15 March 2017

Synopsis

Scroll to read full summaries with links to news articles.

The **European Commission's** Digital Single Market Commissioner and Vice President **Andrus Ansip** has expressed confidence in the future of the EU-US **Privacy Shield** following a meeting with his US counterparts.

Germany have produced a draft law that will allow it to fine social media firms if they fail to act against hate speech on their platforms. The law would allow the government to fine firms up to €50 million.

The Ministry of Digital Affairs in **Poland** has released a draft proposal for its future **cybersecurity** strategy for 2017-2022. Among the plans included in the draft strategy is a call for a dedicated fund to develop Poland's cyber-defences.

In the **United States** this week the White House has released its annual cyber report detailing the number of **security** incidents that affected the Federal Government during the 2016 fiscal year. The report found that 30,000 incidents compromised federal systems, though only 16 of these were classified as major incidents requiring a report to Congress.

State legislators in **New Hampshire** have unanimously approved legislation that will require law enforcement to seek **consent** or warrants before using **stingray surveillance** technology on suspects. The new law will place considerable restrictions on the use of stingray, which is widely used across the US for warrantless surveillance.

A new report by **Trend Micro** has found that countries in the **Asia Pacific** region were victims of the largest number of **cyberattacks** in 2016. The company's Global Roundup Report found that the company had helped to prevent a total of 80 billion attacks worldwide.

Following the leak of CIA **cyberespionage** by **Wikileaks** last week, **China** has expressed concern at the revelations. Particular concern was given to the alleged ability of the **CIA** to target Chinese made servers developed by **Huawei** and **ZTE**.

In **India** the telecoms regulator **TRAI** has proposed that small entrepreneurs and businesses be allowed to become **WiFi** hotspots as a way to grow the country's internet services.

The **African Union** has this week launched the first .africa domain name as part of an effort for businesses and individuals to further champion Africa in **cyberspace**.

ICANN have launched a new testing platform for network operators ahead of the October rollover of the **DNSSEC** Key Signing Key. ICANN is aiming to provide a smooth transition for the 750 million people likely to be affected by the rollover.

IEEE Global Internet Policy Monitor

15 March 2017

Table of Contents

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

Europe

Internet governance

14.03.17

Euractiv

Germany set to fine social media platforms millions over hate speech

Germany's Justice Minister Heiko Maas has proposed a new draft law that would allow the Government to fine social media firms if they fail to remove hate speech from their platforms. The maximum fine will be €50 million for organisations and €5 million for individuals. The European Commission is currently deciding what action will be taken as a whole by the EU to counter online hate speech.

"A new draft German law would fine social media firms up to €50 million if they fail to remove hate speech, jumping ahead of EU plans. The European Commission is still weighing up whether it will propose rules to crack down on online hate speech.

German Justice Minister Heiko Maas (SPD) has lost his patience with big tech firms. He had been speaking out against their slow response to online hate speech for months. In an effort to defuse growing tensions, Facebook hired extra staff in Germany last year just to deal with social media users' complaints more quickly."

Cybersecurity

13.03.17

SC Magazine

Poland's Digital Affairs Ministry Releases Draft Cyber-Security Strategy

The Polish Government has published its draft Cybersecurity strategy for 2017-2022. The major proposal of the strategy is a dedicated fund for the development of cyberdefence capabilities, which will consolidate the mechanisms currently divided amongst varios departments and institutions in Poland.

"The Polish Ministry of Digital Affairs has released the draft Cyber-Security Strategy for the years 2017 to 2022 after concluding the phase of inter-ministerial consultation.

The document identifies the measures and mechanisms that are to strengthen Poland's cyber-security capabilities by 2022, and states that it is

indispensable to create a dedicated fund which would serve to finance the development of cyber-defence capacities within the state budget. Currently, a number of projects related to cyber-security are financed from the budgets of separate ministries and state institutions."

14.03.17

Reuters

Germany's Merkel warns against cyber attacks on infrastructure

Chancellor Angela Merkel has called for greater collaboration between federal and local state actors to improve the cybersecurity of Germany's key infrastructure. In her speech the Chancellor highlighted previous attacks in the Ukraine and elsewhere which had had significant repercussions.

"German Chancellor Angela Merkel said on Tuesday protecting infrastructure from potential cyber attacks was a top priority and the federal government had to work together with localities on that.

"Today we have a huge amount of possibilities to paralyze infrastructure from cyber attacks and it is... very very difficult. There are examples from Ukraine that are worrying. Therefore cyber security is of great, great importance," she said."

14.03.17

SC Magazine

Cyber-security pros say more industrial IoT cyber-attacks expected

A new study by IT security experts Tripwire has found that a majority of cybersecurity experts believe that IoT devices will face an increasing number of cyber attacks in the coming years as the technology becomes more widespread.

"The results of a recent survey querying IT security pros about the threats posed by devices tethered to the internet were practically unanimous: 96 percent of them said they expect to see an increase in security attacks on IoT.

While the study by Tripwire recognised the enormous promise of these devices in facilitating tasks and bringing convenience, ultimately simplifying life for millions, IoT devices also hold a risk as they are not always built with security in mind. In fact, nearly three-quarters of the IT security experts Tripwire polled at Black Hat USA 2016 said their organisation wasn't prepared for IoT-related threats."

14.03.17

SC Magazine

Cybercriminal's skills now on par with nation states: Mandiant

The 2017 M-Trends report by Mandiant has found that whilst companies have improved their ability to identify and respond to breaches in their security they are now facing sophisticated hackers, whose skills are now comparable to those of a national government level actor

"There was some good news reported in Mandiant's M-Trends 2017 report, but this was heavily outweighed by many negative points discovered by the security firm, including cybercriminals being found to use more sophisticated methods and the slow evolution of defensive measures on the part of their victims..

Mandiant, which is a Fireye company, found that in 2016 companies are becoming better at identifying breaches with the average number of days between being compromised and discovery now at 99 day, down from 146 days in 2015. However, Mandiant noted this length of time is more than sufficient for a malicious actor to inflict damage or make off with data. At the same time some cybercriminals have increased their skillset to being comparable to that of a state-level actor."

14.03.17

SC Magazine

Report: Cyber-threat to UK business is "significant and growing"

The UK's National Cyber Security Centre (NCSC) has published a new report into the cybersecurity threats facing UK businesses in conjunction with the National Crime Agency, the UK's equivalent of the FBI. The report details the number of attacks the UK has faced since the NCSC became operational.

"The cyber-threat to UK business is "significant and growing", according to a new report from the UK's National Cyber Security Centre (NCSC) and National Crime Agency (NCA).

The report titled Cyber-Threat to UK Business details how in the three months since the NCSC was created, "the UK has been hit by 188 high-level attacks which were serious enough to warrant NCSC involvement, and countless lower level ones."

Privacy

10.03.17

SC Magazine

U.S., EU both committed to strong Privacy Shield, Ansip says

The European Commission's Digital Single Market Commissioner and Vice President Andrus Ansip has expressed confidence in the future of the EU-US Privacy Shield following a meeting with his US counterparts. Mr Ansip had recently held discussions with U.S. Commerce Secretary Wilbur Ross to establish the future of the EU-US Privacy Shield under the Trump Administration.

"After meeting with U.S. Commerce Secretary Wilbur Ross Thursday, European Commissioner for Digital Single Market and Vice President of the European Commission Andrus Ansip expressed confidence that the U.S. continues to support a strong Privacy Shield.

Ansip tweeted that he and Ross "agreed on the need for a robust and predictable Privacy Shield for safe and secure US-EU data flows." He also took to Twitter to say that he and Rep. Michael McCaul, R-Texas, were aligned regarding "strong US-EU cooperation on cybersecurity," which he said was "essential for IoT and network security."

14.03.17

SC Magazine

Facebook, Instagram prohibit firms from using platform for surveillance

Social media platforms Facebook and Instagram have announced new privacy policies that will prevent third party firms from using custom surveillance tools to investigate users. The changes were developed in collaboration with civil liberties groups like the ACLU and the Center for Media Justice.

"Facebook and Instagram announced that the social media platforms have updated their privacy policies to prohibit private firms from using data obtained from the platforms for surveillance.

The platform announced that over the past few months it has taken enforcement action against developers that have created and marketed surveillance tools in violation of existing Facebook policies, according to a March 13 Facebook post."

Internet Inclusion

No new items of relevance

United States of America

Internet governance

No new items of relevance

Cybersecurity

10.03.17

The Hill

Bipartisan bill would let DHS team with consortiums on cybersecurity

Legislation has been reintroduced to allow the Department of Homeland Security to work with non-profit consortiums in order to aid the development of cybersecurity at the local level. The legislation has been reintroduced by a bipartisan alliance of Texan Senators and Congressmen and will seek to avoid the fate of previous similar legislation.

"Rep. Joaquin Castro (D-Texas) and Sen. John Cornyn (R-Texas) reintroduced legislation Thursday to allow the Department of Homeland Security to work with non-profit consortiums to aid local cybersecurity efforts.

The National Cybersecurity Preparedness Consortium Act would allow the DHS to use consortia to help train local law enforcement and other government, develop information sharing programs and plan local cybersecurity strategies.

The legislation comes as cybersecurity issues are receiving new attention following amid high-profile data breaches and accusations that Russian-backed hackers attempted to sway the election for President Trump."

14.03.17

SC Magazine

Cyber-security pros say more industrial IoT cyber-attacks expected

A new study by IT security experts Tripwire has found that a majority of cybersecurity experts believe that IoT devices will face an increasing number of cyber attacks in the coming years as the technology becomes more widespread.

"The results of a recent survey querying IT security pros about the threats posed by devices tethered to the internet were practically unanimous: 96 percent of them said they expect to see an increase in security attacks on IoT.

While the study by Tripwire recognised the enormous promise of these devices in facilitating tasks and bringing convenience, ultimately simplifying life for millions, IoT devices also hold a risk as they are not always built with security in mind. In fact, nearly three-quarters of the IT security experts Tripwire polled at Black Hat USA 2016 said their organisation wasn't prepared for IoT-related threats."

14.03.17

SC Magazine

Cybercriminal's skills now on par with nation states: Mandiant

The 2017 M-Trends report by Mandiant has found that whilst companies have improved their ability to identify and respond to breaches in their security they are now facing sophisticated hackers, whose skills are now comparable to those of a national government level actor

"There was some good news reported in Mandiant's M-Trends 2017 report, but this was heavily outweighed by many negative points discovered by the security firm, including cybercriminals being found to use more sophisticated methods and the slow evolution of defensive measures on the part of their victims..

Mandiant, which is a Fireye company, found that in 2016 companies are becoming better at identifying breaches with the average number of days between being compromised and discovery now at 99 day, down from 146 days in 2015. However, Mandiant noted this length of time is more than sufficient for a malicious actor to inflict damage or make off with data. At the same time some cybercriminals have increased their skillset to being comparable to that of a state-level actor."

14.03.17

Nextgov

White House's annual Cyber report counts 30,000 incidents but only 16 are "Major"

The White House has published its annual Federal Information Security Management Act report for 2016. The report identifies 30,000 data security incidents across the federal government, along with the 16 incidents that required a report to Congress.

"Federal agencies have made solid progress securing their sensitive data against malicious hackers and employee lapses, but there's still a long road ahead, according to a recently released White House report.

More than 30,000 data security incidents compromised federal information systems during the 2016 fiscal year, 16 of which were categorized as major incidents that needed to be reported to Congress, according to the White House's 2016 Federal Information Security Management Act report released March 10."

Privacy

10.03.17

SC Magazine

U.S., EU both committed to strong Privacy Shield, Ansip says

The European Commission's Digital Single Market Commissioner and Vice President Andrus Ansip has expressed confidence in the future of the EU-US Privacy Shield following a meeting with his US counterparts. Mr Ansip had recently held discussions with U.S. Commerce Secretary Wilbur Ross to establish the future of the EU-US Privacy Shield under the Trump Administration.

"After meeting with U.S. Commerce Secretary Wilbur Ross Thursday, European Commissioner for Digital Single Market and Vice President of the European Commission Andrus Ansip expressed confidence that the U.S. continues to support a strong Privacy Shield.

Ansip tweeted that he and Ross "agreed on the need for a robust and predictable Privacy Shield for safe and secure US-EU data flows." He also took to Twitter to say that he and Rep. Michael McCaul, R-Texas, were aligned regarding "strong US-EU cooperation on cybersecurity," which he said was "essential for IoT and network security."

13.03.17

SC Magazine

New Hampshire House approve Stingray legislation

State legislators in New Hampshire have unanimously approved legislation that will require law enforcement to gain a warrant before using stingray surveillance technology on suspects. The new law will place considerable restrictions on the use of stingray, which is widely used across the US for warrantless surveillance.

"The New Hampshire House unanimously approved a bill restricting warrantless stingray surveillance.

The state's House Bill 474 received the bipartisan support of all the state representatives and the bill mandates that the devices can't be used without the

individuals, informed consent, or a detailed probable cause warrant, or a judicially-recognized exception to the warrant requirement, according to the bill."

14.03.17

SC Magazine

Facebook, Instagram prohibit firms from using platform for surveillance

Social media platforms Facebook and Instagram have announced new privacy policies that will prevent third party firms from using custom surveillance tools to investigate users. The changes were developed in collaboration with civil liberties groups like the ACLU and the Center for Media Justice.

"Facebook and Instagram announced that the social media platforms have updated their privacy policies to prohibit private firms from using data obtained from the platforms for surveillance.

The platform announced that over the past few months it has taken enforcement action against developers that have created and marketed surveillance tools in violation of existing Facebook policies, according to a March 13 Facebook post."

14.03.17

SC Magazine

U.S. Air Force personnel data exposed on internet

MacKeeper Security have identified a misconfigured storage device that had been disclosing the personal identifiable information of US Air Force Officers, on-going criminal investigations and instructions for the recovery of encryption keys for military documents.

"A United States Air Force officer mistakenly exposed not only the personally identifiable information (PII) of many service members, but also the records of on-going criminal investigations and instructions for recovering encryption keys for military documents.

The data was discovered by MacKeeper Security located on a misconfigured storage device, since taken offline, owned by an unnamed lieutenant that was inadvertently made public on the internet."

Internet Inclusion

No new items of relevance

Pan-Asia

Internet governance

No new items of relevance

Cybersecurity

14.03.17

SC Magazine

Cyber-security pros say more industrial IoT cyber-attacks expected

A new study by IT security experts Tripwire has found that a majority of cybersecurity experts believe that IoT devices will face an increasing number of cyber attacks in the coming years as the technology becomes more widespread.

"The results of a recent survey querying IT security pros about the threats posed by devices tethered to the internet were practically unanimous: 96 percent of them said they expect to see an increase in security attacks on IoT.

While the study by Tripwire recognised the enormous promise of these devices in facilitating tasks and bringing convenience, ultimately simplifying life for millions, IoT devices also hold a risk as they are not always built with security in mind. In fact, nearly three-quarters of the IT security experts Tripwire polled at Black Hat USA 2016 said their organisation wasn't prepared for IoT-related threats."

14.03.17

SC Magazine

Cybercriminal's skills now on par with nation states: Mandiant

The 2017 M-Trends report by Mandiant has found that whilst companies have improved their ability to identify and respond to breaches in their security they are now facing sophisticated hackers, whose skills are now comparable to those of a national government level actor

"There was some good news reported in Mandiant's M-Trends 2017 report, but this was heavily outweighed by many negative points discovered by the security firm, including cybercriminals being found to use more sophisticated methods and the slow evolution of defensive measures on the part of their victims..

Mandiant, which is a Fireye company, found that in 2016 companies are becoming better at identifying breaches with the average number of days between being compromised and discovery now at 99 day, down from 146 days in 2015. However, Mandiant noted this length of time is more than sufficient for a malicious actor to inflict damage or make off with data. At the same time some cybercriminals have increased their skillset to being comparable to that of a state-level actor."

16.03.17

Network Asia

Asia Pacific endured the most cyberattacks in 2016, says Trend Micro report

Trend Micro's 2016 Global Roundup Report has found that countries in the Asia Pacific region encountered the most cyberattacks in 2016. The study also found that whilst the number of known threats grew over the last year, there had also been a more troubling increase in the number of previously unknown threats and mixed attacks attempting to bypass conventional cyberdefences.

"Asia Pacific (APAC) encountered the most cyberattacks in 2016 across multiple threat types, compared to other regions, according to Trend Micro Incorporated's 2016 Global Roundup Report.

The data were derived from Trend Micro's threat intelligence database. The company detects and analyzes swathes of threats globally every year, including ransomware, vulnerabilities, exploit kits, mobile apps, online banking software, and so on."

Privacy

09.03.17

Reuters

China expresses concern at revelations in Wikileaks dump of hacked CIA data

Following the disclosure of the CIA's alleged hacking arsenal by Wikileaks, China has stated its alarm at the revelations. China has also reiterated its opposition to cyber hacking and called on the US to end its use of the alleged cyber weapons.

"China expressed concern on Thursday over revelations in a trove of data released by Wikileaks purporting to show that the CIA can hack all manner of devices, including those made by Chinese companies.

Dozens of firms rushed to contain the damage from possible security weak points following the anti-secrecy organization's revelations, although some said they needed more details of what the U.S. intelligence agency was up to."

14.03.17

SC Magazine

Facebook, Instagram prohibit firms from using platform for surveillance

Social media platforms Facebook and Instagram have announced new privacy policies that will prevent third party firms from using custom surveillance tools to investigate users. The changes were developed in collaboration with civil liberties groups like the ACLU and the Center for Media Justice.

"Facebook and Instagram announced that the social media platforms have updated their privacy policies to prohibit private firms from using data obtained from the platforms for surveillance.

The platform announced that over the past few months it has taken enforcement action against developers that have created and marketed surveillance tools in violation of existing Facebook policies, according to a March 13 Facebook post."

Internet Inclusion

09.03.17

Economic Times (India)

TRAI favours PCO-type model for low-cost public Wi-Fi services

The telecoms regulator TRAI has proposed that small entrepreneurs and businesses be allowed to become WiFi hotspots as a way to grow the country's internet services.

"Telecom regulator TRAI today recommended small entrepreneurs and shop owners be allowed to become Wi-Fi hotspot venues and team up with 'aggregators' to offer low-cost public Internet services in a PCO-type model.

"Since there is a significant section of the population still to be connected, measures taken to enable larger service providers to provide public Wi-Fi...will not suffice....Steps need to be taken to ensure that in addition to existing service providers, small providers can also enter the public Wi-Fi ecosystem and have the capability and incentives to provide public Wi-Fi on a small scale," TRAI said."

11.03.17

Philippine Daily Inquirer

National broadband project seen to boost reach of telcos

The Philippine Government has approved a new national program for broadband provision that will aim to improve both access to the internet and internet speed. The program will specifically focus on connecting rural areas as part of a national network.

"The national broadband program, recently approved by President Rodrigo Duterte, is expected to improve internet speed in the country and provide more Filipinos with access to the internet. This will be achieved through a nationwide network that will link previously unconnected rural areas.

Department of Information and Communications Technology (DICT) Secretary Rodolfo Salalima said the national broadband network was needed not only by the public but also by private telecommunication firms to expand the reach of their services toward the countryside."

Rest of the World

Internet governance

10.03.17

Yahoo

Africa Gets Its Own Internet Domain, 26 Years After the World Wide Web Launched

The African Union has this week launched the first .africa domain name as part of an effort for businesses and individuals to champion Africa in cyberspace.

"More than three decades after the first domain name was registered, and over 25 years after the World Wide Web launched, Africa has its own internet domain.

The African Union (AU) launched the .africa domain name Friday, enabling African businesses, companies and individuals to champion their continent in the cybersphere."

Cybersecurity

14.03.17

SC Magazine

Cyber-security pros say more industrial IoT cyber-attacks expected

A new study by IT security experts Tripwire has found that a majority of cybersecurity experts believe that IoT devices will face an increasing number of cyber attacks in the coming years as the technology becomes more widespread.

"The results of a recent survey querying IT security pros about the threats posed by devices tethered to the internet were practically unanimous: 96 percent of them said they expect to see an increase in security attacks on IoT.

While the study by Tripwire recognised the enormous promise of these devices in facilitating tasks and bringing convenience, ultimately simplifying life for millions, IoT devices also hold a risk as they are not always built with security in mind. In fact, nearly three-quarters of the IT security experts Tripwire polled at Black Hat USA 2016 said their organisation wasn't prepared for IoT-related threats."

14.03.17

SC Magazine

Cybercriminal's skills now on par with nation states: Mandiant

The 2017 M-Trends report by Mandiant has found that whilst companies have improved their ability to identify and respond to breaches in their security they are now facing sophisticated hackers, whose skills are now comparable to those of a national government level actor

"There was some good news reported in Mandiant's M-Trends 2017 report, but this was heavily outweighed by many negative points discovered by the security firm, including cybercriminals being found to use more sophisticated methods and the slow evolution of defensive measures on the part of their victims..

Mandiant, which is a Fireye company, found that in 2016 companies are becoming better at identifying breaches with the average number of days between being compromised and discovery now at 99 day, down from 146 days in 2015. However, Mandiant noted this length of time is more than sufficient for a malicious actor to inflict damage or make off with data. At the same time some cybercriminals have increased their skillset to being comparable to that of a state-level actor."

Privacy

14.03.17

SC Magazine

Facebook, Instagram prohibit firms from using platform for surveillance

Social media platforms Facebook and Instagram have announced new privacy policies that will prevent third party firms from using custom surveillance tools to investigate users. The changes were developed in collaboration with civil liberties groups like the ACLU and the Center for Media Justice.

"Facebook and Instagram announced that the social media platforms have updated their privacy policies to prohibit private firms from using data obtained from the platforms for surveillance.

The platform announced that over the past few months it has taken enforcement action against developers that have created and marketed surveillance tools in violation of existing Facebook policies, according to a March 13 Facebook post."

Internet Inclusion

No new items of relevance

Global Institutions

11.03.17

ICANN

Call for Public Comment on the Draft 2016 African Domain Name System Market Study

ICANN has launched a consultation as part of the draft 2016 African Domain Name System Market Study, which aims to identify the developmental goals for the African DNS industry's ecosystem.

*"Today, the Internet Corporation for Assigned Names and Numbers (ICANN) announced **a call for public comment** on the draft 2016 African Domain Name System Market Study, which was commissioned in March 2016 and managed by the South African Communications Forum (SACF) for ICANN.*

The goal of the study is to identify and define the strengths and weaknesses in the African DNS industry ecosystem, and develop recommendations on how to advance the industry by bringing it closer to available opportunities."

13.03.17

ICANN

ICANN Launches Testing Platform for the KSK Rollover

ICANN have launched a new testing platform for network operators ahead of the October rollover of the DNSSEC Key Signing Key. ICANN is aiming to provide a smooth transition for the 750 million people likely to be affected by the rollover.

"ICANN is offering a testing platform for network operators and other interested parties to confirm that their systems can handle the automated update process for the upcoming Root ZoneDomain Name Systems Security Extensions (DNSSEC) Key Signing Key (KSK) rollover. The KSK rollover is currently scheduled for 11 October 2017.

"Currently, seven hundred and fifty million people are using DNSSEC-validating resolvers that could be affected by the KSK rollover," said ICANN's Vice President of Research, Matt Larson. "The testing platform is an easy way for operators to confirm that their infrastructure supports the ability to handle the rollover without manual intervention."

Diary Dates

Building the European data economy – 10.01.17-26.04.17

ENISA evaluation and review – **18.01.17 – 12.04.17**

Open from 18 January to 12 April 2017.

ITU Council 2017 – 15.05.17 – 25.05.17

Geneva, Switzerland

Africa Internet Summit (AIS) 2017 – 29.05.17 – 02.06.17

Nairobi, Kenya

European Dialogue on Internet Governance – 06.06.17-07.06.17

Tallinn, Estonia

World Summit on the Information Society Forum (WSIS) 2017 – 12.06.17 – 16.06.17

Geneva, Switzerland

16th European Conference on Cyber Warfare and Security ECCWS – 29.06.17-30.06.17

Dublin, Ireland

ITU WTDC-17 – 09.10.17 – 20.10.17

Buenos Aires, Argentina

IGF 2017 – 18.12.17 – 21.10.17

Geneva, Switzerland