BYTE QUEST

Vasavi College Of Engineering

Department Of Computer Science and Engineering

July 31, 2016

Volume 24

Contents:

Byte Quest is the article published by the CSE dept of Vasavi College of Engineering regarding the latest innovative Technologies and Software that have been emerged in the competitive world. The motto of this article is to update the people regarding the improvement in technology. The article is designed by the active participation of students under the guidance of faculty coordinators.

- Good ,bad or indifferent if you are not investing in new technology , you are going to be left behind.

  -Philip Green

- Once a new technology rolls over you, if you're not part of the steamroller, you're part of the road.

  -Stewart Brand.

FACULTY COORDINATORS

DIVYA (ASST. PROFESSOR)

T.NISHITHA (ASST. PROFESSOR)

STUDENT COORDINATORS

AMREEN KOUSAR(4/4 CSE-A)

D.SWAPNA(3/4 CSE-A)

NIKITHA(2/4 CSE-A)

KRISHNA CHAITHANYA(4/4 CSE-B)

RAHUL(3/4 CSE-B)

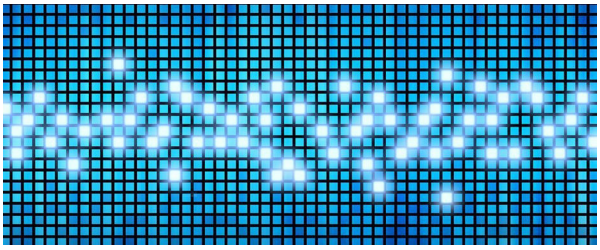
ABHINAV(2/4 CSE-B)

SCIENTISTS PRODUCED A NEW KIND OF PARTICLE THAT CARRIES ENERGY

New types of particles called 'topological plexcitons' have been engineered which helps to pave the way for more efficient energy transfers in solar cells and other forms of photonic circuits.

The University of California, San Diego team has managed to improve on a process known as exciton energy transfer (EET) that describes the way light and matter exchange energy when they meet.

EET is only possible over very short distances. But one way to extend this is by creating plexcitons, where excitons in a molecular crystal are combined with plasmons – the energy created from light interacting with metal which increases the range of EET to about the width of a human hair, but the energy flow is very difficult to harness.



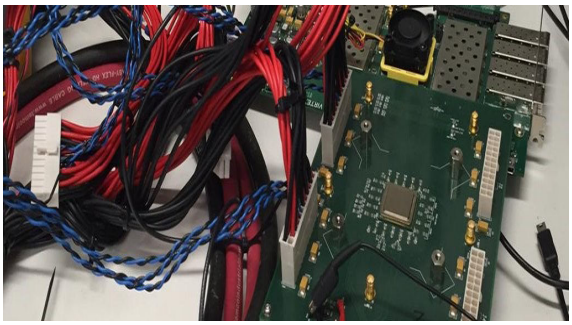
Materials called topological insulators have been used to act as conductors for EET, forcing the plexcitons to move in one direction, and that means scientists can control the flow of light energy at an incredibly small scale.

Miniaturised photonic circuits have the potential to be dozens of times smaller than today's silicon circuits, so it's possible that topological plexcitons will end up in lot of the devices we use everyday.

A.SRIHITH(CSE-A 3/4)

WORLD'S FIRST 1,000 - PROCESSOR COMPUTER CHIP

Scientists have just unveiled the world's first 1,000-processor microchip, capable of working through 1.78 trillion instructions every second. Each of those 1,000 processors can run independently, which makes the chip supremely suited to intensive tasks like encryption and weather forecasting – and thanks to some low-energy engineering, it can be powered by just one AA battery.



Today's top-end smartphones come with quad- or octa-core processors, so we're talking about more than a 100-fold increase in terms of the number of cores. The more cores, the more tasks you can get through simultaneously. While today's laptop CPUs are based on a 14-nanometre scale, the 1,000-processor chip was developed using older 32-nanometre technology.

Applications already developed for the KiloCore chip cover wireless coding and decoding, video processing, encryption, and a variety of scientific data applications.

RAMYA(CSE-B 4/4)

SCIENTISTS JUST SHOWED YOU CAN HACK AN OFFLINE PC BY LISTENING TO IT'S FANS

Scientists in Israel have demonstrated a new way for data to be extracted from even air-gapped (physically isolated) computers, with a new malware attack that combs data from the whirring sound of your PC's internal fan.

That's right – the sound of your computer keeping itself cool can now be turned against it, thanks to a malware program called Fansmitter, devised by researchers at the Ben-Gurion University of the Negev Cyber Security Research Centre.

Once a computer is infected with Fansmitter, the program can "acoustically exfiltrate data from air-gapped computers, even when audio hardware and speakers are not present," the researchers write in their paper.

The malware does this by regulating the internal fans' speed to generate an acoustic waveform emitted by the PC. In other words, like a parasite, Fansmitter takes some data from your PC, then takes over the fan, and uses it like a mouthpiece to generate subtle audio signals based on the data, which can then be detected and interpreted by a nearby device.

It's not the first time that audio signals have been used to extract data from air-gapped machines. Previous malware demonstrations have shown that PCs' internal and external speakers could use similar techniques to broadcast data signals via audio to capture devices.

This capability led some to think that, to make computers truly secure, they need to be audio-gapped (with all audio speakers disabled) in addition to being air-gapped (cut off from any non-secure networks) – but the new approach shows that even audio-gapping may not be enough in some circumstances to entirely lock down a PC.

Of course, for the Fansmitter attack to work, before the computer can be coerced into spilling its secrets, it has to be infected with the malware in the first place. And for an air-gapped computer that could be easier said than done, requiring physical access to the machine – although workers being less than careful with compromised USB keys have unwittingly infected PCs in very delicate situations before.

There's also the matter of how sluggish Fansmitter is. The researchers were able to exfiltrate data at a rate of 900 bits per hour, which on the whole is very slow – but, of course, it's likely to be fast enough to transmit potentially valuable portions of things like text.

RAHUL (CSE-B 3/4)