Attacks Target Bitcoin Virtual Currency

A wave of cyberattacks has hit online services and exchanges that work with bitcoin, just as interest in the virtual currency, as well as its value, was skyrocketing. Hackers hit both the Japan-based Mt. Gox bitcoin exchange and Instawallet, a bitcoin storage website.

Mt. Gox, the world's most popular exchange, said it was struck recently by an ongoing distributed denial-of-service attack that caused trading and connectivity issues. Although no individual accounts were compromised, many users reportedly had difficulty logging into their accounts.

According to a statement the company issued, "The sheer volume of this DDoS left us scrambling to fine-tune the system every few hours."

Instawallet remained offline after attackers broke into its database and stole bitcoins. The company says it is working on better security and has begun a process enabling customers to claim stored funds.

Other bitcoin-related operations have also been targeted. For example, the Bitcoin-Central exchange and its affiliate Paytunia reported a recent security breach and suspended operations pending an investigation and implementation of better security. The services have since come back online.

According to Mt. Gox, the attacks had two primary goals: destabilizing the bitcoin system in general by hitting its largest exchange and abusing the system for profit. The company said hackers want to drive down the bitcoin's value, cause panic selling, and then buy large volumes of the currency for future sale when prices rise again.

So far, investigators say, they have been unable to identify the attacks' source.

Before the incidents, the bitcoin's highest exchange value was about $142, having risen steeply after increased media focus on the system and growing concern about the global economy caused by the Cyprus banking crisis. After the attacks, the bitcoin's value dropped to about $120, rose to about $184 on at least one exchange, and then fell again.

The bitcoin system has been running for about four years, providing a digital currency independent of government control that can be used for payment among participating users. Its daily trade volume is reportedly about 40,000 transactions worth about $1 million. About $300 million worth of bitcoins are currently in circulation.

Industry observers and security experts note that financial institutions regularly face cybertattacks but that such incidents have a bigger impact on a small operation like the bitcoin system.

Technology Use Could Increase Greenhouse-Gas Emissions

Continued rapid growth in the use of smartphones, PCs, and other communications and computing devices could cause greenhouse-gas (GHG) emissions to increase substantially through the end of this decade, according to a recent report.

GHGs absorb and emit infrared radiation and thus contribute to global climate change.

Currently, the information and communications technology (ICT) industry creates 2 percent of global GHG emissions. By 2020, though, that portion will likely jump to 4 percent, according to a study for Alcatel-Lucent by BIO Intelligence Service, a French environmental and sustainable-development consultancy.

Conceivably, the report said, network traffic volumes could be 35 times larger than they are today. If the process isn't made more energy efficient, the ICT industry's GHG emissions would be 10 times more than all other emissions sources combined.

The study said that the use of ICT products and services is growing faster than energy-use reductions. On the other hand, BIO noted, their utilization also enables the global economy to operate more efficiently, resulting in a GHG reduction.

BIO recommended that public and ICT companies work together to enable economic growth while improving efficiency by, for example, deploying smart public infrastructures, increasing cloud computing usage, and implementing more energy-efficient technologies. This would require ongoing support for advanced research, stated the report.

Researchers Develop Flexible Silicon Chips

A Germany-based research team has developed technology that could make building flexible silicon chips practical.

The Institut für Mikroelektronik Stuttgart (IMS-CHIPS) scientists'

0018-9162/13/$31.00 © 2013 IEEE

NEW ARMBAND LETS USERS CONTROL DEVICES WITH GESTURES

A start-up has developed an armband that lets users control their computers, smartphones, and other devices via gestures.

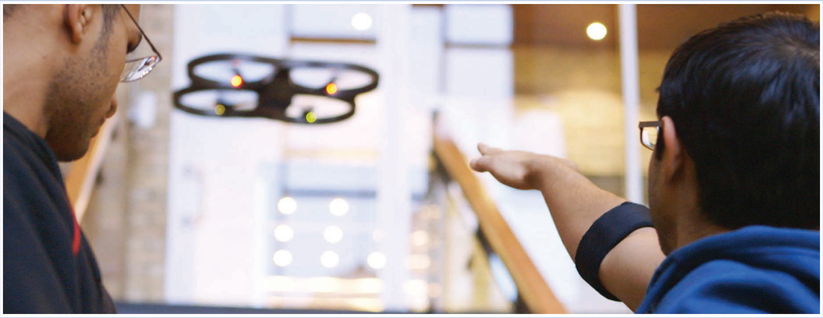
Thalmic Labs' MYO armband—worn just above the elbow—detects the multiple types of electrical activity caused when people use their hand or arm muscles to make different gestures. It uses software to convert this information into various device commands.

Thalmic says this approach makes device control more natural and integrates technology more closely with users.

The MYO armband—which supports Windows, Mac, iOS, and Android devices—contains electrodes that identify the electrical events that occur when a user, for example, moves an arm in a circular motion, waves a hand, or twitches a finger. The product's initial version recognizes 20 gestures. It connects to a computer, phone, or other device via Bluetooth 4.0 Low Energy.

The armband could provide enough control to let users play games, scroll webpages up and down, raise and lower sound volumes, divert incoming calls to voice mail, and even fly small drones. MYO's muscle-sensing technology makes it more accurate and easy-to-use than controllers that work via cameras.

Thalmic—founded in 2012 by three University of Waterloo graduates—plans to begin shipping MYO, which is available for preorder (https://getmyo.com), later this year. Meanwhile, the company is working on an API for developers interested in building MYO-based applications.



Thalmic Labs has designed an armband that lets users wirelessly control computers or other devices—in this case, a quadrocopter—simply by making gestures.

technique could enable the installation of processors in objects such as clothing, rugs, paper, and TV and computer screens, adding appealing functionality to many items.

For example, sensor chips in car seats could make sure parents don't leave young children inside. And chips with RFID tags could enable the tracking of objects, animals, and humans. Someday, flexible chips could be used as medical implants.

Thin chips could easily be stacked, making them suitable for the increasingly popular high-performance 3D chips. In fact, the industry road map for electronics miniaturization shows 3D chips using layers of 5- to 10-nanometer-thick chips by 2020.

There are flexible electronics today, but they typically use semiconductors made from substances other than silicon. However, these chips don't perform as well as those made with silicon. Researchers have thus been seeking ways to make flexible silicon chips.

Thin silicon wafers—between 50 and 100 micrometers—tend to break. Below 50 µm, however, they become structurally strong yet flexible. At less than 10 µm, they are transparent, which makes them suitable for embedding in objects such as windows.

A challenge is enabling thin chips to survive the rough manufacturing process, which includes grinding the processors to a uniform thickness. Previous approaches to coping with this have included either starting with thick chips and cutting them down after the fabrication process, or adding layers to strengthen the chip and removing the layers after manufacturing. However, both these approaches are wasteful and expensive.

The IMS-CHIPS researchers decided to build thin chips from scratch, using a technique they call Chipfilm. They grew crystalline silicon, layer upon layer, and anchored it to a foundation strong enough to provide support during manufacturing but sufficiently fragile to snap off cleanly afterward.

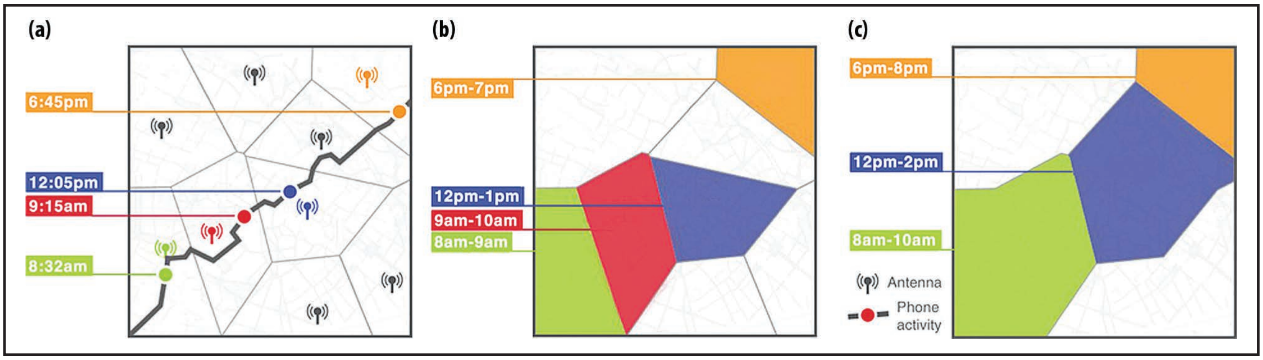
The scientists say Chipfilm could yield chips as thin as 10 µm. However, they note, more work remains to eliminate problems that occasionally either damage chips or cause flaws that make them unusable or less effective.

Hate-Speech Database Could Help Predict Genocide

An organization dedicated to stopping genocide is compiling a database that experts could use to detect early indications of the impending mass killing of a racial, religious, or political group.

The Sentinel Project for Genocide Prevention is building Hatebase, a crowdsourced collection of hate-speech words and phrases in multiple languages. Having a multilingual database would make it easier for researchers who don't speak a local language to recognize the increased use of hate speech in that region.

The researchers could study communications in various parts of the world and identify a localized increased use of such



MIT research indicates that the identity of many mobile phone users could be determined simply by tracking GPS signals from their phones. (a) Trackers first trace a user's signals. They mark dots representing call times and locations. They also record the nearest antenna locations. (b) The trackers then note the antennas' entire reception areas. (c) Further aggregation based on two-hour time intervals helps narrow down the trace. Trackers could then identify users by identifying locations they regularly visit.

messages, potentially indicating impending genocidal violence.

Experts say the increased use of hate speech dehumanizes groups of people and is frequently a precursor to genocide. For example, the Nazis in Germany used hate speech about Jews before the Holocaust.

Users who want to contribute can log into the Hatebase website (www.hatebase.org) and enter the types of hate speech used in their communities. The database will be available to casual users via a Wikipedia-like interface.

Developers for nonprofit and other organizations could use an API to mesh Hatebase data with their own genocide-prevention-related applications. The Sentinel Project said this ability to work with other groups is important and would magnify Hatebase's usefulness and effectiveness.

The Sentinel Project plans to increase the database's functionality over time.

Report: Trackers Could Identify Users by Tracing GPS Signals

MIT researchers have shown how someone could access and analyze information about a mobile phone's GPS signals and identify its user without great difficulty. This has caused privacy advocates such as the Electronic Frontier Foundation to express concern. The EFF said the capability to track users from anonymized mobile phone data threatens privacy.

The MIT researchers studied 15 months of GPS-based location data for about 1.5 million unidentified mobile phone users. They determined that with ongoing information about an individual's location and travel patterns, they could correctly identify the user 95 percent of the time.

Various mobile applications gather information about users' locations that a determined tracker could access. In addition, mobile operating system vendors are making anonymous GPS-based location data available to developers of applications that, for example, target advertising to users.

By establishing at least four places a person regularly goes to, the researchers found they could determine who the individual is, using publicly available information such as home or work addresses or geotagged tweets and online photos. ■

Editor: Lee Garber, *Computer*; l.garber@computer.org