

# Investigating safety and security interactions using the BDMP formalism: case study of a DDoS attack on Liberia

Radu-Cristian Basarabă  
University of Twente  
P.O. Box 217, 7500AE Enschede  
The Netherlands  
r.basaraba@student.utwente.nl

## ABSTRACT

Safety and security issues are converging on many innovative and worldwide connected systems. As the risks are also evolving, it is important that safety and security interactions are identified and formally addressed, in order to reduce threats that can endanger critical systems. This paper performs a detailed case study analysis on an international cyberattack to assess the presence of interactions between safety and security. The interactions found are further characterized following well-known definitions and standards, followed by the modelling of the case study through the BDMP (Boolean logic Driven Markov Processes) formalism. BDMP represents a modelling formalism that enables the dynamic graphical representation of an attack process, which can also give insights into how a system can fail. The case study concerns a distributed denial-of-service attack (DDoS) against the main telecommunication company in Liberia, a small West African nation. The high complexity of the attack provided aid in identifying diverse interactions at different levels between safety and security, some of which lead to critical vulnerabilities that made possible the attack.

## Keywords

Security, safety, BDMP, DDoS, modelling, interactions, interdependencies, Mirai, Liberia

## 1. INTRODUCTION

Safety and security are domains that represent distinct concepts in theory [8] and have been studied in a separate manner by particular communities [26]. Despite frequent use, the terms *safety* and *security* have definitions that vary widely in technical communities [8]. For use in the context of this paper, the concept of safety is associated with the risks originating from inside a system's environment, which can have unacceptable consequences on the outside, such as human losses or injuries, nature deterioration or heavy capital losses [18]. Security is associated with prevention and protection against malicious attacks or risk originating from the outside of a system's environment [18]. The increased interconnectivity in modern systems has opened a vast range of potential risks, which are not always identified by traditional risk analysis tech-

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

35<sup>th</sup> Twente Student Conference on IT Jul. 2<sup>nd</sup>, 2021, Enschede, The Netherlands.

Copyright 2021, University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science.

niques [25]. Interdependencies between safety and security started to converge in systems that were concerned by only one of the two, with prevalence in safety-critical systems [25], cyber-physical systems [30], industrial control systems [18], complex embedded systems [26], along with others. Therefore, it is crucial to consider possible interactions between safety and security in order to provide a complete risk analysis and management [25] of systems concerned with such interactions.

In addition to consideration, the existence of dependencies or conflicting states between safety and security calls for a more formal understanding of how these processes occur in real-world scenarios. For example, a locked door prevents unauthorized entry from outside the house, enforcing security, but proves to be an obstacle in case the house catches fire, blocking a vital exit for the people inside and endangering their safety. In the present literature, a systematic categorisation of all the types of interactions has been proposed by Cambacédès [25]. The interactions are grouped in the following categories:

- *Conditional dependency*: Completion of a security requirement conditions safety. The reciprocal situation holds as well.
- *Reinforcement*: Safety and security measures complete each other, resulting in a strengthening of both.
- *Antagonism*: Safety and security measures lead to conflicts when considered together.
- *Independence*: No interaction whatsoever between safety and security.

All interactions identified inside the case study will be considered according to these four kinds of relationships between safety and security. The case study chosen in this research is a DDoS attack that severely damaged Internet access in Liberia. The attack has been powered by the Mirai botnet, which used hundreds of thousands of Internet of things (IoT) devices from across the globe to power the attack, reaching a scale never seen before [2]. The inflicted damage has been heavy, as around 75% of the total share of Internet users from Liberia were dependant on the services of the targeted company, including public institutions such as hospitals or schools [1, 9].

The goal of this paper is to investigate how safety and security interact in practice. In particular, the following research questions will be investigated:

1. At what level do safety and security interact?
2. What is the nature of the elements that interact?

3. Do the interactions highlight any unforeseen vulnerabilities that may require countermeasures, additional factors or requirements?

To answer these research questions, this paper will perform a comprehensive investigation of the case study aiming to determine the presence of interactions between safety and security. The interactions will then be categorized according to well-known definitions and categories from existent literature. The case study is later modelled through the BDMP formalism in order to graphically represent these interactions and to draw meaningful conclusions out of the analysis. It is found that interdependencies between safety and security exist in multiple components of the case study, and security is the predominant origin of the interaction with safety.

## 2. RELATED WORK

Typical search engines such as Microsoft Academic, Google Scholar, ResearchGate, Scopus, and IEEE were used for gathering resources and related work in the fields tackled by this research. The search was done mainly using the keywords "security", "safety", "BDMP", "interactions", "DDoS", "interdependencies", "Mirai", and "Liberia", or combinations of these keywords.

Papers studying the interaction between safety and security were written in the fields of IoT and cyber-physical systems [30], global navigation satellite systems [14], industrial control systems [17], safety-critical systems [25] and cyber-attacks [19]. In the field of BDMP, Bouissou and Bon [7] introduce the formalism, which is later proposed as a better alternative to event trees [6]. A complete implementation of BDMP in security modelling has been addressed [23, 22] and uses have been documented in the analysis of dynamic repairable systems [24]. KB3 represents a modelling platform [23] developed for inputting graphical BDMP models, which generates textual descriptions used in computing the probability of the top event and visualise different scenarios leading to it. Safety and security interactions modelled with BDMP appear in multiple papers as well [14, 17, 19, 25]. As for the case study, the main area of research is represented by the Mirai malware, which is the main factor that made possible the attack. The malware is studied in depth by Antonakakis [2], regulatory measures against it have been advanced [13] and potential realistic systems that can mitigate the associated risks of a DDoS attack powered by botnets like Mirai have been proposed [27].

The structure of this paper is as follows. Section 3 presents the case study and assess through analysis the presence of safety and security interactions. In Section 4, the BDMP formalism is presented alongside an example of its use and the interactions identified in the case study are modelled. The results are then discussed. Finally, Section 5 presents the conclusions and gives indications towards future work in the field.

## 3. CASE STUDY

The selected case study is a DDoS attack that targeted the main telecommunication company in Liberia. Around 1.5 million people were using the services of Lonestar Cell MTN at the moment of the attack [9], which represents around 30% of the total population of Liberia (5.2 million people, as of June 2021 [1]).

## 3.1 Presentation and key points

The company's servers were the most targeted victims of Mirai in terms of the number of attacks sustained [2], which lasted from October 2016 until February 2017. The large scale attack effectively slowed down the Internet access of the customers of Lonestar considerably, reaching the point of total crash several times in the four months in which the attacks took place [9]. The effects were amplified by the fact that in Liberia there is virtually no fixed-line telephone network, as it was almost fully destroyed during their two civil wars [12].

The attack has been powered by a number of the order of hundreds of thousands of small Internet-of-things (IoT) devices, such as routers, security cameras or DVRs [2]. The devices were controlled by the Mirai malware and acted as "slaves" which executed the commands received from the report server controlled by the attacker. A flowchart with the timeline of the events is found in Appendix B.

## 3.2 Mirai botnet

Mirai is a computer malware that targeted IoT devices and was designed to use the infected devices as bots in large scale DDoS attacks [20]. The first public report of Mirai was on 1<sup>st</sup> of September 2016 [5], but the malware received more public attention around mid-September when massive attacks on the website of respected security journalist Brian Krebs took place [15]. The attack recorded a volume of 620 Gigabits of traffic per second, one of the largest on record at that time [2]. On the 30<sup>th</sup> of September, the authors of Mirai released publicly the source code [20], which led to considerable growth in the number of variants [2]. This release has been followed by another two high profile attacks powered by Mirai. Firstly, on 21<sup>st</sup> of October, the rerouting internet company Dyn was targeted by another massive attack, which caused major platforms like Reddit, Github, Spotify or Netflix (clients of Dyn) to be unavailable for a couple of hours [29]. The second attack concerned the case studied in this research, namely, the attacks on Lonestar's infrastructure made with the variant Mirai#14, developed by Daniel Kaye [9].

The malware's functionality and propagation will now be addressed [2]. Initially, the bot enters a scanning phase in which it sends stateless packages through the TCP protocol to random IPv4 addresses, excluding the addresses present on a blacklist of the malware. If potential victims are uncovered by the scanning phase, the malware enters in a brute-force login attempt, which is using 10 random combinations of username and passwords. The botnet selects the combinations from a pre-configured dictionary of common default credentials [2]. If the authentication is successful, the particular details of the device (IP and credentials) are sent to a report server, from which a loader program that will execute architecture-specific malware is then downloaded [2]. After this step, the malware will try to avoid detection by deleting the downloaded files and change the name of the process into a random string. Additionally, Telnet and open TCP ports are closed in order to prevent patch fixes through updates or infections with other variants. At this point, the infected devices will act as "slaves" controlled from the report server and can be used at any time in DDoS attacks. The output size and the severity of the attack grow proportionally with the number of controlled devices.

Analysis of the bandwidth of infected devices and their scanning rate has shown that Mirai target mainly devices with low computational power or devices that were placed

Nr.	Interaction	Name	Type
1	Conditional Dependency	Default passwords	security requirement
2	Conditional Dependency	Lack of supporting security measures	measure
3	Conditional Dependency	Jurisdiction problems	safety requirement
4	Conditional Dependency	Only one undersea fibre cable	safety requirement
5	Reinforcement / Antagonism	Fingerprinting	preventive measure
6	Reinforcement	Machine learning use in DDoS recognition	preventive measure
7	Reinforcement	Routing Around Congestion	preventive and combat measure
8	Antagonism	Ports TCP/7547 and TCP/5555	safety and security requirements
9	Antagonism	Update functionality	service/measure
10	Independence	Update functionality and fibre cable	measure and requirement

**Table 1. Nature of the interactions**

in areas with low bandwidth [2].

### 3.3 Interactions between safety and security

#### *Justification of choices.*

Every interaction between safety and security mentioned in Table 1 will be taken one by one and a justification on why it fits a current type will be provided.

1. Passwords represent a key part in the authentication process, and malicious authentication attempts may result in gaining control over a device, raising safety risks. In this case, security conditions safety, because the completion of a security requirement (secure passwords) conditions the safety risks associated with malicious control over a device. A detailed explanation of this case can be found in chapter 3.4.
2. The absence or lack of actions towards protecting the system against a cyberattack represents itself a security concern, which generates safety issues related to the correct functioning of the devices (slow performance, crashing). This case represents a conditional dependency of security over safety, as the presence of protective measures influences the effects of a security breach on safety. If implemented, these measures might reduce the safety risks associated with a breach, otherwise, the risks are higher due to security vulnerabilities and slow responses in case a breach happens. Security practices against the Mirai botnet are stated in the Appendix A.
3. Security practices of the world’s top manufacturer’s of electronic devices are influenced by inconsistent legal jurisdiction across the world and lack of international coordination through unified standards [2]. This represents a safety concern, as the purpose of the legislation is to maintain citizens well-being, and, thus, a failure to do so would have negative effects on security practices, leaving potential vulnerabilities exposed to attackers. Therefore, safety conditions security in this case.
4. Internet access in Liberia heavily relies on the only undersea ACE fibre cable that goes into the country [3], as satellite Internet proves to be costly and slow [10]. A failure of this point would generate great safety risks for the population of Liberia, as safety-critical systems such as hospitals or power plants are dependent on it, making it a safety requirement. Local security measures would be cancelled out by damage sustained by the fibre cable, as all the Internet firstly passes through it, so security is conditioned by safety in this case.
5. Fingerprinting is a preventive measure against IoT botnets [30] that hardens security through classifying entire networks of devices uniquely. However, security exploits can also be developed through fingerprinting, as IoT devices cannot differentiate between two messages that look the same (one malicious and one friendly), so critical-safety systems can be affected by this disclosure of private data. As a result, the measure of fingerprinting can be considered a reinforcement, as both safety and security will be reinforced by the security hardening associated with fingerprinting, but in safety-critical systems this measure develops new safety risks, even though it increases the security, representing, therefore, an antagonism.
6. Use of machine-learning in DDoS attacks recognition proves to be an efficient and promising technique of mitigating and identifying an ongoing attack [31]. Such a measure would reinforce the overall security, and because in most cases the targeted system will remain up and running instead of crashing, safety risks are also ameliorated. Therefore, this measure would reinforce both security and safety.
7. Routing Around Congestion is a system design that can effectively mitigate a modern DDoS attack, regardless of the traffic, and functions without outside cooperation or Internet redesign. More details on how this system works can be found in the chapter 3.4 and in the paper where it was first proposed [27]. Through this measure, the security of the system would be hardened and the potential safety risks related to the failure of the system would be ameliorated, reinforcing both safety and security.
8. The case of the TCP ports 7547 and 5555 represents a concise example of conflicting requirements of safety and security. On one hand, the ports are open by default (i.e. they do not require user authentication when used), motivated by usage in the CPE WAN Management Protocol (CWMP) [4]. On the other hand, these ports were primarily used by the Mirai botnet in its spreading strategy. Using active scanning to ping those ports, the malware would try to authenticate with some default usernames and passwords and get control over the device, if succeeded. This creates an antagonistic situation between the two requirements and is analysed in detail in chapter 3.4.
9. The update mechanism provides a way for the developer to patch fixes, bugs or vulnerability through timed updates of the system, with minimal user intervention [2]. However, in the case study, the Mirai botnet used this mechanism in its self-spreading

functionality, effectively using it to propagate very fast through entire networks [2]. As a result, this represents an antagonistic case, because it increases security and acts as a mitigation measure on one hand, but it also presents an exploit that can compromise the safety of an entire network on the other hand.

10. The update functionality (security measure) and the presence of only one undersea fibre cable (safety requirement) were chosen to illustrate the category of independence. When active, the update functionality concerns the devices targeted by the Mirai malware and the fibre cable is responsible for the Internet connectivity in Liberia, which does not interact directly. When both fail there is no interaction whatsoever as well between safety and security, so an independent relation between safety and security can be assumed.

### 3.4 Analysis

#### *Antagonism.*

The particular situation of default open TCP ports 77547 and 5555, two ports associated with use inside the CPE WAN Management Protocol [4], represents well the antagonistic interaction between safety and security. The role of this application-layered protocol is to provide a configured and secure way between the user equipment and auto-configuration servers. For smooth usage, devices kept the ports open by default, so the whole process would be automated and without user intervention.

However, the fact that the ports were open and actively listening to messages represented a security vulnerability, which Mirai was able to exploit. The initial communication with potential targets was done by sending requests through the two TCP ports, which would indicate if the devices had the ports open. That being the case, the malware would start its dictionary attack with the purpose of gaining access to that particular device, through the same open ports.

Therefore, an antagonistic interaction between these factors can be outlined. On the safety side, the open ports play a role in automatic management, configuration and protection of the user equipment. On the security side, the ports represent a breach, which was present in millions of devices all around the world at the time of the attack, easing the spread and infection rate of the Mirai.

Interestingly, after a successful infection, another antagonistic situation would arise, as the malware will try to erase other variants already present inside the device and close the ports, so to solidify its control. This represents a security measure and in fact, it increases the overall protection of the device, however, it represents a safety concern as the device is already compromised. The malevolent person controlling the bot would have access to all the data passing through the infected device, raising safety concerns over the privacy and integrity of the network.

#### *Conditional dependency.*

The most representative case of a conditional dependency inside the case study is represented by the default passwords of IoT devices attacked by the Mirai botnet. The infection and spreading mechanism of the malware relied heavily on this aspect [2].

Passwords represent an important security factor [11]. Consequently, bad security practices, such as common or weak

passwords, represent a security concern. The safety concerns associated with this breach of security are important and, as seen in the case study, the damage can be significant. The greatest safety concern is the fact that a compromised device infected with Mirai provides control over the devices to a malicious person. Alongside, an infected device represents another point in a network of infected devices, with each point being a source that tries to infect more potential targets from the network. Studies [28] show that even if a device would get rid of the Mirai infection (through a system restart, for example), it would be infected back again in around 5 to 10 minutes [16]. The safety concerns go even further, as the infected devices were used in large scale DDoS attacks all over the Internet, acting as the main source of the output of the attack. The damages differ, but go from crashing gaming servers (Minecraft servers) to crashing hundreds of thousands of consumer routers and effectively cutting the Internet access for 30% of the population of Liberia.

As a result, a security requirement (passwords) condition safety measures and responses related to malware infection and cyberattacks, while the failure to complete this security requirement conditions the potential safety risks and effects.

#### *Reinforcement.*

In the case study discussed in this paper, there is no clear reinforcement interaction between safety and security, mainly due to the chaotic nature of the event. There was a great unbalance between the attacker and the defendant, with the attacking side having a considerable advantage. This was mainly because of two factors. Firstly, the attacker possessed great attacking power and available resources and secondly, the defender did not possess enough mitigation measures. Furthermore, the critical infrastructure that was targeted was totally unprepared for an attack of such a scale, due to the two Liberian civil wars that slowed down the progress of the country and virtually cut all the landlines [12], leaving the population dependent on the mobile network.

For this reason, a potential realistic system that effectively mitigates a modern DDoS attack, regardless of the amount of adverse traffic, will be discussed. There will be a brief description of the main functionalities of the system and then a link is made on how safety and security will be reinforced by the adoption of such a system. Proposed by Smith and Schuchard [27], the system Nyx uses routing around congestion to mitigate the effects of a possible DDoS attack, regardless of the size of traffic flows generated by the attacking side and without outside cooperation or Internet redesign.

The first key point in the functionality of this system is that it controls only the benign traffic in a network, without having to rely on filtering or prioritization techniques. The second key point is that it uses traffic engineering techniques to route around congestion from DDoS attacks, enabling the deployer of the system to communicate with any other autonomous system without loss of quality even when is under attacks with sizes of the order of hundreds of Gigabits per second.

Lastly, the system demonstrates realistic deployment in a network, as it does not require outside cooperation from other autonomous systems, apart from the deploying system. The capabilities presented by this preventive measure would fit well the security needs against an attack comparable to the one presented in the case study, by ef-

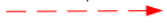

Representation	Modeled behavior
	Defines the dynamic aspect of BDMP. The element pointed by the trigger link is not activated until the realization of the origin gate/leaf of the trigger. When this element becomes activated, it transmits the activation signal it receives from its parents to the sub-tree targeted by the trigger.
	Creates a constraint in the order of realization of instantaneous events (on-demand failure leaves), in the case where they are required simultaneously.

Figure 1. Types of special links in BDMP



Representation	Modeled behavior
	This leaf is used to model a failure in operation, when the modeled component is active. Failure occurs after a time exponentially distributed (parameter $\lambda$ ) and can also be repaired in a time exponentially distributed (parameter $\mu$ ).
	This leaf is used to model a failure on demand, likely to arise instantaneously when the leaf changes of mode (activated or not), with a probability $\gamma$ . Failure can be repaired in a time exponentially distributed (parameter $\mu$ ).

Figure 2. Typical safety leaves



Representation	Modeled behavior
	The “Attacker Action” (AA) leaf models an attacker’s step towards the realization of his/her objective. In Idle mode, the action has not yet been tried. Active mode corresponds to attempts with a time to success exponentially distributed with a parameter $\lambda$ . The Mean Time To Success (MTTS) for this action is equal to $1/\lambda$ .
	“Instantaneous Security Event” (ISE) leaf models a security event that can happen instantaneously with a probability $\gamma$ when the leaf switches from the Idle mode to the Active mode.

Figure 3. Typical security leaves

fectively rerouting malicious traffic at critical points in the network, leaving the end users unaffected. The Liberia attack made use of a critical point, which was proven to be a single failure point of the Internet infrastructure in the African nation, namely, its only undersea fibre cable.

The deployment of the Nyx system would harden the security of the system and, consequently, neutralize safety concerns associated with a system crash or overload, thus, reinforcing both safety and security.

## 4. THE BDMP FORMALISM

Introduced by Bouissou and Bon in 2003 [7], the BDMP formalism was initially used in complex systems dependability assessment, and due to its modelling capabilities has later been adopted to attack and defence modelling [22].

### 4.1 Foundations

BDMP is a dynamic model, which enables graphical modelling of dependencies between events (the leaves of the tree) and how the top event can be reached through a sequence of events. The dynamic aspect of this formalism is characterized by the new types of links between components (called “triggers”) and through the fact that each BDMP event can have two possible modes that will realise the basic event. In this way, new semantics are added to

the representation of event trees instead of creating new types of gates, combining the properties of fault trees and Markov models.

Additionally, BDMP possesses interesting mathematical properties, which greatly reduce the calculation complexity for Markov processes with huge state spaces [6]. Combinatorial problems can be greatly reduced in complexity while they are being processed through methods based on sequences exploration and relevant event filtering. The complete mathematical background of BDMP and the demonstration of its properties are discussed in [7].

### 4.2 Modeling with BDMP

The structure of BDMP is hierarchical and the complexity goes from top to bottom. The top event represents the attack goal and is the starting point in creating a model. Later, the analyst goes down the levels of the tree adding more and more details. In this way, the top event has a high-level abstraction, which is then processed into smaller details that present a lower level of abstraction as the levels of the model go down. The relatively reduced number of elements per level also minimizes the risk of a mistake and through its easy readability models can be easily checked and revised. [17].

As already mentioned, BDMP possesses two types of special links between their components, which are described



in Figure 1 [25]. Besides this, they also inherit the traditional links used in event trees, denoted by a solid black line, which connects a gate to its sons.

A typical safety leaf has two distinct states that are described in Figure 2 [25]. These leaves usually describe accidental events that can happen either when the failure happens in operation or on-demand. For example, a wire responsible for transmitting electric energy can fail in time due to reaching its maximum usage capabilities or can fail because it was broken by a falling tree. Both ways describe the same event, but the distinction between the ways in which it can fail represents an important detail for the risk analysis [19]. Since the adoption of BDMP to attacking modelling, two other types of leaves have been added to the semantics. These are described in Figure 3 [25]. As an example, the event in which an attacker gains control access of a device through brute force of the credentials represents an "Attacker Action" (AA) leaf, as it represents a step in the realization of the attack and has a success time exponentially distributed. On the other side, the event in which the correct combination username-password has been guessed represents an instantaneous event that can further trigger other events and change their state. With these additions, the analysis will benefit from added details in an attacking scenario, providing more depth to the possible failures of the system.

Leaves can be represented in BDMP models also through graphical notations of dynamic events, such as Petri nets. Petri nets are composed of places, transitions and arcs that run in-between places and transitions. The boolean value of the leaf is true if the Petri net process outputs true, and false otherwise. This offers the possibility to detail even more the significant events that lead to the realisation of the top event. For example, the detection of an attack can be modelled through a Petri net, with an associated probability that the attack is detected while ongoing. The detection of an attack has a great influence on the realisation other events (rapid detection → diminished damage, slow or not detection → increased damage). In this way, the readability and the structure of the model is maintained, while dynamic and processes are integrated as leaves. Additionally, Petri nets possess complete mathematical theory [21].

The BDMP model developed for this research has been created through the website <https://www.diagrams.net/>, which offers great flexibility in modelling, while also offering diverse templates. The initial template used was for a decision tree, but with added logical gates and links which were then matched to the semantics of BDMP.

### 4.3 System modelling

The proposed case study will be modelled from an attacking perspective and the goal is to show how the system can fail. The system is composed of the following:

- Critical Internet infrastructure such as servers, submarine fibre optics or gateways.
- An attacker who tries to compromise the system.
- Maliciously-controlled IoT devices that power the attack.
- Manufacturers of the affected devices and Internet service providers (ISPs).

For better visualisation, the gates and the leaves of the diagram were coloured based on their type. Light-blue

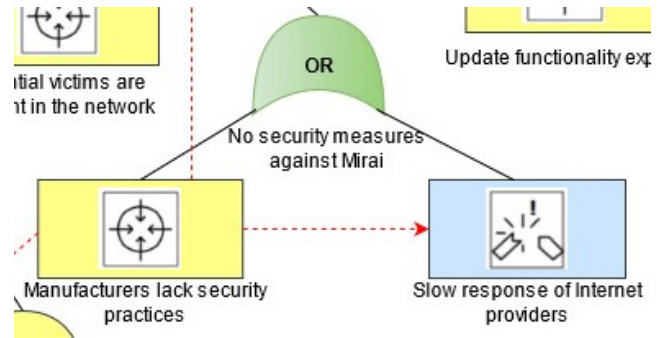


Figure 4. Example

represents a component that belongs to safety, yellow represents security components and in green were marked the elements that have properties in both safety and security.

A small example taken from the model will be discussed to illustrate this partitioning by colours. In Figure 4, the OR gate indicating the lack of measures against the Mirai infection has two leaves, namely, manufacturers lack security practices and slow response of the Internet providers. The first leaf represents a security measure, as it concerns the lack of mitigation and preventive measures taken by the manufacturers of the devices targeted by Mirai, and is represented in *yellow* in the model. Additionally, the behaviour that this leaf model is the "Attacker action", as the exploit of a vulnerability represents a necessary step in the attacker's goal to compromise the system. In active mode, it will correspond to attempts that will lead to success in a time exponentially distributed (i.e. when the attacker will start exploiting these vulnerabilities).

The change of state of the first leaf will activate the second leaf through the trigger, which models the slow response to an infection. This represents a safety concern, as the users of those devices can experience negative effects due to the infection (crashing, slow performance) and threats like DDoS attacks are also possible, should the number of devices be large enough. Being concerned with safety, the leaf is coloured in *blue* and the behaviour modelled is a safety failure in operation. The change of state cannot happen instantaneously in this case and happens rather in time, due to the insufficient mitigation measures in response to an attack which led to negative effects experienced by the people using those services. Finally, the gate is naturally marked in *green*, as one leaf represents security and the other one safety. As it is an OR gate, once any of its leaves becomes true, the gate will also output true further up the tree.

### 4.4 Analysis of safety and security interactions

The proposed system is an information centre responsible for Internet connection, used by the company Lonestar Cell MTN, the main telecommunication operator in Liberia. The goal of the analysis is to show how the system can be compromised in an attacking scenario and to graphically model the interdependencies between safety and security.

The complete BDMP of the case study is present in Figure 5. The top event represents the failure of the system, a case in which the Internet connection is down for the subscribers of Lonestar. This breakdown can happen if the critical infrastructure responsible for Internet connectivity fails and if the ISPs do not have enough mitiga-

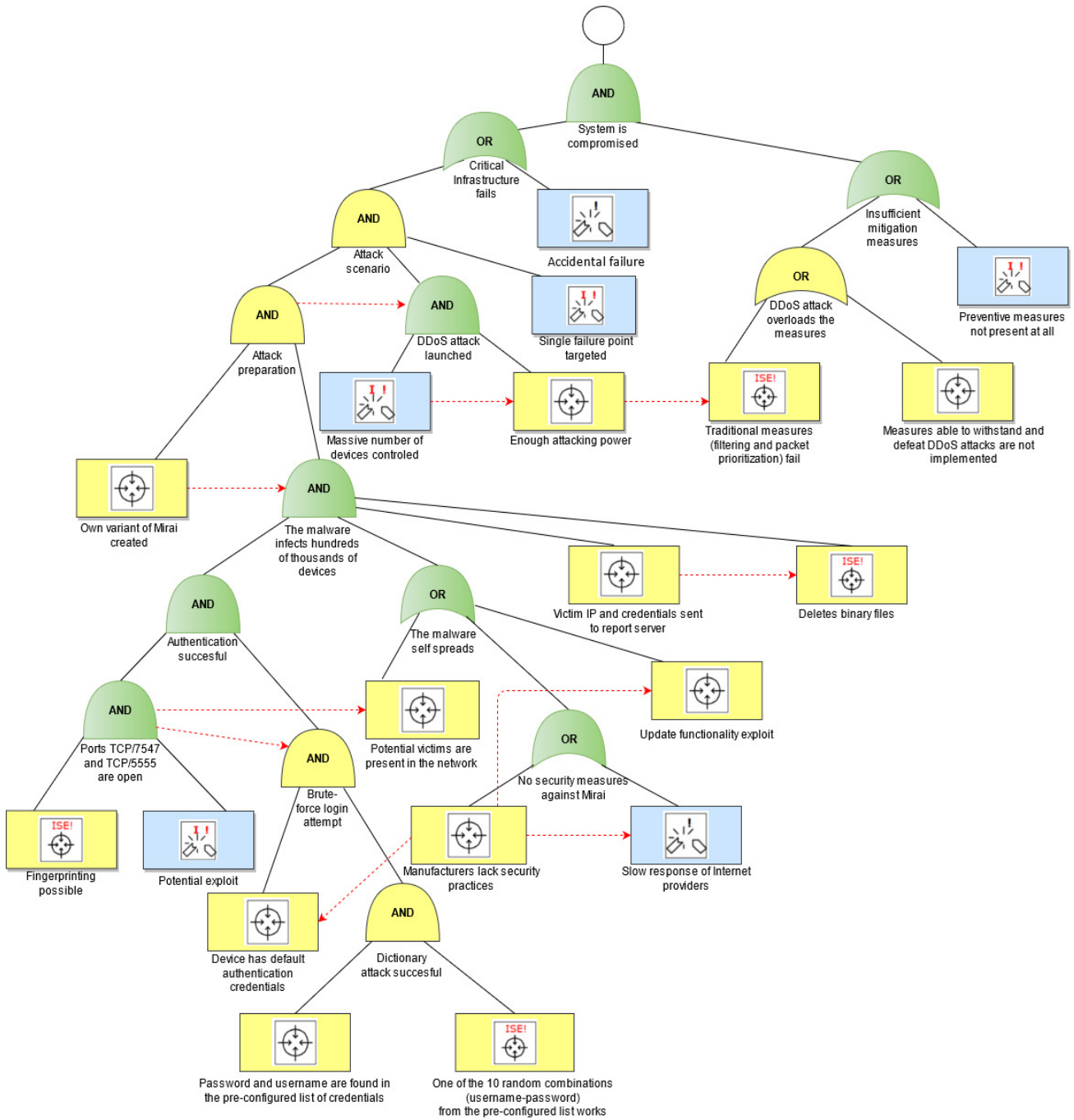


Figure 5. BDMP model of the case study

tion measures to alleviate the associated risks. One possible sequence that leads to the top event can already be pointed out, in a pure safety scenario: accidental failure of the critical infrastructure and no mitigation or preventive measures present in the system will lead to the realisation of the top event.

The other way in which the critical infrastructure can fail is through the attacking scenario, which represents the main part of the model. The attacking scenario resembles the Liberia attack, with a DDoS launched against critical infrastructure and a preparation phase, in which the resources of the attack were gathered. The attack will be launched only when the preparation phase is complete, which is represented through a trigger in the model, activating the attack as soon as the preparation outputs

true. The attack is successful if the number of controlled devices offers enough power to compromise the critical infrastructure, represented again through a trigger between the events. This will further activate the failure of the measures against a DDoS, changing the state of the right subtree in true.

The preparation requires firstly that the attacker creates an own variant of Mirai, which triggers the activation of the infection process, which represents in the BDMP the behaviour of Mirai. The process of infecting devices requires that the authentication is successful, that the malware self-spreads continuously to other devices and that the device information is received by the report server. After the device information is received by the server, this will trigger the deletion of the files from the device, in or-

der to avoid detection. The behaviour of Mirai is already discussed in Section 3.2, so the focus will be moved to the interdependencies between safety and security captured in the model.

The case of lack of security practices that influence the slow response to a malware infection has already been discussed as an example for the system modelling in the previous section. For reference, interactions found in Table 1 and the most relevant interactions detailed in chapter 3.4 will now be highlighted in the model.

**Antagonism.** As the model is created from an attacking perspective, only the attacking side of the antagonistic action can be seen. The default-open TCP ports are considered as an antagonism case in the model and it is represented by an AND gate marked in green, which combines safety and security events. The change of state of the event of the open port triggers brute-forcing attempts from the attacker and also makes devices vulnerable to Mirai infection. The exploit of this vulnerability can have negative effects on the population, therefore, it represents safety and can happen instantaneously, if the fingerprinting measure is implemented in the network and triggers its activation. The technical details of the exploit that happens in practice have been abstracted into the action of possible exploit, as they were not so relevant for the graphic representation.

The defending side of this antagonism could not be captured, as it concerned the positive effects of fingerprinting a network, but it can be deduced from the negation of the leaf representing fingerprinting. If the measure is considered in a non-safety-critical system, where it has solely positive effects, then the authentication would not output true (as the brute force attempt is not triggered and the leaf is inactive) and as a consequence, the system would not be compromised. As a result, fingerprinting would represent a *reinforcement* in this case, as security is hardened against exploits and safety is increased because the system remains up and running.

**Conditional dependency.** The case of default passwords is modelled in the BDMP as an attacker action leaf, as it is a step that brings the attacker closer to its goal. This conditional dependency can be seen in Figure 6. It represents a critical event, as without it, the failure of the system would not happen, as for a successful authentication both this event and the successful dictionary attack event have to be true. The event of default credentials is triggered by the lack of security practices of the manufacturers. The branch of this leaf is solely security-oriented, so the dependency of safety on security cannot be seen as clear as in other interactions, but the fact that it leads to a compromised system is enough to raise safety concerns.

**Reinforcement.** The implementation of preventive measures such as routing around congestion would help in easing and effectively combating the effects of a DDoS attack [27]. In the BDMP, this is modelled as an attacker action, as the absence of such measures represents a step in achieving the attacker’s goal of compromising the system. Should the measure be implemented, this would change the state of the leaf to false and make the entire tree false, as a system breakdown is avoided and the population is no longer in danger of losing Internet connection. Therefore, this measure reinforces both safety and security.

**Independence.** As the purpose of a BDMP representation of the system was to show interdependencies between safety and security, cases of independence between factors are not displayed explicitly. For the discussion in Sec-

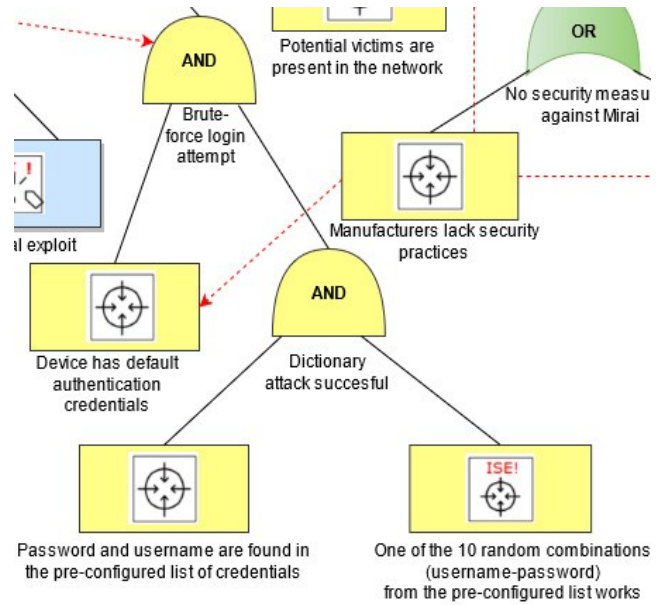


Figure 6. Conditional dependency

tion 3.3, the security measure of updating and the safety requirement of having an undersea fibre cable in Liberia were considered. In the BDMP, the undersea fibre cable is noted as a "single failure point", as it is modelled from an attacking perspective and models the behaviour of a safety failure on demand. The update functionality models the behaviour of an attacker action, as this functionality is a necessary step for the propagation of the malware inside a network, exploiting a vulnerability present inside its implementation [2]. Even though both events belong to the attacking scenario branch and are important events that will lead to the failure of the system if both are true, they do not have any direct interaction whatsoever. To sum up, the update functionality concerns security, the fibre cable safety, there is no trigger in between the events, they are on different levels of the BDMP, therefore, it is fair to assume an independent relation between safety and security in this case.

## 4.5 Findings

In Table 2, findings and discoveries uncovered by the analysis, aside of the themes discussed by the research questions, were noted.

Nr.	Textual description
1	Security is frequently the origin of the dependency
2	Safety issues have great influence on security
3	Small-scale security issues have great potential effects on safety, with prevalence in safety-critical systems
4	The presence of interactions between safety and security has not been considered in the risk analysis of the systems present in the case study
5	Avoidable security vulnerabilities made possible a large scale attack that affected millions of people

Table 2. Noteworthy findings of the research

Considering that a cyberattack was studied, security proved to be the origin of many interactions, as security requirements or measures frequently conditioned, reinforced or had an antagonistic relationship with safety elements. Seen from an attacking perspective, the vulnerabilities exploited



were represented by basic security requirements, such as default passwords or open ports to which devices actively listen, but these proved to be essential steps in making a large scale attack. The consequences of these exploits were clearly not considered in the risk analysis by the manufacturers of the devices, which can be concluded from the fact that the mitigation measures in place were ineffective or not present at all. When safety conditioned security, it was usually the case that the effects were influential and reached even the cancellation of security measures as a result (the only fibre cable going into Liberia failed in the transmission of Internet packages → local security measures were totally ineffective).

As a result, the attack kept on going for around four months, in which public institutions, doctors treating the Ebola virus epidemic [9] or simply citizens of Liberia were deprived of a stable Internet connection, endangering their safety.

## 5. CONCLUSION AND FUTURE WORK

In this paper, the interdependencies between safety and security present in an international cyberattack were identified and formally analysed. Through the analysis, the research questions proposed in the introduction could be answered.

Firstly, safety and security elements were shown to interact at multiple levels inside the case study. The two concepts interacted firstly at a low level of abstraction, for example, in the case of default-open TCP ports from the configuration of the compromised devices that powered the DDoS attack. Interactions were found also in higher levels of abstraction, such as in the case of the lack of security practices that would condition safety responsive measures and go even to very high levels of abstraction. That is the case when the assumption that critical infrastructure fails as a result of a malicious attack powered by exploits of security vulnerabilities, which puts citizens' safety at risk.

Secondly, the nature of the identified interactions is variable, usually consisting of measures and requirements of both safety and security. Section 3.3 presents the nature of all the identified cases. Most of the measures identified inside the case study were concerned exclusively with security or exclusively with safety, and did not take into consideration any overlapping between the two. This gave rise to vulnerabilities that were later exploited maliciously.

As for the last research question, interactions that require additional factors in order to properly function were found. Such an interaction is represented by the antagonistic case of the update function, which was used by both the attacker and the defender and requires additional security measures to be used solely in a secure way by the Internet service providers. More countermeasures against the Mirai are discussed in Section 3.4 and in Appendix A.

This research gives a platform for future work in the field and a more in-depth analysis of the present components exposed in this paper can be performed. BDMP modelling can be augmented with probabilities of events and used in the KB3 environment in order to generate a textual description for a larger model. The adoption of Petri nets as leaves can also improve the precision of the analysis, as more decision making can be incorporated in the events of the BDMP. Other case studies of cyberattacks that target critical-safety systems might also be analyzed through the same process exemplified in this paper, which may potentially lead to the discovery of unthought interactions between safety and security.

## 6. REFERENCES

- [1] C. I. Agency. The central intelligence agency side for liberia. <https://www.cia.gov/the-world-factbook/countries/liberia/>, June 2021.
- [2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, et al. Understanding the mirai botnet. In *26th security symposium (Security 17)*, pages 1093–1110, 2017.
- [3] L. T. Authority. Public consultation document on the definition of relevant telecommunications markets. <https://emansion.gov.lr/doc/CONSULTATION-DOCUMENT.pdf>, June 2016.
- [4] J. Blackford and M. Digdon. Tr-069 issue 1 amendment 5. [https://www.broadband-forum.org/technical/download/TR-069\\_Amendment-5.pdf](https://www.broadband-forum.org/technical/download/TR-069_Amendment-5.pdf), 2013.
- [5] M. Blog. Mmd-0056-2016 - linux/mirai, how an old elf malware is recycled.. <https://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html>, September 2016.
- [6] M. Bouissou. Bdmp (boolean logic driven markov processes) as an alternative to event trees. 09 2008.
- [7] M. Bouissou and J.-L. Bon. A new formalism that combines advantages of fault-trees and markov models: Boolean logic driven markov processes. *Reliability Engineering & System Safety*, 82(2):149–163, 2003.
- [8] G. Boustras and A. Waring. Towards a reconceptualization of safety and security, their interactions, and policy requirements in a 21st century context. *Safety Science*, 132:104942, Dec. 2020.
- [9] K. Chellel, L. de Bassompierre, J. Levin, Y. Benmeleh, and J. Robertson. The hacker who took down a country. <https://www.bloomberg.com/news/features/2019-12-20/spiderman-hacker-daniel-kaye-took-down-liberia-s-internet>, December 2019.
- [10] J. Deutschmann, K.-S. Hielscher, and R. German. Satellite internet performance measurements. In *2019 International Conference on Networked Systems (NetSys)*, pages 1–4, 2019.
- [11] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, pages 657–666, 2007.
- [12] V. F. Foster and N. P. Pushak. Liberia's Infrastructure : A Continental Perspective, volume 2011. 2010.
- [13] J. A. Jerkins. Motivating a market or regulatory solution to iot insecurity with the mirai botnet code. In *2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC)*, pages 1–5, 2017.
- [14] C. Johnson. Using assurance cases and boolean logic driven markov processes to formalize cyber security concerns for safety-critical interaction with global navigation satellite systems. *ECEASST*, 45, 01 2011.
- [15] B. Krebs. Krebsonsecurity hit with record ddos. <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>, September 2016.
- [16] B. Krebs. New mirai worm knocks 900k germans offline.

<https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/>, November 2016.

- [17] S. Kriaa and M. Bouissou. Safety and security interactions modeling using the bdmp formalism: case study of a pipeline. 09 2014.
- [18] S. Kriaa, M. Bouissou, L. Piètre-Cambacèdes, and Y. Halgand. A survey of approaches combining safety and security for industrial control systems. *Reliability Engineering [?] System Safety*, 139:156–178, 02 2015.
- [19] S. Kriaa, M. Bouissou, and L. Piètre-Cambacèdes. Modeling the stuxnet attack with bdmp: Towards more formal risk assessments. In *2012 7th International Conference on Risks and Security of Internet and Systems (CRISIS)*, pages 1–8, 2012.
- [20] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim. An in-depth analysis of the mirai botnet. In *2017 International Conference on Software Security and Assurance (ICSSA)*, pages 6–12, 2017.
- [21] T. Murata. Petri nets: Properties, analysis and applications. *Proceedings of the IEEE*, 77(4):541–580, 1989.
- [22] L. Pietre-Cambacèdes and M. Bouissou. Attack and defense modeling with bdmp. pages 86–101, 09 2010.
- [23] L. Pietre-Cambacèdes, Y. Deflesselle, and M. Bouissou. Security modeling with bdmp: From theory to implementation. pages 1 – 8, 06 2011.
- [24] P.-Y. Piriou, J.-M. Faure, and J.-J. Lesage. Generalized boolean logic driven markov processes: A powerful modeling framework for model-based safety analysis of dynamic repairable and reconfigurable systems. *Reliability Engineering & System Safety*, 163:57–68, 07 2017.
- [25] L. Piètre-Cambacèdes and M. Bouissou. Modeling safety and security interdependencies with bdmp (boolean logic driven markov processes). In *2010 IEEE International Conference on Systems, Man and Cybernetics*, pages 2852–2861, 2010.
- [26] E. Schoitsch. Design for Safety and Security of Complex Embedded Systems: A Unified Approach. In J. S. Kowalik, J. Gorski, and A. Sachenko, editors, *Cyberspace Security and Defense: Research Issues*, pages 161–174, Dordrecht, 2005. Springer Netherlands.
- [27] J. M. Smith and M. Schuchard. Routing around congestion: Defeating ddos attacks and adverse network conditions via reactive bgp routing. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 599–617, 2018.
- [28] J. B. Ullrich. Port 7547 soap remote code execution attack against dsl modems. <https://isc.sans.edu/forums/diary/Port+7547+SOAP+Remote+Code+Execution+Attack+Against+DSL+Modems/21759/>, November 2016.
- [29] D. S. Updates. Update regarding ddos event against dyn managed dns on october 21, 2016. <https://www.dynstatus.com/incidents/5r9mppc1kb77>, October 2016.
- [30] M. Wolf and D. Serpanos. Safety and security in cyber-physical systems and internet-of-things systems. *Proceedings of the IEEE*, 106(1):9–20, 2018.
- [31] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu. Iot security techniques based on machine learning: How do iot devices use ai to enhance security? *IEEE Signal Processing Magazine*, 35(5):41–49, 2018.

## APPENDIX

### A. ADDITIONAL SECURITY PRACTICES AGAINST THE MIRAI BOTNET

1. *Eliminate default credentials*: This will prevent hackers from constructing a credential main list that allows them to compromise a myriad of devices as Miraidid.
2. *Make auto-patching mandatory*: IoT devices are meant to be “set and forget,” which makes manual patching unlikely. Having them auto-patch is the only reasonable option to ensure that no widespread vulnerability like the Deutsche Telekom one can be exploited to take down a large chunk of the Internet.
3. *Implement rate limiting*: Enforcing login rate limiting to prevent brute-force attack is a good way to mitigate the tendency of people to use weak passwords.
4. *Using captcha or proof of work*: Effective measure against bots.

### B. TIMELINE OF THE CASE STUDY

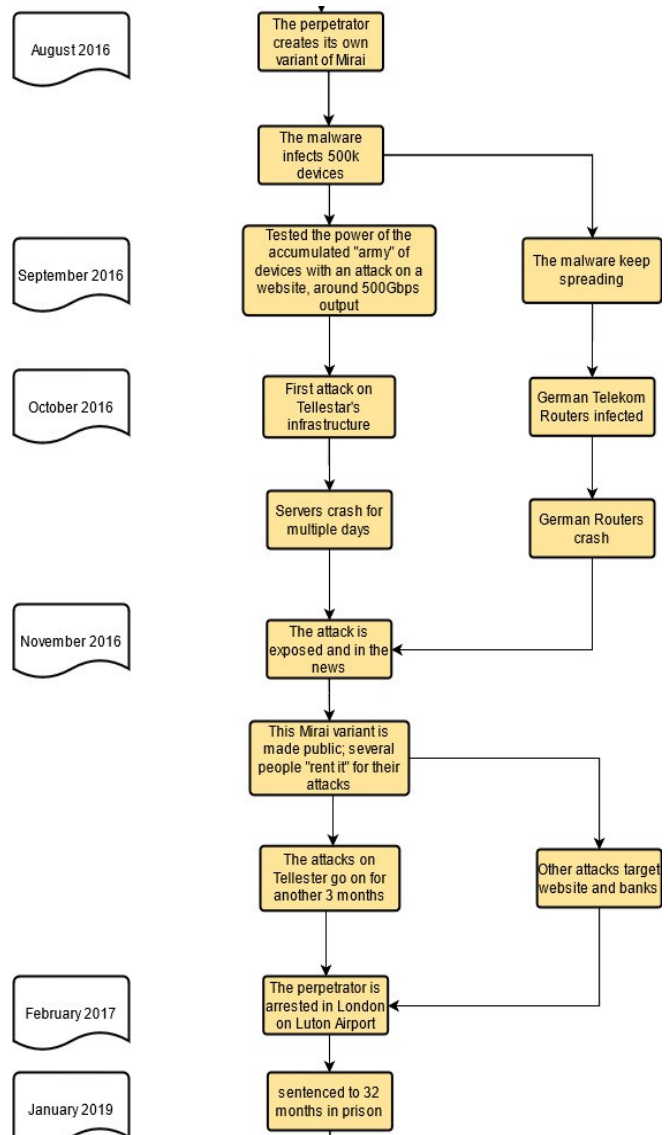


Figure 7.