CPIDER

Cyber Patrol for Identification of Emergent Risks

1.2 billion records exposed on unsecured Google Cloud server

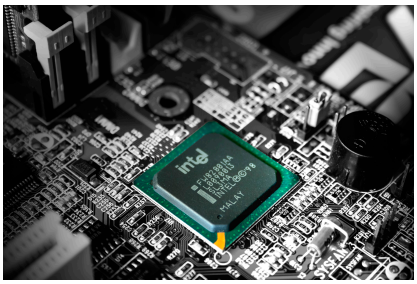
Four terabyte of unsecured data containing peoples' personal information as well as social media profiles was found lying on an unsecured Google Cloud server. The data, originally sourced from People Data Labs, a US based data company, was left unsecured by one of company's customers. The server has been shut down since then.
(https://www.techradar.com/in/news/google-cloud-server-left-a-billion-peoples-data-unsecured)

Browser extensions used for collecting data

Browser extensions Avast Online Security and AVG Online Security, widely installed on Chrome and Firefox have been found gathering user data including detailed browser history. Although these extensions have been designed to warn users when visiting any malicious site they were found sharing data with the companys' servers unauthorisedly.
(https://thehackernews.com/2019/12/avast-and-avg-browser-plugins.html)

'Deepfakes' an emerging cyber threat

'Deepfakes' refers to manipulated digital representations (mostly videos), produced by artificial intelligence tools that look and sound real but are fake. The content is created from scratch or using existing videos or images. The technology called 'Generative Adversarial Network' (GAN) was developed in 2014 by a graduate student Ian Goodfellow. The technology basically involves the use of two competing algorithms, one keeps on generating fake imagery and the other tries to spot the fakes. The process keeps repeating until the second algorithm can no longer spot the fake imagery created. The use of this technology was mostly limited to researchers in the field of artificial intelligence however, in 2017, a Reddit user used it to post altered videos. Although the videos were removed by Reddit, the use of the technology has spread having become available to common masses. The danger from the technology arises as it can be used to make people believe something is real when it is not. The fake videos can be used to spread misinformation with the objective of influencing the decision making abilities of the people. This comes in addition to the fact that the misuse



Intel CPUs vulnerable to security attack

Modern intel CPUs have been found vulnerable to a security attack that can be used to extract highly sensitive information. The attack described as 'Plundervolt' targets the safeguards used by computer operating systems to control the voltage and frequency to alter the bits held inside Intel Software Guard Extensions (SGX), a set of security-related instruction codes that are built into Intel CPUs. The vulnerability was discovered by researchers at the University of Birmingham. Intel has advised the users to update to the latest BIOS version which addresses the issue. (https://threatpost.com/intel-cpus-plundervolt-attack/151006/)

Google fixes Android camera vulnerability

Google has fixed a bug in Android OS that could allow attackers to hijack the phone camera. The bug allowed a third-party application to request "storage permissions" from an Android phone user, following which it was able to access the camera, record video and access geolocation data embedded in stored photos.

(https://threatpost.com/google-android-camera-hijack-hack/150409/)

of the technology can be carried out for perpetrating cyber frauds and online security breaches. Deepfakes pose a threat not only to individuals but companies, organisations and even governments. As deepfake technology evolves it is becoming increasingly harder to spot the videos without using sophisticated tools. Nevertheless, as a simple rule, any online content whether audio, video or images must be checked for the credibility of its source before believing in it.

(https://www.welivesecurity.com/2019/10/31/deepfakes-seeing-isnt-believing/ https://www.csoonline.com/article/3293002/deepfake-videos-how-and-why-they-work.html)

AirDrop Denial of Service (DoS) bug fixed by Apple

Apple has fixed a bug in its file sharing feature AirDrop that allowed nearby hackers to render iPhones and iPads inoperable. The vulnerability could be exploited by hackers for a denial of service (DoS) attack by spamming the nearby Apple devices with AirDrop share notifications blocking the UI of the phone. When a file is shared through AirDrop the recipient phone receives a popup notification asking the user to accept or decline the request. The popup however, blocks the user interface of the phone until it receives a response. By spamming the recipient phone with a large number of files the hacker can initiate an infinite loop of popup notifications that persist on the screen denying the owner the use of the phone. The bug which has been called 'AirDoS' was discovered by an independent researcher Kishan Bagaria. Apple has fixed the bug in its latest security patch.

(https://threatpost.com/airdos-bug-cripples-nearby-iphones/151030/)