FutureHorizons

The Global Semiconductor Industry Analysts

# FH MONDAY

15 January 2017

## Graphene Research Targets Wireless Sensors

Researchers at The University of Manchester in the United Kingdom have embedded graphene sensors into radio-frequency identification (RFID) devices to enable a battery-free, wireless, smart humidity monitor.

read more

## MediaTek Pushes AI to the Edge

LAS VEGAS — MediaTek demonstrated at the Consumer Electronics Show its readiness for the post-smartphone era by moving into several new sectors, including chips for data switches, automotive and AI processors for edge devices.

read more

## Meltdown, Spectre Repeat Hard Security Lessons

SAN JOSE, Calif. — Vendors are still issuing patches and starting to think about optimizations for them after last week’s disclosure of one of the largest security flaws ever to hit microprocessors

read more

FutureHorizons

## TALK TO US

## AMD Updates GPU, CPU Road Maps

SAN JOSE, Calif. — AMD updated its x86 and graphics roadmaps at CES, giving first details of plans for 12-nm CPUs and a 7-nm GPU. It also rolled out six x86 chips with integrated graphics targeting a variety of desktop and notebook sockets.

read more

## EVENTS

Silicon Chip Industry Seminar

– March 2018 – London UK

Industry Forecast Briefing

– 16 January 2018 – London UK

DON’T MISS OUT.- BOOK NOW BY CALLING

+44 1732 740440

OR EMAIL

***mail@futurehorizons.com***

## Intel Says Security Bug Not Specific to its Processors

SAN FRANCISCO — Intel responded to reports that a design flaw in Intel processors makes computers using them susceptible to a newly discovered hack, saying the issue is not specific to Intel chips and that it is working closely with other tech companies to develop an industry-wide fix for the issue.

read more

## Graphene Research Targets Wireless Sensors For Iot

LONDON— Researchers at The University of Manchester in the United Kingdom have embedded graphene sensors into radio-frequency identification (RFID) devices to enable a battery-free, wireless, smart humidity monitor. The work targets Internet of Things (IoT) applications in manufacturing, food safety, health care, and sensitive operating environments such as nuclear waste handling.

The researchers describe their work in a paper just published in Scientific Reports. By layering graphene oxide (GO, a derivative of graphene) over graphene to create a flexible heterostructure, the team developed humidity sensors for remote monitoring with the ability to connect to any wireless network. The experimental device requires no battery source, as it harvests power from the receiver. According to the researchers, the sensors can be printed layer by layer to enable scalable mass production at very low cost.

## Mediatek Pushes AI To The Edge

MediaTek demonstrated at the Consumer Electronics Show its readiness for the post-smartphone era by moving into several new sectors, including chips for data switches, automotive and AI processors for edge devices.
David Ku, MediaTek's chief financial officer, discussed plans to bring "a certain AI function" that requires only small computational power to a large volume of devices including light switches. "We want to become an edge AI enabler," he told EE Times in a one-on-one interview at CES.

Downplaying the company's dependence on the smartphone market, Ku said smartphones — the single biggest driver for the company's growth over the past several years — generated "less than 40 percent" of its revenue last year.

## Meltdown, Spectre Repeat Hard Security Lessons

SAN JOSE, Calif. — Vendors are still issuing patches and starting to think about optimizations for them after last week's disclosure of one of the largest security flaws ever to hit microprocessors. Meltdown and Spectre provided the latest painful lesson about the nature of what's known in the security world as common vulnerabilities and exposures (CVEs).

The U.S. maintains what aims to be an authoritative list of CVEs. As of this writing it included a whopping 94,971 entries.

Vendors typically assign teams to keep up with the flow of new hacks and patches for them. But few are as broad as Meltdown and Spectre that effect microprocessors that support speculative execution. The technique is used widely in high-end chips shipped over the last several years from companies including AMD, ARM, Apple, IBM, Intel, Oracle and others.

## AMD Updates GPU, CPU Road Maps

SAN JOSE, Calif. — AMD updated its x86 and graphics roadmaps at CES, giving first details of plans for 12-nm CPUs and a 7-nm GPU. It also rolled out six x86 chips with integrated graphics targeting a variety of desktop and notebook sockets.

The company is now sampling a 12-nm upgrade of its Ryzen desktop processors launched last year in a 14-nm process. The chips will be in production in April using the upgraded process that Globalfoundries disclosed last year. Meanwhile, a Ryzen 2 design has been completed, but AMD gave no details of its internals or shipping dates.

AMD's first 7-nm GPU will be a version of its Vega design targeting machine learning. The company is playing catch-up with GPU rival Nvidia, which dominates the emerging area after rolling out Volta in 2017, its first chips with dedicated hardware for machine learning.

## Intel Says Security Bug Not Specific To Its Processors

SAN FRANCISCO — Intel responded to reports that a design flaw in Intel processors makes computers using them susceptible to a newly discovered hack, saying the issue is not specific to Intel chips and that it is working closely with other tech companies to develop an industry-wide fix for the issue.

The issue, reported by the online tech publication the Register on Tuesday (Jan. 2), is described as a software analysis method that can enable the improper gathering of sensitive data from computers. The Register reported that the bug is present in Intel x86 processors produced in the last decade and that it allows normal user programs to discern to some extent the layout or contents of protected kernel memory areas.