*DOI:*
10.1093/cybsec/tyae005

*Document Version*
Peer reviewed version

# The Cybersecurity of Fairy Tales *

Luca Viganò
Department of Informatics
King's College London
London, UK
luca.vigano@kcl.ac.uk

**Abstract**

The timeless nature of fairy tales can help uncover the timeless nature of many cybersecurity notions. Using 16 classical tales as illustration, in this article I show that fairy tales are full of cybersecurity motifs and examples, and can thus be used extensively and effectively to explain cybersecurity notions. Obviously not cybersecurity as we know it today, but rather the fundamental and archetypal concepts that are at its heart. Fairy tales can thus be employed to mediate in conversations with less-knowledgeable, misinformed or even skeptical laypersons about cybersecurity, increase their understanding and awareness, and thereby strengthen the overall cybersecurity of systems and applications.

**Keywords:** Security Properties. Security attacks. Science and technology, art and literature. Public understanding of science and technology. Representations of science and technology.

# 1 Introduction

## 1.1 Fairy Tales and Cybersecurity

What is the earliest fairy tale that you remember? The one that your parents first told or read to you to lull you to sleep? Was it *Cinderella*, *Little Red Riding Hood* or *Sleeping Beauty*, perhaps confusing the versions of these three fairy tales collected by Perrault [47] and by the Brothers Grimm [30]? Was it maybe the Grimms' *Snow White and the Seven Dwarfs*, *Hansel and Gretel*, *The Wolf and the Seven Young Goats*, *The Devil with the Three Golden Hairs*, or *Rumpelstiltskin*? *Puss in Boots* in one of the versions of Straparola, Basile or Perrault [17]? Perrault's *Donkey Skin* or *Hop-o'-My-Thumb*? The Grimms' *The Girl Without Hands or* one of its versions famous in Japan, Russia, Lousiana or Africa? Galland's *Ali Baba and the 40 Thieves* [27]? Or maybe some other fairy tale, famous or less famous, depending on where and when you were born and, of course, on the personal taste of whoever read or told you the tale.

Whichever fairy tale it was, it most likely contains, explicitly or implicitly, some cybersecurity element. All of the 13 fairy tales listed above for sure do, as shown in Table 1, which includes three other fairy tales: the Grimms' *Simeli Mountain*, Harris' *Cutta Cord-La!* [32] and Andersen's *The Shadow* [1]. Of course, none of these fairy tales actually deals with cybersecurity: they were all written well before the advent of digital technology and the now widespread use of the word 'cyber' as a prefix in front of 'security' and of 'space', as well as 'sex', 'punk', 'crime', 'terrorism' and other words that the Internet has lifted from the physical, analogical, world to the digital, cyber, world (along with other usages that predate the Internet such as 'cybernetics' and 'cyborg').[1]

*To appear in the Journal of Cybersecurity (2024).

[1]One should perhaps rather speak of *information security*, which is more general than cybersecurity and is independent of computer systems, as it "means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction" (cf. Table 2). Information is more general than data: data conveys information, but information may also be revealed without revealing data, e.g., by statistical

| *Fairy Tale* | *Cybersecurity Notion* | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Access Control | Advanced Persistent Threat / Multi-Stage Attack | Anonymity | Authentication | Coercion | Confidentiality | Denial of Service | Eavesdropping of Secret or Password | Encryption | Escalation of Privilege | Fake Credentials, Masquerading, Identity Theft | Integrity | Replay Attack | Tracing |
| **Ali Baba and the 40 Thieves** | • | • | • | • | • | • | | • | | | • | | • | |
| **Cinderella** | | | | • | | | | | | | • | | | |
| **Cutta Cord-La!** | • | | | • | | | | | | | | | | |
| **The Devil with the Three Golden Hairs** | | | | | | • | | | | | | • | | |
| **Donkey Skin** | | | | • | | | | | | | | | | |
| **The Girl Without Hands** | | • | | • | | • | | | | | • | • | | |
| **Hansel and Gretel** | | | | | | | • | | | | | | | • |
| **Hop-o'-My-Thumb** | | | | | | | • | | | | | | | • |
| **Little Red Riding Hood** | | | | • | | | | | | | • | | | |
| **Puss in Boots** | | • | | | • | | | | | • | | | | |
| **Rumpelstiltskin** | | | | | | | | • | | | | | • | |
| **The Shadow** | | | | | | | | | | | • | | | |
| **Simeli Mountain** | • | | | • | • | • | | • | | | | | | |
| **Sleeping Beauty** | | | | | | | • | | • | | | | | |
| **Snow White and the Seven Dwarfs** | | | | • | | | • | | • | | • | | | |
| **The Wolf and the Seven Young Goats** | • | | | • | | | | | | | • | | | |

Table 1: Fairy Tales and Cybersecurity Notions

So, what does it mean to speak of cybersecurity in the context of fairy tales? Marie-Louise von Franz, the Jungian scholar renowned for her psychological interpretations of fairy tales, remarked that "Fairy tales are the purest and simplest expression of collective unconscious psychic processes. [...] They represent the archetypes in their simplest, barest, and most concise form. In this pure form, the archetypal images afford us the best clues to the understanding of the processes going on in the collective psyche" [71, p. 13]. To paraphrase von Franz, fairy tales represent cybersecurity archetypes in their simplest and barest form, and afford us (some of) the best clues to the understanding of the processes going on in the collective psyche of the cyberworld. Cybersecurity experts have developed solutions to cybersecurity problems that are similar to, and in some cases are simply the digital version of, the ones invented by fairy tale authors centuries before. The problems, and their solutions, are archetypal, they are part of who we are, much in the same way as the stories in the fairy tales are. Again quoting von Franz, "We have written tradition for three thousand years, and what is striking is that the basic motifs have not changed much" [71, p. 16].

For instance, *Cinderella*, *Little Red Riding Hood*, *Snow White and the Seven Dwarfs*, *The Wolf and the Seven Young Goats*, *Donkey Skin*, *The Girl Without Hands*, *Ali Baba and the 40 Thieves*, *Simeli Mountain* and *Cutta Cord-La!* all deal, in one way or the other, with the cybersecurity notion that is called *authentication*, which the glossary of the Computer Security Resource Center of the National Institute of Standards and Technology of the U.S. Department of Commerce (NIST [42]) defines as "verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system" (cf. Table 2, which gives the definition of

summaries or by actions carried out by agents, be they human agents or computer agents. For instance, if an agent Alice sends an encrypted message to another agent Bob, the encryption might prevent an attacker Charlie from reading the content of the message if he cannot decrypt it (so the message is confidential), but the fact that Charlie can see that Alice is communicating with Bob might already constitute a breach of security, e.g., when Alice is a whistleblower reaching out to a journalist Bob unbeknownst of her malicious employer Charlie. In this article, I will abstract away from the manners in which information is stored and transmitted, and use cybersecurity rather than information security as it is the more fashionable and widespread term these days.

authentication and other cybersecurity notions provided by NIST or by other sources when NIST did not provide one).

Table 2: Cybersecurity Notions (as defined in the glossary published by NIST)

| *Notion* | *Definition* |
|---|---|
| **Access Control** | The process of granting or denying specific requests to 1) obtain and use information and related information processing services and 2) enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances). |
| **Advanced Persistent Threat / Multi-Stage Attack** | An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception), to generate opportunities to achieve its objectives which are typically to establish and extend its presence within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives. |
| **Anonymity** | A condition in identification whereby an entity can be recognized as distinct, without sufficient identity information to establish a link to a known identity. |
| **Authentication** | Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. |
| **CAPTCHA** | Completely Automated Public Turing test to tell Computers and Humans Apart. |
| **Cipher** | Series of transformations that converts plaintext to ciphertext [...]. |
| **Code** | System of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. |
| **Confidentiality** | Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. |
| **Cryptanalysis** | Operations performed in defeating cryptographic protection without an initial knowledge of the key employed in providing the protection. |
| **Denial of Service** | The prevention of authorized access to resources or the delaying of time-critical operations. |
| **Eavesdropper** | A party that secretly receives communications intended for others. |
| **Encryption** | Cryptographic transformation of data (called plaintext) into a form (called ciphertext) that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called decryption, which is a transformation that restores encrypted data to its original state. |
| **Escalation of Privilege** | An attack in which a program or a user is technically able to do things that they're not supposed to do. (Not defined by NIST; definition taken from [57].) |
| **Identity** | The set of physical and behavioral characteristics by which an individual is uniquely recognizable. |
| **Identity Theft / Identity Fraud** | Terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. |
| **Information Security** | Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. |
| **Integrity** | Guarding against improper information modification or destruction. |
| **Malware** | A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. |
| **Masquerading** | A type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity. |

Continued on next page

Table 2 – continued from previous page

| *Notion* | *Definition* |
|---|---|
| **Multi-Factor Authentication (MFA)** | Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password/personal identification number (PIN)); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). |
| **Password** | A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization. |
| **Replay Attack** | An attack that involves the capture of transmitted authentication or access control information and its subsequent retransmission with the intent of producing an unauthorized effect or gaining unauthorized access. |
| **Social Engineering** | The act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust. |
| **Steganography** | The art, science, and practice of communicating in a way that hides the existence of the communication. |
| **Zero-Knowledge Protocol** | A password-based authentication protocol that allows a claimant to authenticate to a verifier without revealing the password to the verifier. |

Authentication is an archetypal notion. It is a cornerstone of cybersecurity, one which we all have to deal with on a daily basis, frequently in its enhanced form called *multi-factor authentication (MFA)*, which requires one to provide two or more factors that they know, that they have or that they are (cf. Table 2). MFA is used also because humans are very bad at keeping and remembering secrets, including passwords as Cassim does in *Ali Baba and the 40 Thieves* as I will discuss later[2], but one can't really forget their fingerprints, or their eyes for a retina scan, or their feet that match perfectly the size of a shoe.[3]

## 1.2 An Example: Cinderella and Multi-Factor Authentication

As a concrete example, consider *Cinderella*: the Prince is able to authenticate the girl that he has fallen in love with by the fact that she is the only one whose foot fits into the glass slipper, or fur slipper, sandal or shoe, depending on the tale's version (cf. [15, 22, 49]) or on the modifications that have been made for the cinematographic adaptation. In Perrault's version *Cendrillon ou La Petite Pantoufle de Verre* (and, e.g., in Georges Méliès' short film *Cendrillon ou La Pantoufle Merveilleuse* shot in 1912), Cinderella authenticates herself not only by something that she is (her foot is the only one in the realm that fits) but also by something that she has: she completes the multi-factor confirmation of her identity by pulling out of her pocket the second slipper. As a side note, I have always wondered about the actual security of this authentication as it predicates on the quite unlikely fact that Cinderella's feet are the only ones in the whole realm that are tiny enough to fit the slippers. Similarly, *Donkey Skin* is the only one who has fingers so small to fit a ring. But these are tales of wonder after all.[4]

[2]Moreover, people tend to write down complex passwords, which opens up new possible attacks, such as those based on *social engineering*, when an attacker tricks a victim into handing over information (password, bank details, etc.) or carrying out a desired action by taking advantage of the victim's natural emotional responses and reactions. Note that NIST's glossary provides a shorter definition of social engineering as shown in Table 2.

[3]Fingers, eyes and feet can, of course, be 'stolen' in brutal or more gentle ways, such as in the films *Minority Report* (the eyes [60]) and *National Treasure* (the fingers [62]), for instance, but that is another story, one which I am not going to discuss in detail here.

[4]Both Bettelheim [7] and Do Rozario [23] discuss extensively these 'tests for fit as queen' from a psychological and a sartorial point of view. In particular, Do Rozario [23, p. 121] observes that "the foremost claim of Cinderella and Donkey Skin to social status is through the perfect fit of their wardrobe" and, about Cinderella, that "The smallness of the shoe thus stands in for the smallness of the foot, highlighting an attribute that has long been associated with beauty. [...] The shoe test proves that her foot itself is fashionably small, that she is whom she claims to be. The shoe manifests Cinderella herself" [23, p. 184]. So, the shoe is indeed an authenticator. Moreover,

The more factors are used during an authentication process, the more confidence a service has that the user is correctly identified. That is why, because it is a matter of life and death, in *The Wolf and the Seven Young Goats* the mother goat tells her children not to open the door to any caller unless they recognize their true mother by her white feet (technically, hoofs) and sweet voice. This is MFA for *access control*, to protect the children inside the house. It is, again, not a very secure form of authentication as all goats have white feet, but the other goats would hopefully not devour the children, and the mother's voice is, at least, a unique factor, or so she hoped. The wolf has namely eavesdropped the instructions of mother goat, so he eats some chalk to soften his voice, but the children ask also to see his feet (technically, paws) and, seeing that they are black, they do not let him in: one authentication factor is not enough! So, he also smears flour over his coat, turning his black feet white. He is now able to *masquerade* as mother goat and gains access to the house and eats six of the children (fortunately, the seventh one will save the day with the help of mother goat). A masquerading attack is contained also in *Aschenputtel*, the gorier version of *Cinderella* collected by the Brothers Grimm (and in the theatrical/cinematographic version of the tale told in Stephen Sondheim's musical *Into the Woods*): inspired by the evil stepmother, Cinderella's two stepsisters attempt to authenticate as the object of the Prince's affection by mutilating their feet, but are exposed by the blood trickling from their wounds.

Finally, MFA also allows for a form of 'recovery' if one of the authentication factors fails: in Disney's 1950 *Cinderella* film, the evil stepmother trips the servant who is carrying the glass slipper, which shatters before Cinderella can try it on, but Cinderella produces the second slipper from her pocket and the happy end ensues. I will return to authentication later and discuss the other notions defined in Table 2 in detail.

### 1.3 Explaining Cybersecurity: Cybersecurity Show and Tell

Before I do, let me put this article into context. I have published a series of articles [65, 67, 66] that discuss how, in the context of research in *Explainable Security* [69], popular films, TV shows, novels and other artworks can be used to explain cybersecurity notions as well as algorithms and solutions that have been developed to attempt to secure systems, and the vulnerabilities and attacks that they might suffer from. While experts typically only accept detailed technical explanations, laypersons are often scared off by explanations of cybersecurity (say, how to interact with a system or an app) that are detailed but too technical. Such an explanation might even repulse the laypersons and make them lose all trust in the explanation and, ultimately, in the cybersecurity of the system that is being explained. This repulsion and lack of trust might lead to users interacting with systems in ways that, unbeknownst to the users and possibly even to the developers and administrators of the systems, are vulnerable to attacks (to the systems and to the users themselves).

In practice, however, laypersons are rarely given explanations that are tailored to their needs and their ability to understand. On the other hand, a clear and simple explanation, with something that laypersons can immediately relate to or perhaps are even already familiar with, such as popular films or other artworks, helps make laypersons less irritated, stressed and annoyed, and indeed more captivated and receptive. It allows experts who provide the explanations to target the laypersons, reducing the mental and temporal effort required of them and increasing their understanding, and ultimately their willingness to engage with cybersecurity systems. This is what I have called *Cybersecurity Show and Tell*: the added power of telling (i.e., explaining notions in a technical way) and showing (via visual storytelling or other forms of storytelling) helps experts to convey not only the technical definition but also the intuition underlying that technical definition.

Recognizing the transformative role that the arts play in our society, they can be employed to open up conversations with the less-knowledgeable, misinformed or even skeptical public about cybersecurity, thereby increasing the laypersons' understanding and awareness, and strengthening

in some versions of the tale the shoe has magical powers and changes its shape to a perfect fit only when it recognizes Cinderella's foot.

the systems' overall security. The general public enjoy considering science through novel and innovative means, but cybersecurity, also because of the anxiety it can generate in people's daily (online) lives, is a particularly challenging area for non-specialists which requires accessible mediation and interpretation. Art's power to target the emotions and intuition of an audience can be particularly effective, especially with the support of psychology to understand the variety of humans' stances and states of mind that cause cybersecurity vulnerabilities. As Marlow and Johnstone [39] observed, the fields of psychology and mental health have a long history of interdisciplinary explorations with the arts with a view to promoting increased understanding and awareness; other disciplines have a history too, e.g., social sciences [56], international relations and politics [64], and management [19]. The overall aim of my research is to establish such interdisciplinary explorations for cybersecurity. The contribution of this article is to show that, like films and other artworks, also classical fairy tales can be used extensively and effectively to explain cybersecurity notions.[5]

### 1.4 Structure of the Paper

In the next section, I provide more details on the relationships between fairy tales and cybersecurity, and discuss *Ali Baba and the 40 Thieves* as a concrete example. Then, in the following section, I discuss archetypes and motifs, and describe different cybersecurity notions that are contained in fairy tales. I then elaborate how cybersecurity can be explained with fairy tales and other forms of storytelling. Finally, I provide some concluding remarks and discuss several directions for future work.

## 2 The Educational Opportunities Offered by Fairy Tales

Fairy tales have been fascinating children and adults alike for centuries because they are entertaining, of course, but also because they are educational; they encourage critical thinking, while feeding our imaginations. The psychologist Bruno Bettelheim affirmed that "the fairy tale confronts the child squarely with the basic human predicaments" and thus helps the child understand the meaning of life" [7, p. 16]. Jerome Bruner, also a psychologist, affirmed that narratives simultaneously activate both the *paradigmatic or logico-scientific mode of thought*, which "attempts to fulfill the ideal of a formal, mathematical system of description and explanation" and essentially formalizes cause and effect relationships, and the *narrative mode of thought*, which "deals in human or human-like intention and action and the vicissitudes and consequences that mark their course" and "strives to put timeless miracles into the particulars of experience, and to locate the experience in time and place" [11, pp. 12–13].

Fairy tales can be used to teach and explain. Cleto and Warman echo Jones and Schwabe [36] to emphasize "the educational opportunities offered by fairy tales, which can fill a broad range of curricular needs: instructors in a variety of academic fields can draw on fairy tales to help students improve critical-thinking abilities, strengthen writing skills, and explore cultural values" [20, p. 6]. Moreover, as observed by Laura Packer [44], "Fairy tales endure because they are, at their most basic, the stories of our lives in their most stripped-down form. [...] They are the unadorned stories of what drives us, without the civilizing details of technology and manners. They teach us how to survive in this wily and wicked world. They are a shortcut to a common understanding of the way the world works. Fairy tales help us understand that the values of once upon a time aren't so different from our values now."

Although Packer was not writing about cybersecurity, her observation applies to it too: the cyberworld (e.g., the Internet and social media) is a wily and wicked world much alike, if not possibly even more than, the physical world that we live in, and fairy tales, which are part of our collective imagination and of our cultural good, can act as a shortcut to a common understanding of the way this cyberworld of ours works, including explaining, and understanding, cybersecurity

[5] Modern fairy tales (such as those by Angela Carter or Gianni Rodari) or tales written on purpose can be used too, but are out of the scope of this article. I will return to this in the conclusions.

notions if one strips away the details of technology. The timeless nature of fairy tales can help uncover the timeless nature of some cybersecurity notions and methods, thus establishing fairy tales as an effective mediation between the two modes of thought, between the cyber world and the physical world.

Children "play games with exactly the same ritual and exactly the same phrases, in some instances, as the children of thousands of years ago" [6, p. 2] and a similar situation applies for cybersecurity. While, of course, technology is omnipresent in our life today and lies at the heart of cybersecurity as we know and experience (and sometimes dread) it today, 'analogical' cybersecurity notions and solutions have been around since almost the dawn of humankind, or actually as soon as people had information that they wanted to protect (hence, the more general term 'information security' that I mentioned above). Over the course of the centuries, most civilizations invented solutions to protect their valuable information, such as *ciphers* (e.g., the *Caesar Cipher* used by the Romans in the $1^{st}$ century BC or the cipher *scytale* used by the Spartans as early as the $7^{th}$ century BC) or *codes* (a fascinating example are rhyming slangs such as the *Cockney rhyming slang* first used in the $19^{th}$ century in the criminal underworld of the UK [45, 46, 2]). There are also solutions based on *steganography*, in which messages are hidden in other messages (in his *Histories*, written around 430 BC, Herodotus mentions one of the first recorded uses of steganography: Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of his most trusted servant, 'marking' the message onto his scalp, then sending him on his way once his hair had regrown, with the instruction, "When thou art come to Miletus, bid Aristagoras shave thy head, and look thereon").[6] Ciphers, codes and steganography are examples of solutions to achieve *confidentiality*, but can be used to achieve also other cybersecurity properties such as *integrity* (cf. Table 2).

Technology advancements have obviously changed the concrete realizations, implementations and devices by which we guarantee cybersecurity properties: except perhaps in spy movies, the Caesar Cipher or the scytale are not used anymore but have been replaced by their modern successors along with modern codes and steganography techniques. However, the main ideas underlying the properties and solutions have not changed, and many of these ideas are already present in fairy tales. "The values of once upon a time aren't so different from our values now", as remarked by Packer.

## 2.1 Ali Baba and the 40 Thieves: A Fairy-Tale Goldmine for Cybersecurity Notions

Let me give another example. One of the most complex cybersecurity notions is *anonymity* (cf. Table 2), which comes into play when we want to keep secret the identity or location of an agent participating in a certain event (in voting, delation, donations, sending emails, ...). Different degrees of anonymity exist with formal definitions requiring advanced number theory and probability theory, but the quintessence of existing cybersystems for anonymity can be illustrated through *Ali Baba and the 40 Thieves*, which also serves to discuss several other cybersecurity notions and is thus quite the fairy-tale goldmine for cybersecurity notions (cf. Table 1). To demonstrate this, let me give a quick summary of the fairy tale. One day, as he is cutting wood in the forest, the poor woodcutter Ali Baba observes a group of 40 thieves visiting the cave in which they have stored their treasure. The mouth of the cave is sealed by a huge rock, and opens and closes by uttering the magic words "open sesame" and "close sesame", respectively. Ali Baba has thus involuntarily become an *eavesdropper* as he now knows the thieves' *password*, which is the confidential information that the thieves use to convince the magic door that they are authorized to enter (and exit) the cave.[7] When the thieves are gone, Ali Baba enters the cave by repeating

[6] Detailed descriptions of these and other historical cybersecurity solutions can be found, e.g., in the books by Singh [59] and Dooley [24].

[7] The cave that opens with a password has also been used by Quisquater and Guillou (and their children), with the help of Berson, as a metaphor to explain *zero-knowledge protocols* to children and other non-expert users [53], where a zero-knowledge protocol is "a password-based authentication protocol that allows a claimant to authenticate to a verifier without revealing the password to the verifier" [42].

the password (and thus carrying out a *replay attack*). As he is fundamentally honest and humble, he takes only a single bag of gold coins home. A few days later, under pressure from his brother Cassim, Ali Baba is forced to reveal the secret of the cave; this is *coercion*, a notion that is relevant in cybersecurity in the context of electronic voting (where systems are required to resist the attacks of an adversary who attempts to coerce voters that they vote in a particular manner or abstain from voting).[8] Unlike his brother, Cassim is greedy, so he goes to the cave aiming to take as much treasure as possible. He enters the cave with the magic words and the door seals behind him. He starts collecting jewels and gold pieces but, in his greed and excitement over the treasure, he forgets the words to get out again and ends up trapped — who of us has not forgotten a password one time or the other, albeit maybe not because of greed but simple forgetfulness?[9]

The thieves find Cassim in the cave and kill him. When his brother does not come back, Ali Baba goes to the cave to look for him, finds the body, and brings it home for a proper burial. The thieves, finding the body gone, realize that a second person must know their secret. In order to track that person down, the chief sends one of the thieves to the town. The thief finds Ali Baba's house and marks the door with a symbol so he and the other thieves can come back that night and kill everyone in the house. However, Morgiana, a clever slave-girl from Cassim's household, has seen the thief. She foils his plan by marking all the houses in the neighborhood similarly. When the 40 thieves return that night, they cannot identify the correct house, and the chief kills the unsuccessful thief in a furious rage. The next day, another thief tries again and this time marks the target house by chipping a chunk out of the stone step at Ali Baba's front door. Again, Morgiana foils the plan by making similar chips in all the other doorsteps, and the second thief is killed for his failure as well.

What just happened? Given that all the houses have the same mark(s), it is impossible for the thieves to identify which one is Ali Baba's real house. In other words, Ali Baba's house is *anonymous* as it is not identifiable from the other houses in the neighborhood. To protect Ali Baba's family, Morgiana has created what in technical terms is called an *anonymity set*, which in this case is the set containing all houses in the neighborhood, and the thieves are none the wiser and they would have to try out all the houses one by one. So, the larger the set, the worse for the thieves and the better for Ali Baba and his family.

Formally, an anonymity set is the set of all possible subjects who might cause an action, and then anonymity can be defined as the state of being not identifiable within a set of subjects, namely, the anonymity set [48]. One can of course give this formal definition of anonymity and maybe accompany it with a mathematical one — and this is what one would do in front of an expert audience, say in a talk at a conference or in a university lecture on cybersecurity — but the point here is that even non-specialists immediately understand what Morgiana is doing and why. In fact, I dare say that we all, more or less, intuitively understand that anonymity cannot really exist in a vacuum (one cannot be anonymous by oneself) but rather requires a large enough set of similar 'things', a large enough set of similar people, actions, messages, etc., so that one's identity, actions, or messages are not distinguishable from those of the others and thus not identifiable.

The repeated and manifold efforts of the thieves amount to what is called an attack by an *advanced persistent threat*, namely an attack that consists of multiple and diverse stages, pursuing the "objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives". So, given the failure of his two men, the chief of the thieves takes matters in his own hands: he masquerades as an oil merchant in need of Ali Baba's hospitality, bringing with him mules loaded with 38 oil jars, one filled with oil, the other 37 hiding the other remaining thieves. They plan to kill Ali Baba and his family once they are asleep. Again, Morgiana discovers and foils the plan, killing the 37 thieves in their jars by pouring boiling oil on them. When the chief comes to rouse his men, he discovers they are all dead and escapes. Ali Baba shows his gratitude by giving Morgiana her freedom. In a final attempt to exact revenge, the chief of the thieves establishes himself as a merchant (this is again masquerading), befriends Ali Baba's son, and arranges to be

[8] NIST's glossary does not provide definitions of coercion and of electronic voting, but I trust them to be understandable by the non-expert based on what I have written.

[9] A similar situation occurs in the Grimm Brothers' *Simeli Mountain*.

invited to dinner at Ali Baba's house. However, the thief is yet again recognized by Morgiana, who kills him. Ali Baba rewards Morgiana by marrying her to his son. Ali Baba is then left as the only one knowing the secret of the treasure in the cave and how to access it.

# 3 Archetypes, Motifs and Cybersecurity Notions

As remarked earlier, cybersecurity experts have developed solutions to cybersecurity problems that are similar to, and in some cases are simply the digital version of, the ones invented by fairy tale authors centuries before. In this section, I will complement the examples given above with several other examples of cybersecurity archetypes that fairy tales represent in their simplest and barest form.

To analyze and compare fairy tales, folklorists such as Antti Aarne, Stith Thompson and Hans-Jörg Uther have worked at identifying their building-blocks and patterns: fairy tales are composed of elements called *motifs*, which are combined in different ways to create a plot of a tellable tale. Many tales have the same patterns of motifs, which are called *tale-types*. The *Aarne-Thompson-Uther (ATU) Index* allows researchers to identify the underlying structure of a tale and to cross-reference it with other tales that share the same elements or themes [63]. Each entry in the ATU index describes which themes and motifs comprise a specific tale-type, and each motif has an identifying number, which can be cross-referenced with *Thompson's Motif-Index of Folk-Literature* [61]. While these two indices are often used in tandem by folklorists, for this article I will focus on Thompson's index, which gives each motif a letter from A to Z to designate its type and a number to identify it. In particular, the letter H designates *tests*, which abound in fairy tales and folk literature and are part of Bettelheim's predicaments mentioned above, including tests to prove one's identity, tests of cleverness, strength or skill, riddles, and quests that heroes are sent on.[10]

Tests abound in cybersecurity, too. For instance, anyone who has surfed the web has come across a *CAPTCHA*, which is a test that websites use to identify whether the user is a human and thus prevent access by bots (i.e., web robots attempting to pass as humans).

Thompson defines the tests from H0 to H199 as "Identity tests: recognition" and indeed identity and recognition play a major role in fairy tales, especially those in which the hero(ine) embarks on a journey that will allow them to discover their own true identity or unlock somebody else's identity (see also the essays by Campbell [13] and Vogler [70]). Propp also noted this and defined two of his *functions* accordingly: "XXVII. The Hero is Recognized. [...] He is recognized by a mark, a brand (a wound, a star marking), or by a thing given to him (a ring, towel). In this case, recognition serves as a function corresponding to branding and marking. The hero is also recognized by his accomplishment of a difficult task (this is almost always preceded by an unrecognized arrival)..." and "XXVIII. The False Hero or Villain is Exposed. [...] This function is, in most cases, connected with the one preceding..." [50, p. 179].

## 3.1 Authentication, Identity Theft, Escalation of Privilege and Advanced Persistent Threat

We have already seen an example of exposition of the villain in *Ali Baba and the 40 Thieves* when Morgiana twice exposes the chief of the thieves, and I have already pointed out that several of the fairy tales I mentioned (and many more that I did not mention) are about authentication, namely the process of verifying the identity of a person, which is recognition in the terminology of both Thompson and Propp.

*Cinderella*, *Donkey Skin* and *The Wolf and the Seven Young Goats* are examples of Thompson's "H50. Recognition by bodily marks or physical attributes", along with Homer's *The Odyssey* [35] in which Odysseus, when he finally returns to Ithaca after 20 years, is recognized by his old wet-nurse Eurycleia by a scar he received during a boar hunt many years before, and by his faithful

[10] Tests are present also in the ATU Index, but for the most part they are 'distributed' among the different entries rather than collected under a dedicated label.

dog Argos by his smell. Odysseus is also an example of "H30. Recognition through personal peculiarities" and "H31. Recognition by unique ability" as he is the only one able to bend his old bow and shoot an arrow through twelve axe shafts. Similar stories exist in Hindu mythology.

An authentication by voice similar to that of *The Wolf and the Seven Young Goats* occurs in Harris' *Cutta Cord-La!* [32], although Thompson mistakenly labels it "H18. Recognition by password" (this is mistaken because what matters is not really what is said but rather the voice that says it). Authentication and masquerading occur also in *Little Red Riding Hood* when the wolf pretends to be the grandmother (masqueradings of this form are related to some of Thompson's motifs "D0-D699: Transformation"), whereas *Snow White and the Seven Dwarfs* is about authentication, masquerading and fake credentials: the queen disguises herself to give the poisoned apple to Snow White, after the huntsman she hired to kill Snow White spared the girl's life and brought the queen the heart of an animal instead. Similar fake credentials are used for fake authentication also in *The Girl Without Hands* when the tongue and eyes of a deer are used instead of the girl's tongue and eyes as a proof of her death.

These examples illustrate how identity and authentication, and several related cybersecurity notions, occur very frequently in fairy tales. As noted by Thompson in H0, "elaborate means are employed in folk-literature for the recognition of persons even though they have been separated a very short time", many of which have an equivalent in modern MFA.

In addition to these physical authentication factors and the other ones mentioned above, it is interesting to highlight the following motifs. "H10. Recognition through common knowledge" and in particular "H17. Recognition by reminders of what has been said" list many of the possible factors that could be used for authentication, ranging from a password (a secret known to both authenticator and authenticatee) to an overheard conversation (which might suggest some forms of malevolent or benevolent eavesdropping). "H80. Identification by tokens", "H90. Identification by ornaments" and "H110. Identification by cloth or clothing", such as a ring, a necklace, an amulet, golden apples or a garment, are akin to producing a card to be authenticated by something that one possesses. Finally, "H163. Recognition of own cow in herd of twenty thousand" is, in a sense, the opposite of anonymity, namely the ability to identify, by certain factors, that specific cow in the midst of an anonymity set that contains twenty thousand elements.

Cybersecurity in fairy tales is, however, much more than what relates, in one way or the other, to Thompson's tests (although I will mention a few more below). For instance, there is also, in a sense, the opposite of identity: *identity theft*. Masquerading is already a case of identity theft in which the attacker illegitimately poses as another, authorized entity, but in Andersen's *The Shadow* [1], the identity theft is taken to the extreme when the shadow has become the man and offers to the real man to become its shadow.

A cybersecurity notion related to identity theft and masquerading is *escalation of privilege*: although the Marquis of Carabas is a fictional entity, and thus there is no real identity to steal, he is brought to life by the trickster cat in *Puss in Boots* and its variants [17], who embodies an advanced persistent threat to ensure that his poor master acquires privileges that he could only dream of.

## 3.2 Integrity, Confidentiality and Eavesdropping

In addition to authentication, *The Girl Without Hands*, with its international versions spanning from Straparola's Italy to Japan via the Grimms' Germany (ATU 706 and Thompson E782.1), provides an example also of confidentiality and integrity, and of an advanced persistent threat. The devil forces the girl's father to chop off her hands (in other versions, e.g., the Japanese one, it is not the devil but the girl's evil stepmother). After many vicissitudes, the girl marries the king and gives birth to a beautiful son. The king's mother sends a messenger to deliver a letter with the joyful news to the king, who in the meantime has gone to war. However, tired from the long journey, the messenger stops to rest and falls asleep, and the devil (again the stepmother in other versions), who still wants to harm the girl, takes the letter out of the messenger's satchel, reads its (which constitutes a breach of confidentiality) and then replaces it with a letter stating that the queen has brought a changeling into the world (this is a breach of integrity, as the original

content is maliciously altered). Although frightened and saddened by this letter, the king writes an answer to his mother asking her to take good care of the queen until his return. The messenger returns with this letter, but again he stops to rest and falls asleep, and again the devil replaces the letter with one in which the king orders that the queen should be killed with her child. The king's mother does not believe the letter and writes to the king again, but she receives the same answer, because each time the devil substitutes a false letter, and in the last one even orders that they should keep the queen's tongue and eyes as proof, but the king's mother has a deer killed instead and its tongue and eyes used for the fake authentication as mentioned above, thus thwarting the devil's evil plan.

I already mentioned confidentiality in *Ali Baba and the 40 Thieves*, and secrets play a role also in other entries in Thompson's index, such as "C420. Tabu: uttering secrets", "C820. Tabu: finding certain secret" and "N450. Secrets overheard". The latter is, essentially, eavesdropping. In addition to the examples of eavesdropping given above (and in many other fairy tales, since eavesdropping is quite a common trope), another example is given by *Rumpelstiltskin* and its variants [18]. The queen eavesdrops as the imp hops about his fire and sings "tonight tonight, my plans I make, tomorrow tomorrow, the baby I take. The queen will never win the game, for Rumpelstiltskin is my name." The queen thus learns his name and is then able to repeat it to win the bargain that she and Rumpelstiltskin had made.

### 3.3 Encryption, Denial of Service and Tracing

Finally, one can, perhaps with a little fantasy, see enchantment as a form of *encryption*. For instance, Snow White and Sleeping Beauty have been locked (i.e., encrypted) into an enchanted sleep by a *malware* (a poisoned apple and a poisoned spindle, respectively), similar to *viruses* and *cryptoworms* that lock computers when users unknowingly visit malicious websites or click on *phishing* emails, such as in the infamous WannaCry ransomware attack in 2017. Attempts to wake them up are akin to *cryptanalysis*, namely trying to break the enchantment without possessing the 'decryption key', which instead, in Disney's versions more than in the original fairy tales, can only be reversed by 'true love's kiss'. Similarly, kissing the frog is the key to 'decrypt' it and recover the prince in many fairy tales.

When Snow White and Sleeping Beauty are 'encrypted', they are also, in a sense, victims of a form of *denial of service*: they are denied living their normal life and others are denied interacting with them. A much better example of denial of service is, however, provided by *Hop-o'-My-Thumb*, which also provides an example of *tracing*[11]: when his poor parents take Hop-o'-My-Thumb and his siblings to the forest to abandon them there, he uses some stones he had collected to mark a trail that enables him to lead his brothers back home, but the second time round, he uses breadcrumbs instead, which the birds eat up. The birds thus deny Hop-o'-My-Thumb from accessing the pieces of information he had dropped to reconstruct the trace leading back to his parents' house. The same situation occurs in *Hansel and Gretel* and in many other fairy tales in which children are forsaken in forests [16].

## 4 Explaining Cybersecurity with Fairy Tales and Other Forms of Storytelling

In May 1886 [72], the Russian playwright and short-story writer Anton Chekhov wrote a letter to his brother Alexander, who too had literary ambitions, providing him with a fundamental advice that, slightly misquoting, can be summarized as:

> Don't tell me the moon is shining; show me the glint of light on broken glass.

[11] Again, NIST's glossary does not provide a definition of tracing, but I trust the notion to be understandable by the non-expert especially given one of the definitions given in the Merriam-Webster dictionary: to follow footprints, a track, or a trail.

This concise injunction has become a literary commandment for any writer: *show, don't tell*! The distinction between telling and showing was popularized by the literary scholar Percy Lubbock in his 1921 book "The Craft of Fiction" [38]. In a nutshell: telling states, showing illustrates. More in detail, *show, don't tell* is a writing technique (adopted by several prominent writers including, for example, Ernest Hemingway and Stephen King) in which story and characters are related to the reader through action, words, dialogues, thoughts, senses, and feelings rather than through the author's exposition and description.

*Show, don't tell* applies to all forms of fiction, including poetry, scriptwriting and playwriting. It also applies to non-fiction, including speech writing and scientific writing. In fact, even though I am not aware of any explicit theoretical or practical investigation of the use of *show, don't tell* in scientific writing, the *show, don't tell* spirit lies at the heart of many successful scientific communication and storytelling approaches, such as those discussed in John Brockman's "The Third Culture: Beyond the Scientific Revolution" [9][12]. Storytelling has been used widely, and very successfully, as a pedagogical device in textbooks and science outreach endeavors, e.g., [14, 26, 29, 31, 40] to name a few. Rina Zazkis and Peter Liljedahl, in particular, have been instrumental in promoting storytelling in the mathematics classroom. They begin their book "Teaching Mathematics as Storytelling" by writing:

> We like to tell stories. We tell stories about mathematics, about mathematicians, and about doing mathematics. We do this firstly because we enjoy it. We do it secondly because the students like it. And we do it thirdly because we believe that it is an effective instructional tool in the teaching of mathematics. We are not alone in this. There is ample literature to support the enjoyment of storytelling on the part of both the story teller and the story listener. There is also an abundance of anecdotal data that suggest "telling a story creates more vivid, powerful and memorable images in a listener's mind than does any other means of delivery of the same material" [33, p. xvii]. Aside from the educational value, however, there is also beauty. There is beauty in a story well told, and there is beauty of a story that can move a listener to think, to imagine, and to learn. [73, p. ix]

I find this remark about beauty particularly fascinating, especially since my colleague Giampaolo Bella and I have been reflecting about beauty in security [5], which has led us to work with Jacques Ophoff, Karen Renaud and Diego Sempreboni to investigate the beautification of security ceremonies (i.e., protocols that are executed by machines and human users) [4, 3]. A few lines after the quote above, Zazkis and Liljedahl discuss the purpose of telling stories in the classroom:

> We tell stories in the mathematics classroom to achieve an environment of imagination, emotion, and thinking. We tell stories in the mathematics classroom to make mathematics more enjoyable and more memorable. We tell stories in the mathematics classroom to engage students in a mathematical activity, to make them think and explore, and to help them understand concepts and ideas. [73, p. ix]

They quote Egan:

> Telling a story is a way of establishing meaning. [25, p. 37]

and then talk about the power of images:

> One result of the development of language was the discovery that words can be used to evoke images in the minds of their hearers, and that these images can have as powerful emotional effects as reality might, and in some cases even more. [73, p. 15]

In fact, when Egan, Haven, Zazkis and Liljedahl, as well as many others, speak of telling, and then, more concretely, of storytelling, they invoke images and imagery. So, if storytelling

[12] See also Edge.org, the website of the Edge Foundation, Inc., which was launched in 1996 as the online version of "The Reality Club" to display the activities of "The Third Culture."

is powerful, and images and pictures even more so, why not combine them? Why not tell *and* show? Or, better, *show and tell*? Dan Roam has written a number of books, including "The Back of the Napkin" [54] and "Show and Tell" [55], in which he has been proposing visual thinking and storytelling for problem solving.[13] Specifically, Roam proposes to draw pictures in real time when presenting an idea, when addressing a problem and pitching its possible solution. This is one of the possible ways in which one can realize *show and tell*. In my works, I have explored another way, namely the use of existing artworks, fairy tales and films, in particular, but not only. The idea is that while *show, don't tell* is the commandment for fiction, in the case of non-fiction, *show and tell* is often the best approach when one wants to present, teach or explain complicated ideas such as those underlying notions and results in mathematics and science, and specifically in cybersecurity.

As I already remarked in the introduction, fairy tales and films have been used to teach and explain in a variety of academic fields [19, 20, 36, 56, 64]. There are some examples of using films in cybersecurity too [8, 58], but, to the best of my knowledge, this work is the first to discuss fairy tales and cybersecurity.

I have been using popular films to explain cybersecurity for several years, both in lectures and in public engagement talks, and I have complemented the anecdotal evidence that I collected at these events with systematic user studies, which showed that popular films are indeed a successful tool to explain cybersecurity to different kinds of people. More specifically, in these user studies, which are still unpublished, participants were asked questions about specific cybersecurity notions, including multi-factor authentication, password security, integrity, anonymity and steganography. For each notion, participants were asked a "before" question about their current understanding of that notion, then they were shown a clip from a popular film that had been selected to "explain" that notion, and finally they were asked an "after" question about their, hopefully improved, understanding of the notion. The answers showed a significant improvement in the participants' understanding for most notions, whereas for a few notions (in particular, anonymity and steganography) the film clips alone were not always enough but required additionally the explanations provided by an expert mediator who is able to relate the clips and the notions, and thus support the understanding.

A number of years ago, I started using fairy tales in lectures and talks, too, and in the course of 2023 I have been invited to speak about the cybersecurity of fairy tales not only at events dedicated to cybersecurity experts but also at *New Scientist Live 2023* in London (which, according to the organizers, is the world's greatest festival of ideas and discoveries) and at *Festival della Scienza 2023* in Genoa, Italy. These two science festivals provided an excellent opportunity to assess the effectiveness of this research with a popular audience comprising for the vast majority of laypersons and even children. This was even more so the case for the talk that I gave at the *Andersen Festival 2023* in Sestri Levante, Italy, the most important Italian festival dedicated to fairy tales. The feedback that I received thanks to these talks is that fairy tales are at least as effective as films and actually work even better than films with a lay audience, who are likely to be more familiar with fairy tales than with films, no matter how popular the chosen films are. The audiences found that fairy tales are at the same time more surprising than films as they did not expect fairy tales to be related or even relatable to cybersecurity notions, and more comfortable than films as fairy tales belong to our collective imagination and our cultural good, most often regardless of our background, level of education or level of cinephilia. Fairy tales thus appear to provide a much more effective and powerful bridge between the technical cybersecurity notions and their underlying, archetypal nature than that provided by films. To validate these speculations and insights, I plan to complement the anecdotal evidence that I have been collecting by carrying out systematic, both quantitative and qualitative, user studies on fairy tales and cybersecurity. I expect that these too will reveal signification improvements in understanding, but also highlight the occasional need for the presence of an expert mediator. It will be particularly interesting to

[13] "Show and tell" is also the name of a common classroom activity in elementary schools, especially in English-speaking countries, in which a child brings an item from home and explains to the class why he/she chose that item and other relevant information. This activity is useful also for adults [41], but it is quite different from the *show and tell* that Roam champions and the one that I discuss here.

consider not just written fairy tales read aloud or summarized by a presenter/mediator, but also the cinematic versions of fairy tales, in particular those by Disney (i.e., the Walt Disney Company) and other studios producing animated films. The talks that I have given suggest that fairy tale films will likely be more powerful tools for explaining cybersecurity than their original literary versions.

# 5 Conclusions

## 5.1 Summary

Fairy tales are wonderful. Not only because they objectively are, most often, full of wonder, but also thanks to the different social functions they have assumed throughout the centuries, ranging from amusement to instruction according to the basic tenets of the civilizing process in each particular country, from social critique to aids for therapy "with disturbed or abused children because they enable a child to gain distance from trauma and deal with it on a symbolical level that enables the therapist to understand and work with the child" [74, p. 24]. Fairy tales have always been a powerful discourse, capable of being used to shape or destabilize attitudes and behavior within culture: "we initiate children and expect them to learn the fairy-tale code as part of our responsibility in the civilizing process" [Zipes, 2009, p. 29]. The fairy tale has become "a staple of education throughout the west", it has become "totally institutionalized in our society, part of the public sphere, with its own specific code and forms through which we communicate about social and psychic phenomena" [74, p. 24 and p. 29].

This article shows that fairy tales are full of cybersecurity motifs, examples and, in some cases, allegories. Of course, not cybersecurity as we know it today (although I am sure that there are contemporary fairy tales in which cybersecurity plays a role), but rather the fundamental notions that are at the heart of cybersecurity. Much in the same way as fairy tales were "intended to play a major role in the socialization process" [74, p. 21], they can also play a major role in the 'cybersecurity alphabetization' of laypersons, be they children or adults, and favor a first conversation before, if and when needed, plunging into the technical details that underlie cybersecurity notions and solutions.

## 5.2 Future work

The investigation in this article is by no means exhaustive and can be extended in many different ways. In addition to the directions for future work that I have already mentioned above, I plan to consider more fairy tales and more cybersecurity notions. Moreover, my focus here has been on fairy tales popular in the Western world. Although fairy tales are known to have a certain universality, with the same themes and plots reoccurring in story form all over the world, examples coming from the traditions in, e.g., Asia, Africa, South America and Eastern Europe deserve a further study. I also plan to consider more recent fairy tales, as well as their adaptations in film (I already mentioned a few above) and in popular culture, including the *Harry Potter* saga by J.K. Rowling, which contains several examples of cybersecurity notions as I discussed in my previous papers.

Following in the footsteps of scholars such as Bettelheim, von Franz and Zipes who studied the relationship between fairy tales and myths, I would like to investigate the similarities and differences of how cybersecurity is immanent in both. For instance, the search for one's identity, along with the need to prove one's identity, is a common topos. So are MFA (for example, Thor is the only one able to lift the Mjøllnir hammer in Norse mythology, Arthur is the only one able to pull out the sword Excalibur from a stone, and Odysseus is the only one able to use his old bow as mentioned above) and masquerading attacks (in fairy tales but also in myths this often occurs by the attacker magically or divinely shape-shifting into somebody or something else, such as in the *Epic of Gilgamesh* [28] or in Ovid's *Metamorphoses* [43], or by wearing somebody's clothes as in Homer's *The Iliad* [34], which, besides the feats of the gods, describes how Patroclus wears the

Pelides' armor in order to be mistaken for Achilles). This investigation of cybersecurity in fairy tales and myth will hopefully also provide a deeper understanding of the connections between cybersecurity notions and the indices of Thompson and of Aarne-Thompson-Uther, as well as the functions of Propp.

I would also like to define a full-fledged methodology for extracting cybersecurity examples from fairy tales and other forms of storytelling, including also definitions of what may be considered strong and weak metaphors, allegories, archetypes and motifs, along with categorizations of which notions are more likely to require the intervention of an expert mediator who will facilitate the explanation and thus help the audience understand. I also plan to identify and categorize the cybersecurity notions that are not represented in fairy tales, and investigate why. Are there historical, semantical or technological reasons? This would help shed a further light on the notions and on their (non-)archetypal nature. Finally, I would like to follow in the footsteps of Fénelon and Brough. In the 1690s, the Archbishop Fénelon was the tutor of the Dauphin's 7-year-old son and wrote didactic fairy tales to make the lessons more enjoyable. In 1859, John Cargill Brough published *The Fairy Tales of Science — A Book for Youth* [10], in which he used popular myths and fairy tales to provide an entertaining introduction to topics in science for children (cf. also [37]). In addition to using existing fairy tales, I plan to plot new fairy tales oriented to explain cybersecurity (possibly inspired by the books by Quaglia [51, 52] or by the ideas in [12, 21], and, ideally, covering notions that are not already contained in classical fairy tales) or maybe even to influence novel cybersecurity solutions. The goal will be to explore how venturing into the 'cybersecurity woods' allows for understanding the pathways and journeys that leave us more vulnerable and open to cyber harm, in the hope that we will then be able to live cybersecurely ever after.

# 6 Acknowledgments

It takes a village to write a paper like this. I would like to thank the following people for their suggestions and comments: Alessandra Di Pierro, Aldo and Claudia Viganò, Giampaolo Bella, Oya Celiktutan, Gabriele Costa, Elisabetta Cremaschi, Emma De Angelis, Anne E. Duggan and Cristina Bacchilega, Graeme Earle, Ziad Elmarsafy, Barbara Fiorio, Daniele Gouthier, Ali Hossaini, Michael Kölling, Ashwin Mathew, Georgia Panteli, Katia Pizzi, Anna Ploszawski, Roberta Profeta, Carlo Sciaccaluga, Diego Sempreboni, Elena Tchougounova-Paulson, Ben Thomas, Marco Volpe, Sarah Werts, Lorenzo Zucca, and a few more that I am sure I have forgotten to mention.

# References

[1] Hans Christian Andersen. *The Complete Hans Christian Andersen Fairy Tales.* Gramercy, 1993.

[2] John Ayto. *The Oxford Dictionary of Rhyming Slang.* Oxford University Press, 2003.

[3] Giampaolo Bella, Jacques Ophoff, Karen Renaud, Diego Sempreboni, and Luca Viganò. Perceptions of beauty in security ceremonies. *Philosophy & Technology*, 35(3), 2022.

[4] Giampaolo Bella, Karen Renaud, Diego Sempreboni, and Luca Viganò. An Investigation into the "Beautification" of Security Ceremonies. In *Proceedings of the 16th International Joint Conference on e-Business and Telecommunications, ICETE 2019 - Volume 2: SECRYPT, 16th International Conference on Security and Cryptography*, pages 125–136. Scitepress Digital Library, 2019.

[5] Giampaolo Bella and Luca Viganò. Security is Beautiful. In *Security Protocols XXIII, Revised Selected Papers*, LNCS 9379, pages 247–250. Springer, 2015.

[6] Henry Bett. *Nursery Rhymes and Tales. Their Origin and History.* Methuen & Co. LTD, 1924.

[7] Bruno Bettelheim. *The Uses of Enchantment: The Meaning and Importance of Fairy Tales*. Thames & Hudson, 1976.

[8] Jorge Blasco and Elizabeth A. Quaglia. InfoSec Cinema: Using Films for Information Security Teaching. In *2018 USENIX Workshop on Advances in Security Education, ASE 2018*. USENIX Association, 2018.

[9] John Brockman. *The Third Culture: Beyond the Scientific Revolution*. Simon & Schuster, 1995. See also the website of the Edge Foundation, Inc. at `https://www.edge.org`.

[10] John Cargill Brough. *The Fairy Tales of Science — A Book for Youth*. Griffith and Farran, 1859.

[11] Jerome Bruner. *Actual Minds, Possible Worlds*. Harvard University Press, 1986.

[12] Xavier Bultel, Jannik Dreier, Pascal Lafourcade, and Malika More. How to Explain Modern Security Concepts to Your Children. *Cryptologia*, 41(5):422–447, 2017.

[13] Joseph Campbell. *The Hero with a Thousand Faces*. New World Library, 3 edition, 2008.

[14] Andrea Capozucca. *Comunicare la matematica*. Egea, 2018.

[15] Amelia Carruthers. *Cinderella — And Other Girls Who Lost Their Slippers*. Origins of Fairy Tales from Around the World. Pook Press, 2015.

[16] Amelia Carruthers. *Hansel and Gretel — And Other Siblings Forsaken in Forests*. Origins of Fairy Tales from Around the World. Pook Press, 2015.

[17] Amelia Carruthers. *Puss in Boots — And Other Very Clever Cats*. Origins of Fairy Tales from Around the World. Pook Press, 2015.

[18] Amelia Carruthers. *Rumpelstiltskin — And Other Angry Imps With Rather Unusual Names*. Origins of Fairy Tales from Around the World. Pook Press, 2015.

[19] Joseph E. Champoux. *Management: Using Film to Visualize Principles and Practice*. South-Western, 2000.

[20] Sara Cleto and Brittany Warman. Teaching with Stories: Empathy, Relatability, and the Fairy Tale. *Marvels & Tales*, 33(1):102–115, 2019.

[21] Véronique Cortier and Itsaka Rakotonirina. How to Explain Security Protocols to Your Children. In Daniel Dougherty, José Meseguer, Sebastian Alexander Mödersheim, and Paul D. Rowe, editors, *Protocols, Strands, and Logic — Essays Dedicated to Joshua Guttman on the Occasion of his 66.66th Birthday*, volume 13066 of *Lecture Notes in Computer Science*, pages 112–123. Springer, 2021.

[22] Marian Roalfe Cox. *Cinderella — Three hundred and forty-five variants of Cinderella, Catskin, and Cap o'Rushes, abstracted and tabulated, with a discussion of mediæval analogues, and notes*. The Folk-lore Society, 1893.

[23] Rebecca-Anne C. Do Rozario. *Fashion in the Fairy Tale Tradition (What Cinderella Wore)*. Palgrave Macmillan, 2018.

[24] John F. Dooley. *History of Cryptography and Cryptanalysis: Codes, Ciphers, and Their Algorithms*. Springer Cham, 2018.

[25] Kieran Egan. *Teaching as Story Telling: An Alternative Approach to Teaching and Curriculum in the Elementary School*. University of Chicago Press, 1986.

[26] Martin Erwig. *Once Upon an Algorithm: How Stories Explain Computing*. MIT Press, 2011.

[27] Antoine Galland. *Les mille et une nuits — Édition illustrée*. Archipoche, 2021.

[28] *The Epic of Gilgamesh: The Babylonian Epic Poem and Other Texts in Akkadian and Sumerian*. Penguin Books, 2003.

[29] Daniele Gouthier. *Scrivere di scienza*. Codice, 2019.

[30] Jacob Grimm and Wilhelm Grimm. *Kinder- und Hausmärchen*, volume 1. In der Realschulbuchhandlung, 1 edition, 1812.

[31] Ansie Harding. Storytelling for tertiary mathematics students. In *Invited Lectures from the 13th International Congress on Mathematical Education*, pages 195–207. Springer, 2018.

[32] Joel Chandler Harris. *Nights with Uncle Remus. Myths and Legends of the Old Plantation*. Houghton Mifflin Company, 1883.

[33] Kendall F. Haven. *Super simple storytelling: A can-do guide for every classroom*. Teacher Ideas Pr, 2000.

[34] Homer. *The Iliad*. Penguin Classics, reprint edition edition, 1987.

[35] Homer. *The Odyssey*. Penguin Classics, reprint edition edition, 2003.

[36] Christa C. Jones and Claudia Schwabe. Introduction: Cross-Disciplinary Perspectives on Teaching Folklore and Fairy Tales in Higher Education. In Christa C. Jones and Claudia Schwabe, editors, *New Approaches to Teaching Folk and Fairy Tales*, pages 3–18. Utah State UP, 2016.

[37] Melanie Keene. *Science in wonderland — the scientific fairy tales of Victorian Britain*. Oxford University Press, 2015.

[38] Percy Lubbock. *The Craft of Fiction*. Jonathan Cape, 1921.

[39] Sally Marlow and Kate Johnstone. The Power of the Arts. *The Psychologist*, 30:102–115, 2017.

[40] Alexander Mehlmann. *The Game's Afoot!: Game Theory in Myth and Paradox*. American Mathematical Society, 2000.

[41] Dorothy H. Nelson. D. and E.: Show and Tell, Grown Up. *Language Arts*, 53:203–205, 1976.

[42] Computer Security Resource Center of the National Institute of Standards and Technology of the U.S. Department of Commerce (NIST). Glossary of terms and definitions. `https://csrc.nist.gov/glossary`, last updated: 20 September 2022, last accessed: May 2023.

[43] Ovid. *Metamorphoses*. Oxford University Press, 2008.

[44] Laura Packer. Why We Need Fairy Tales. `https://storynet.org/why-we-need-fairy-tales/`, last accessed: May 2023.

[45] Eric H. Partridge. *Slang: To-Day and Yesterday*. Routledge, 1933.

[46] Eric H. Partridge and Jacqueline Simpson. *A Dictionary of Historical Slang*. Penguin, 1972.

[47] Charles Perrault. *The Complete Fairy Tales*. Oxford University Press, 2010.

[48] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Version v0.34), Aug. 10, 2010. `https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf`.

[49] Neil Philip. *The Cinderella Story*. Penguin, 1989.

[50] Vladimir Propp. *Morphology of the Folktale*. University of Texas Press, 2 edition, 1968.

[51] Elizabeth A. Quaglia. *Learning Together — Cryptography for Toddlers*. CyBOK, 2022. Available at `https://www.cybok.org/media/downloads/Learning_Together_Cryptography_for_Toddlers.pdf`, last accessed May 2023.

[52] Elizabeth A. Quaglia. *Learning Together — Cyber Security for Toddlers*. CyBOK, 2022. Available at `https://www.cybok.org/media/downloads/Learning_Together_Cyber_Security_for_Toddlers.pdf`, last accessed May 2023.

[53] Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis C. Guillou, Marie Annick Guillou, Gaïd Guillou, Anna Guillou, Gwenolé Guillou, Soazig Guillou, and Thomas A. Berson. How to Explain Zero-Knowledge Protocols to Your Children. In *CRYPTO'89*, LNCS 435, pages 628–631. Springer, 1989.

[54] Dan Roam. *The Back of the Napkin: Solving Problems and Selling Ideas With Pictures*. Portfolio Hardcover, 2008.

[55] Dan Roam. *Show and Tell: How Everybody Can Make Remarkable Presentations*. Portfolio Hardcover, 2014.

[56] William B. Russell III. The Art of Teaching Social Studies with Film. *The Clearing House: A Journal of Educational Strategies, Issues and Ideas*, 85(4):157–164, 2012.

[57] Adam Shostack. *Threat Modeling: Designing for Security*. Wiley, 2014.

[58] Adam Shostack. *Threats: What Every Engineer Should Learn From Star Wars*. Wiley, 2023.

[59] Simon Singh. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Fourth Estate, 1999.

[60] Steven Spielberg (directed by). *Minority Report*, 2002. Screenplay by Scott Frank and Jon Cohen based upon a short story by Philip K. Dick, `https://www.imdb.com/title/tt0181689/`.

[61] Stith Thompson. *Motif-Index of Folk-Literature: A Classification of Narrative Elements in Folktales, Ballads, Myths, Fables, Mediaeval Romances, Exempla, Fabliaux, Jest-Books, and Local Legends*. Indiana University Press, 1955–1958.

[62] Jon Turteltaub (directed by). *National Treasure*, 2004. Screenplay by Jim Kouf, Cormac Wibberley and Marianne Wibberley, `https://www.imdb.com/title/tt0368891/`.

[63] Hans-Jörg Uther. *The Types of International Folktales: A Classification and Bibliography. Based on the system of Antti Aarne and Stith Thompson*. Suomalainen Tiedeakatemia, Academia Scientiarum Fennica ( FF communications no. 284-286), 2004.

[64] Brandon Valeriano. Teaching Introduction to International Politics with Film. *Journal of Political Science Education*, 9:52–72, 2013.

[65] Luca Viganò. Explaining Cybersecurity with Films and the Arts. In Michele Emmer and Marco Abate, editors, *Imagine Math 7*, pages 297–309. Springer, Cham, 2020.

[66] Luca Viganò. Nicolas Cage is the Center of the Cybersecurity Universe. In Carmelo Ardito, Rosa Lanzilotti, Alessio Malizia, Helen Petrie, Antonio Piccinno, Giuseppe Desolda, and Kori Inkpen, editors, *Human-Computer Interaction — INTERACT 2021*, volume 12932 of *Lecture Notes in Computer Science*, pages 14–33. Springer, Cham, 2021.

[67] Luca Viganò. Don't Tell Me the Cybersecurity Moon is Shining... (Cybersecurity Show and Tell). In Michele Emmer, editor, *Imagine Math 8*. Springer, Cham, 2022.

[68] Luca Viganò and Daniele Magazzeni. Explainable Security. *CoRR*, 2018. `http://arxiv.org/abs/1807.04178`.

[69] Luca Viganò and Daniele Magazzeni. Explainable Security. In *IEEE European Symposium on Security and Privacy Workshops, EuroS&P Workshops 2020, Genoa, Italy, September 7-11, 2020*, pages 293–300. IEEE, 2020. A preliminary version appeared as [68].

[70] Christopher Vogler. *The Writer's Journey: Mythic Structure for Writers*. Michael Wiese Productions, 25th anniversary edition edition, 2020.

[71] Marie-Louise von Franz. *The Interpretation of Fairy Tales*. Shambhala, revised edition edition, 2017.

[72] Avrahm Yarmolinsky. *The Unknown Chekhov: Stories and Other Writings Hitherto Untranslated*. Noonday Press, 1954.

[73] Rina Zazkis and Peter Liljedahl. *Teaching Mathematics As Storytelling*. Sense Publishers, 2009.

[74] Jack Zipes. The Changing Function of the Fairy Tale. *The Lion and the Unicorn*, 12(2):7–31, 2009.