INGLÉS II

# TEXT 1

## New Transparent Metal Could Make Smartphones Cheaper.

By Nathaniel Scharping

As smartphones get smaller, cheaper and faster, one essential component remains costly: the screen.

Almost 90 percent of smartphone touchscreens utilize a rare and expensive compound called indium tin oxide, which has kept the price of such screens high. Now, researchers at Pennsylvania State University have developed a new material, called strontium vanadate, that shares the transparent and conductive properties of indium tin oxide at a fraction of the cost.

The researchers detailed their findings in an article published earlier this month in the journal *Nature Materials*. They crafted a transparent metal composed of strontium and vanadium with an unusual configuration of electrons that allows light to pass through while retaining the electrically conductive properties of metals.

### A New Way To Look At Screens

The researchers see smartphone screens, which need to be electrically conductive and transparent, as the most immediate application of their discovery. Indium tin oxide possesses those integral properties but its cost comes in around $750 per kilogram. As a result, when you shell out several hundred dollars for a new smartphone, roughly 40 percent of the cost is tied up in the screen. Both strontium and vanadium sell for just $25 or less per kilogram, according to the researchers. In addition, researchers produced the compound in a film only 10 nanometers thick, making it perfect for touchscreens.

Typically, metals share their electrons freely, which allows them to move throughout the structure uninhibited, much like gaseous molecules. This gives metals their distinctive properties, such as malleability and conductivity. The electrons in strontium vanadate, a so-called correlated metal, behave more like a liquid than a gas, moving slower and interacting with each other in curious ways.

Electrons in strontium vanadate molecules exhibit stronger forms of electrostatic interaction — the forces acting between positively and negatively charged articles. These forces slow down the electrons and cause them to interact in complex ways, according to the researchers. The end result is a metal that retains its conductivity, but is less reflective when light is shined on it, making it transparent. This combination of properties makes it perfect for use in smartphone screens. The researchers also see applications for their compound in a new form of solar cells, as well as smart windows and television screens.

Transparent metal sounds like an oxymoron, but you could one day be reading this story through it.

New Transparent Metal Could Make Smartphones Cheaper - D-brief. (2017). [online] D-brief. Available at: <http://blogs.discovermagazine.com/d-brief/2015/12/24/new-transparent-metal-could-> make-smartphones-cheaper/#.WAuYxo8rLIU [Accessed 19 Feb. 2017].

# TEXT 2

## Researchers want to use hardware to fight computer viruses



Dmitry Ponomarev, professor of computer science at Binghamton University, State University of New York. *Credit: Jonathan Cohen/Binghamton University*

Fighting computer viruses isn't just for software anymore. Binghamton University researchers will use a grant from the National Science Foundation to study how hardware can help protect computers too.

"The impact will potentially be felt in all computing domains, from mobile to clouds," said Dmitry Ponomarev, professor of computer science at Binghamton University, State University of New York. Ponomarev is the principal investigator of a project titled "Practical Hardware-Assisted Always-On Malware Detection."

More than 317 million pieces of new malware -- computer viruses, spyware, and other malicious programs -- were created in 2014 alone, according to work done by Internet security teams at Symantec and Verizon. Malware is growing in complexity, with crimes such as digital extortion (a hacker steals files or locks a computer and demands a ransom for decryption keys) becoming large avenues of cyber-attack.

"This project holds the promise of significantly impacting an area of critical national need to help secure systems against the expanding threats of malware," said Ponomarev. "[It is] a new approach to improve the effectiveness of malware detection and to allow systems to be protected continuously without requiring the large resource investment needed by software monitors."

Countering threats has traditionally been left solely to software programs, but Binghamton researchers want to modify a computer's central processing unit (CPU) chip -- essentially, the machine's brain -- by adding logic to check for anomalies while running a program like Microsoft Word. If an anomaly is spotted, the hardware will alert more robust software programs to check out the problem. The hardware won't be right about suspicious activity 100 percent of the time, but since the hardware is acting as a lookout at a post that has never been monitored before, it will improve the overall effectiveness and efficiency of malware detection.

"The modified microprocessor will have the ability to detect malware as programs execute by analyzing the execution statistics over a window of execution," said Ponomarev. "Since the hardware detector is not 100-percent accurate, the alarm will trigger the execution of a heavy-weight software detector to carefully inspect suspicious programs. The software detector will make the final decision. The hardware guides the operation of the software; without the hardware the software will be too slow to work on all programs all the time."

The modified CPU will use low complexity machine learning -- the ability to learn without being explicitly programmed -- to classify malware from normal programs, which is Yu's primary area of expertise.

"The detector is, essentially, like a canary in a coal mine to warn software programs when there is a problem," said Ponomarev. "The hardware detector is fast, but is less flexible and comprehensive. The hardware detector's role is to find suspicious behavior and better direct the efforts of the software."

Much of the work -- including exploration of the trade-offs of design complexity, detection accuracy, performance and power consumption -- will be done in collaboration with former Binghamton professor Nael Abu-Ghazaleh, who moved on to the University of California-Riverside in 2014.

Lei Yu, associate professor of computer science at Binghamton University, is a co-principal investigator of the grant.

Grant funding will support graduate students that will work on the project both in Binghamton and California, conference travel and the investigation itself. The three-year grant is for $275,000.

New Transparent Metal Could Make Smartphones Cheaper - D-brief. (2017). [online] D-brief. Available at: <http://blogs.discovermagazine.com/d-brief/2015/12/24/new-transparent-metal-could-> make-smartphones-cheaper/#.WAuYxo8rLIU [Accessed 19 Feb. 2017].

# TEXT 3

## Encryption method takes authentication to a new level, improves privacy protection

VTT Technical Research Centre of Finland has developed new kinds of encryption methods for improving the privacy protection of consumers to enable safer, more reliable and easier-to-use user authentication than current systems allow.

The method combines safety, usability and privacy protection, when, until now, implementing all three at the same time has been a challenge.

"Our method protects, for example, the user's biometric data or typing style," says Senior Scientist Kimmo Halunen.

In biometric authentication, the risk is that a person's permanent biometric identifiers, which cannot be changed, leak out of the database. VTT's method stores data in the database in an encrypted form and all comparisons between measuring results and the database are conducted using encrypted messages so there is no need to open any biometric data at this stage of the process.

VTT integrates new kind of encryption methods, such as homomorphic cryptography and secure exchange of cryptographic keys, to known measuring methods of typing styles.

The traditional authentication based on passwords has proved to be weak, since users mostly select weak passwords, and hackers often succeed in stealing quite large password databases. Recently, companies such as Dropbox and Yahoo have fallen prey to such data breaches.

In addition, new types of user environments, such as smart devices, cars, and home appliances, create challenges for user authentication with the help of passwords.

VTT is now looking for a partner for further processing and commercialisation of this method, which could be available to consumers within a year or two.

Encryption method takes authentication to a new level, improves privacy protection. (2017). [online] Science Daily. Available at: https://[www.sciencedaily.com/releases/2016/09/160929082204.htm](http://www.sciencedaily.com/releases/2016/09/160929082204.htm) [Accessed 19 Feb. 2017].

# TEXT 4

## No GPS, no problem: Next-generation navigation



Simulation results for a unmanned drone flying over downtown Los Angeles showing the true trajectory (red line), from GPS only (yellow line), and GPS aided with cellular signals (blue line). *Credit: ASPIN Laboratory at UC Riverside*

A team of researchers at the University of California, Riverside has developed a highly reliable and accurate navigation system that exploits existing environmental signals such as cellular and Wi-Fi, rather than the Global Positioning System (GPS). The technology can be used as a standalone alternative to GPS, or complement current GPS-based systems to enable highly reliable, consistent, and tamper-proof navigation. The technology could be used to develop navigation systems that meet the stringent requirements of fully autonomous vehicles, such as driverless cars and unmanned drones.

Led by Zak Kassas, assistant professor of electrical and computer engineering in UCR's Bourns College of Engineering, the team presented its research at the 2016 Institute of Navigation Global Navigation Satellite System Conference (ION GNSS+), in Portland, Ore., in September. The two studies, "Signals of Opportunity Aided Inertial Navigation" and "Performance Characterization of Positioning in LTE Systems," both won best paper presentation awards.

Most navigation systems in cars and portable electronics use the space-based Global Navigation Satellite System (GNSS), which includes the U.S. system GPS, Russian system GLONASS, European system Galileo, and Chinese system Beidou. For precision technologies, such as aerospace and missiles, navigation systems typically combine GPS with a high-quality on-board Inertial Navigation System (INS), which delivers a high level of short-term accuracy but eventually drifts when it loses touch with external signals.

Despite advances in this technology, current GPS/INS systems will not meet the demands of future autonomous vehicles for several reasons: First, GPS signals alone are extremely weak and unusable in certain environments like deep canyons; second, GPS signals are susceptible to intentional and unintentional jamming and interference; and third, civilian GPS signals are unencrypted, unauthenticated, and specified in publicly available documents, making them spoofable (i.e., hackable).

Current trends in autonomous vehicle navigation systems therefore rely not only on GPS/INS, but a suite of other sensor-based technologies such as cameras, lasers, and sonar.

"By adding more and more sensors, researchers are throwing 'everything but the kitchen sink' to prepare autonomous vehicle navigation systems for the inevitable scenario that GPS signals become unavailable. We took a different approach, which is to exploit signals that are already out there in the environment," Kassas said.

Instead of adding more internal sensors, Kassas and his team in UCR's Autonomous Systems Perception, Intelligence, and Navigation (ASPIN) Laboratory have been developing autonomous vehicles that could tap into the hundreds of signals around us at any point in time, like cellular, radio, television, Wi-Fi, and other satellite signals.

In the research presented at the ION GNSS+ Conference, Kassas' team showcased ongoing research that exploits these existing communications signals, called "signals of opportunity (SOP)" for navigation. The system can be used by itself, or, more likely, to supplement INS data in the event that GPS fails. The team's end-to-end research approach includes theoretical analysis of SOPs in the environment, building specialized software-defined radios (SDRs) that will extract relevant timing and positioning information from SOPs, developing practical navigation algorithms, and finally testing the system on ground vehicles and unmanned drones.

"Autonomous vehicles will inevitably result in a socio-cultural revolution. My team is addressing the challenges associated with realizing practical, cost-effective, and trustworthy autonomous vehicles. Our overarching goal is to get these vehicles to operate with no human-in-the loop for prolonged periods of time, performing missions such as search, rescue, surveillance, mapping, farming, firefighting, package delivery, and transportation," Kassas said.

University of California - Riverside. (2016, October 13). No GPS, no problem: Next-generation navigation. *ScienceDaily*. Retrieved February 19, 2017 from www.sciencedaily.com/releases/2016/10/161013150039.htm