18 October 2017

Synopsis

Scroll to read full summaries with links to news articles.

A security expert from **Belgian** university KU Leuven, **Mathy Vanhoef**, has found a security flaw that leaves nearly all devices that support **WI-FI** vulnerable to **hacking**. **Cybersecurity** teams across the world are examining these vulnerabilities.

The **UK** and **Canada** have committed to working collaboratively to strengthen **digital government** developments in both countries. They plan to provide better services, teach children how to code, share information and promote open data and standards to tackle issues of **cybersecurity**.

Following a review of the **EU-US Privacy Shield**, the **European Commission** has stated that whilst the agreement had "ensured adequate protection and safeguards" it had identified eight areas in which the data sharing agreement could improve.

A coalition of 40 organisations including, the American Civil Liberties Union **NAACP** and the **Freedom of the Press Foundation**, told the House Judiciary Committee that it is opposing the **USA Liberty Act**. These groups believe that the act would give the USA too much power to gather data on innocent Americans without a warrant.

Kaspersky Lab and **Interpol** signed a **cybersecurity** sharing agreement last Thursday to strengthen their relationship. Kaspersky hopes this will rehabilitate their reputation with the **United States** after they decided to ban the company's security products last September.

Tech Central has discovered personal information online relating to the unique ID numbers, income and employment history of some 30 million **South Africans**. It is suspected that the data belonged to the government at one point however this has not yet been confirmed.

The **Australian** Cyber Security Centre's **2017 Threat Report** has confirmed that Australian companies continue to see a rise in **cyberattacks**, with a rise in Phishing attacks, highlighting the need for companies to build **cybersecurity** into

supply chain contracts and for businesses to be more open about cyber incidents.

Disclaimer: Please note that this monitor is a summary of news sources and does not reflect the official views of IEEE.

For more information, visit the IEEE Internet Initiative website, and see *IEEE Global Internet Policy Monitor* past issues. Join IEEE Collabratec™ Internet Technology Policy Community discussions related to internet policy issues and to collaborate with other members of the global technical and policy communities.

IEEE Global Internet Policy Monitor

18 October 2017

Table of Contents

Europe

Internet governance

13.10.17

GOV.UK

Memorandum of understanding between Canada and United Kingdom

The UK and Canada have committed to working collaboratively to strengthen digital government developments in both countries. They plan to provide better services, teach children how to code, share information and promote open data and standards to tackle issues of cyber security.

"The UK and Canadian Governments have signed a Memorandum of Understanding (MOU) relating to each nation's ambitions for Digital Government."

Cybersecurity

13.10.17

Computer Weekly

London issues call to arms to cyber security community

The London Digital Security Centre met with small businesses last Thursday to call for cooperation on cyber-crime, as often SME's have fewer resources to protect themselves against hackers.

"London is calling on the cyber security community to help keep the city's more than one million small businesses safe from cyber-crime."

"Cyber-crime is a growing problem for everyone, but while individuals are protected by their banks, small businesses can be sunk if their [banking] details are hacked," said Rebecca Lawrence, chief executive, Mayor's Office for Policing and Crime.

16.10.17

Guardian

[‘All Wi-Fi networks’ are vulnerable to hacking, security expert discovers.]

A security expert from Belgian university KU Leuven, Mathy Vanhoef has found a security flaw, which leaves nearly all devices that support WI-FI vulnerable to hacking. Cybersecurity teams across the world are examining these vulnerabilities.

“The security protocol used to protect the vast majority of WIFI connections has been broken, potentially exposing wireless internet traffic to malicious eavesdroppers and attacks, according to the researcher who discovered the weakness.”

16.10.17

SC Media

[Iran is being blamed for a cyber-attack against Parliamentary emails]

The 9,000 UK Parliamentary email accounts that were hacked earlier this year are now being blamed on Iran, making this the countries first major cyber-attack against the UK.

“The 23 June 12-hour brute force hack-attack against 9,000 parliamentary email accounts, including minsters and the PM, is now being blamed on Iran.”

“If correct, this unpublished assessment by British intelligence reported in the Times and claimed to be independently verified by The Guardian, would be Iran's first significant act of cyber-warfare against the UK – disclosed at a time when the UK is opposing Trump moves to rescind an agreement to drop sanctions against Iran if it ceased nuclear arms development.”

16.10.17

SC Media

[Defence Minister says Poland fended off Russian cyber- attack on business]

Polish Defence Minister, Antoni Macierewicz, has announced that Poland successfully blocked another cyber-attack from Russia after hackers attempted to infiltrate businesses in the Ukraine and Poland.

"Less than two weeks after news surfaced of Russian hackers accessing the phones of 4,000 NATO troops in Poland and other European nations, Poland's defence minister reportedly disclosed that his country successfully stopped yet another Russian cyber-attack."

Privacy

12.10.17

SC Media

Homes and Communities Agency breach reported to ICO

The Homes and Communities Government Agency has notified the Information Commissioner's Office (ICO) that there has been a minor breach of its information security policy. Government agencies are becoming more active in reporting limited breaches to the ICO ahead of the introduction of GDPR next year.

"*No doubt getting itself ready for the 72-hour breach reporting requirements of GDPR, on Wednesday 11 October the UK government agency, the Homes and Communities agency, reported that it has notified the Information Commissioner's Office of a limited breach of its information security policy on Monday 9 October."*

16.10.17

ARS Technica

Dutch Privacy Regulator says Windows 10 breaks the law

The Dutch Data Protection Authority has announced that Microsoft's Windows 10 system breaches Dutch law as a lack of transparency in how Microsoft uses data collected from Windows 10 means that consumers are prevented from giving their informed consent.

"To comply with the law, the DPA says that Microsoft needs to get valid user consent: this means the company must be clearer about what data is collected and how that data is processed. The regulator also complains that the Windows 10 Creators Update doesn't always respect previously chosen settings about data collection."

16.10.17

Euractiv

Data protection and digital single market struggle to combine in Europe

EU Director General for Justice, Tiina Astola has argued that the introduction of GDPR in 2018 will make the EU the world leader on digital privacy issues.

"Despite a growing number of cyber-attacks in Europe and the increased use of the Internet by criminal and terrorist groups, Tiina Astola, head of DG Justice, delivered a positive message during the fourth Congress of European Notaries in Santiago de Compostela.

"The new EU law on data protection that will enter into force in May 2018 is highly advanced. We are at the forefront of data protection in Europe. We did a lot of work to get here," she said."

18.10.17

Computer Weekly

EU-US Privacy Shield data pact is working but needs improvement, says EC

Following a review of the EU-US Privacy Shield, the European Commission has stated that whilst the agreement had "ensured adequate protection and safeguards" it had identified eight areas in which the data sharing agreement could improve.

"After one year of operation, the EU-US data transfer deal Privacy Shield is "working well" but has a lot of "room for improvement", says the European Commission (EC).

More than 2,400 companies are signed up to the voluntary agreement that safeguards the privacy rights of Europeans when their data is transferred to the US. The deal was drawn up after the European Court of Justice did away with the previous Safe Harbour agreement following the Edward Snowden revelations about security services' data gathering."

Internet Inclusion

16.10.17

Computer Weekly

Government launches £25m trial fund to develop UK 5G industry

The Department for Digital, Culture, Media and Sport has awarded £25m of the National Productivity Investment fund to develop 5G mobile technology and position the UK as a leader in the technology.

"The Department for Digital, Culture, Media and Sport (DCMS) is inviting interested parties from around the UK to apply for match-funded grants out of a £25m funding pot to develop and test 5G mobile network technology and help cement the country's position as a leader in 5G."

United States of America

Internet governance

18.10.17

The Hill

Google to offer enhanced Gmail security to journalists, government officials

Google announced last week that it is creating stronger security protections for journalists and government officials who are more vulnerable to attacks. Once they have signed up to the Advanced Protection Program their accounts will be updated continuously to deal with vulnerabilities.

"Google announced Tuesday that it's rolling out new, stronger security protections for a small set of users, such as journalists and government officials, who face a higher risk of being targeted by hackers."

"The protections are a part of a new Advanced Protection Program, which provides what Google says are its strongest security features. Once users sign up for the program, their accounts' security will be continuously updated by Google as it patches different vulnerabilities and beefs up its cybersecurity."

Cybersecurity

12.10.17

SC Media

Kaspersky Lab renews threat sharing relationship with INTERPOL

Kaspersky Lab and Interpol have signed a cybersecurity sharing agreement last Thursday to strengthen their relationship. Kaspersky hopes this will rehabilitate their reputation with the United States after they decided to ban the company's security products last September.

"Kaspersky Lab and Interpol announced on Thursday that they have signed a new cybercrime threat sharing pact that will strengthen the two organizations' collaborative relationship."

12.10.17

Ars Technica

Equifax website hacked again, this time to redirect to fake Flash update

Equifax's website has been targeted again with hackers directing customers to install fake updates to their Flash software.

"In May credit reporting service Equifax's website was breached by attackers who eventually made off with Social Security numbers, names, and a dizzying amount of other details for some 145.5 million US consumers.

"For several hours on Wednesday, and again early Thursday morning, the site was maliciously manipulated again, this time to deliver fraudulent Adobe Flash updates, which when clicked, infected visitors' computers with adware that was detected by only three of 65 antivirus providers."

16.10.17

Guardian

'All Wi-Fi networks' are vulnerable to hacking, security expert discovers.

A security expert from Belgian university KU Leuven, Mathy Vanhoef has found a security flaw, which leaves nearly all devices that support WI-FI vulnerable to hacking. Cybersecurity teams across the world are examining these vulnerabilities.

"The security protocol used to protect the vast majority of WIFI connections has been broken, potentially exposing wireless internet traffic to malicious eavesdroppers and attacks, according to the researcher who discovered the weakness."

Privacy

12.10.17

SC Media

Another AWS leak exposes 150,000 Patient Home Monitoring Corp. client records.

150,000 US patients have been affected after 316,363 reports containing blood test results, names of doctors and patients and management notes have been breached.

"Another publicly accessible Amazon S3 repository has been once again been left exposing sensitive consumer information, this time affecting approximately 150,000 U.S. patients."

13.10.17

SC Media

Coalition, including ACLU, write House committee to oppose USA Liberty Act

A coalition of 40 organisations including, the American Civil Liberties Union NAACP and the Freedom of the Press Foundation, have told the House Judiciary Committee that it is opposing the USA Liberty Act. These groups believe that the act would give the USA too much power to gather data on innocent Americans without a warrant.

"A coalition of rights organizations, including the American Civil Liberties Union (ACLU), told the House Judiciary Committee Friday that it will not support the USA Liberty Act, the latest version of a surveillance reform bill meant to extend the federal government's spying authority under Section 702 of the Foreign Intelligence Surveillance Act (FISA)."

16.10.17

Computer Weekly

Pizza Hut data breach shows need for board control

Pizza Hut failed to notify their customers that personal credit card details had been compromised for over two weeks. 60,000 US customers names, postcodes, delivery addresses, payment card information was all hacked.

"Pizza Hut has come under fire for failing to notify affected customers for two weeks after discovering a data breach that exposed credit card details."

"Affected customers took to Twitter to complain about the delay in notification, with some reporting fraudulent card transactions that may be linked to the breach."

18.10.17

Computer Weekly

EU-US Privacy Shield data pact is working but needs improvement, says EC

Following a review of the EU-US Privacy Shield, the European Commission has stated that whilst the agreement had "ensured adequate protection and safeguards" it had identified eight areas in which the data sharing agreement could improve.

"After one year of operation, the EU-US data transfer deal Privacy Shield is "working well" but has a lot of "room for improvement", says the European Commission (EC).

More than 2,400 companies are signed up to the voluntary agreement that safeguards the privacy rights of Europeans when their data is transferred to the US. The deal was drawn up after the European Court of Justice did away with the previous Safe Harbour agreement following the Edward Snowden revelations about security services' data gathering."

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

13.10.17

The Epoch Times

South Korea Rushes to Patch Up Cybersecurity After North Korea Steals Top Secret War Plans.

South Korean Defence Minister, Song Young-Moo ordered the military, last Thursday, to patch up vulnerabilities in their systems to prevent further cyber-attacks from North Korea.

"South Korea is scrambling to patch up vulnerabilities in cyberspace, after a shocking report emerged that North Korean hackers had stolen a large cache of military documents last year. The compromised information includes a top-secret war plan to remove Kim Jong Un, the head of the North Korean regime."

16.10.17

Guardian

'All Wi-Fi networks' are vulnerable to hacking, security expert discovers.

A security expert from Belgian university KU Leuven, Mathy Vanhoef has found a security flaw, which leaves nearly all devices that support WI-FI vulnerable to hacking. Cybersecurity teams across the world are examining these vulnerabilities.

"The security protocol used to protect the vast majority of WIFI connections has been broken, potentially exposing wireless internet traffic to malicious eavesdroppers and attacks, according to the researcher who discovered the weakness."

Privacy

No new items of relevance

Internet Inclusion

No new items of relevance

Rest of the World

Internet governance

No new items of relevance

Cybersecurity

12.10.17

SC Media

Kaspersky Lab renews threat sharing relationship with INTERPOL

Kaspersky Lab and Interpol have signed a cybersecurity sharing agreement last Thursday to strengthen their relationship. Kaspersky hopes this will rehabilitate their reputation with the United States after they decided to ban the company's security products last September.

"Kaspersky Lab and Interpol announced on Thursday that they have signed a new cybercrime threat sharing pact that will strengthen the two organizations' collaborative relationship."

13.10.17

Computer Weekly

Australia's state of cyber security report reveals rise in phishing attacks.

The Australian Cyber Security Centre's 2017 Threat Report has confirmed that Australian companies continue to see a rise in cyberattacks, with a rise in Phishing attacks, highlighting the need for companies to build cybersecurity into supply chain contracts and for businesses to be more open about cyber incidents.

"Australian companies saw a 15% increase in cyber incidents last year, underscoring Australia's position as one of the most targeted countries in the Asia-Pacific region."

15.10.17

Ars Technica

Australian defence firm was hacked and F-35 data stolen, DOD confirms

At an IT conference in Sydney, Mitchell Clarke, ASD Incident Response Manager has confirmed further details regarding the amount of data stolen from an Australian defence company. He said that, "the compromise was extensive and extreme" as 30 gigabytes of data was taken.

The Australian Cyber Security Centre noted in its just-issued 2017 Threat Report that a small Australian defence company "with contracting links to national security projects" had been the victim of a cyber-espionage attack detected last November.

16.10.17

Guardian

'All Wi-Fi networks' are vulnerable to hacking, security expert discovers.

A security expert from Belgian university KU Leuven, Mathy Vanhoef has found a security flaw, which leaves nearly all devices that support WI-FI vulnerable to hacking. Cybersecurity teams across the world are examining these vulnerabilities.

"The security protocol used to protect the vast majority of WIFI connections has been broken, potentially exposing wireless internet traffic to malicious eavesdroppers and attacks, according to the researcher who discovered the weakness."

16.10.17

SC Media

Iran is being blamed for a cyber-attack against Parliamentary emails

The 9,000 UK Parliamentary email accounts that were hacked earlier this year are now being blamed on Iran, making this the countries first major cyber-attack against the UK.

"The 23 June 12-hour brute force hack-attack against 9,000 parliamentary email accounts, including minsters and the PM, is now being blamed on Iran."

"If correct, this unpublished assessment by British intelligence reported in the Times and claimed to be independently verified by The Guardian, would be Iran's first significant act of cyber-warfare against the UK – disclosed at a time

when the UK is opposing Trump moves to rescind an agreement to drop sanctions against Iran if it ceased nuclear arms development."

16.10.17

SC Media

Defence Minister says Poland fended off Russian cyber- attack on business

Defence Minister, Antoni Macierewicz, has announced that Poland successfully blocked another cyber-attack from Russia after hackers attempted to infiltrate businesses in the Ukraine and Poland.

"Less than two weeks after news surfaced of Russian hackers accessing the phones of 4,000 NATO troops in Poland and other European nations, Poland's defence minister reportedly disclosed that his country successfully stopped yet another Russian cyber-attack."

Privacy

17.10.17

Huffington Post

Data Breach: Millions of South Africans' Personal Info Exposed

Tech Central has discovered personal information online relating to the unique ID numbers, income and employment history of some 30 million South Africans. It is suspected that the data belonged to the government at one point however this has not yet been confirmed.

"A massive data bank containing millions of South Africans' personal information -- including property ownership, income and employment history -- has been discovered by information security researcher Troy Hunt, Tech Central revealed on Tuesday."

Internet Inclusion

No new items of relevance

Global Institutions

11.10.17

Computer Weekly

Cyber Threats are among top dangers, says NATO

According to the Assistant Secretary General for emerging security challenges, Sorin Ducaru, cyber security threats are now one of the most pressing priorities for NATO.

"NATO's adviser on emerging security challenges tells conference of growing challenge posed by security threats"

"Cyber threats are one of the most pressing priorities for NATO, according to Sorin Ducaru, the organisation's assistant secretary general for emerging security challenges."

Diary Dates

ICANN 60 – 28.10.17-03.11.17

Abu Dhabi, United Arab Emirates

BSG – 02.11.17

Bride Street, London, United Kingdom

GCCS – 23.11.17-21.11.17

Aero City, New Delhi, India.

IGF 2017 – 18.12.17–21.12.17

Geneva, Switzerland

Manusec Europe – 07.02.18-08.02.18

Munich, Germany

Global Internet And Jurisdiction Conference 2018 – 26.02.18-28.02.18

Ottawa, Canada

RSA – 16.04.18–20.04.18

San Francisco, USA

Africa Internet Summit – 29.04.18-11.05.18

Dakar, Senegal