2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE),
16-17 August 2018, Southend, Essex, UK. DOI:10.1109/iCCECOME.2018.8658720

A Survey on CAN Bus Protocol: Attacks, Challenges, and Potential Solutions

Mehmet Bozdal, Mohammad Samie, Ian Jennions

IVHM Centre, Cranfield University, Bedford, MK43 0AL, UK

{mehmet.bozdal, m.samie, i.jennions} @cranfield.ac.uk

***Abstract*— The vehicles are equipped with electronic control units that control their functions. These units communicate with each other via in-vehicle communication protocols like CAN bus. Although CAN is the most common in-vehicle communication protocol, the lack of encryption and authentication causes series security shortcomings. There are many attacks reported and the number is estimated to increase with the rising connectivity of the cars. In this paper, we present CAN protocol and analyze its security vulnerabilities. Then we survey the implemented attacks and proposed solutions in the literature.**

Keywords—CAN bus, in-vehicle communication, CAN bus security, electronic control unit

I. INTRODUCTION

The automobile industry has changed

The modern vehicles are equipped with around 100 Electronic Control Unit (ECU) to control the electrical systems to improve driving comfort and safety[1][2]. ECUs control most of the car's functions including safety critical engine control, airbag deployment, and anti-lock braking system. To have a safe driving, ECUs should have a reliable communication network. The main in-vehicle communication protocol is Controller Area Network (CAN). Its well-recognized advantages such as high immunity to electrical interference, easy wiring, and ability to self-diagnose and repairing errors make CAN bus suitable for the automobile industry. Although CAN is resilient to electrical noise and has some security features, it is vulnerable to attacks. As security of systems is becoming a significant concern, extensive research on vulnerabilities of the CAN and possible solutions are carried out. Some of these studies performed successful experimental attacks on commercial cars. Although most of the attacks are implemented via physical access to the bus, wireless attacks are increasing. With the new wireless interfaces like vehicle-to-vehicle and vehicle-to-infrastructure, wireless attack surface will increase. We believe that wireless attacks will become the main attack surface for the future attacks.

This paper aims to analyse the security of CAN protocol and show the vulnerabilities modern cars have. After identifying the attacks, it will present the solutions in the literature. The rest of the paper is structured as follows: In the following Section II the general overview of CAN protocol with security shortcomings are given. In Section III implemented attacks and proposed solutions in the literature are surveyed. In Section IV the work is summarised and the paper is concluded.

II. BACKGROUND

A. Controller Area Network

CAN protocol, developed by Robert Bosh GmbH in 1980, is a multi-master communication interface designed for the in-vehicle communication. It is a broadcast network and can provide up to one megabit per second (bps). CAN bus has high immunity to electrical interference, is easy to wire, and has the ability to self-diagnose and repairing errors. The distributed architecture of the network makes maintenance easier and decreases the overall system cost.

The robustness of CAN comes from the built-in security features. CAN protocol use differential wiring to eliminate the noise and has two voltage levels: dominant logic '0' and recessive logic '1'. Hence there is no dedicated clock line, synchronisation is provided via signal edges and bit-stuffing. Bit-stuffing rule limits the number of repeated bits and after five consecutive bits of the same logic level, the next bit must be the complement of the previous logic level. If data have more than five successive corresponding bits, a complement bit is inserted by transmitter CAN controller and it is ignored by the receiver CAN controller.

Collision Detection and Arbitration on Message Priority (CD+AMP) resolves the collisions with the help of message identifier bits. When two nodes start transmitting at the same time, a higher priority node continues to transmit and other node/s will stop transmitting. Another collision prevention mechanism is Carrier Sense, Multiple Access with Collision Avoidance (CSMA/CA) which rules the nodes to wait for a certain amount of inactivity before transmitting the data to sense the node is idle and collision will not occur.

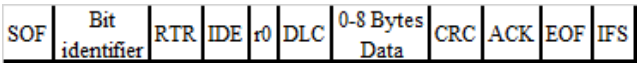

Fig. 1. The bits of standard CAN bus frame

There are also five error checking methods. These are; Start of Frame (SOF) single dominant bit for synchronization, Cylindrical Redundancy Check (CRC) checksum of the data for data integrity, Acknowledgement (ACK) bits for successful data transmission, and End of Frame (EOF) bit for stuffing error and frame finalization.

CAN protocol also resilient to physical errors. It can eliminate the faulty nodes from the bus traffic with Error Confinement Mechanism (ECM). ECM utilises two error counters in each node; Received and Transmitted Error Counters. The value of counter increases by eight at the occurrence of an error during the transmission and by one at the occurrence of an error during the receiving. Then node will enter the Error Passive state if counter's value exceeds

XXX-X-XXXX-XXXX-X/XX/$XX.00 ©20XX IEEE

© 2019 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

127; however, its error frames will not affect the bus traffic. If the counter value exceeds 255, the node will be in the Buss-Off state and will no longer take part in the bus traffic.

B. Security Shortcomings of CAN Protocol

When CAN bus was initially designed in (1980), security was not the main consideration. It was used to connect a few ECUs and not accessible to the end user. However, the automobile industry has changed drastically and now there are dozens of ECUs connected and it is required by law that bus should be accessible for the diagnostic purpose[3].

Although CAN has many security features, it is still vulnerable to the attacks. The main problem with CAN protocol is lack of encryption and authentication. The lack of authentication allows any unauthorised nodes to join the network and take part in the communication. CAN is a broadcast network so there is no source and destination addresses and every node can listen to any messages. Hence data is not encrypted, an adversary can listen and understand the data. This may cause privacy problems because modern cars also collect data related to drivers like location and address book. It also allows an adversary to inject faulty data on the system.

CAN protocol also vulnerable to denial of service (DoS) attacks. Arbitration mechanism of CAN allows higher priority nodes to speak first. If there is a malicious node with the highest priority and active all the time, the other nodes cannot communicate because of the prioritization in CAN bus. Another Dos attack implementation can be a misuse of ECM. If an attacker generates an error during the communication, this will increase the error counters and eventually cause the elimination of the node.

III. RELATED WORK

After overview and security shortcomings of CAN protocol, in this section we analysis CAN bus and present the attacks with the proposed solutions in the literature.

A. Security Analysis of CAN Network

In this chapter, we analysed CAN protocol based on CIA (Confidentiality, Integrity, and Availability) triad. CIA triad is simple security model to assess the system vulnerability. CIA triad analyses three essential principles which any secure system should have.

Confidentiality is providing the data to only authorised people. Cryptographic and encryption methods are used to provide confidentiality. Although CAN protocol does not have inherit security measures for confidentiality, some car manufacturers use cryptographic methods for local functionalities like keyless entry[4].

Integrity can be defined as the accuracy and validity of the data. The data must not be changed during the transmission. CAN has CRC checksum for verification of integrity so if any bit is corrupted during the transmission, it can be detected by the receiver. But CRC cannot detect the altered data by malicious node because there is no authentication. Therefore CAN protocol fails to sustain the integrity of data.

Availability means data or network can be accessed by the authorised user at all times. This is not possible by the nature of CAN protocol because of the arbitration rule and physical implementation of the protocol. The arbitration rule allows the higher priority node to access the network. If a node with the highest priority transmits the data all the time, the bus cannot be accessible by the other nodes.

B. Existent Attacks

In this chapter, we summarise the attacks have been implemented in the literature. The first known attack on CAN bus is implemented on the electric window lift on the simulation environment by Hoppe and Dittman in 2007[5]. Since then, different attack scenarios have been implemented. We can categorise the attacks into three main categories: eavesdropping, data insertion, and denial of service (DoS).

Eavesdropping is the starting point of the many attacks. Lack of encryption allows any node to understand the bus traffic so an adversary can sniff CAN frames and gather the information. This may cause the invasion of the privacy. The modern car collects information about the driver and has the capability to connect driver's mobile phone. The adversary can steal this personal information by only passively listening to the bus. Enev et al. [6] show that it is possible to identify the driver based on the sensory data travel through the CAN bus. They were able to identify 15 drivers with 100% accuracy. The research says that it is also possible to identify the driver with even one sensory data (brake pedal). They successfully show that monitoring in-vehicle network can invade personal privacy. Eavesdropping can be classified as passive attack hence it is not disturbing the communication. However, it can lead to active attacks. For instance, Palanca et al. [7] captured CAN frames and identify the ID of the node they plan to attack. When they gathered the ID and data of the parking sensor, they implemented DoS attack.

Data manipulation can be defined as the insertion of the unauthorised CAN frame to the network. Hence CAN protocol does not have an authorisation mechanism a malicious node can attach the network and insert data. Frame falsifying, frame injection, and replay attacks are an example of the data manipulation. Koscher et al. [8] were able to hack the instrument cluster, body control module, brake control module, and engine control module. They connected a laptop to On-Board Diagnostics II (OBD-II) port and implemented their attacks on a real car. They manipulated the fuel level and speedometer readings and showed false data on the instrument cluster. The research was able to disable engine and change engine parameters like engine timing and engine RPM. They released the brakes and prevent their activation while car was running 40 MPH with continues fuzzing method. Hoppe et al. [4] implemented four different attack plots and analysed their effects based on comfort, security, and safety. One of the attacks was removing the airbag warning. The attack can hide the theft event while endangering the passengers' lives. The research shows that driver cannot rely on the system security checks although manual checking is unfeasible.

Denial of service (DoS) is preventing any particular node/s or the whole network to provide service. There are different types of the DoS attack implemented on CAN network. Mukherjee et al. [9] implemented DoS attack on SAE J1939. SAE J1939 standard is used in commercial vehicles and it is implemented on top of the CAN physical layer. They implemented three separate DoS attack. The attacks were sending too many request messages for a supported Parameter Group Number (PGN) to overload recipient ECU, sending manipulated False Request to Send (RTS) and causing overflow at the recipient buffer, and keeping the connections

open via Clear to Send (CTS) messages and occupy the whole network. The work shows that the protocols implemented on top of the CAN physical layer can be also vulnerable to attacks. Palanca et al. [10] implemented selective DoS attack via attaching a stealthy node to the network. They have implemented their attack based on the CAN protocol weakness, therefore, any car with CAN bus are vulnerable. The malicious node overwrites the bits and generates error frame. Because of the CAN error confinement, after a certain number of error occurrence, the transmitter node will go to buss-off state and no longer will be available. The attack is implemented on 2012 Alfa Romeo Giulietta. The attack method can disable any node connected to the bus. However, they disable the parking sensor for the ethical reasons. This attack is different than other DoS attacks because it does not send a whole CAN frame to the network.

Some critics say that physical access requirement of the CAN attacks make them infeasible[11]. Although attacks mentioned above require the physical access to the CAN network, there are increasing number of remote attacks. The modern cars are equipped with different types of wireless interfaces. These are namely passive anti-theft system, tire pressure monitoring system (TPMS), remote keyless entry, Bluetooth, radio data system, and telematics. These wireless interfaces may have communication with CAN network via a gateway ECU which has a firewall. Some researchers pass over the firewalls and access to the CAN network. Checkowat et al. [12] compromised TPMS, Bluetooth, FM channel, and cellular network of the car. Then, they modified the ECU of the car. With this method they claim that a thief can steal a car hence car doors can be unlock via CAN network. Woo et al. [13] implemented a remote attack via malicious self-diagnostic smartphone app. If a driver download a malicious app to monitor/diagnose the car, he/she allows the adversary to take control of the car without attaching any device physically. Then, attacker can implement their attack from long distance via using the phone's internet. Valasek and Miller [14] carried out remote attack survey on 12 car brands and 21 commercial cars. They have identified remote attack surfaces and difficulty to compromise each car. The attack was three stage. The first stage was compromising the ECU responsible from wireless interface. The second stage was injecting messages to communicate with safety-critical ECU. The last stage was modifying the ECU to behave maliciously. The researchers believe that increasing number of cyber-physical systems in cars will increase the vulnerability but they cannot practically verify this because of the high number of different applications in cars. Another wireless attack method is over-the-air (OTA) software update. OTA provides manufactures to reprogram the ECU to patch software bugs or add new features. It provides flexibility and saves money. But it is another attack surface that hackers can dive in the car's communication network. There is no reported attack related to OTA updates yet but it should be considered as a critical threat.

C. Proposed Solutions

The attacks on CAN bus are analysed and some solutions are put forward. The solutions can be categorised as network segmentation, encryption methods, authentication methods, and intrusion detection systems.

The simplest way to provide security is changing the network topology. Critical ECUs and non-critical ECUs are separated and the end user cannot access easily to the critical ECU network. The connection between networks is provided via a gateway ECU. This security measure is already implemented on commercial cars. However, the gateway ECU can be manipulated and the critical network can be accessed. If the gateway ECU is programmed to pass relevant IDs to the subnetwork, it can be fooled by sending malicious CAN frame with an ID of a node which belongs to subnetwork[4]. Kammerer et al. [15] implemented star coupling router topology. The router not only separate single-bus based CAN system to multiple CAN segments but also bring new security features like unidirectional channels, traffic shaping, traffic partitioning, message integrity, and intrusion detection. In the paper [15], CAN segment security was taken out of the scope but replay or masquerade attacks in a CAN segment may pass the router's security checks and attack the other CAN segments. The safest solution will a node in a segment but it is not feasible for cost and timing perspective. It is also questionable that how much network segmentation increases the maintenance difficulty compare to the traditional CAN network.

Due to the broadcast nature of the CAN protocol, any node can listen to the bus traffic. Hence CAN system does not have encryption mechanism, an adversary can listen CAN traffic easily and understand the communication. To prevent attacks and provide confidentiality different encryption mechanism are proposed in software and hardware levels. There are some software-based encryption methods [16] and some companies implementing propriety encryption techniques on their commercial cars. However software-based encryption methods are not strong enough because of the low computational power which results in weak encryption mechanism. There are reports that claim some of the encryption mechanism on commercial cars are broken[17]. ECUs do not have much computational power, therefore, software-based encryption can cause latency which is not acceptable for the safety-critical automotive industry. The limited bandwidth is also another restriction. Software-based encryption may work with a limited traffic but it is not promising for the currently increasing CAN traffic. Shreejith and Fahmy [18] proposed FPGA based zero latency encryption. They enhanced the network protocol layer. The encryption and decryption processes are done while the data is buffered at the network layer. This will prevent any additional latency. However, if we consider the automotive industry and cost of ECU, FPGA based solutions are luxury. Any change in protocol layer will also require custom-made CAN controllers which is not feasible to change.

In the current CAN protocol, it is not possible to trace a CAN frame and find its source. There is also no authentication which means that any node can attach to the network and send messages. If a malicious node injects a CAN frame, other nodes will accept it and process. To prevent data injection to CAN network, some authentication methods are proposed. Wang and Sawhney [19] proposed VeCure can authentication method with 50 us processing delay. The authentication mechanism work based on trust groups where high-trust group/s share a symmetric secret key. Although this method decreases the number of keys and the key number is independent of the ECU number, compromising of a node from the trust group will fail to protect the system. The authentication is achieved by sending data message followed by authentication message. The latency of the proposed method can be ignored but the bus traffic is doubled in the high-trust group which is not acceptable if we consider the

limited bandwidth in CAN protocol. Woe et al. [13] proposed encryption and authentication method using AES-128 and A 32-bit truncated message authentication code (MAC). The proposed method latency is about 378us at 60MHz. They claim that latency will decrease if proposed protocol implemented on Application Specific Integrated Circuits (ASICs). Although method looks promising, it is not compatible with the standard CAN protocol. Another drawback of this method can be using the symmetric key at the initial stage of the communication. If we consider a car's average life 20 years, brute force attack can be implemented to compromise the method. Nowdehi et al. [20] identified five criteria for authentication systems to be implemented in commercial cars. These criteria are cost-effectiveness, backward compatibility, support for vehicle repair and maintenance, sufficient implementation details, and acceptable overhead. They have tested 10 methods they have found in the literature including the methods mentioned above. Not surprisingly, none of the methods can pass all the five criteria. The CAN protocol was not designed security in mind, therefore, it is hard to find a feasible security solution.

Siddiqu et al. [21] proposed a physical unclonable function (PUF) based encryption and authentication and provide secure communication over CAN bus. They used elliptic curve Diffie-Hellman based asymmetric encryption method also called as public-private key cryptography. Asymmetric key encryption is safer than symmetric key encryption but it requires high computational power for current ECU controllers. According to their data, AES-128 encryption generates 366.66 ns and 110 ns latency at 60 MHz and 200MHz clock frequency respectively. However, most of the ECUs have limited computational power like clock speed of tens of MHz[19]. In reality, latency will increase significantly. The other negative side of this proposal is it requires hardware change in the CAN controller and a server to authenticate the nodes. This will increase the system cost and having a server can create other potential attacks. Murvay and Groza [22] proposed to analyse signal pattern to gather footprints of the transceivers to authenticate the node. The proposed method does not increase the traffic or changes the CAN controller but it requires intensive signal processing. If the network is compromised by software attack, the method will fail.

CAN protocol has obvious security vulnerabilities. Implementing security features to CAN bus is a challenging job due to limited resources (bandwidth, memory, and computational power) and time constraint. This lead to extensive research on intrusion detection / prevention system (IDS / IPS). IDS analyses the CAN traffic and detect the abnormalities. If any abnormality is detected, they warn the driver. The difference of the IPS from IDS is they can take an active role and prevent the attack. Fang et al. [23] implemented an adaptive network-based fuzzy inference system. They use information like busload, change in message number in a certain period, and a number of dropped messages and messages with illegal ID. They implemented the five-level Sugeno algorithm and trained the network. They tested their method on a commercial electrical car. The proposed method detected the attacks but it is questionable that it will prevent complex attacks. Adding more methods

There are also some commercial intrusion detection systems [24][25] but their algorithms are not shared with the public.

IV. Conclusion

In this paper, we explained the CAN protocol and its vulnerabilities. We analysed the security of the protocol using CIA triad. Although CAN is the most widely used in-vehicle communication protocol, it fails all three benchmarks of CIA triad. The lack of encryption and authentication mechanism caused multiple attacks. We summarised the implemented attacks in the literature. Although most of the attacks implemented require the physical access to the CAN network, wireless attacks are increasing. We estimate that wireless attacks will increase and supress the physical access attacks. The reason behind this is cars are getting more connected and this will increase the attack surface.

The main vulnerability of CAN bus is lack of encryption and authentication mechanisms. Extensive research carried out to find a solution to this problem. We categorised the proposed solutions. Some solutions provide large overhead to limited bandwidth, some change the standard CAN controller. There is no optimal solution hence CAN system was not designed security in mind. As a result, there is no approved solution by the industry and academia. The problem is mitigated with network segmentation and IDS. Although IDS does not provide complete solutions to CAN vulnerabilities, some of the methods are commercially available.

Extend conclusion

References

[1] P. Mundhenk, *Security for Automotive Electrical / Electronic (E / E) Architectures*. Cuvillier Verlag, 2017.

[2] "'ECU' is a Three Letter Answer for all the Innovative Features in Your Car: Know How the Story Unfolded," *Embitel*, 2017. [Online]. Available: https://www.embitel.com/blog/embedded-blog/automotive-control-units-development-innovations-mechanical-to-electronics. [Accessed: 23-May-2018].

[3] R. Buttigieg, M. Farrugia, and C. Meli, "Security Issues in Controller Area Networks in Automobiles," in *18th international conference on Sciences and Techniques of Automatic Control & Computer Engineering*, 2017, pp. 21–23.

[4] T. Hoppe, S. Kiltz, and J. Dittmann, "Security Threats to Automotive CAN Networks -- Practical Examples and Selected Short-Term Countermeasures," in *SAFECOMP 2008 : 27th International Conference on Computer Safety, Reliability, and Security*, 2008, pp. 235–248.

[5] B. Groza and S. Murvay, "Security solutions for the Controller Area Network: Bringing Authentication to In-Vehicle Networks," *IEEE Vehicular Technology Magazine*, 2018.

[6] M. Enev, A. Takakuwa, K. Koscher, and T. Kohno, "Automobile Driver Fingerprinting," in *Proceedings on Privacy Enhancing Technologies*, vol. 2016, no. 1, pp. 34–51.

[7] A. Palanca, E. Evenchick, F. Maggi, and S. Zanero, "A stealth, selective, link-layer denial-of-service attack against automotive networks," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, 2017, vol. 10327 LNCS, pp. 185–206.

[8] K. Koscher *et al.*, "Experimental security analysis of a modern automobile," in *Proceedings - IEEE Symposium on Security and Privacy*, 2010, pp. 447–462.

[9] S. Mukherjee, H. Shirazi, I. Ray, J. Daily, and R. Gamble, “Practical DoS Attacks on Embedded Networks in Commercial Vehicles,” 2016, vol. 10063.

[10] S. Zanero, “A Stealth, Selective, Link-layer Denial-of-Service Attack Against Automotive Networks,” 2015.

[11] B. Rebecca, “Proof-of-Concept CarShark Software Hacks Car Computers, Shutting Down Brakes, Engines, and More,” *Popular Science*. [Online]. Available: https://www.popsci.com/cars/article/2010-05/researchers-hack-car-computers-shutting-down-brakes-engine-and-more. [Accessed: 29-May-2018].

[12] S. Checkoway *et al.*, “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” *System*, pp. 6–6, 2011.

[13] S. Woo, H. J. Jo, and D. H. Lee, “A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN,” *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 2, pp. 993–1006, 2015.

[14] C. Miller and C. Valasek, “A Survey of Remote Automotive Attack Surfaces,” 2014.

[15] R. Kammerer, B. Frömel, and A. Wasicek, “Enhancing security in CAN systems using a star coupling router,” in *7th IEEE International Symposium on Industrial Embedded Systems, SIES 2012 - Conference Proceedings*, 2012, pp. 237–246.

[16] “CAN Bus Can Be Encrypted, Says Trillium | EE Times.” [Online]. Available: https://www.eetimes.com/document.asp?doc_id=1328081&page_number=2. [Accessed: 29-May-2018].

[17] W. KYLE, “WTF ! It Should Not Be Illegal to Hack Your Own Car ’ s Computer,” 2015. [Online]. Available: https://www.wired.com/2015/01/let-us-hack-our-cars/. [Accessed: 29-May-2018].

[18] S. Shreejith and S. A. Fahmy, “Zero latency encryption with FPGAs for secure time-triggered automotive networks,” in *Proceedings of the 2014 International Conference on Field-Programmable Technology, FPT 2014*, 2015, pp. 256–259.

[19] Q. Wang and S. Sawhney, “VeCure: A practical security framework to protect the CAN bus of vehicles,” in *2014 International Conference on the Internet of Things, IOT 2014*, 2014, pp. 13–18.

[20] N. Nowdehi, A. Lautenbach, and T. Olovsson, “In-vehicle CAN message authentication: An evaluation based on industrial criteria,” in *IEEE Vehicular Technology Conference*, 2017, vol. 2017–Septe, pp. 1–7.

[21] A. S. Siddiqui, Y. G. J. Plusquellic, and F. Saqib, “Secure communication over CANBus,” in *Midwest Symposium on Circuits and Systems*, 2017, vol. 2017–Augus, pp. 1264–1267.

[22] P.-S. Murvay and B. Groza, “Source Identification Using Signal Characteristics in Controller Area Networks,” *IEEE Signal Process. Lett.*, vol. 21, no. 4, pp. 395–399, 2014.

[23] F. Li, L. Wang, and Y. Wu, “Research on CAN Network Security Aspects and Intrusion Detection Design,” in *Intelligent and Connected Vehicles Symposium*, 2017.

[24] “ECUSHIELD - The only Proven Ready for Integration Automative Cyber Security Solution.” [Online]. Available: http://tower-sec.com/ecushield/. [Accessed: 30-Mar-2018].

[25] “Argus Cyber Security - Automotive Cyber Security.” [Online]. Available: https://argus-sec.com/. [Accessed: 30-Mar-2018].

https://dspace.org/

A survey on CAN bus protocol: attacks, challenges, and potential solutions

Bozdal, Mehmet; Samie, Mohammad; Jennions, Ian

2019-03-07
IEEE
https://doi/10.1109/iCCECOME.2018.8658720
Bozdal M, Samis M, Jennions I. (2019) A survey on CAN bus protocol: attacks, challenges, and potential solutions. In: 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), 16-17 August 2018, Southend, UK

Downloaded from a DSpace repository. https://dspace.org/