WWW.NEWELECTRONICS.CO.UK

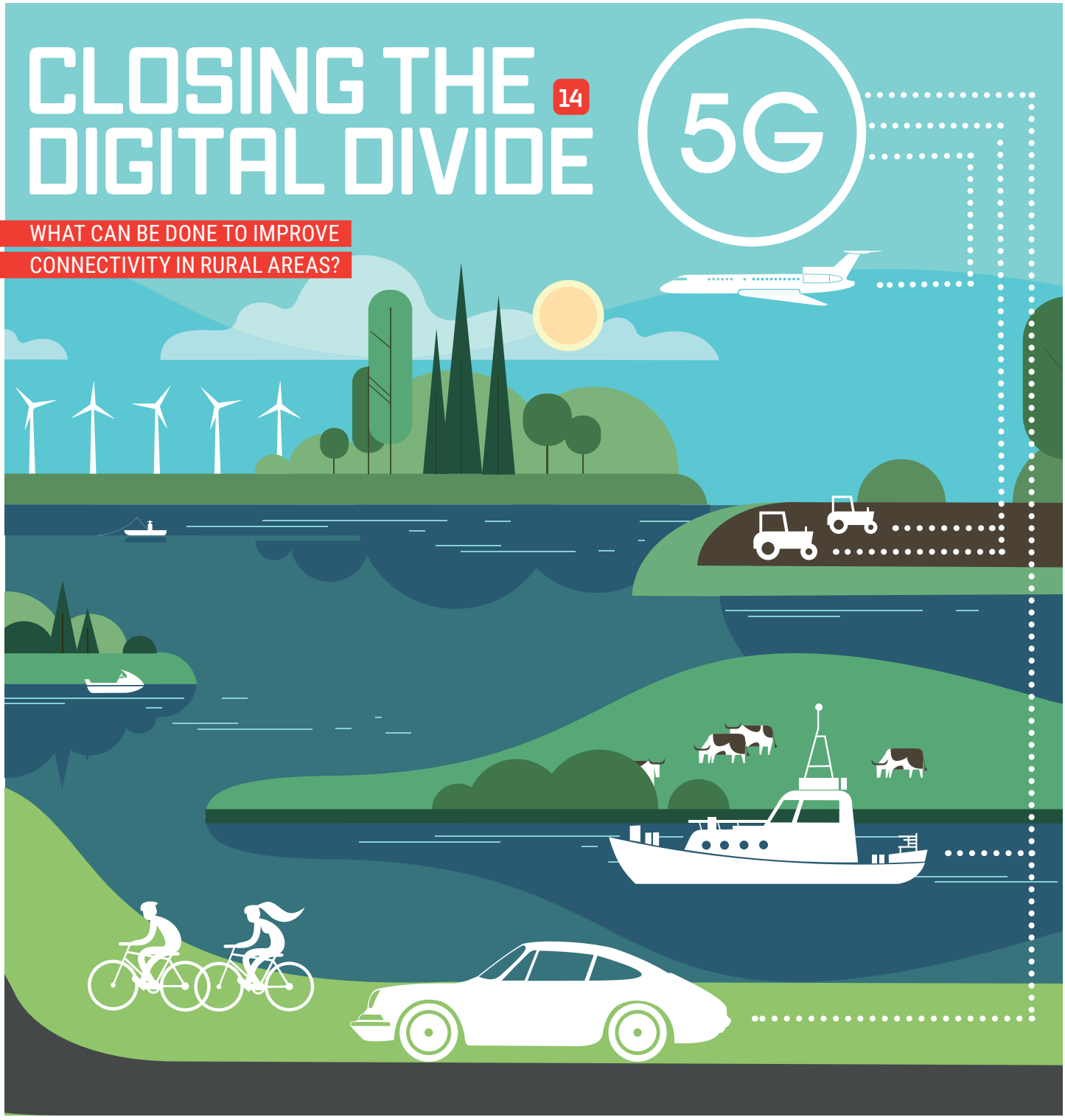
VOLUME 54 / ISSUE 15
OCTOBER 2021

new electronics

CLOSING THE DIGITAL DIVIDE 14

5G

WHAT CAN BE DONE TO IMPROVE CONNECTIVITY IN RURAL AREAS?



newelectronics

New Electronics keeps designers and managers abreast of the latest developments in the world's fastest moving industry

Editor	**Neil Tyler** neil.tyler@markallengroup.com
Contributing Editors	**Chris Edwards, John Walko** editor@newelectronics.co.uk
Art Editor	**Chris Charles** chris.charles@markallengroup.com
Illustrator	**Phil Holmes**
Sales Manager	**James Creber** james.creber@markallengroup.com
Publisher	**Peter Ring** peter.ring@markallengroup.com
Managing Director	**Jon Benson** jon.benson@markallengroup.com
Production Manager	**Nicki McKenna** nicki.mckenna@markallengroup.com

New Electronics editorial advisory panel

Trevor Cross, Chief Technology Officer, Teledyne e2v
Pete Leonard, Electronics Design Manager, Renishaw
Pete Lomas, Director of Engineering, Norcott Technologies
Neil Riddiford, Principal Electronics Engineer, Cambridge Consultants
Adam Taylor, Embedded Systems Consultant

ISSN 0047-9624 Online ISSN 2049-2316

Annual subscription (12 issues):
UK £108. Overseas; £163. Airmail; £199.
New Electronics, incorporating Electronic Equipment News and Electronics News, is published twice monthly by MA Business, Hawley Mill, Hawley Road, Dartford, DA2 7TJ. T: 01322 221144
E: ne@markallengroup.com

Moving on?
If you change jobs or your company moves, please contact **circulation@markallengroup.com** to continue receiving your free copy of New Electronics

MA Business
Part of
Mark Allen
www.markallengroup.com

OCTOBER ISSUE

NEW ELECTRONICS WEEKLY EZINE

NEW ELECTRONICS' weekly eZine features the latest blogs, news, articles and more. To register for your copy, go to **www.newelectronics.co.uk**

AUTHOR DETAILS
Michael Barrett
Managing Director of Nexus Industrial Memory

DID YOU KNOW?
29.3bn connected devices by 2023, according to Cisco's Annual Internet Report

EMBEDDED... BUT EXPOSED

With more and more operational technology systems becoming IoT-enabled, the attack surface for cyber-attacks is getting larger. MICHAEL BARRETT discusses the threats and solutions.

In the world of consumer electronics, the internet of things (IoT) provides authorised users with remote access to a wealth of smart appliances.

Similarly, the industrial IoT (IIoT) provides authorised users with access to operational technology (OT); essentially embedded systems used to control industrial processes.

Without sufficient security measures in place, hackers have access to the systems too. And the level of security is only as strong as the weakest link - the story of data being stolen from a Las Vegas casino is a case in point; because the access point to the network was a smart thermometer in a fish tank.

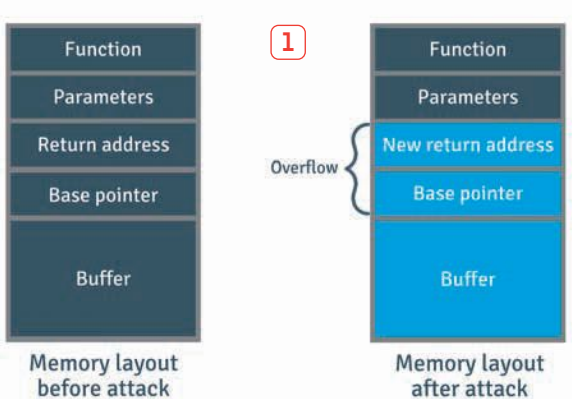
A more recent hack, and for which theft was not the objective, attempted to poison the water supply of a city in Florida by increasing the levels of sodium hydroxide (safe in low concentrations and added to regulate the water's pH level) from 100 to 11,000ppm. The weak link in this case was an instance of TeamViewer that had not been used for months but was still on the system. Also, an official investigation reported that "...all computers shared the same password for remote accesses and appeared to be connected directly to the Internet without any type of firewall protection installed."

OVERFLOW

Many hacks, like the water treatment plant attack, do not alter the system's program. The hacker simply uses it as would an authorised user, but in a malicious way. Other hacks though change the program with a view to making it perform in ways for which it was never intended; to reveal passwords or provide access to other systems, for example.

A common form of attack is through a forced memory (or stack) buffer overflow. These can happen in programs written in low-level languages like C that allow direct memory manipulation. They occur when data is written to memory reserved for run-time activities (such as accepting a password or data from another device) that is larger than intended, and overflows into other memory space and overwrites machine code that governs the system's behaviour.

If a hacker knows how the memory of an embedded system is architected - and in this respect if it is an off-the-shelf product, it can be reverse-engineered to work that out - then the overflow data can, for example, be used to overwrite a return address (see Figure 1) and the system will execute a different part of its program next. This might be to perform a legitimate function, such as



the restoration of factory settings, including resetting passwords to defaults. Or the hacker can simply set a new password. Either way, the hacker has access to the system.

Equally well, the overflow can be used to introduce shellcode (see Figure 2) to give the system new behaviour. This might be to reveal the password set by the legitimate user of the system. Or it could be to reveal the password the device uses to get on to the network and communicate with other devices.

The issue with low level languages like C and C++ is that they are unbounded. For example, the get(s) function in C reads data into a buffer. But there is no limit to the size of that data. Granted, you could add additional code to validate the length of such inbound data or automatically crop it to its expected length.

Alternatively, you could code in a more secure language such as C# or Java. Also, many operating systems have memory management mechanisms too. These include declaring some areas of memory as non-executable and allowing memory spaces used during

© WrightStudio - stock.adobe.com

runtime/execution to be given random locations.

MAKING SECURE

Securing an IoT-enabled embedded system needs to happen at three levels: the network(s) to which the system is connected (and they might be wired or wireless), the system's software and the system's hardware. Of these, a network's communications protocols can always be kept up to date with security patches. Device software (including its OS) can always up be updated too, provided there is sufficient memory space.

System hardware is difficult to update, so a high level of security needs to be designed in from the very start, bearing in mind OT embedded systems are expected to have a much longer life than consumer products.

As mentioned, an embedded OS will have a degree of memory management. It is responsible for ensuring minimal fragmentation and, if it is an RTOS, deterministic memory allocation (malloc) times. However, not all embedded systems have an OS, and a memory management unit (MMU, a hardware component) can be used. Indeed, even when an OS is present, an MMU can be used to augment its capabilities.

Moreover, there is a kind of stripped-down MMU called a memory protection unit (MPU). Also implemented in hardware and typically within the CPU core, it allows only privileged software to allocate memory locations and assign their properties, such as read only or read/write depending on which function is to have access. MPU is, for example, present in Arm's Cortex-M family of processor cores, which are popular in safety critical applications.

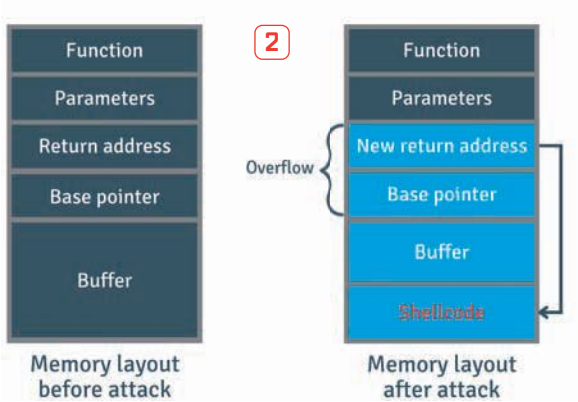
Recent advances in memory devices such as SSDs are providing even stronger countermeasures to cyberthreats. For example, Singapore-based memory device OEM Flexxon is claiming to be the first to market with an embedded AI cyber secure drive. The AI resides in a dedicated co-processor and firmware that monitors for cyberthreats in real time.

The SSDs are proving popular with PC and laptop manufactures (Flexxon has just done a deal with Lenovo, for example) because X-PHY's machine learning algorithms observe how the drive reads and writes data, plus responds to other commands, during normal operation. Ransomware, Zero-day and other cyberattacks result in out-of-the ordinary behaviour, and that is what the AI is looking for.

In the event of such behaviour, X-PHY locks down all data. It can even execute a 'Secure Erase' function, under which the memory mapping table and storage blocks are deleted, and random data is written to the SSD, even if power to the drive is removed. And another Flexxon SSD, popular in the defence sector, even has a Self-destruct feature. It burns out all the drive's NAND flash ICs using a high voltage.

An embedded system's functionality is defined by its program and the movement of data, both of which reside in memory. That is what must be protected. IT specialists assume that hackers are always trying to get in, hence the frequency with which security patches are issued for networks, operating systems and applications; notably after a new variant of cyberthreat has been discovered.

Updating hardware, which may have been in the field for years, in response to a newly discovered cyberthreat is not so easy. It is also not easy (read unnatural), when designing a product to interface with other systems via the IoT, for designers to assume inbound data will be anything other than what is expected. We're an honest bunch. However, increasingly, we must all operate a Zero Trust policy, if the IoT-enabled OT embedded systems we are designing are to be as cybersecure as possible. NE



1 2 Overflow attacks can overwrite return addresses to alter the execution of the program and, for example, set a new password or restore the default one. They can also be used to introduce shellcode.