RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **MBS-W01**

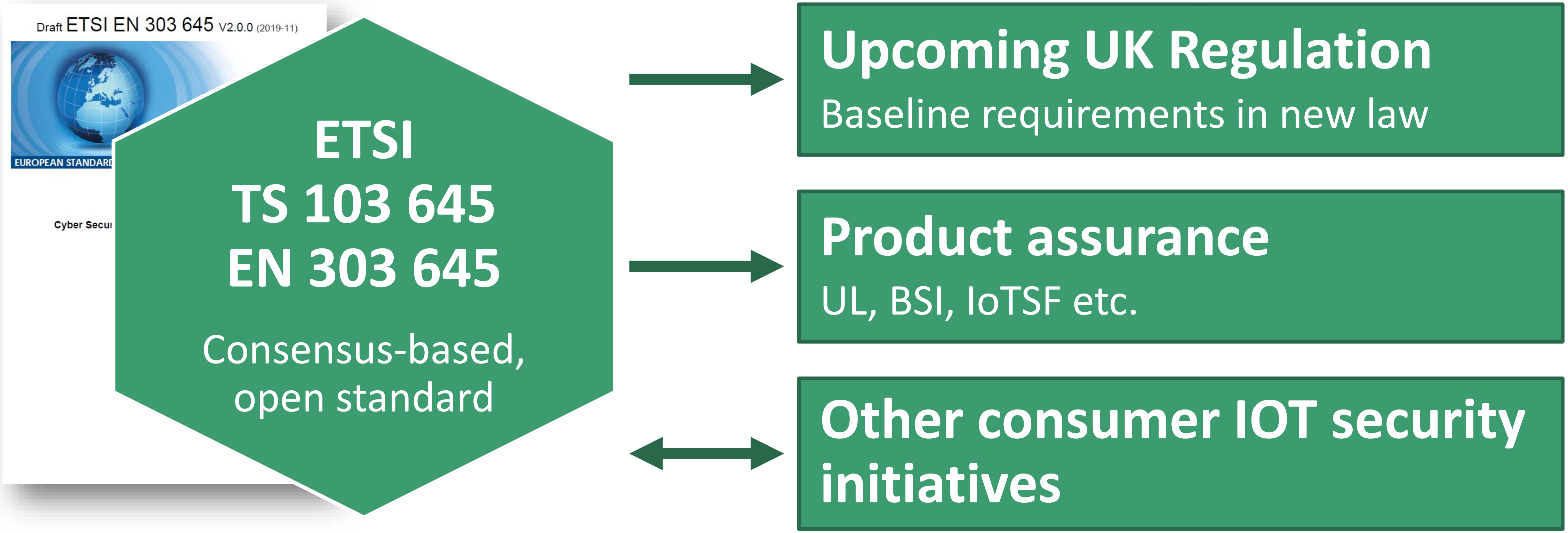
Consumer IoT Security: Creating a Baseline Standard

Jasper Pandza

Jasper Pandza
UK Department for Digital, Culture, Media & Sport
ETSI TS 103 645 / EN 303 645 rapporteur

#RSAC

Progress in “smart” consumer product security



ETSI
TS 103 645
EN 303 645

Consensus-based, open standard

Upcoming UK Regulation

Baseline requirements in new law

Product assurance

UL, BSI, IoTSF etc.

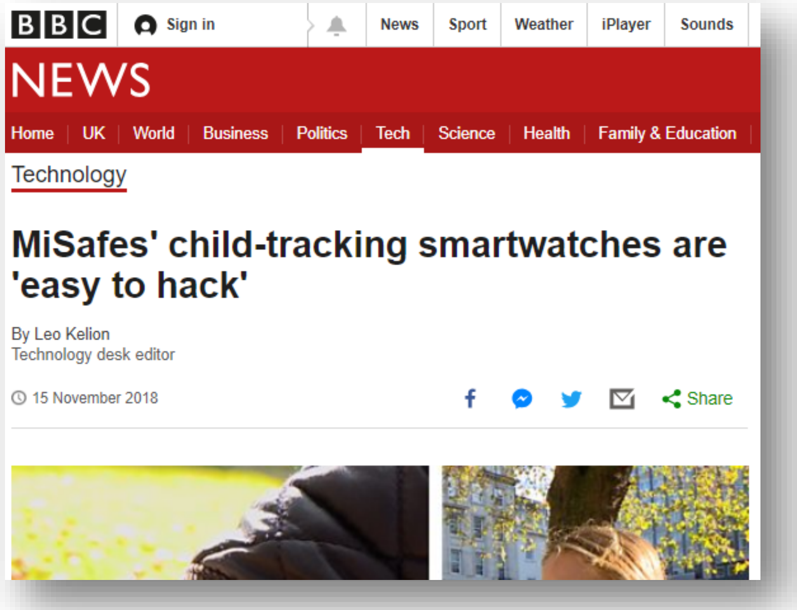
Other consumer IOT security initiatives

If you’ll remember only one thing…

good consumer IoT security = 103 645

Insecure consumer IoT threatens:

Our privacy / safety



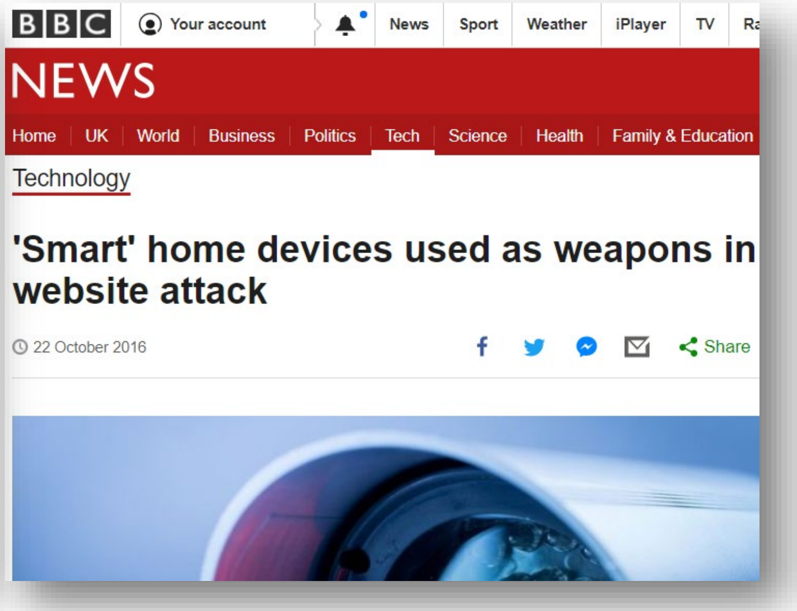
Technology

MiSafes' child-tracking smartwatches are 'easy to hack'

By Leo Kelion
Technology desk editor

15 November 2018

Third parties (DDoS)

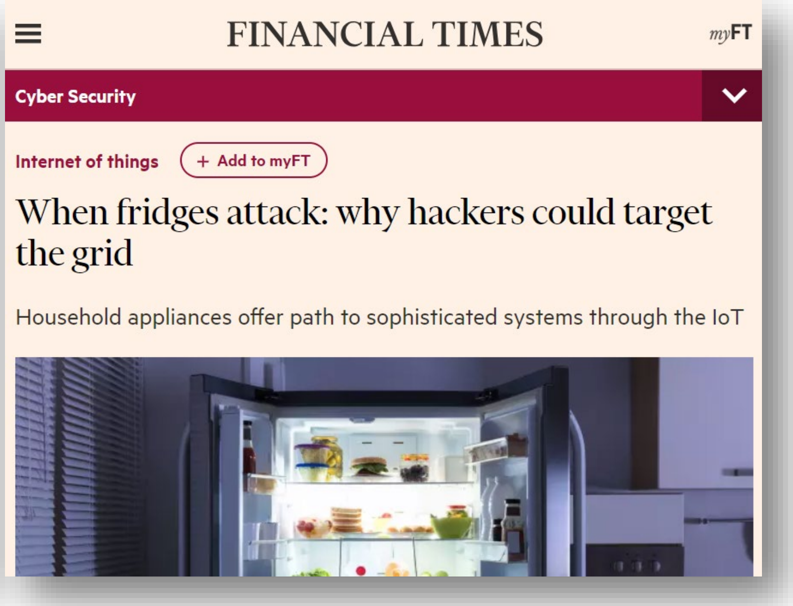


Technology

'Smart' home devices used as weapons in website attack

22 October 2016

Infrastructure



Internet of things

When fridges attack: why hackers could target the grid

Household appliances offer path to sophisticated systems through the IoT

- IoT manufacturers:
  - “My organization is new to cyber security - where to begin?”
  - “There is a jungle of guidance out there, with no common baseline.”

RSAConference2020

The ETSI standard

Technical Specification (TS) 103 645 / draft European Standard (EN) 303 645

Why technical standards?

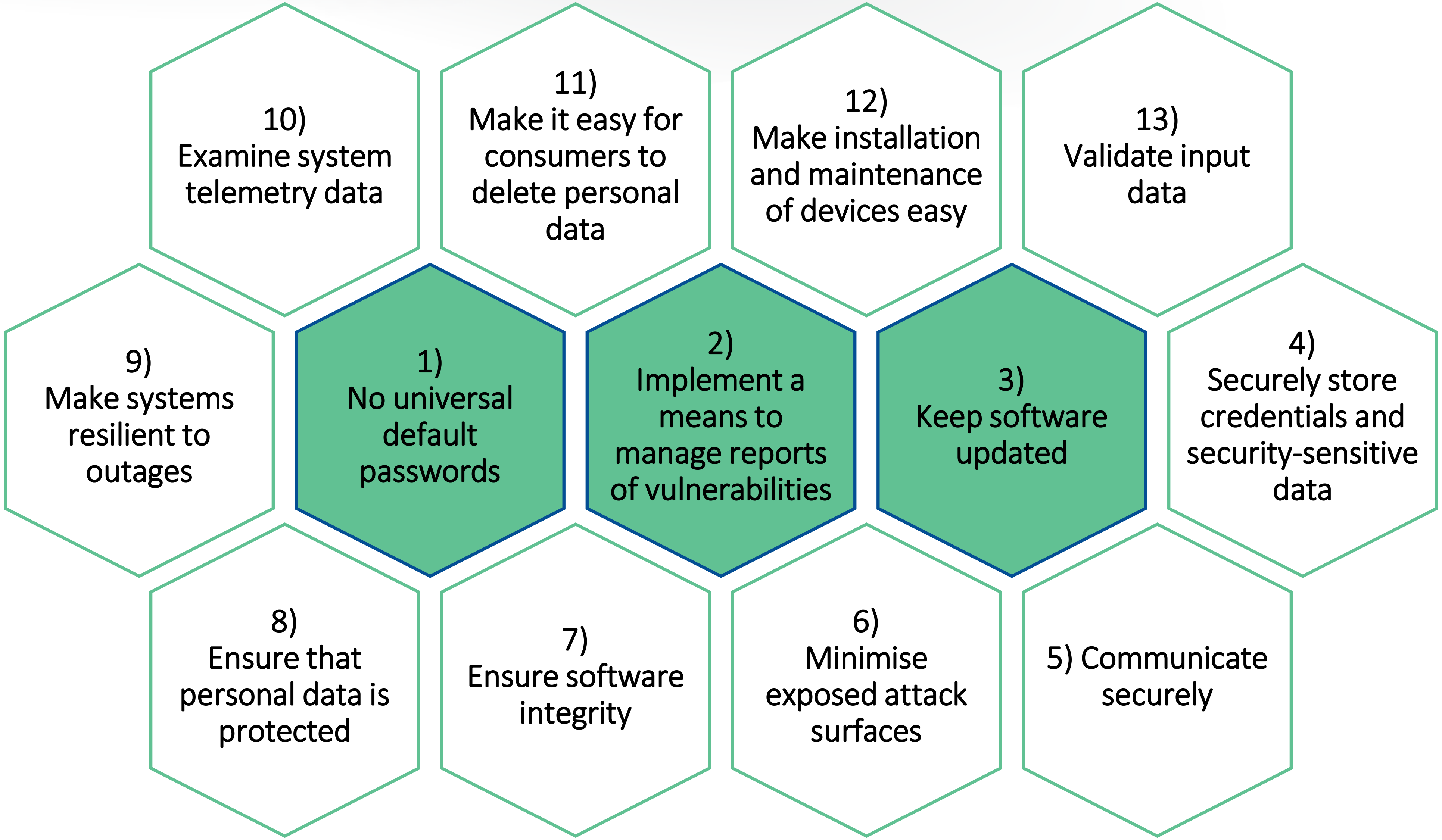
- Negotiated through a SDO in an inclusive process
- Why ETSI?
  - Develops globally-applicable standards for digital systems
  - 850 member organizations from 65 countries. A special role in Europe.
  - All standards are free to download
- It’s hard to get IoT standards right:
  - Cover all consumer IoT vs. specific verticals?
  - Just the essentials vs. aiming for 100% security?
  - Outcome-focused vs. prescriptive?

TS 103 645 / EN 303 645: development

- Guiding principles:
  - Is it sufficiently important?
  - Are we placing an acceptable burden on small businesses?
  - Are we accommodating future innovation?
  - Is it appropriate for the full spectrum of consumer IoT?
- Based on well-established guidance, including:
  - UK Code of Practice for Consumer IoT Security (2018)
  - German DIN SPEC 27072 (2019)
- Contributors include: ANEC Raising standards for consumers, BOSCH, BT, Bundesamt für Sicherheit in der Informationstechnik, cen, CENELEC, hp, HUAWEI, IBM, legrand®, National Cyber Security Centre a part of GCHQ, PHILIPS, SAMSUNG, SIEMENS

TS 103 645 / EN 303 645: content

- TS 103 645 v1 published in February 2019
- Currently developed as EN 303 645. Latest public draft: November 2019
- (free download)



10) Examine system telemetry data

11) Make it easy for consumers to delete personal data

12) Make installation and maintenance of devices easy

13) Validate input data

9) Make systems resilient to outages

1) No universal default passwords

2) Implement a means to manage reports of vulnerabilities

3) Keep software updated

4) Securely store credentials and security-sensitive data

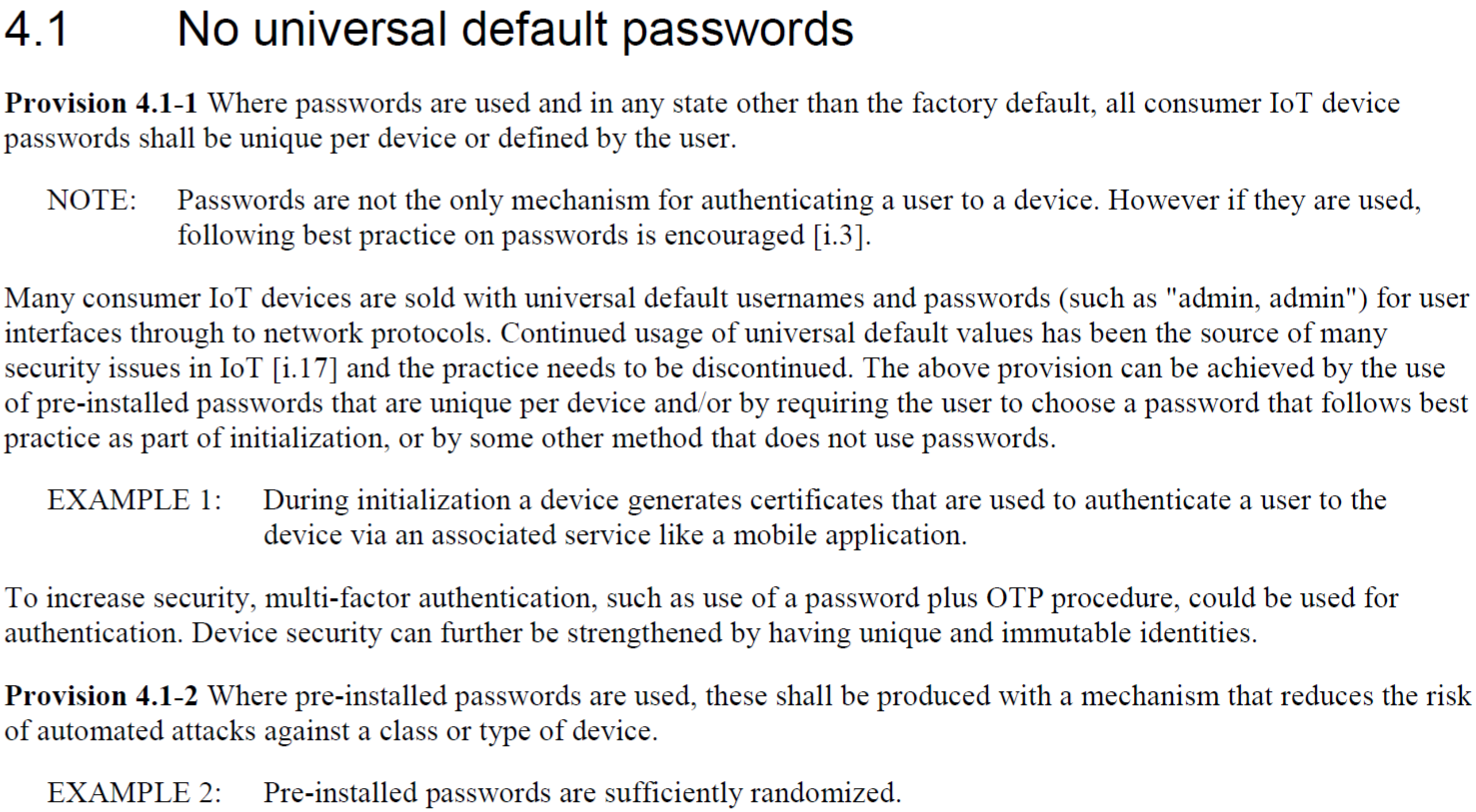
8) Ensure that personal data is protected

7) Ensure software integrity

6) Minimise exposed attack surfaces

5) Communicate securely

Example extract



4.1 No universal default passwords

Provision 4.1-1 Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.

NOTE: Passwords are not the only mechanism for authenticating a user to a device. However if they are used, following best practice on passwords is encouraged [i.3].

Many consumer IoT devices are sold with universal default usernames and passwords (such as "admin, admin") for user interfaces through to network protocols. Continued usage of universal default values has been the source of many security issues in IoT [i.17] and the practice needs to be discontinued. The above provision can be achieved by the use of pre-installed passwords that are unique per device and/or by requiring the user to choose a password that follows best practice as part of initialization, or by some other method that does not use passwords.

EXAMPLE 1: During initialization a device generates certificates that are used to authenticate a user to the device via an associated service like a mobile application.

To increase security, multi-factor authentication, such as use of a password plus OTP procedure, could be used for authentication. Device security can further be strengthened by having unique and immutable identities.

Provision 4.1-2 Where pre-installed passwords are used, these shall be produced with a mechanism that reduces the risk of automated attacks against a class or type of device.

EXAMPLE 2: Pre-installed passwords are sufficiently randomized.

Example extract

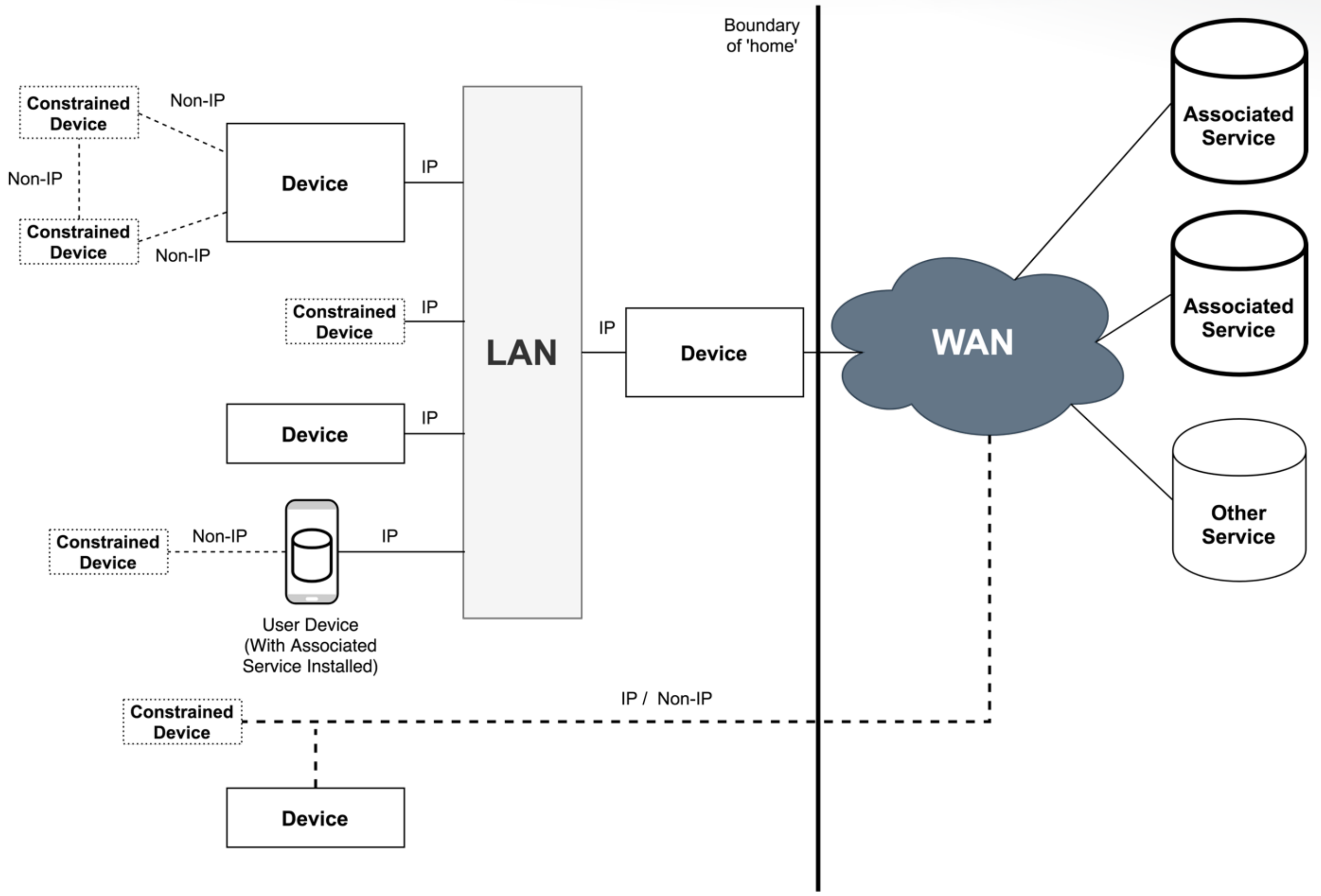
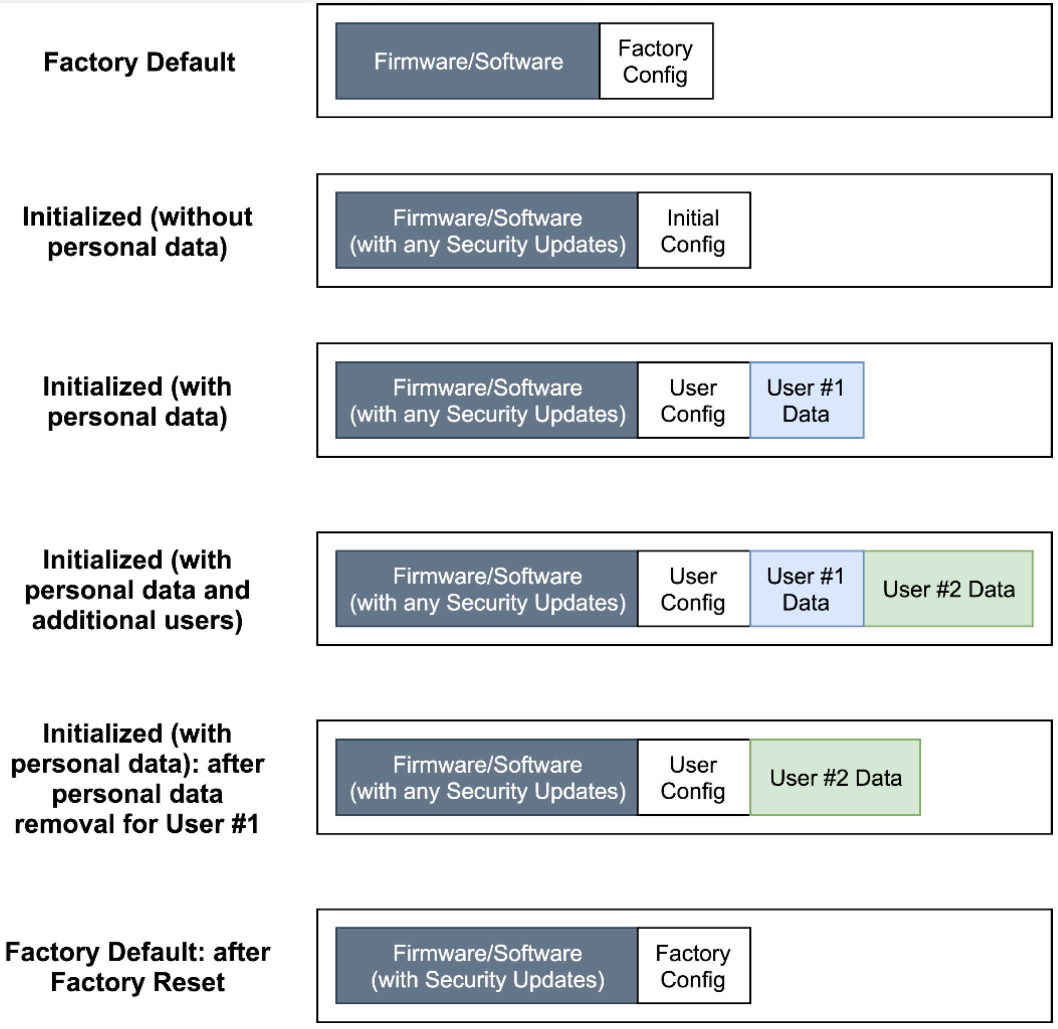


Figure A.2



Factory Default	Firmware/Software	Factory Config		
Initialized (without personal data)	Firmware/Software (with any Security Updates)	Initial Config		
Initialized (with personal data)	Firmware/Software (with any Security Updates)	User Config	User #1 Data	
Initialized (with personal data and additional users)	Firmware/Software (with any Security Updates)	User Config	User #1 Data	User #2 Data
Initialized (with personal data): after personal data removal for User #1	Firmware/Software (with any Security Updates)	User Config	User #2 Data	
Factory Default: after Factory Reset	Firmware/Software (with Security Updates)	Factory Config		

Figure A.5

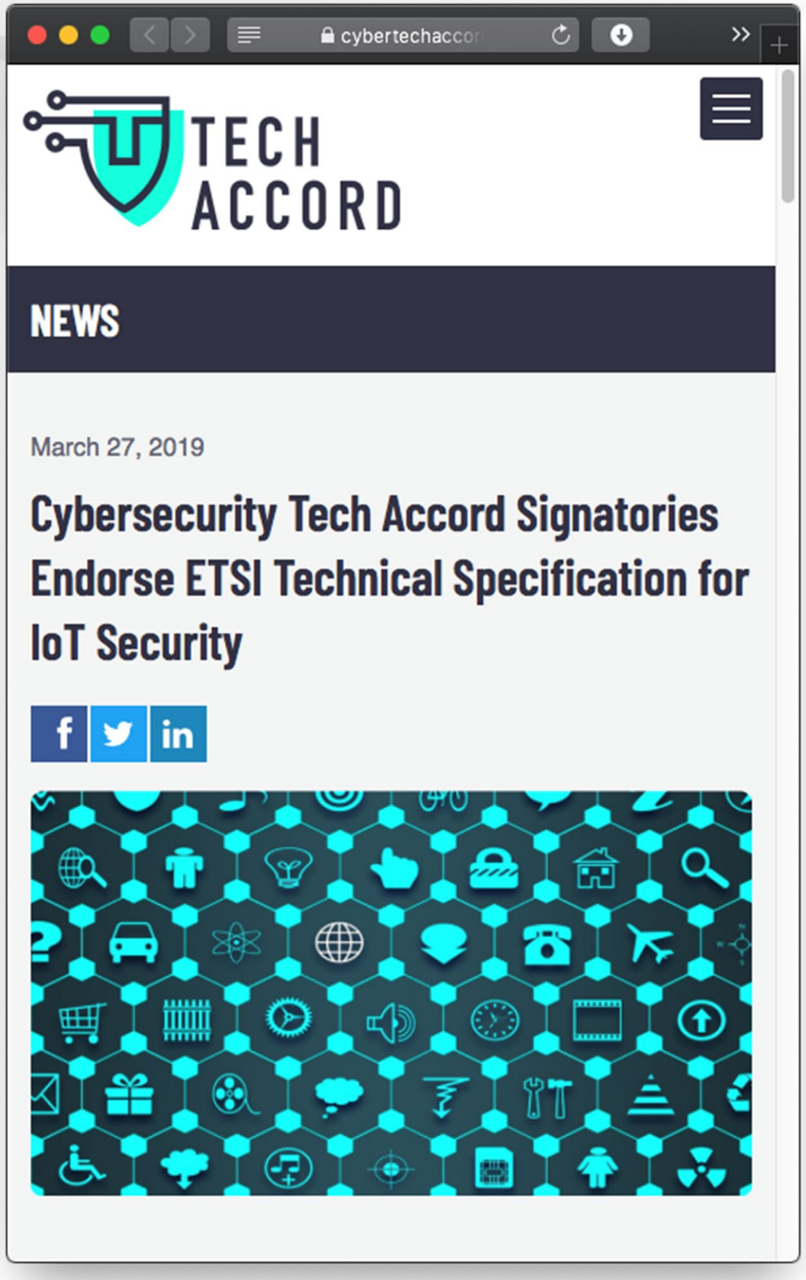
Reception

"ANEC trusts it will become the landmark specification for consumers and industry alike."

"IoT Security Foundation welcomes the ETSI announcement as a significant and important development."

"It is testament to the international consensus on what needs to be done to ensure consumers all around the world can feel their internet-connected devices are safe and secure to use."

"If we are to deliver the very real benefits that IoT can make to people's life's we must address these justified concerns and therefore welcome the publication of the ETSI standard."



NEWS

March 27, 2019

Cybersecurity Tech Accord Signatories Endorse ETSI Technical Specification for IoT Security

Uptake in product assurance schemes

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

“Finland becomes the first European country to certify safe smart devices … The Cybersecurity label can be awarded to networking smart devices if the devices meet the certification criteria, which are based on **EN 303 645**.”

“UL’s IoT Security Rating framework aligns with prominent industry standards, including **ETSI TS 103 645**”

“BSI Kitemark certification for Internet of Things connected devices is now based on the newly published **ETSI TS 103 645** specification.”

“DTG are launching a ‘Secure by Design’ cyber security conformance scheme [for smart TVs]. The conformance specifications will be developed based on the […] **ETSI TS 103 645**.”

“IASME has defined a set of 30 checks which can be verified by a national network of certifying bodies.” [Mapped to **TS 103 645** v1.1.1]

“IoTSF has published a mapping document which translates the high-level provisions of **ETSI TS 103 645** to the more detailed requirements contained in the IoT Security Compliance Framework”

Next steps

- Europe-wide consultation on EN 303 645 just closed
- Publication expected in summer 2020
- TS 103 645 to be the most up to date version, with updates to the EN made in slower time
- The standard is expected to influence:
  - Europe-wide certification schemes under the EU Cybersecurity Act
  - Potential Europe-wide regulation under the EU Radio Equipment Directive
  - National laws, such as in the UK
  - Assurance and certification schemes

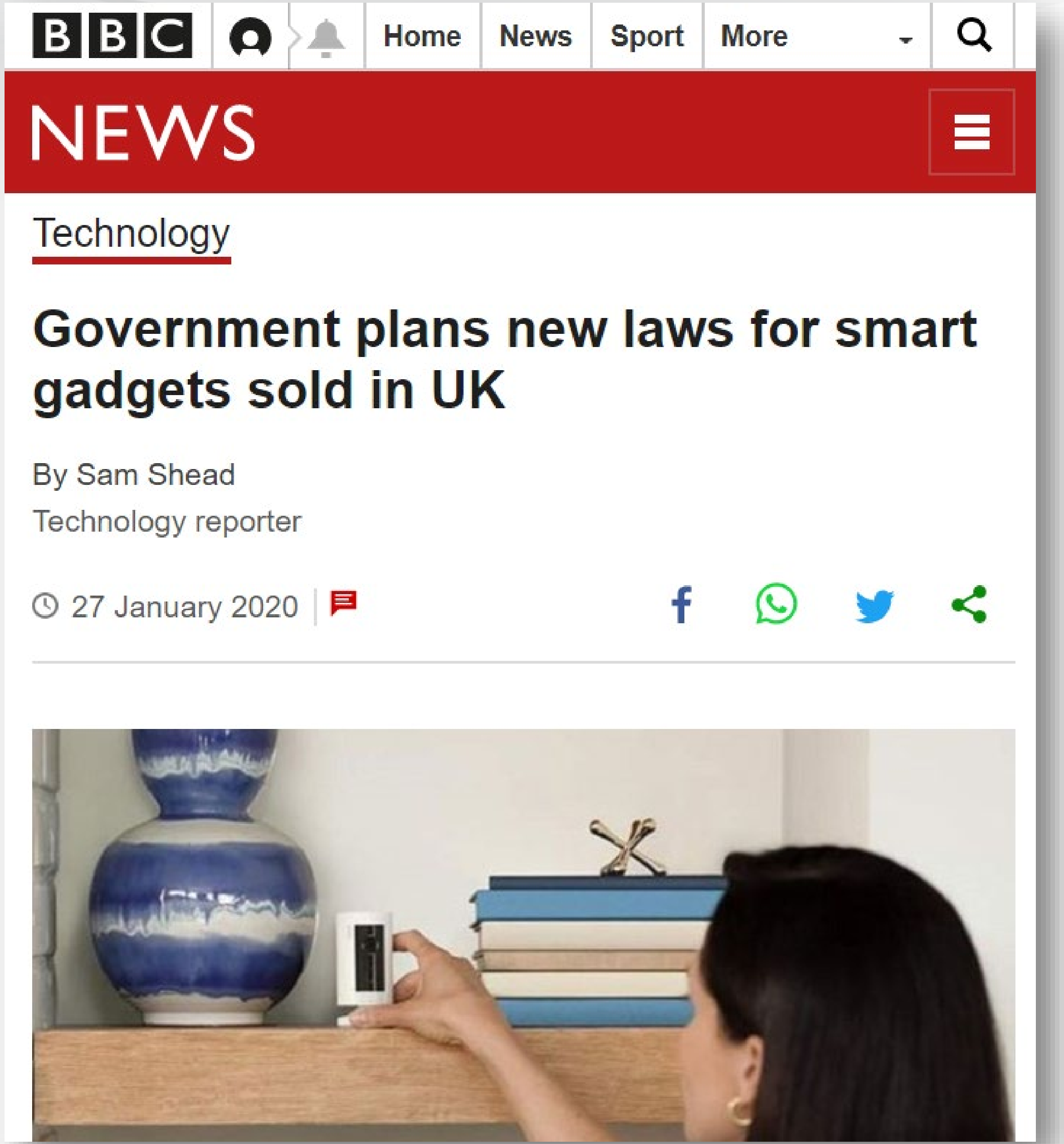
UK regulation on consumer IoT security

Regulation is needed

- Despite much guidance, bad practice remains widespread
- It’s hard to get regulation right:
  - Risk of unintended consequences
  - Need to make it futureproof
  - Enforcement? Liability?
- California IoT security Bill SB-327
  - Important first step
- US IoT Cybersecurity Improvement Act of 2019
  - Will it protect consumers?

UK regulation development

- May 2019: public consultation
- January 2020: government response
- Our intention is to require all “smart” consumer products sold in the UK to meet basic requirements
- New legislation is now being prepared



Government plans new laws for smart gadgets sold in UK

By Sam Shead
Technology reporter

27 January 2020

Draft proposals for mandated requirements in the UK

1. Where passwords are used, all device passwords shall be unique per device or defined by the user, unless:
   a) the device is in a pre-initialized state in which network connectivity and functionality are limited to those that are needed for the user to set a password or another authentication method.

(ETSI draft EN 303 645 provision 4.1-1)

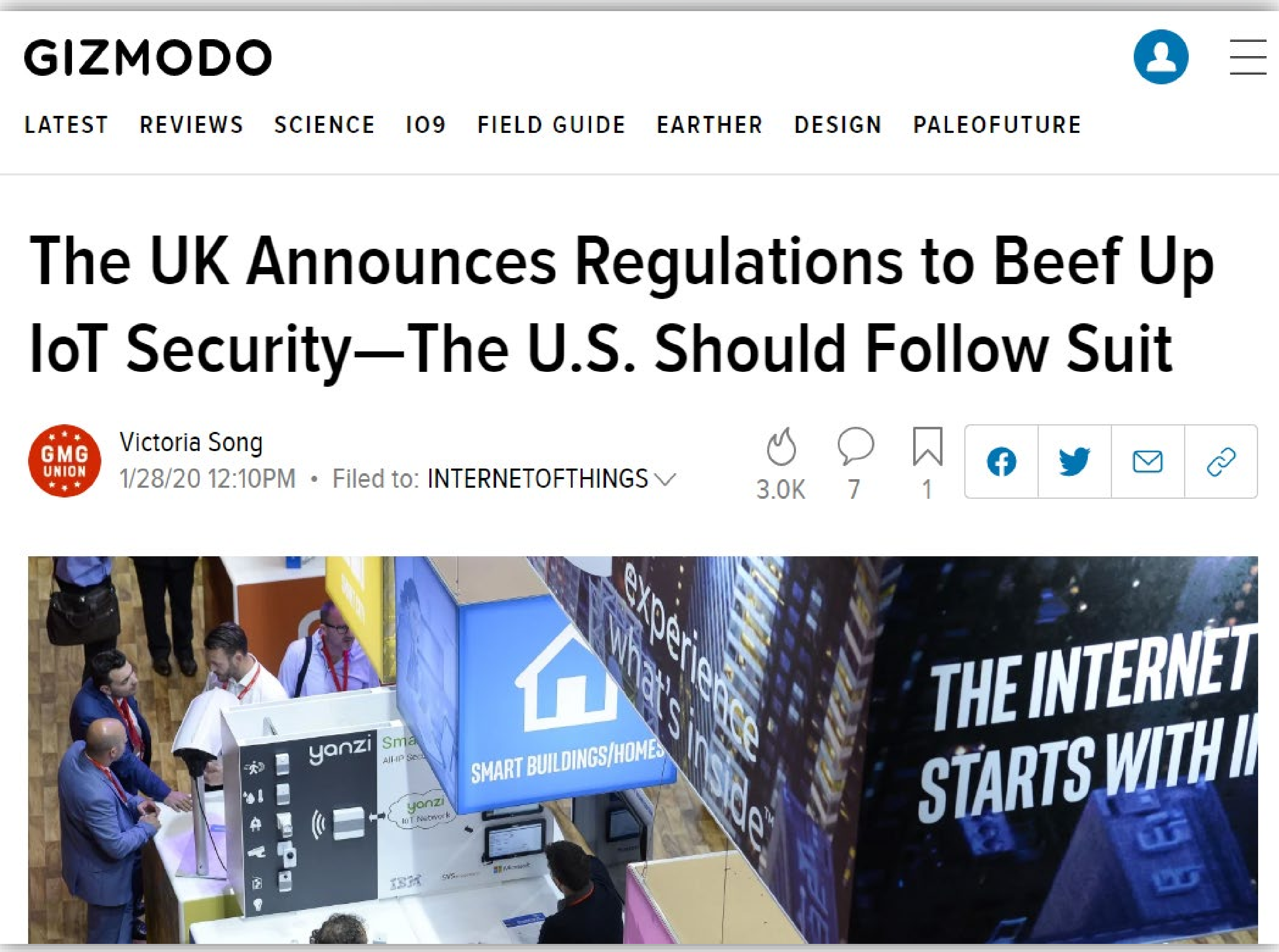
2. A vulnerability disclosure policy shall be publicly available that is clear and transparent. This policy shall provide a process that allows for issues to be reported in an accessible way and include, at a minimum:
   a) contact information; and
   b) information on timelines for (1) initial acknowledgement of receipt and (2) status updates until resolution of the reported concern.

(ETSI draft EN 303 645 provision 4.2-1)

3. The defined support period for security updates shall be published at the point of sale in an accessible way that is clear and transparent.

(ETSI draft EN 303 645 provision 4.3-8)

Will others follow?



The UK Announces Regulations to Beef Up IoT Security—The U.S. Should Follow Suit

Victoria Song
1/28/20 12:10PM • Filed to: INTERNETOFTHINGS

Apply It

Apply It

- Download a free copy of the latest draft
  - (draft EN 303 645 v 2.0.0, November 2019)
- Use ETSI TS 103 645 / draft EN 303 645 to achieve a good level of “smart” product security
- Contribute to future development through ETSI
- If UK regulation came into force tomorrow, would your products (your client’s products) comply?
- Help us work towards alignment of consumer IoT security initiatives

Contact & resources

- Jasper.pandza@culture.gov.uk

- DCMS Secure by Design program: https://www.gov.uk/government/collections/secure-by-design
- January 2020 regulation announcement: https://www.gov.uk/government/news/government-to-strengthen-security-of-internet-connected-products
- Work item of ETSI EN 303 645 and download of draft 2.0.0: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=57991
- Work item of ETSI TS 103 701 “Cybersecurity assessment for consumer IoT products” https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58434
- October 2019 webinar on ETSI TS 103 645: https://brighttalk.com/webcast/12761/371636