Sharing is Caring: Collaborative Analysis and Real-time Enquiry for Security Analytics

George D. Webster*, Ryan L. Harris†, Zachary D. Hanif‡, Bruce A. Hembree§, Jens Grossklags*, Claudia Eckert*
*Technical University of Munich, †Zions Bancorp, ‡University of Maryland, §Palo Alto Networks

***Abstract*—For decades it has been acknowledged that sharing security information and collaboration between security practitioners are a necessity. Yet, effective sharing and collaboration are rare. A gamut of legislative acts, executive orders, academic works, and private sector initiatives have discussed aspects of the problem and aimed to be the catalyst needed to fix the situation. But almost 30 years since these efforts started, the state of sharing and collaboration is still technically complicated, slow, untrusted, and impeded by bureaucratic woes.**

This work identifies the challenges of sharing security artifacts and uses real-world examples to illustrate our findings. Based on this knowledge, we propose a new model for sharing and collaboration, CARE. The CARE architecture eases many of the privacy, secrecy, lineage, and structure issues that plague current sharing communities and platforms. We then build upon this foundation to introduce a marketplace based on smart contracts with transactional privacy over a distributed blockchain. Therefore, CARE incentivizes sharing, combats free riding, and provides an immutable ledger for the attribution of events. This paradigm shift, overcomes the challenges of sharing while providing new opportunities for business models, insurance risk assessments, and government backed incentivisation.

***Index Terms*—Threat Intelligence, Information Sharing, Malware, Computer Security**

I. Introduction

The modern day security team struggles with deriving accurate analytic assessments and with overcoming the status quo of just-too-late reactive defensive strategies. We posit that a core reason behind the current state of affairs is that our defensive tools and processes are often incapable to enable truly collaborative environments, and sharing security artifacts between industry peers is a technically complicated, slow, untrusted, and an overly bureaucratic task [1], [2]. As a result, analytic insight and assessments are less accurate and defensive actions are delayed or ineffective [3], [4].

Compounding the issues above, shared security artifacts do not provide the impact needed to defend systems. For instance, after a well publicized and major security incident, the malicious actors still used similar tools and techniques to steal millions from hardened banking targets [5]–[7]. This should be no surprise to the informed security expert. Most research in this problem area has focused on the necessities of sharing and the ontologies to use [2], but does not address the underlying problems. There is a reluctance to share, and the context needed to make shared artifacts valuable is often stripped. This makes adjusting defenses challenging and hinders proactive investigations and collaboration. To illustrate, the *United States Computer Emergency Response Team* (US-CERT) proudly released a slew of *Indicators of Compromise* (IoCs) for a significant security incident [8]. However, these IoCs were nothing more than a collection of hashes with a quick description (i.e. “Lightweight backdoor”), a set of signatures with no details on how or why they were created, and Internet Protocol (IP) addresses with a port and country. Thus, researchers given these IoCs can either blindly deploy the rules, or spend considerable effort to rebuild the context and perform their own investigation. However, deploying these rules will not prevent attacks by any moderately devoted malicious actor, because these actors can simply move infrastructure and conduct a re-signature of their tools [9]. Making matters worse, actors can automate this process with methods such as polymorphism, metamorphism, and Domain Generating Algorithms (DGAs). On the other hand, performing an investigation is costly and on average takes even specialized companies 54 days [10]. Given this, it is no revelation that it takes around 198 days for a company to discover they have been victimized, with some taking upwards of six years [11].

To move forward, we need a change in paradigm. We propose a new model for sharing computer security artifacts, CARE, which aims to provide the mechanisms required to perform analytic collaboration with a collective pool of knowledge in near real-time. It does this by providing a cryptographically backed exchange for sharing, derived through a set of common, verifiable extraction methods and analytic algorithms. As a result, the CARE model provides the foundations for overcoming the privacy and secrecy issues with sharing; it maintains the context and lineage associated with derived information; and it provides a common structure to allow shared artifacts to be easily ingested in analytic pipelines. Furthermore, the cryptographically backed method increases overall trust in the system, while also providing the ledger and infrastructure required to develop a sharing marketplace. In turn, this provides the necessary incentives needed to encourage companies and individuals to share, and have the immutable records needed to identify offenders of trust.

Our work makes the following main contributions:

- We discuss real-world initiatives for sharing security artifacts and dissect the associated failures and challenges.
- We propose an architectural model that alleviates many

of the privacy, secrecy, lineage, and structure issues that are prevalent in the current sharing paradigms.

- We introduce a secure ledger model that records who shared what, with whom, and when; and also guarantees the lineage and structure for shared artifacts.
- We present a design pattern for sharing that creates a marketplace based on smart contracts with transactional privacy over a distributed blockchain.
- We describe how our model creates new opportunities and business models by providing the metrics needed for identifying insurance risk and providing the structure needed for allowing governments to provide tax incentives.

II. The Problem in Perspective

In November 2014, Sony Pictures Entertainment became the victim of an unprecedented attack that not only leaked Sony's private business records and communications but also destroyed valuable data [12]. In response, a combined governmental and corporate initiative immediately went into action to identify the threat, perform mitigation operations, and share across the community in the hopes of preventing future attacks [8], [13]. This effort was deemed a major success and a textbook example for which future responses should be modeled; now named the "Sony Model" [13]. One of the reasons behind why the response was deemed so successful is because the *Federal Bureau of Investigation* (FBI) treated the victims as a partner and encouraged the proactive sharing of IoCs.

Sadly, a year later millions of dollars were stolen from a bank by means of fraudulent *Society for Worldwide Interbank Financial Telecommunications* (SWIFT) transactions [7]. Initially the SWIFT and Sony attacks appeared unrelated. However, security researchers were able to attribute the attacks to the same actor, the Lazarus Group, and conclude that multiple other banks were also victims [5], [6].

The quick response to the Sony attack and the fact that details of the Sony attack greatly aided the SWIFT investigation clearly demonstrates the value of sharing within the security community. Specifically, the breakthrough in the SWIFT investigation, and attribution to the Lazarus Group, was in large part due to the widespread sharing of IoCs [6]. However, this example also highlights many of the major failures in the current sharing paradigm. For instance, the IoCs shared by the FBI through US-CERT were not what was cited as providing significant value during the SWIFT investigation. This credit went to an independent mitigation operation that occurred two years later, called Operation Blockbuster [5], [6], [12]. This is because the information originally shared by the FBI was heavily stripped of context to protect privacy, secrecy, and tradecraft. Taking a more critical point of view, one could even consider it a significant failure that the Lazarus Group was still able to use similar tools and techniques a year after the Sony attack in the SWIFT attack; even more so since the Sony attack received much publicity.

This episode highlights the potential benefits of sharing, but also the problems with the current sharing paradigm, which are rooted in a storied history. Dating back to the 1980s, numerous legislative acts, executive orders, and private sector initiatives have singled out sharing as a necessity for effective computer security and the lack of sharing as a major weakness. In response, these acts and initiatives were intended to be the catalyst needed to fix the problems with sharing within the security community [14]–[17]. Subsequently, communities and organizations were formed to act as facilitators for sharing, specifically *Computer Emergency Response Team*s (CERTs), sector-specific *Information Sharing and Analysis Center*s (ISACs), and private tight-knit community trust groups [1], [15], [16], [18]. Furthermore, these private trust groups are often orientated around a single mission. For example, Yara Exchange is an exclusive group of researchers that focuses on creating a collective set of Yara signatures [19]. While, Ops-T is a vetted community that aims to thwart malicious behavior through collective action and sharing blacklists [20]. As these associations matured, they created common ways for their participants to communicate through the development of numerous standardized ontologies for cataloging information about computer security incidents, collectively known as IoCs [2]. Furthermore, to facilitate the communication of these IoCs, multiple sharing protocols and platforms were formed along with a new business sector focusing on cyber threat intelligence feeds [2], [21], [22].

Despite the above efforts, most sharing is typically done (i) through an ad hoc exchange of unstructured data by means of work acquaintances, small community trust groups, and between individual ISAC members, or (ii) via cyber threat intelligence feeds that are delayed and of questionable value [1], [23], [24]. Despite the delay in sharing actionable information, the level of sharing that occurred after the Sony attack and the details that were provided as part of Operation Blockbuster are a positive anomaly. Simply put, widespread sharing and collaboration of timely information that crosses sectors rarely happens and when it does its impact is often less than it should be [24], [25].

III. The Realities of the Current Sharing Paradigm

The major issues surrounding why sharing and collaboration do not regularly occur and lack effectiveness can be summarized as follows [1]–[4], [25]–[29]:

- **Privacy of Victims** - Exchanging raw data can leak information regarding the victim's identity and their sensitive data. This inadvertent disclosure can directly harm the victim and their reputation, eroding market share, as well as cause contractual, legal, and regulatory violations on behalf of the sharer.
- **Secrecy of Attack Patterns** - Raw data can divulge the methods and techniques used by the attacker as well as details about the victims' infrastructure and computer security posture. This can empower and encourage other malicious actors. In an infamous case, Zeus' leaked source code was used to create Citadel and ICE IX [30].
- **Tradecraft of Investigators** - Requesting and exchanging information can alert attackers that an investigation is occurring. This can allow attackers to shift tactics and

increase their chances of evading future detection by defensive monitoring and controls. Additionally, this can leak business secrets to peers, which can reduce competitive advantage.
- **Lack of lineage** - Shared information is often stripped of vital context, and how the information was obtained is frequently unknown. This causes a situation where shared information is untrusted, the relevance to the recipient is not immediately apparent, and the information must be reprocessed or amended through informal channels to be useful for the receiving party.
- **Lack of structure** - Shared information may be unstructured, poorly structured, or in a myriad of different *Indicator of Compromise* (IoC) formats. As such, significant time and manual intervention is required to ingest the feeds in the recipient's own workflow.
- **Absence of ledger** - No universal method to track in a verifiable fashion who shared what, with whom, and when exists. This leaves little potential to identify offenders of trust or allow for crediting the contributors of valuable data.
- **Lack of incentives** - There is no directly apparent economic benefit to community-wide sharing. Additionally, commercial security companies may be disincentivized to share freely for fear of diminishing their competitive advantage.

In total, these reasons create an environment where organizations and individuals are reluctant to share, and when sharing occurs the information is stripped to the point that the immediate value becomes questionable. Unfortunately, this culminates into a paradigm where potentially vital information that can mitigate threats often never reaches (potential) victims in time.

A. Wisdom Without Context is Merely Data

In the Sony case, the response team proactively shared information, including a summary of some of the attacker's tools and unstructured IoCs containing import hashes, binary MD5s, command-and-control IP addresses, Snort Signatures, and Yara rules [8]. While sharing publicly at this level is rare, what was shared is typical of information broadcasted via ISACs, community trust groups, and cyber threat intelligence feeds. For example, the *Financial Services - Information Sharing and Analysis Center* (FS-ISAC) advertises that they provide the sharing of different types of reports and the means for members to ask for further information through submitting a *Request for Information* (RFI) [31]. Similar to ISACs, two of the most popular trust groups, Yara Exchange and Ops-T, regularly share Yara signatures, lists of blacklisted domains, hashes for malicious samples, and allow members to directly request additional information about an object [19], [20].

Regretfully, this proactive sharing of IoCs was not enough to hinder the Lazarus Group from using similar tools and techniques during the SWIFT attacks. The issues around why this occurred are best described when viewing information security analytics under the perspective of the *Data-Information-Knowledge-Wisdom* (DIKW) model [32]. As illustrated in Figure 1, analytic insights or actions are achieved by building upon each layer of the DIKW model: *data*, *information*, *knowledge*, and *wisdom*. Applying this to computer security analytics, we can derive the following:

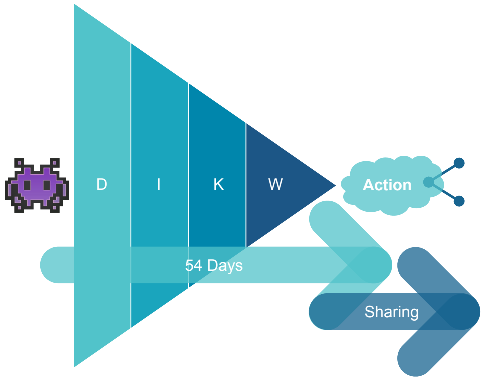

Fig. 1. DIKW Pyramid with Respect to Average Mitigation Time and Sharing

- ***Data*** - The raw object: PE32, PCAP, memory dump, domain, IP, file, etc.
- ***Information*** - Details about the *data* that can be determined through static analysis, dynamic analysis, or other extraction mechanisms.
- ***Knowledge*** - Organizing a set or a subset of *information* into useful forms using statistics, knowledge-based rules, machine learning, or other analytic techniques.
- ***Wisdom*** - Developing an understanding of the *knowledge*, based on experience, to allow a judgment or action to be made.

Only once *wisdom* has been derived, can the defender fully comprehend the threat and formulate an effective response. Thus, the common practice of sharing IoCs that contain nothing more than the derived *wisdom* without the lineage of how there were generated (for instance, various lists of hashes, IP addresses, a specific import used by a binary, or a signature) does not greatly assist in the analytic loop. Shared *wisdom* without context is just *data*. In turn, this makes it difficult for the recipient to work with or generate *wisdom* when they do not understand the context of how the *information* was generated and how the *knowledge* was pieced together. This makes it challenging to apply the received *wisdom* to their own investigation and ask different questions to derive a different meaning. Furthermore, without a common structure it is not easy for shared artifacts to be merged into the recipient's analytic pipeline in order to identify further meaning or understanding. Hence, the situation occurs where the receiving party needs to gather the original *data* behind shared IoCs and reprocess them before further analytics or effective action can take place. However, a catch-22 occurs because the original *data* is often restricted and rarely exchanged due to issues of privacy, secrecy, and tradecraft.

B. The Need For Speed

The current paradigm is lacking in timeliness to be effective. For instance, the Lazarus Group used the same tools and techniques to attack multiple victims over a period lasting longer than a year. This is unsettling, but it should come as no surprise. As illustrated in Figure 1, it takes an average of 54 days for a specialized company to move from *data* to *wisdom* and develop a response after a malicious action has been identified [10]. Furthermore, 15% of known malicious files are still not detected, let alone mitigated, until 180 days after being released [10]. The Sony case was faster than average, sharing an initial set of IoCs in less than 30 days and then amending the IoCs about a year and a half afterwards [8]. Unfortunately, this is still much too slow, especially when considering that 75% of attacks spread from the first victim to the second in less than 24 hours [33].

Regrettably, even when information is shared, the security community still faces an issue where the sharing recipients must enter a cycle of reprocessing any received *data*, then ask for more *data* based on what they identified, and then reprocess this newly received *data* to generate the *information* and create the *knowledge* needed to develop their own *wisdom*. This process is required because what is shared is a static snapshot of a previous attack and does not contain any lineage. As such, given a shared IoC the recipient can only understand, at a general level, what was previously used in an attack and the details are obfuscated. Unfortunately, this allows attackers the ability to easily overcome the threat posed by sharing through moving infrastructure and obfuscating malicious code in any fashion that is faster than the defender can complete this resource-intensive cycle [9].

C. Lack of Trust In Exchanged Items

The current sharing paradigm does not have a verifiable lineage. The Sony case study is no different in that the originally shared *information* provided minimal context and little details regarding how the *information* was generated. Unfortunately, this causes issues of trust between sharing partners and inaccurate assessments. One of the reasons behind this is that different methods can be used for generating similar types of *information*. However, while similar, the *information* is not always interchangeable and may even contain flaws. For example, Wesley Shields recently reported that the implementation of PEHash [34] used by widely popular tools such as Totalhash [35], Collaborative Research Into Threats (CRITs) [36], and VIPER [37] incorrectly generated the hashes [38]. This caused a problem when generating *knowledge* and *wisdom* based on shared *information* because the hashes would not match and inaccurate results were produced. Unfortunately, this issue is not rare and as such it is common practice to validate any received IoCs until a level of trust in the originator can be established [26].

Eroding trust further, the current model's reliance on sharing by either massively distributing IoCs or providing specifically requested details among peers exacerbates the concerns surrounding privacy, secrecy, and tradecraft. This is because these methods lack a universal and trusted ledger of what was shared, with whom, and when. As such, the originator loses traceability, which hinders the identification of abuses of trust. Thus, it is nearly impossible to enforce any security and privacy controls or perform retribution against violators. This fear is evident in the exclusivity of trust groups and ISACs as well as the level of context that was stripped from the originally released IoCs in our case study.

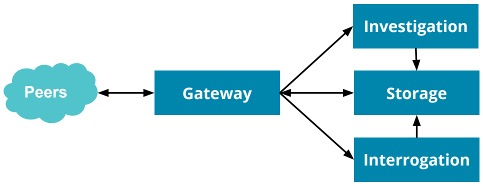

Fig. 2. CARE architectural components and interaction.

IV. The CARE Model

CARE is a design pattern for developing analytic systems that enable collaboration and alleviate the current issues with sharing. At its core, CARE is an architectural foundation for generating and exchanging security artifacts across the DIKW model; thus, allowing partners to overcome the challenging and time-consuming burden of rebuilding the context and *information* behind IoCs, finished reporting, and *data*. Building upon this foundation, CARE then leverages smart contracts on top of blockchain technology to enable a cryptographically backed exchange (CAREconomy).

In this section, we will describe the CARE architecture, explain the CAREconomy, and lastly discuss how sharing partners interact with the system.

A. CARE Architecture

The architecture for CARE builds upon the Skald concept of *planner*s and *service*s [39]. In this, the *planner* is centered on supporting the goals for a specific theme and orchestrates the execution of *service*s. The *service* component is "loosely coupled" and performs the execution of a task. For example, the Investigation *planner* smartly orchestrates *information* extraction *service*s for *data*. Under this structure, the CARE architecture primarily provides the (i) ability to manage partner interaction, (ii) generation of artifacts, and (iii) creation of an abstract method for storing artifacts and system data. As shown in Figure 2, the architecture is composed of four core *planner*s: Gateway, Investigation, Interrogation, and Storage. As will be discussed in this section, these *planner*s are designed to overcome the privacy and secrecy issues with sharing *data*; to maintain the lineage associated with *information*, *knowledge*, and *wisdom*; and to provide a common structure for shared artifacts. Together this empowers peers to exchange across the DIKW model and to more effectively collaborate.

The Gateway *planner* is central for managing partner interactions and exchanging artifacts across the DIKW model. The Gateway provides four key functionalities: (i) notifying peers what artifacts are available, (ii) authenticating and validating requests, (iii) orchestrating the exchange of artifacts, and (iv) administrating of the CAREconomy.

Gateways communicate with each other in a peer-to-peer fashion. This communication method keeps the artifacts in the control of the owner while also providing the foundational building blocks on which collaborative trust groups can be built. The peer-to-peer approach also allows peers to have fine grained control over what artifacts are available and who can access their system. For instance, a peer can restrict the sharing of an artifact based on a taxonomy or specific *service*s as well as which peers are able to access these artifacts. This is a dramatic difference over traditional sharing platforms, such as CRITs and Malware Information Sharing Platform (MISP), because those model access based around the concept of group level access or access based on the source of *data* in which the artifact was generated [22], [36]. Furthermore, the peer-to-peer method removes the necessity of trusting a sharing platform provider with protecting all the assets; a key finding highlighted by Clemens et al. [2].

Illustrating how the Gateway functions, in CARE, partners submit all requests for exchanging artifacts through the Gateway. When Gateway receives a request, it first authenticates the requester and validates that the request is properly formatted. After that, Gateway gathers the requested artifact from Storage or submits a request to Investigation or Interrogation to generate the requested artifact. In its final step, Gateway gathers the artifact, adds the pertinent metadata to the artifact, updates the distributed ledger, and submits the results back to the requester.

The next set of *planner*s, Investigation and Interrogation, are charged with transforming artifacts to the next higher level in the DIKW model. Regarding the Investigation *planner*, this *planner* is responsible for generating *information* from *data*. Investigation does this by orchestrating the execution *service*s that perform static analysis and dynamic analysis as well as gathering *information* from 3rd parties. In a similar vein to Investigation, the Interrogation *planner* focuses on transforming information into *knowledge* and empowering an analyst to create *wisdom* through assessing collective *knowledge*. For example, an Interrogation *service* can execute a machine learning algorithm to cluster samples or help to label artifacts by executing statistical or knowledge-based analysis. With respect to *wisdom*, a *service* could help with visualizing sets of artifacts, creating a standardized set of IoCs, or generating blacklists.

In this model, the Investigation and Interrogation *service*s that are available for sharing are known and agreed upon by the peers or an ombudsman. This helps to overcome some major challenges with sharing unstructured artifacts or IoCs, because the lineage and structure is maintained and understood by all parties. As such, the results a *service* provides and how the artifacts propagated through the system are known. This allows these results to be immediately incorporated into the receiver's analytic pipeline because the context is understood. Thus, it reduces the time required to process any newly shared artifact a party receives. Additionally, this overcomes the challenges that stem from only providing an exchange for IoCs even if the lineage is known. As discussed prior, and can be witnessed with the MISP platform, there are a plethora of different ontologies that can be classified as an IoC and these ontologies can have extensive vocabularies. To illustrate, the MISP document that describes the subset of vocabulary for ontologies they support is 326 pages [40]. This makes immediately leveraging a shared IoC difficult because the receiver of an IoC must first validate the format, ensure it is being used in the same way, and convert the format to the in-house style.

Lastly, this method helps to overcome the privacy and secrecy issues that stem from sharing *data*. As the context behind an artifact is known and the requirements for the transformation of *information* and *knowledge* are available, direct access to *data* is not required for an investigation.

The Storage *planner* in CARE is akin to the original design of Skald [39]. Specific to sharing, Storage manages the repository of *data*, *information*, *knowledge*, and *wisdom* for each peer in addition to CARE-specific data. Storage also provides an abstraction layer between database systems. This abstraction allows peers to incorporate the model over existing systems, leverage a single or hybrid back-end solution, and select their preferred database.

B. CAREconomy

The CARE architecture provides a foundation for generating and exchanging security artifacts in a way that alleviates the current sharing paradigm's issues of privacy, secrecy, lineage, and structure. However, many of the issues with sharing are caused from the fact that sharing platforms are based on the reputation of individual contributors [2]. This can erode trust in these groups due to accident or malice by the participants. For example, original authorship can be mis-attributed or forgotten, community engagement can go unnoticed, and breaches of confidence can occur. Unfortunately, these fears are well-founded. Greed, the desire for recognition, and forgotten ownership has caused sharing partners to release or act upon restricted details early at the detriment of the collaborative effort [41]. For example, during the Mariposa botnet take-down, the DNS registrar was successfully bribed into helping the malicious actors regain control of the botnet [42]. Furthermore, as groups grow, the problem of free riding, where participants reap the benefits but do not contribute, becomes prevalent [3], [43], [44]. If left unchecked, these issues will erode participation and wear down the perceived benefits to sharing. To combat these issues, CAREconomy is focused on developing overall trust in CARE through an immutable ledger and providing incentives to share by creating a smart contract based marketplace.

Unfortunately, the realities of publication size limits the ability to provide details behind a proposed implementation for the CAREconomy.

V. Discussion

The CARE model creates a new way forward for sharing and collaborating in the security community. In this section, we discuss how this new model presents previously unattainable opportunities for the creation of sharing partnerships, expands how contributors can take part, and presents new possibilities for incentivizing and assessing partner collaboration and effectiveness of sharing.

A. Creating Collaborative Communities

Security communities have historically been established to fill a community need or to service a specific sector. For example, FS-ISAC was created to foster collaboration and sharing in the financial sector, Yara Exchange was created to crowdsource the creation of Yara signatures, and Ops-T brought together vetted security practitioners with the goal of exchanging information to collaborate in the mitigation of security threats. For reasons explained in the previous section, these groups are almost universally tight-knit and have processes in place that attempt to vet new members, encourage participation, and overall maintain a level of trust. Unfortunately, this is often a losing battle and over time the level of quality in what is shared degrades and member participation declines [3], [43]. In sum, while the goals of these communities are noble, the effectiveness and utility of theses communities and cyber threat intelligence feeds are often left in question.

1) Sharing Communities: CARE empowers these communities and intelligence feeds by overcoming the challenges discussed in Section III. In turn, this enables traditional security communities to more effectively share and collaborate while providing the infrastructure needed to keep them healthy and encourage participation. Additionally, the secure ledger and incentives that CAREconomy provides open the opportunity for larger collaborative efforts by lessening free riding and overcoming the risks associated with sharing *data* widely. CARE is envisioned as becoming the new method for collaboration and exchanging artifacts within private trust groups, ISACs and CERTs, corporate partnerships, and be the driver needed to enable the creation of large communities that span multiple sectors and security specializations.

2) Community Management: To manage sharing communities, CARE necessitates the use of an ombudsman or other structured form of governance. In the traditional cryptocurrency world, an informal method of governance has been the dominating force [45], [46]. These governance models provide many benefits and have been surprisingly long lasting. However, they also have their issues, specifically with managing access, evolving to change, and responding to abuse [47], [48]. Furthermore, a smart contract that lives on the blockchain is immutable by nature. This creates a challenge because these contracts are difficult to write and are not immune to vulnerabilities [49]. For instance, the Decentralized Autonomous Organization (DAO) smart contract that provided a form of informal governance had numerous flaws in its design [47]. In one particular case, this allowed an attacker to steal 50 million dollars while the community could only watch [50].

When these issues with decentralized governance models are posed together with the unique challenges created by computer security investigations and the handling of security artifacts, it is clear that a different approach to governance is required. As such, we propose that CARE models its community management in a manner that is more akin to the ISAC model. In this, the community should have a structured form of governance that serves to foster trust and encourage collaboration within the community [51]. At a minimum, we propose that the management of a sharing community should provide the:

- **Management of users** - Approve access to the community and perform traditional user management functions.
- **Organization of the CAREconomy** - Declare sanctioned contract types, maintain a set of approved *service*s, select the method for generating money and validate the blockchain, and oversee the economy.
- **Remediation for security and privacy concerns** - Mediate member disputes and perform remedies in cases of information leaks and inadvertent exposures.
- **Proactive reduction of security risks** - Vet service code and the code used for creating smart contracts.

B. Sharing Partners

The current sharing paradigm has fostered ad hoc exchanges and intelligence feeds of questionable value. As discussed, these exchanges are often delayed, and the received artifacts need to be re-validated and reprocessed before they can provide utility. Within a sharing community, this creates an all-or-nothing situation where participants typically must perform all the steps required to create and disseminate IoCs or otherwise advance the community's mission. However, the ability in CARE to share artifacts across the DIKW model presents new opportunities and grants sharing partners the ability to collaborate with asymmetric resources in near real-time. This allows participants the ability to specialize in different types of threat research while still furthering the collective knowledge of the community. For example, independent researchers can maintain sets of honeypots that collect *data* and leverage the community's *knowledge* to help identify what was collected. University researchers can obtain *information* that enables research in new machine learning algorithms and return the *knowledge* they derive. Corporate security teams can perform automated triage, such as Portable Executable (PE32) header extraction, on new *data* to generate *information* and leverage the collective knowledge to better defend their networks. And threat intelligence providers can sell *wisdom* (e.g., actionable IoCs) or specialized *information* and *knowledge*.

C. New Opportunities

Critics of historic efforts to promote sharing and collaboration in the security community have identified that the government needs to incentivize healthy sharing and security practices. Unfortunately, the identification of how to measure the effectiveness of a security team and their sharing practices has been a hotly discussed item for decades [52]. The underlying reasons have been discussed in this work but the core issue is that there are no good metrics for what makes a security team effective and what defines the value of shared artifacts. Moreover, the current sharing paradigm does not provide the infrastructure and records needed to create these metrics.

The CARE model provides a ledger recording all interactions; even if the details of what specifically is exchanged can be encrypted. This presents new possibilities in how to determine and rate how companies collaborate and in turn the effectiveness of the security teams' efforts. This can provide the metrics needed for developing useful government incentives. Additionally, insurance companies can use these metrics to determine the risk factors associated with insuring a company and adjust rates accordingly. These incentives and overhead adjustments combined with the ability to accumulate wealth through the CAREconomy help break the mold of corporate security groups being taxing cost centers. In turn, this provides the potential of these groups to become not just a necessary evil in the form of a red-line on a balance sheet to mitigate risk but profit centers or at least groups that can articulate their worth.

VI. Related Work

The belief that sharing security information among peers will improve the overall defensive posture of the community has been well-established. For instance, after the Morris Worm attack the U.S. government created CERT, and PDD-63 created ISACs to help combat the perceived threat to critical infrastructure [15], [18]. Providing academic rigor behind the notion that sharing is critical, Gordon et al. evaluated the state of sharing and developed an economic model that analyzed the organizational cost [43]. This work was then expanded by Gal-Or et al. who used game theory to study the demand side effects occurring under the current sharing paradigm [3]. Both works are critical to understanding the major benefits that sharing provides to the participants and community at large while also identifying the underlying flaws in the current system. Specifically, sharing provides mutual benefits to security and cost savings, but the effects are negated because the current sharing paradigm does not provide incentives to prevent *free riding* and overcome participants' concerns. Unfortunately, as shown in a recent study, the identification of incentives is still an area ripe for research [52].

Little research has been conducted about the technologies to enable sharing in the security community. To address this, Sauerwein et al. perform an exploratory study of twenty-two cyber threat intelligence platforms and the state of scientific research [2]. Their analysis identifies eight key findings and highlights the current issues of trust, structure, speed, and overall need to migrate these systems from sharing IoCs to sharing information across the Intelligence Cycle.

The theoretical concept of smart contracts for formalizing and securing digital relationships dates back to the late 1990s [53]. One of the first implementations of this concept based on *Proof of Work* (PoW) was KARMA [54]. In KARMA, the researchers devised a method for overcoming freeloaders (free riding) in peer-to-peer file exchanges through the use of a secure decentralized ledger. In a similar vein, Nakamoto proposed a hash-based PoW system for payment, which is now famously named Bitcoin [55]. While Bitcoin's blockchain has given rise to numerous applications, its scripting language is not Turing complete and difficult to retrofit. Ethereum addresses this issue and provides a blockchain with a Turing-complete language with the possibility to implement smart contracts [56]. Expanding on the concepts of Ethereum, Kosba et al. present a blockchain based smart contract system that incorporates transactional privacy, HAWK [57].

These works highlight many of the underlying problems and provide parts of the solutions to the issues of sharing security information. However, these works only identify the problems or provide solutions to specific issues that are surrounding the challenges of sharing computer security artifacts. Our work combines and builds upon these works and is the first to our knowledge that combines these concepts to tackle the holistic problem of developing a framework for securely exchanging computer security artifacts across the Intelligence Cycle, while overcoming the issues of privacy, secrecy, tradecraft, lineage, structure, ledger, and incentives.

VII. Conclusion

In this paper, we presented a new model for sharing security information, CARE. We discussed how CARE improves upon the existing sharing paradigm and alleviates many of the current issues for why sharing is often ineffective. We first discussed the need for the new model by presenting a study of the current state of sharing and identified the associated issues. We then show how CARE overcomes these issues by providing the ability to exchange security artifacts across the DIKW model while preserving the artifacts' lineage and mitigating privacy and secrecy concerns. We then discuss the CAREconomy and describe how this cryptographically backed method incentivizes sharing through the creation of a marketplace and provides new opportunities to encourage healthy collaboration and develop trust. Finally, we discuss how CARE opens new possibilities in how security groups can collaborate, governments can foster effective security practices, and insurance companies can more accurately identify risk through a secure and distributed ledger.

Acknowledgments: We thank the anonymous reviewers for their valuable comments. The research activities of Jens Grossklags are supported by the German Institute for Trust and Safety on the Internet (DIVSI).

References

[1] G. Fisk, C. Ardi, N. Pickett, J. Heidemann, M. Fisk, and C. Papadopoulos, "Privacy Principles for Sharing Cyber Security Data," in *Proceedings of the IEEE International Workshop on Privacy Engineering*. IEEE, 2015, pp. 193–197.

[2] C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives," in *Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017)*, 2017, pp. 837–851.

[3] E. Gal-Or and A. Chose, "The economic incentives for sharing security information," *Information Systems Research*, vol. 16, no. 2, pp. 186–208, 2005.

[4] L. Gordon, M. Loeb, and W. Lucyshyn, “An Economics Perspective on the Sharing of Information Related to Security Breaches: Concepts and Empirical Evidence,” in *Workshop on the Economics of Information Security (WEIS)*, 2002.

[5] S. Shevchenko and A. Nish, “Cyber Heist Attribution,” *BAE Systems Threat Research Blog*, 2016. [Online]. Available: http://baesystemsai.blogspot.fi/2016/05/cyber-heist-attribution.html

[6] Symantec, “SWIFT Attackers’ Malware Linked to More Financial Attacks,” May 2016. [Online]. Available: http://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

[7] T. Bergin and J. Finkle, “Exclusive: SWIFT Confirms New Cyber Thefts, Hacking Tactics,” *Reuters*, Dec. 2016, http://www.reuters.com/article/us-usa-cyber-swift-exclusive/exclusive-swift-confirms-new-cyber-thefts-hacking-tactics-idUSKBN1412NT.

[8] US-CERT, “Alert (TA14-353A),” Dec. 2014.

[9] D. Bianco, “The Pyramid of Pain,” *Enterprise Detection & Response*, Mar. 2013. [Online]. Available: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

[10] Damballa Inc, “3% to 5% of Enterprise Assets are Compromised by Bot-driven Targeted Attack Malware,” Mar. 2008. [Online]. Available: https://www.prnewswire.com/news-releases/3-to-5-of-enterprise-assets-are-compromised-by-bot-driven-targeted-attack-malware-61634867.html

[11] S. Farhang and J. Grossklags, “When to Invest in Security? Empirical Evidence and a Game-Theoretic Approach for Time-Based Security,” in *Workshop on the Economics of Information Security*, Jun. 2017.

[12] Novetta Threat Research Group, “Operation Blockbuster - Unraveling the Long Thread of the Sony Attack,” Feb. 2016.

[13] A. Boyd, “How FBI Cyber Division Helps Agencies Investigate Intrusions,” *Federal Times*, Oct. 2015.

[14] U. S. Legislature, “H.R. 145 - Computer Security Act of 1987,” pp. 100–235, 1988.

[15] B. Clinton, “Presidential Decision Directives/NSC-63,” p. 68, 1998.

[16] 107th Congress, “Homeland Security Act of 2002,” in *Public Law*, 2002, vol. 25, pp. 107–296.

[17] B. Obama, “Promoting Private Sector Cybersecurity Information Sharing, Executive Order 13691,” 2015.

[18] CERT-Coordination Center, “CSIRT Frequently Asked Questions (FAQ),” pp. 1–10, 2016. [Online]. Available: https://www.cert.org/incident-management/csirt-development/csirt-faq.cfm?

[19] DeepEnd Research, “YaraExchange,” May 2017. [Online]. Available: https://github.com/YaraExchange

[20] Trust, Operations Security, “Ops-T,” 2017. [Online]. Available: https://portal.ops-trust.net/

[21] J. Connolly, M. Davidson, and C. Schmidt, “The Trusted Automated eXchange of Indicator Information (TAXII),” OASIS Cyber Threat Intelligence Technical Committee, Tech. Rep., 2014.

[22] C. Wagner, A. Dulaunoy, G. Wagener, and A. Iklody, “MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform,” in *Proceedings of the 2016 Workshop on Information Sharing and Collaborative Security*. ACM, 2016, pp. 49–56.

[23] P. Vixie, “Internet Security Marketing: Buyer Beware,” *CircleID*, Apr. 2015. [Online]. Available: http://www.circleid.com/posts/20150420_internet_security_marketing_buyer_beware/

[24] T. Moore and R. Clayton, “The consequence of non-cooperation in the fight against phishing,” in *Proceedings of the eCrime Researchers Summit (eCrime)*, 2008.

[25] Communications Security, Reliability and Interoperability Council, “Working Group 5: Cybersecurity Information Sharing - Information Sharing Barriers,” Jun. 2016.

[26] C. Johnson, L. Badger, D. Waltermire, J. Snyder, and C. Skorupka, “Guide to Cyber Threat Information Sharing,” *NIST Special Publication 800–150*, 2016.

[27] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, “Computer Security Incident Handling Guide-Recommendations of the National Institute of Standards and Technology,” *NIST Special Publication*, 2012.

[28] S. Laube and R. Böhme, “Strategic aspects of cyber risk information sharing,” *ACM Computing Surveys*, vol. 50, no. 5, pp. 77:1–77:36, Nov. 2017.

[29] T. Moore, R. Clayton, and R. Anderson, “The Economics of Online Crime,” *Journal of Economic Perspectives*, vol. 23, no. 3, pp. 3–20, Summer 2009.

[30] J. Milletary, “Citadel Trojan Malware Analysis,” *Dell SecureWorks*, 2012. [Online]. Available: https://portal.secureworks.com/intel/mva?Task=ShowThreat&ThreatId=623

[31] FS-ISAC, “Financial Services Information Sharing and Analysis Center,” 2015. [Online]. Available: https://www.fsisac.com/

[32] R. Ackoff, “From Data to Wisdom,” *Journal of Applied Systems Analysis*, vol. 16, no. 1, p. 3–9, 1989.

[33] Verizon, “2015 Data Breach Investigations Report,” 2015.

[34] G. Wicherski, “peHash: A Novel Approach to Fast Malware Clustering,” in *Proceedings of the 2nd USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2008.

[35] Team Cymru, “#totalhash,” 2018. [Online]. Available: https://totalhash.cymru.com/

[36] The MITRE Corporation, “Collaborative Research Into Threats (CRITS),” 2014. [Online]. Available: http://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/collaborative-research-into-threats-crits

[37] C. Guarnieri, “Viper - Time to Do Malware Research Right,” 2015. [Online]. Available: https://github.com/viper-framework/viper/releases

[38] W. Shields, “Problems with PeHash Implementations,” 2014. [Online]. Available: https://gist.github.com/wxsBSD/07a5709fdcb59d346e9e

[39] G. Webster, Z. Hanif, A. Ludwig, T. Lengyel, A. Zarras, and C. Eckert, “SKALD: A Scalable Architecture for Feature Extraction, Multi-user Analysis, and Real-Time Information Sharing,” in *Proceedings of the 19th International Conference on Information Security*. Springer, 2016, pp. 231–249.

[40] Project MISP, “MISP Taxonomies and Classification as Machine Tags,” 2018. [Online]. Available: http://www.misp-project.org/taxonomies.pdf

[41] D. Dittrich, “So You Want to Take Over a Botnet ...” *Proceedings of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, pp. 1–8, 2012.

[42] B. Krebs, “’Mariposa’ Botnet Authors May Avoid Jail Time,” Mar. 2010. [Online]. Available: https://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time/

[43] L. Gordon, M. Loeb, and W. Lucyshyn, “Sharing Information on Computer Systems Security: An Economic Analysis,” *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461–485, 2003.

[44] J. Grossklags, N. Christin, and J. Chuang, “Secure or Insure? A Game-theoretic Analysis of Information Security Games,” in *Proceedings of the 17th International Conference on World Wide Web*, 2008, pp. 209–218.

[45] V. Buterin, “Notes on Blockchain Governance,” 2017. [Online]. Available: https://vitalik.ca/general/2017/12/17/voting.html

[46] F. Ehrsam, “Blockchain Governance: Programming Our Future,” *Coinbase*, 2017. [Online]. Available: https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74

[47] D. Mark, V. Zamfir, and E. G. Sirer, “A Call for a Temporary Moratorium on The DAO,” *Hacking, Distributed*, 2016.

[48] R. Böhme, N. Christin, B. Edelman, and T. Moore, “Bitcoin: Economics, Technology, and Governance,” *Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213–238, 2015.

[49] A. Mavridou and A. Laszka, “Designing Secure Ethereum Smart Contracts: A Finite State Machine Based Approach,” in *Proceedings of the 22nd International Conference Financial Cryptography and Data Security*, 2018.

[50] K. Finley, “A $50 Million Hack Just Showed That the DAO Was All Too Human,” 2016. [Online]. Available: https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/

[51] Financial Services Information Sharing & Analysis, “Operating Rules,” FS-ISAC, Tech. Rep., 2016. [Online]. Available: https://www.fsisac.com/sites/default/files/FS-ISAC_OperatingRules_June2016.pdf

[52] Department of Homeland Security Integrated Task Force, “Executive Order 13636: Improving Critical Infrastructure Cybersecurity, Incentives Study Analytic Report,” 2013.

[53] N. Szabo, “Formalizing and Securing Relationships on Public Networks,” *First Monday*, vol. 2, no. 9, Sep. 1997.

[54] V. Vishnumurthy, S. Chandrakumar, and E. G. Sirer, “KARMA: A secure economic framework for peer-to-peer resource sharing,” in *Workshop on Economics of Peer-to-Peer Systems*, 2003.

[55] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[56] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger,” *Ethereum Project Technical Report*, 2014. [Online]. Available: http://www.cryptopapers.net/papers/ethereum-yellowpaper.pdf

[57] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, “Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts,” in *Proceedings of the 2016 IEEE Symposium on Security and Privacy*, 2016, pp. 839–858.