. Dobil

B. Libra

C. Cryco

D. Digicy

Q10. Name the web mapping service, which launches three new public transport features in India

A. WikiMapia

B. MapQuest

C. Bing Maps

D. Google Maps

Acknowledgement

We are highly thankful for reading out this compilation and hope it will be useful for you in our day to day professional and personal life. We would like to hear your interest areas,suggestions from you to make this newsletter more informative and interesting. Your views will definitely help us to create this newsletter as an effective me- dium to reach you with latest development in the fields of communica- tion and technology.

R&D Team

CTC T&IT CRPF, Ranchi, Jharkhand

 ctcit@crpf.gov.in

1	2	3	4	5	6	7	8	9	10
A	A	B	C	D	B	A	B	B	D