GDPR and the relation to IoT – How assessment of ‘technical measures’ required by the GDPR reduces financial risks by applying to Article 25 & 32

IoT Week 2022 – ‘Privacy by Design’

Jacques Kruse Brandao, Global Head of Advocacy, SGS

INFOCLASS: UNCLASSIFIED
TLP: WHITE

WHEN YOU NEED TO BE SURE

SGS

SGS

PII IS NEARLY EVERYWHERE

Segments:

- Smart Home
- Smart Health
- Industrie 4.0
- Smart City
- Smart Mobility
- Payment
- …

Fitness wearable

CCTV

Connected Car

Pacemaker

Public Transport

Patients File

Smart Home Router

Online Games

PoS Payments

Smart Lighting

-> Many IoT devices are generating, processing, storing or transferring personal data!

„WORST EXAMPLES OF IOT VULNERABILITIES"

MANY IOT DEVICE HACKS AFFECT PRIVATE DATA!

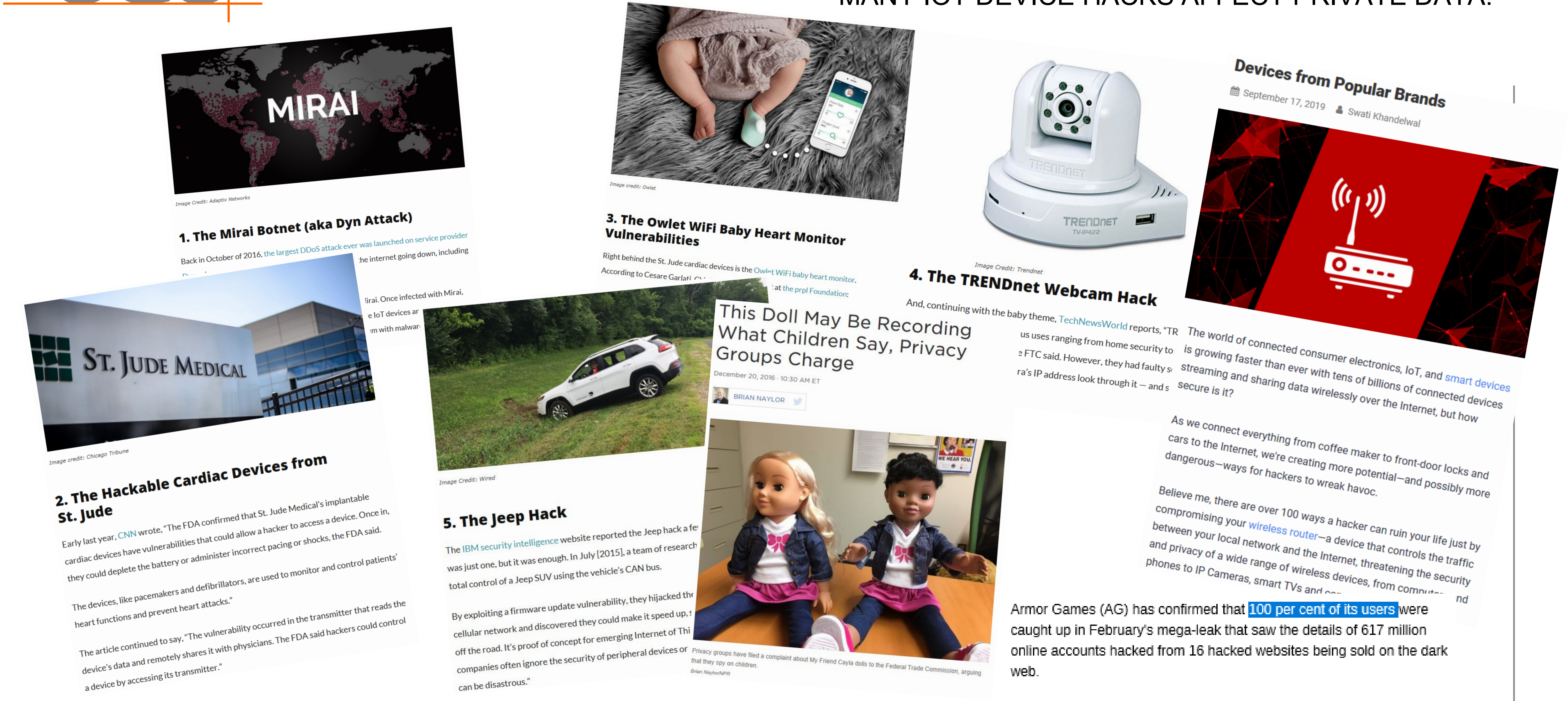


Image Credit: Adaptix Networks

1. The Mirai Botnet (aka Dyn Attack)

Back in October of 2016, the largest DDoS attack ever was launched on service provider ...he internet going down, including

...lirai. Once infected with Mirai,
...e IoT devices ar
...m with malwar

Image credit: Chicago Tribune

2. The Hackable Cardiac Devices from St. Jude

Early last year, CNN wrote, "The FDA confirmed that St. Jude Medical's implantable cardiac devices have vulnerabilities that could allow a hacker to access a device. Once in, they could deplete the battery or administer incorrect pacing or shocks, the FDA said.

The devices, like pacemakers and defibrillators, are used to monitor and control patients' heart functions and prevent heart attacks."

The article continued to say, "The vulnerability occurred in the transmitter that reads the device's data and remotely shares it with physicians. The FDA said hackers could control a device by accessing its transmitter."

Image credit: Owlet

3. The Owlet WiFi Baby Heart Monitor Vulnerabilities

Right behind the St. Jude cardiac devices is the Owlet WiFi baby heart monitor.
According to Cesare Garlati, Ch... at the prpl Foundation:

Image Credit: Trendnet

4. The TRENDnet Webcam Hack

And, continuing with the baby theme, TechNewsWorld reports, "TR...
...us uses ranging from home security to
...e FTC said. However, they had faulty s...
...ra's IP address look through it — and s...

Image Credit: Wired

5. The Jeep Hack

The IBM security intelligence website reported the Jeep hack a fe... was just one, but it was enough. In July [2015], a team of research... total control of a Jeep SUV using the vehicle's CAN bus.

By exploiting a firmware update vulnerability, they hijacked the... cellular network and discovered they could make it speed up, s... off the road. It's proof of concept for emerging Internet of Thi... companies often ignore the security of peripheral devices or... can be disastrous."

This Doll May Be Recording What Children Say, Privacy Groups Charge

December 20, 2016 · 10:30 AM ET

BRIAN NAYLOR

Privacy groups have filed a complaint about My Friend Cayla dolls to the Federal Trade Commission, arguing that they spy on children.

Brian Naylor/NPR

Devices from Popular Brands

September 17, 2019 Swati Khandelwal

The world of connected consumer electronics, IoT, and smart devices is growing faster than ever with tens of billions of connected devices streaming and sharing data wirelessly over the Internet, but how secure is it?

As we connect everything from coffee maker to front-door locks and cars to the Internet, we're creating more potential—and possibly more dangerous—ways for hackers to wreak havoc.

Believe me, there are over 100 ways a hacker can ruin your life just by compromising your wireless router—a device that controls the traffic between your local network and the Internet, threatening the security and privacy of a wide range of wireless devices, from comput... phones to IP Cameras, smart TVs and co... ...nd

Armor Games (AG) has confirmed that 100 per cent of its users were caught up in February's mega-leak that saw the details of 617 million online accounts hacked from 16 hacked websites being sold on the dark web.

Source: https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/ and https://www.theregister.co.uk/2019/02/11/620_million_hacked_accounts_dark_web/

ARTICLE 32 GDPR

- …. controller and the processor shall implement **appropriate technical and organisational measures** to ensure a level of security appropriate to the risk, including inter alia as appropriate:
- (a) the pseudonymisation and **encryption of personal data**;
- (b) the ability to **ensure** the ongoing **confidentiality, integrity, availability and resilience of processing systems and services**;
- (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- (d) **a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures** for ensuring the security of the processing.

ARTICLE 25 GDPR

- Taking into account the **state of the art**, the cost of implementation and the nature, scope, (…) the controller shall, (…), implement appropriate technical and organisational measures, such as pseudonymisation, (…), such as data minimization, (…)

SGS

GENERATING TRUST VIA COMPLIANCE

REDUCING FINANCIAL RISKS BY APPLYING TO ARTICLE 25 & 32

- **Generate Legal certainty** for investors by becoming “GDPR compliant” via proper testing and certification
  - Develop and manufacture GDPR compliant products
  - Become “GDPR compliant” from a holistic point of view via e.g. installing GDPR compliant devices within networks only
- **Data Protection Impact Assessment (DPIA)**: Generate Risk+Impact Assessment for each IoT device

1. **What are appropriate technical measures?**
2. **What is “State-of-the-Art”?**
3. **What can manufacturer do?**

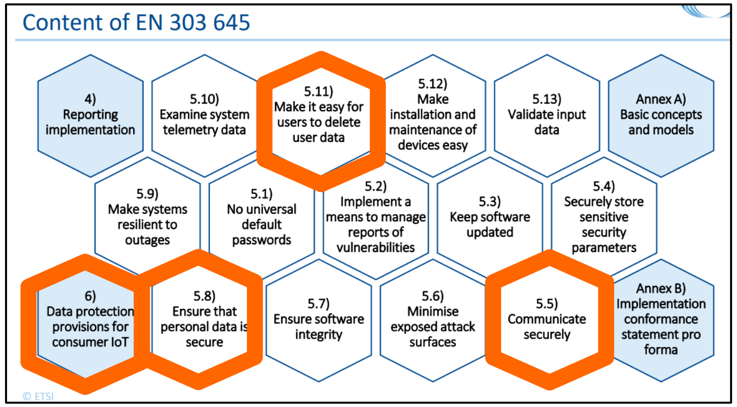
- Up to now **there is no technical catalogue or guideline available** what exactly needs to be implemented in terms of cybersecurity into IoT devices which are processing (generating, processing, storing or transferring) personal data to fulfil the GDPR requirements
- **There are now standards available which include privacy related requirements to protect PII in IoT devices and ancillary services to make them “GDPR-ready/ compliant”.**

IOT CYBERSECURITY STANDARDS

TO PREPARE FOR GDPR REQUIREMENTS

“State-of-the-Art”: Using a strong governance system / management system based on ISO 27K and 27701 (privacy extension to ISMS) as an essential foundation it is about **demonstrating compliance of IoT devices according to existing IoT Cybersecurity standards and certification schemes**:

EN 303 645 and TS 103 701 are well placed to provide the foundation for “basic”-level consumer IoT assurance:



Content of EN 303 645

4) Reporting implementation

5.10) Examine system telemetry data

5.11) Make it easy for users to delete user data

5.12) Make installation and maintenance of devices easy

5.13) Validate input data

Annex A) Basic concepts and models

5.9) Make systems resilient to outages

5.1) No universal default passwords

5.2) Implement a means to manage reports of vulnerabilities

5.3) Keep software updated

5.4) Securely store sensitive security parameters

6) Data protection provisions for consumer IoT

5.8) Ensure that personal data is secure

5.7) Ensure software integrity

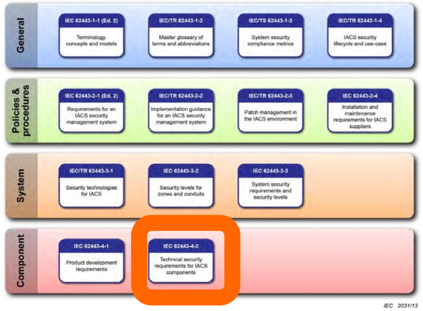
5.6) Minimise exposed attack surfaces

5.5) Communicate securely

Annex B) Implementation conformance statement pro forma

© ETSI

IEC 62443-4-2 Technical security requirements for IACS components:



General	IEC 62443-1-1 (Ed. 2) Terminology, concepts and models	IEC/TR 62443-1-2 Master glossary of terms and abbreviations	IEC/TS 62443-1-3 System security compliance metrics	IEC/TR 62443-1-4 IACS security lifecycle and use-case
Policies & procedures	IEC 62443-2-1 (Ed. 2) Requirements for an IACS security management system	IEC/TR 62443-2-2 Implementation guidance for an IACS security management system	IEC/TR 62443-2-3 Patch management in the IACS environment	IEC 62443-2-4 Installation and maintenance requirements for IACS suppliers
System	IEC/TR 62443-3-1 Security technologies for IACS	IEC 62443-3-2 Security levels for zones and conduits	IEC 62443-3-3 System security requirements and security levels	
Component	IEC 62443-4-1 Product development requirements	IEC 62443-4-2 Technical security requirements for IACS components		

IEC 2031/13

European cybersecurity certification scheme (EUCC) based on common criteria, a voluntary scheme with a set of security requirements for ICT security products

-> SGS is able to support you in generating the right level of trust you want to achieve for your IoT devices and services and support you with the assessment and certification services.

THANK YOU FOR LISTENING!

WWW.SGS.COM

WHEN YOU NEED TO BE SURE