THE EARTH EXPERIMENT Geoengineering field trials begin

NewScientist

WEEKLY September 10 - 16, 2011

WHY MILLIONS OF GENETICALLY MODIFIED ANIMALS ARE BEING RELEASED INTO THE WILD

ET was here

How to find traces of alien visitations

SOLAR MEGASTORMS
They'll destroy Earth's radiation shield

THE MANHATTAN MEMORY PROJECT
What 9/11 reveals about our brains

RISE AND RISE OF HACKTIVISM
Inside the movement that changed the web

Science and technology news
www.newscientist.com
US jobs in science

US$5.95 CAN$5.95 No2829

Ghost flyers in the sky

Security holes in an air traffic control system could compromise safety, warns **Paul Marks**

AN ALARM blares in the cockpit mid flight, warning the pilot of an imminent collision. The pilot checks his tracking display, sees an incoming aircraft and sends the plane into a dive. That only takes it into another crowded air lane, however, where it collides with a different plane. Investigators later discover that the pilot was running from a "ghost" – a phantom aircraft created by a hacker intent on wreaking havoc in the skies.

It's a fictional scenario, but US air force analysts warn that it could be played out if hackers exploit security holes in an increasingly common air traffic control technology.

At issue is a technology called Automatic Dependent Surveillance-Broadcast (ADS-B), which the International Civil Aviation Organisation certified for use in 2002. Gradually being deployed worldwide, ADS-B improves upon the radar-based systems that air traffic controllers and pilots rely on to find out the location and velocity of aircraft in their vicinity.

Conventional ground-based radar systems are expensive to run, become less accurate at determining position the further away a plane is, and are slow to calculate an aircraft's speed. Perhaps worst of all, their limited range means they cannot track planes over the ocean.

So instead of bouncing radar signals off aircraft, ADS-B uses GPS signals to continuously broadcast a plane's identity, ground position, altitude and velocity to networks of ground stations and other nearby aircraft. This way, everyone knows where everyone else is.

ADS-B transmits information in unencrypted 112-bit bursts –

M.WAGNER/AVIATION-IMAGES.COM

Trouble ahead

Electrified roads could power cars from the ground up

THE cars of the future could be powered by electrified roadways. Such technology would allow electric cars to forgo their heavy batteries, which not only add to a vehicle's weight, increasing the energy needed to move it, but also force it to sit idle while recharging.

The idea has been around for decades. Previous attempts used an electrified coil in the road to create an electromagnetic field that interacts with a coil attached to the car. "Since the coils must be exactly aligned face-to-face to achieve a high energy efficiency, such schemes may be useful for [charging] vehicles in a parking lot, but never very effective for cars while running," says Masahiro Hanazawa at Toyota Central R&D Labs in Nagakute, Aichi, Japan.

Hanazawa and Takashi Ohira at Toyohashi University of Technology, also in Aichi, are developing a system that transmits electric power through steel belts placed inside two tyres and a metal plate in the road. "Our approach exploits a pair of tyres, which are always touching a road surface," says Hanazawa.

To test how much energy would be lost as electricity travelled through the tyres' rubber, Hanazawa and Ohira set up a lab experiment in which they put metal plates on the floor and inside a tyre. "Less than 20 per cent of the transmitted power is dissipated in the circuit," says Ohira. The team presented its work in May at the International Microwave Workshop Series on Innovative Wireless Power Transmission in Kyoto, Japan.

With enough power the system could run typical passenger cars, says Ohira, and the team are now developing a small-scale prototype to prove it. He admits, however, that the system's energy loss is "much higher than regular batteries".

John Boys, an electrical engineer at the University of Auckland, New Zealand, notes that with this system, the metal pads on the road would need as much as 50,000 volts to power the car, the same voltage

"The system transmits electricity through steel belts inside two tyres and a metal plate in the road"

a measure intended to make the system simple and cheap to implement. It's this that researchers from the US air force's Institute of Technology at Wright-Patterson Air Force Base in Ohio are unhappy with. Donald McCallie, Jonathan Butts and Robert Mills warn that the unencrypted signals could be intercepted and spoofed by hackers, or simply jammed.

The team says the vulnerabilities it has identified "could have disastrous consequences including confusion, aircraft groundings, even plane crashes if exploited by adversaries" (*International Journal of Critical Infrastructure Protection*, DOI: 10.1016/j.ijcip.2011.06.001).

One attack they label "low difficulty" is a "ground station flood denial": jamming an ADS-B ground receiver mast (like a cellphone mast) by placing a low-power radio transmitter near it. That effectively blinds controllers to where planes are.

Tougher to carry out is a "ghost aircraft injection". This attack mimics the format of ADS-B data packets to create fake aircraft signals, either on the ground controller's screen or on the pilot's tracking display.

"We're aware of the research undertaken by the US air force and have been working for some time with UK and European authorities and agencies to understand and mitigate the issues," says Brendan Kelly, policy chief at National Air Traffic Services in the UK.

But the Federal Aviation Administration, which wants ADS-B fully operational across the US by 2020, says tests it completed in 2009 show ADS-B has no risks over and above those presented by existing radar systems. "The FAA has a thorough risk management process for all possible risks to ADS-B, including intentional jamming," says a spokesman.

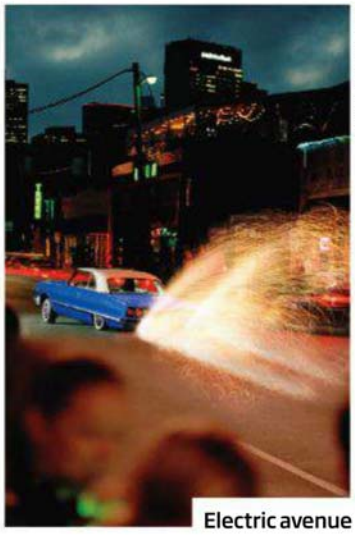
McCallie's team is not convinced, and has asked to see the FAA's test data – which the agency has so far refused to make public, citing security concerns. The team accepts that such concerns are warranted, but insist that additional safeguards must be introduced into ADS-B. Specifically, they say ways to authenticate messages between planes and ground control ought to be explored. "Security as an afterthought will not suffice," they write. ■

"The unencrypted signal giving an aircraft's location could be intercepted and spoofed by hackers

used to operate tasers. "You wouldn't want to step on that," he says.

What's more, at the energy levels needed, the electric plates would produce a large magnetic field that would "cause significant radio-frequency interference that might create chaos with all manner of electrical systems", says Boys.

It would be expensive to "rip up the roads and install the necessary infrastructure", says Daniel Friedman at the University of New South Wales in Sydney, Australia. But he adds that one way around that may be to limit metal plates to main highways, and then run cars on other roads using small batteries. Wendy Zukerman ■



DREAMPICTURES/GETTY

Electric avenue

ONE PER CENT

PRISCILLA GRAGG/GETTY

Music keeps cyclists on the right road

Using satnav while cycling can be tricky, as it's impossible to keep your eyes on the road and on the screen at the same time. So Matthijs Zwinderman at the Eindhoven University of Technology in the Netherlands have come up with a smartphone app, called Oh Music, Where Are Thou?, which uses music played through headphones to guide cyclists. The music appears to come from the direction they want to head, panning around depending on which way the cyclist is travelling. It gets louder as they approach their destination.

Leaked cables go online

WikiLeaks published more than 250,000 leaked US diplomatic cables online on 2 September after *The Guardian* newspaper published an encryption key to the documents in a book. To beat rival sites who were using the key to decrypt the files, WikiLeaks rushed the whole tranche online, but did so with informants' names visible.

Mach 1.2

The velocity at which Blue Origin, a commercial space flight start-up owned by Amazon chief Jeff Bezos, was forced to destroy its test vehicle when it veered out of control over Texas last month

Facebook your doodles

Bored students can now share their doodles using UbiSketch, a paper-based system that uploads drawings to Twitter or Facebook. UbiSketch uses a digital pen to convert images drawn on special paper into pictures on a smartphone. The pen tracks its position by reading a pattern of dots printed on the paper before sending the data to the phone.

For breaking tech news go to:
newscientist.com/onepercent