2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) | 978-1-6654-3775-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ISGT50606.2022.9817541

A Cryptographic Method for Defense Against MiTM Cyber Attack in the Electricity Grid Supply Chain

Shuva Paul, Yu-Cheng Chen, Santiago Grijalva and Vincent John Mooney III
School of Electrical and Computer Engineering
Georgia Institute of Technology
Atlanta, Georgia 30345, USA
{spaul94, ychen414, sgrijalva6, mooney}@gatech.edu

***Abstract*— Critical infrastructures such as the electricity grid can be severely impacted by cyber-attacks on its supply chain. Hence, having a robust cybersecurity infrastructure and management system for the electricity grid is a high priority. This paper proposes a cyber-security protocol for defense against man-in-the-middle (MiTM) attacks to the supply chain, which uses encryption and cryptographic multi-party authentication. A cyber-physical simulator is utilized to simulate the power system, control system, and security layers. The correctness of the attack modeling and the cryptographic security protocol against this MiTM attack is demonstrated in four different attack scenarios.**

Keywords—Cyberattack, Cybersecurity, Supply Chain Cybersecurity, Cryptography, Bulk Power System Security

I. Introduction

Supply chain cybersecurity has become one of today's critical challenges [1][2]. The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) recommend government organizations and the private sector to utilize best security practices to prevent attacks from happening or to reduce their impact [3]. Due to the complexity of Industrial Control Systems (ICS) and Information and Communication Technologies (ICT), the frequency of cyberattack attempts on critical infrastructure is alarming. On the other hand, attackers are becoming more capable of executing sophisticated attacks that can cause significant socio-economic damage. ICSes are used to control electricity grids, often allowing remote connections to update control software.

Recent attacks, such as SolarWinds, Petya/NotPetya, and the U.S. Colonial Pipeline attacks, are examples of damaging attacks on critical infrastructures. The SolarWinds cyberattack is one the most destructive attacks on the supply chain network, which affected several technology organizations such as Microsoft, Intel, Cisco, Nvidia, FireEye, and several U.S. government agencies, including the U.S. Departments of Defense, Energy, Commerce, and Homeland Security. A backdoor was created in the Orion system of SolarWinds and distributed globally hidden in a routine software update. The attack affected almost 18,000 customers globally, who installed the corrupted update and exposed their networks [4][5]. Petya/NotPetya was another attack on the supply chain network of a Ukrainian accounting firm's software update executed in 2017 [6] [7]. The attack on U.S. Colonial Pipeline was based on ransomware attacks on the supply chain network [8]. In order to protect the supply chain from cyber-attacks, the parties involved need to adopt advanced security practices that include robust security and threat intelligence frameworks, continuous employee training, and supply chain security.

In order to improve supply-chain cyber-security for the electricity grid, in this paper we propose a cryptographic protocol based on hash and multi-party software update processes. The contributions of this paper are as follows:

- Multi-party software update process involving utilities, vendors, and control devices at the substation.
- A cryptographic security protocol is proposed for the software update process using multi-party authentication.
- Man in The Middle (MiTM) attack is implemented on the software update process, and simulated on four use cases.

The rest of the paper is organized as follows. Section II discusses the attack surface of the electricity grid, attackers' capabilities, and techniques focusing on the electricity grid supply chain. Section III discusses the cyber-physical simulator. Section IV describes the cryptographic encryption and hashing-based security protocol. The impacts of MiTM cyberattacks on the software update process with and without the security protocol are presented in Section V. Section VI provides the conclusion and future work.

II. Supply Chain Security in the Electricity Grid

A. Electricity Grid Attack Surface

The electric utility exhibits a large attack surface, which arises from the geographically dispersed nature of its physical and control layers, the vast number of control devices, and possible access at the utility substations, technology vendors, and customer systems. The electricity grid cyber-attack surface includes control systems, communication devices, remote access, third-party services, and supply chains.

The electricity grid must be defended against a wide range of attacks involving software, ICS protocols, connections to substations control devices, network devices, sensors, maintenance operations, supply chain integrity, and many more. The potential impacts are loss of access to control system networks, intercepting and altering data during information exchange, losing visibility of the field devices, loss of service to electricity customers and physical damage of power equipment.

B. Attacker's Capabilities

Remote attackers comprise the most considerable portion of the attack surface; they seek information (e.g., power grid operator credentials) through a variety of means, including psychological (i.e., social engineering) and technological (e.g., breaking codes). However, high-level attackers and complex

978-1-6654-3775-2/22/$31.00 ©2022 IEEE

coordination among multiple adversaries (insiders) can amplify the damages by executing sophisticated attacks. A lone-wolf entry-level employee can also be considered as the adversary capable of compromising the system.

Attackers follow multiple tactics and sub-tactics to execute cyberattacks such as reconnaissance, resource development, initial access, execution, etc. [9]. Through these stages, attackers can access and penetrate the system, observe, steal and alter valuable data, and damage the system (example includes changing line energization status, changing generator setpoints, etc.). The attackers' motives might include causing political damage, and social and economic disruption. Terrorist activity also covers a significant portion of the attackers' motives.

III. Security Approach

A. Cyber-Physcial Simulation

In order to assess the impact and cyber-attacks on the electricity grid supply chain, it is necessary to model the physical operation of the electric grid, its control system, and security protocols.

The simulator is tunable to several levels of granularity to achieve balance between performance and accuracy. For instance, actual encryption of communication between devices involved in the control loop can be enabled/disabled. The simulations based on power grid scenarios have several elements such as the power system itself, represented by a model of the physical power network, and the control devices connected to its substations, such as remote terminal units (RTU) and intelligent electronic devices (IED). The simulator supports an extensive set of parameters and options to analyze the effects of attacks on the control system and how these attacks impact the overall security of the power system. Attacks can involve altering data or injecting commands in the IEDs or RTUs. A command can open a breaker to disconnect transmission lines or loads or change the setpoints of generators. The simulator provides various metrics included loss of load and changes to N-1 security according to power system contingency analysis.

B. Security Architecture Components

Supply chain simulation requires modeling a set of actors that represent entities in the real world: a) Utility, is assumed to operate the physical power system using a SCADA system, b) Vendor, one or more organizations that manufacture control devices such as relays, RTUs, communication network switches, etc., c) Security Device, is a control device that provides Root-of-Trust (RoT) authentication and security capabilities, and d) Certificate Authority, an entity responsible for providing encryption and decryption keys to the parties involved. The components of the security architecture interact as a part of the attack use cases. For instance, the Vendor and the Utility need to communicate between themselves and with the Substation (devices) in order to authenticate and transfer data as part of a control device software update. The attacker will attempt to access this process and alter data in order to cause an impact. The impact of the attacker actions is captured by the cyber-physical simulator.

C. Workflow

The multi-party software update process involves actions that take place at three different layers: security layer, control layer, and power system layer as illustrated in Fig. 1. The workflow starts with the Certificate Authority distributing the public keys to the involved entities, mutual authentications, encrypted data transmission, and decryption, representing the architecture's security layer. After mutual authentication among the parties has taken place, the workflow enters the control layer. Once the update file is transferred securely to the device, the update file is scanned to identify the changes in the control parameters or status of any of the components. After identifying the changes in the control layer, the workflow proceeds to the power system layer, where the *loss of load* is selected as a parameter to observe and compare the impact of the attacks on the grid. Then changes mentioned in the update file are executed, the power flow is solved, and the loss of load is calculated from simulation data with and without the proposed security protocol.

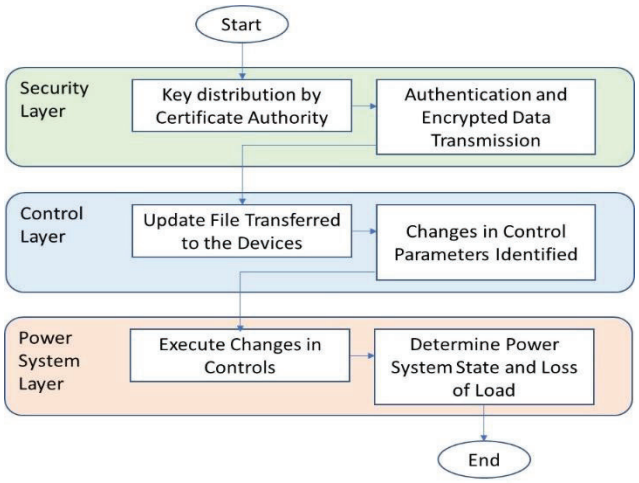

Fig. 1. Simulation workflow of multi-party software update.

IV. Security Protocol for Update Process

This section presents the security protocol to defend against MiTM attack during the software update process. The protocol utilizes cryptographic encryption and an authentication process based on hashing to secure the communication and update process. A cryptographic hash is a one-way function that generates a reliable signature suitable for use for authentication.

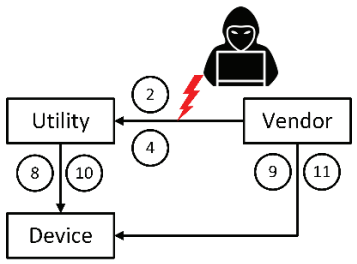

Fig. 2. Securing the supply chain of electricity grid against MiTM attack using mutual authentication based on hashes and encryption-decryption.

During an update process, the MiTM attacker would compromise a communication link between any of the entities involved in the update as illustrated in Fig. 2. In this paper, we assume that the attacker intercepts communications between the Vendor and the Utility; and the attacker then corrupts the update file by including malicious code. Fig. 2 also shows the communication in different stages of the protocol among the Vendor, the Utility, and the Device in accordance with the steps mentioned in the protocol.

Security Protocol for Update Process

```
1  Distribution of public keys by the Certificate Authority
2  Vendor requests to update an IED
3  if a software Update is requested then
4      Vendor sends the Update file to the utility
5      if a malicious update is detected then
6          Utility rejects the Update
7      else
8          Utility mutually authenticates with the
             Device
9          Vendor mutually authenticates with the
             Device
10         Utility sends the encrypted Hash of the
             Vendor's update file to the Device
11         Vendor sends the encrypted update file to the
             Device
12         Device decrypts the encrypted Update file
             from the Vendor
12         Device calculates the Hash from the Update
             File from the Vendor
14         Device decrypts the Hash of the Update file
             sent from the Utility
15         if Hashes match then accept the update
16     end
17 end
```

The protocol starts with the certificate authority distributing the public keys of the Vendor, the Utility, and the Device among themselves. There are multiple Vendors and each Vendor has a list of Devices installed in the grid. However, each Vendor is allowed to update the Devices that are manufactured by the said Vendor. When the Vendor of the Devices requests a software update to the Utility, the Utility checks for any malicious code/command in the update file. If the Utility successfully detects the malicious code/object in the update file, it rejects the update. We assume that the Utility has the capability to inspect the code for bugs and vulnerabilities in order to ensure code quality and security. If the Utility does not detect a malicious code/object in the update file, then the Utility, the Vendor, and the Device start communicating to authenticate themselves and exchange the update file. Initially, the Utility and the Vendor send their ID and generated Nonces to the Device, encrypted using the Device's public key (RSA). The Device decrypts these messages using its private key. The Device then sends its Nonce, the decrypted Nonces from the previous messages, and its ID to the Utility and the Vendor adopting RSA encryption using the receivers' public keys. Nonce is a random or non-repeating value, usually included during the transmission of data by security protocols. The Utility and the Vendor decrypt these messages using their private keys and check the received Nonces from the Device. If the Nonces match, the Utility and the Vendor keep communicating with the Device. At the same time, the Utility and the Vendor send the Device's Nonce (decrypted from the received messages) to the Device, encrypting with the Device's public key. The Device then decrypts these messages and verify the Nonce. If matches, the Device keeps communicating with the Utility and the Vendor. At this stage, the Utility generates a session ID and sends it to the Device by encrypting using the Device's public key (RSA). The Utility generates a Hash of the update file which it received from the Vendor and sends it to the Device by encrypting using the session ID as a key (AES). On the other hand, the Vendor generates another session ID like the Utility and sends it to the Device using RSA. Next, the Vendor sends the Update File with AES encryption using the session ID as the key. The Device then decrypts these messages from the Utility and the Vendor and extracts the session IDs. Using the session IDs as the keys, the Device decrypts the Hash and the Update file from the messages. Finally, the Device generates a Hash of the Update file and compares it with the Hash it received from the Utility. If it matches, then the communication and update file is secured; hence it can be accepted and installed on the Device.

V. Simulation Studies

This section describes the simulation of cyberattacks on the software update process. The cyber-physical simulator is used to model the power system, control, and security layers. In the simulations presented later in this section, it is assumed that the software update includes malicious code that can alter two parameters: the energization status of a transmission line, and the generator active power output setpoints. We use a small power system case with six lines and three generators for four different case scenarios. We use data corresponding to one day analysis of the power system, with an assumed baseline load forecast. Fig. 3 represents the test system in consideration where the G1, G2, and G3 represent the generators; L1 and L2 represent the loads and 1, 2, 3, 4, and 5 represent the buses. The lines are connected between the buses.

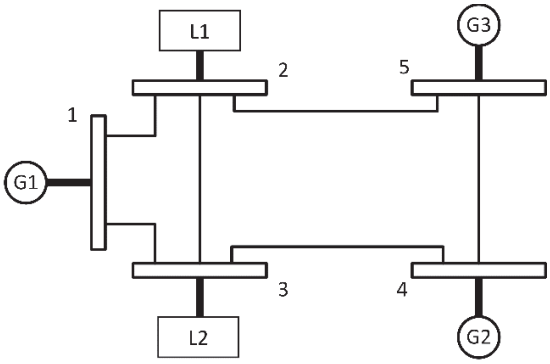

Fig. 3. The test power system with lines and generators

We calculate the probabilities of the lines to be selected as attack target by calculating their weighted probability based on resulting loss of load if the line is open as shown in Table I. The attacker would be interested in controlling the lines that cause the larger impact. From the Table we can interpret that, line 5 causes the maximum loss of load if attacked by the attacker. Line 5 has the maximum probability, and line 2 has the lowest probability of being attacked. The probabilities are assumed and

calculated to represent different ways of attacker attacking the system and different control parameters.

TABLE I: PROBABILITIES OF ATTACK ON LINE STATUSES

Line	Total Loss of Load (MW)	Loss of Load at a specific time (MW)	Attack Probability
1	102.095	0.950	0.023
2	22.762	5.952	0.005
3	243.571	21.214	0.056
4	1292	64.468	0.295
5	2447.116	105.532	0.559
6	272.883	18.104	0.062

A. *Case 1: Attack on Transmission Line Status*

In this attack scenario, the attacker can open the circuit breakers of two lines. The attacker compromises the update file of the control device at the substation by introducing two commands that open corresponding transmission lines at a given time. In order to set up the malicious code, the attacker must have knowledge of the configuration of the control device, with respect to the records and IDs of the line circuit breakers to be open, default statuses of the power devices, etc. The malicious command injected in the update would be:

```
OPEN LINE LineID
```

Fig. 4 shows the active power flow of line 1 before and after the attack. We assume two scenarios: attack opening lines 1 and 2, and attack opening lines 3 and 4. The blue curve in Fig. 4 represents the flow without attack (baseline). The orange curve represents the line flow after disconnecting lines 1 and 2. The green curve represents the active power flow on line 1 after disconnecting lines 3 and 4.

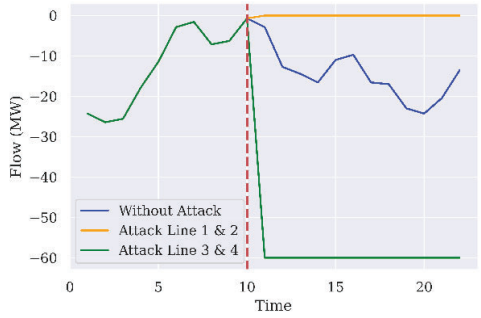

Fig. 4. Flow on line 1 for attacks that change line statuses. The red dotted line represents the time step when the attack initiates.

B. *Case 2: Attack on the Generator Setpoints:*

In this attack scenario, we assume that the attacker can attack generator setpoints. There are three generators in the system. We assume the attacker can modify the setpoints of either one generator at a time or the setpoints of two generators. The generator command would look as follows:

```
SET GEN GenID MW TO Value
```

The blue-colored curve in Fig. 5 shows the line flow without attack (baseline); the orange-colored curve represents the line flow after changing the generator setpoints of generator 2. Similarly, the green curve and the purple curve show the line flow after changing the setpoints of generator 3, and generator 2 and 3 together, respectively. As mentioned earlier, the red dashed line represents the attack time step.

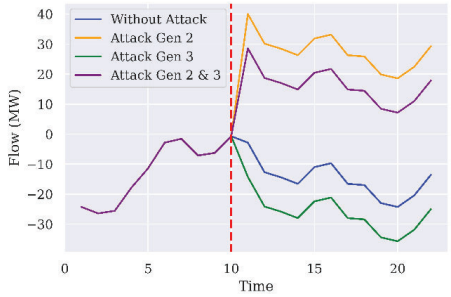

Fig. 5. Flow on Line 1 for attacks that change generator set points.

C. *Case 3: Coordinated Attack on Line Status and Generator Setpoints:*

In this attack scenario, we assume that the attacker can execute hybrid attacks involving changes of line statuses and the generator setpoints, together. Fig. 6. shows the line flow of line 1 before and after the attacks on the line statuses and generator setpoints. The blue-colored curve represents the line without attack (baseline). The purple-colored curve represents the line flow after the attacks on the line statuses (lines 1 and 2) and generator setpoints (generators 2 and 3).

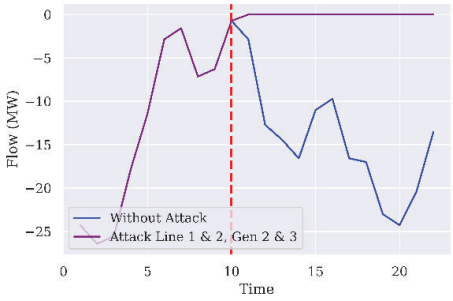

Fig. 6. Flow on line 1 for attacks on line statuses and generator setpoints.

Let us now assume that the attacker can execute commands at different points in time. In this case, we assume the attacker is executing line switching attack at time step 5, and attack on the generator setpoints at time step 15. Fig. 7 shows line flow of line 4 due to the coordinated multi-timescale attack on line 1 and 2 at timestep 5, and on generator 2 and 3 at timestep 15. Note that, these attack scenarios are the for the representation purposes of the attacker's capacity and possibilities of carrying out different types of attacks. The attack commands would be:

```
OPEN LINE LineID AT TIME t
SET GEN GenID MW TO Value AT TIME t
```

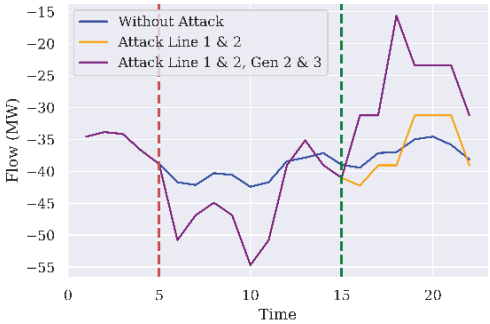

Fig. 7. Flow on line 4 for attacks on line statuses and generator setpoints at different times

D. Case 4: Attack With Security Protocol

In this case, the security protocol is active. The attacker implements a MiTM attack by intercepting the communication, injecting the malicious code on the form of control commands. According to the security protocol, the Device will calculate the hash of the update file coming from the Vendor and compare it with the hash of the update file coming from the Utility. Since the update file was corrupted while transmitting from the Vendor, the hashes will not match. Hence the Device will reject the update and the update installation is not executed. Fig. 8 illustrates the error message returned from the system.

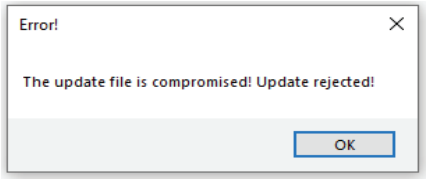

Fig. 8. Error message received when the Hashes did not match.

We execute the attack scenarios mentioned in the previous cases 1, 2, and 3, and observe the results shown in Table II.

TABLE II: ATTACK ON THE TARGET (VIA MALICIOUS UPDATE FILE) WITH THE SECURITY PROTOCOL IN ACTION

Trial	Attack Target	Defense Status
1	Line 1 – Status	Defended
2	Line 5 – Status	Defended
3	Line 2 & 5 – Status	Defended
4	Gen 2 – Setpoint	Defended
5	Gen 3 – Setpoint	Defended
6	Gen 2 & 3 – Setpoint	Defended
7	Line 2 & 3 - Status, Gen 2 & 3 – Setpoint	Defended

As we can observe in Table II, different types of attacks are carried out with the security protocol implanted. In all trials the defend status is "defended", which indicates that the security protocol was able to detect the mismatch in the hashes and hence the presence of an altered file. By utilizing the proposed protocol, all the trials of the MiTM attacks are defended.

VI. CONCLUSION

Supply chain cybersecurity is of utmost importance to electricity grid operations since they can lead to damages to the parties involved and loss of electricity service to customers. The control device software update is a critical use case in the study of supply chain cyber-security. Supply chain cyber-security requires novels methods to model the various actors: utility, vendor, control devices, and the attacker, and the development of protocol that are appropriate for multi-party authentication.

This paper proposes a security protocol for software update process that uses multi-party authentication, and hash-based encryption methods. A certification authority distributed keys ins a security manner. The parties then communicate mutually authenticate. This enables the control device that requires update to be able to compare update files from the vendor and from the utility and determine if there is a match using hash.

The security protocol is illustrated in a small power system, with various control devices and simulations that involve malicious commands in the update software that can disconnect transmission lines and change generator set points. The simulation results show the effectiveness of the proposed protocol during supply chain attacks by rejecting the update process due to hash mismatch.

ACKNOWLEDGMENT

This work was supported in part by The US Department of Energy Office of Cyber-Security, Energy Security and Emergency Response (CESER), Cybersecurity for Energy Delivery Systems (CEDS) Award to the Georgia Institute of Technology, # DE-CR0000004.

REFERENCES

[1] N. Gupta, A. Tiwari, S. T. S. Bukkapatnam, and R. Karri, "Additivemanufacturing cyber-physical system: Supply chain cybersecurity andrisks,"IEEE Access, vol. 8, pp. 47322–47333, 2020.

[2] K.-F. Cheung, M. G. Bell, and J. Bhattacharjya, "Cybersecurity inlogistics and supply chain management: An overview and future researchdirections,"Transportation Research Part E: Logistics and Transporta-tion Review, vol. 146, p. 102217, 2021

[3] "Government agencies and private companies undertake actions to limit the impact of foreign influence and interference in the 2020 u.s. election," American Journal of International Law, vol. 115, no. 2, p. 309–317, 2021.

[4] E. D. Wolff, K. M. GroWlEy, and M. G. GruDEn, "Navigating the solarwinds supply chain attack,"

[5] L. Lazarovitz, "Deconstructing the solarwinds breach," Computer Fraud & Security, vol. 2021, no. 6, pp. 17–19, 2021.

[6] D. U. Case, "Analysis of the cyber attack on the ukrainian power grid," Electricity Information Sharing and Analysis Center (E-ISAC), vol. 388, 2016.

[7] O. Analytica, "Critical infrastructure sees rising cybersecurity risk," Emerald Expert Briefings, no. oxan-db, 2021.

[8] K. Schatz, Armis discloses critical attack vector that allows remote take-over of Schneider Electric industrial controllers, 2021 (accessed July 14, 2021). Available at: https://finance.yahoo.com/news/ armis-discloses-critical-attack-vector-040100118.html.

[9] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. N. Gupta Gourisetti, "Cyber threat dictionary using mitre att&ck matrix and nist cybersecurity framework mapping," in 2020 Resilience Week (RWS), pp. 106–112, 2020.

[10] N. Z. Khidzir, K. A. Mat Daud, A. R. Ismail, M. S. A. Abd. Ghani, and M. A. H. Ibrahim, "Information security requirement: The relationship between cybersecurity risk confidentiality, integrity and availability in digital social media," in Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016) (N. A. Yacob, N. A. Mohd Noor, N. Y. Mohd Yunus, R. Lob Yussof, and S. A. K. Y. Zakaria, eds.), (Singapore), pp. 229–237, Springer Singapore, 2018.

[11] H. Thapliyal and S. P. Mohanty, "Physical unclonable function (puf)- based sustainable cybersecurity," IEEE Consumer Electronics Magazine , vol. 10, no. 4, pp. 79–80, 2021.