Hack-proof drones offer antidote for IoT security “naiveté”: NICTA researcher

David Braue (CSO Online) on 12 October, 2015 15:43

Granular, mathematically-proven security controls built into NICTA's military-grade seL4 operating system will provide a model for countering the “naiveté” of Internet of Things (IoT) developers favouring functionality over security, the head of the organisation's Data61 research program believes.

Developers of IoT devices – which include a growing flood of connected smart watches, home-automation, smart-Internet, sensors, drones, cameras and other equipment that is testing the industry's security capabilities, raising privacy concerns and spurring entreaties for caution from security researchers – have shown “a lot of the same naiveté as in other areas ten years earlier,” professor Gernot Heiser, head of NICTA's Embedded, Real-Time and Operating Systems (ERTOS) Research Program, told CSO Australia.

“Those people are thinking of functionality, but not of security. A lot of people think about functionality but at the moment security is still in the minority. But it's really important that we change that mindset.”

The sense of urgency around addressing the biggest problems with IoT security was rapidly growing after hacks on conventional equipment such as the Jeep Cherokee that was sensationally remote-controlled by hackers earlier this year.

Growing fleets of autonomous cars could, Heiser warned, pose public-safety and economic risks if they were hacked and similarly controlled by malicious outsiders; such threats recently drove the UK to set new rules for driverless cars and inspired Intel to set up the Automotive Security

Featured Whitepapers

Active visibility for multi-tiered security

The need for active visibility

Editor's Recommendations

Quantum Computing threatens to crack Internet Security

As hacks mount, October's cybersecurity push refocuses urgency for user, executive engagement

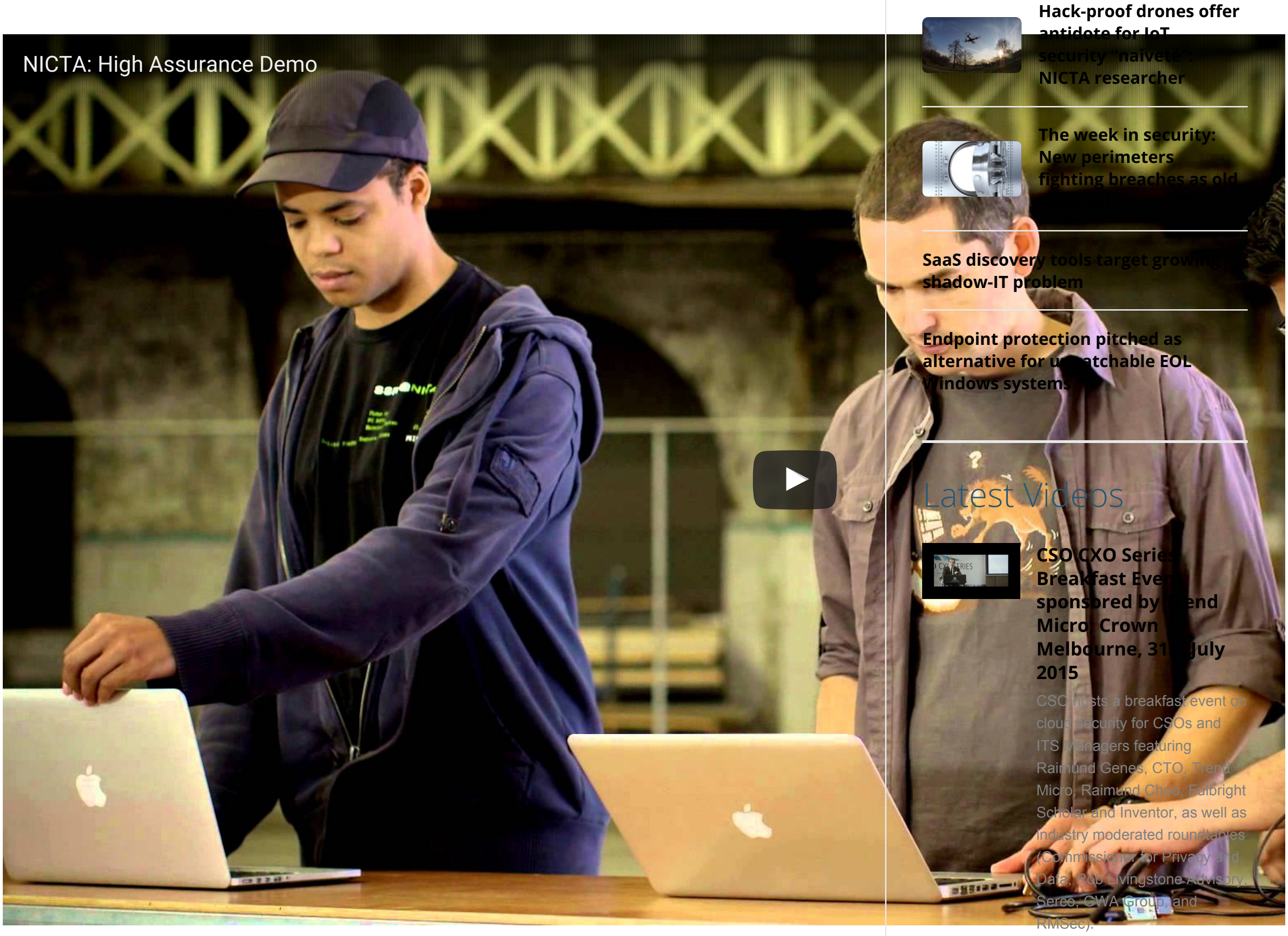
As Stagefright 2.0 emerges, HTC can’t commit to monthly Android patches

Review Board to focus efforts around car security.

Medical equipment was also, frighteningly, proving exposed as “mushrooming functionality” and improved connectivity to equipment like pacemakers was creating looming security threats. “Security is becoming a safety issue,” Heiser said.

Recognising the need for embedded computing environments to be completely secure, Heiser and his team have spent years tweaking the eaL4 environment, a free platform that has been designed from the ground up for security.

Its 10,000 or so lines of code – a fraction of the 10 million lines in the Linux kernel, for example – have been mathematically proven to be completely secure, and a recent field demonstration showed why this was important as researchers hacked into and crashed an off-the-shelf Quadcopter drone – but proved unable to compromise a similar device running an eaL4-based controller.



“The interesting thing is that we could take an existing vehicle, with all its negatives, and secure it in some way,” Heiser said. “It's always easier to build something from scratch when you know what you're doing, but it's a bigger challenge to convert something and make it more secure.”

The eaL4 microkernel has been built using a minimalist approach with carefully architected hardware wrappers, which provide hooks into the overlying components that control specific functionality of each device.

And while those components were not always as secure as the underlying kernel, its intrinsically secure design was able to isolate the components from systems' core functionality.

“We have high-assurance ways of gluing these components together and ensuring that their

Solution Centres

LogRhythm Security Intelligence

F5 Application Security Zone

Stories by David Braue

Hack-proof drones offer antidote for IoT security “naiveté”: NICTA researcher

The week in security: New perimeters fighting breaches as old

SaaS discovery tools target growing shadow-IT problem

Endpoint protection pitched as alternative for unpatchable EOL Windows systems

Latest Videos

CSO CXO Series Breakfast Event sponsored by Trend Micro, Crown Melbourne, 31 July 2015

CSO hosts a breakfast event on cloud security for CSOs and ITS Managers featuring Raimund Genes, CTO, Trend Micro, Raimund Choo, Fulbright Scholar and Inventor, as well as industry moderated roundtables (Commissioner for Privacy and Data, Rob Livingstone Advisory, Serco, CWA Group, and RMSec).

▶ PLAY VIDEO

Technical Issues

Safeguarding the crown Jewels

▶ PLAY VIDEO

Business Challenges

Quality of Security - Defense in Depth

▶ PLAY VIDEO

The Future Ready IT Series

Computerworld Exchange talks to David Siroky, Director Dell Enterprise Solution & Alliances interaction is secure,” Heiser said. “Trustworthy components can interact with untrustworthy components, but in a very controlled way.”

Unsurprisingly, the team's work has found great interest within the military community, and the Data61 team has been working with DARPA's High-Assurance Cyber Military Systems (HACMS) program to build on its secure kernel work as part of the five-year, $US18m Secure Mathematically-Assured Composition of Control Models (SMACCM) project. SMACCM, of which the drone demonstration was a recent deliverable, combines teams from NICTA, Rockwell Collins, Galois Inc, Boeing, and the University of Minnesota.

“The core technology, in terms of the OS kernel, provides very strong isolation guarantees and is hack-proof and crash-proof,” Heiser says. “Using this platform, we can just replace a lot of the existing software and [illegible] cure way.”

0 Comments f 0 4 in 0 g+

With the usage and capabilities of IoT devices exploding – their common vulnerabilities and methods for securing them have become a fundamental part of the security-industry conversation. Organisers of this year's Def Con organised a special workshop for IoT hacking whose sole purpose was to compromise such devices.

Vendors are starting to work towards building IoT frameworks that facilitate management and security of large fleets of devices: Verizon Enterprise Solutions launched one such solution earlier this year, as did Fujitsu. LogMeIn this month updated its Xively Identity Manager with an IoT focus, while startups like ZingBox are garnering attention for their specific focus on IoT security.

There will surely be more hacks before manufacturers get a handle on what it takes to do IoT securely, and a recent survey suggested that most Australian IT departments still lack the skills to implement IoT correctly.

However, work like NICTA's is at least starting to attract some interest. Discussions about channeling eaL4's legacy into the IoT industry had produced “nothing concrete” yet but Heiser said the organisation is having “a number of conversations with people operating in that space”.

READ MORE
Mobile app developers “duped” into distributing data-scraping malware: NICTA

Want to know more?

Why not become a CSO member and subscribe to CSO's mailing list.

Get newsletters, updates, events and more right here.

Tags boeing | Hack-proof drones | OS kernel | Data61 | University of Minnesota | IoT security | Galois Inc | Rockwell Collins | IoT hacking | nicta

More about Assurance | Cherokee | CSO | Intel | Linux | LogMeIn | NICTA | Rockwell | Verizon

Read next

Team about the next generation Data Centre

▶ PLAY VIDEO

A Fireside Chat with Ron Gula

An interview with Ron Gula, CEO and CTO of Tenable Network Security conducted by David Braue, CSO Australia.

▶ PLAY VIDEO

More videos ▸

Blog Posts

From IT security to information security and beyond...
Matthew Hackling

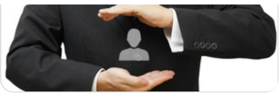
Awareness
Matt Tett

Are you on the backfoot?
Jarrod Loidl

Internet Security....the final word.....well maybe the second final.....ah, maybe one more after that.....
Drazen Drazic

Cisco: notorious hackers using Linux cloak earn $30m a year

IBM wants to stop rogue staff using Dropbox to steal customer databases



As hacks mount, October's cybersecurity push refocuses urgency for user, executive engagement

10 cutting-edge security threats

In Pictures: Hacking Team's hack curated

The Cybersecurity Game: Improving the Odds In the Defender's Favor

0 Comments CSO Australia Исследовательс...

Recommend Share Sort by Best

Start the discussion…

Be the first to comment.

Subscribe Add Disqus to your site Privacy DISQUS

Market Place

Send Us E-mail | Privacy Policy [Updated 3 Mar 14] | Subscribe to emails | Contacts

IDG Sites: PC World | GoodGearGuide | Computerworld Australia | CIO | CMO | Techworld | ARN | CIO Executive