Deconstructing Cybersecurity: From Ontological Security to Ontological Insecurity

Justin Joque
joque@umich.edu
University of Michigan

S M Taiabul Haque
haque@ucmo.edu
University of Central Missouri

ABSTRACT

This paper examines the philosophical aspects of cybersecurity through the lens of deconstruction, as proposed by the French philosopher Jacques Derrida. We offer deconstruction as an analytical orientation to better understand and challenge the very philosophical concepts a security system presupposes, arguing that not only are concrete systems necessarily insecure but that the concepts and structures through which their security is understood are also insecure. By centering our discourse on instability and contradictions, we demonstrate the relevance of deconstruction in cybersecurity through four concrete examples drawn from four different areas: digital rights management, cyberwar, software vulnerability, and user authentication. We further address the concept of ontological security to draw the boundaries between beneficial and detrimental uses of deconstruction. These insights complement other HCISec efforts to conceptualize cybersecurity as a holistic discipline that incorporates art and philosophy in addition to science and technology.

CCS CONCEPTS

• **Security and privacy → Human and societal aspects of security and privacy**; *Usability in security and privacy*;

KEYWORDS

Deconstruction, cybersecurity, ontological security

ACM Reference Format:
Justin Joque and S M Taiabul Haque. 2020. Deconstructing Cybersecurity: From Ontological Security to Ontological Insecurity. In *New Security Paradigms Workshop 2020 (NSPW '20), October 26–29, 2020, Online, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3442167.3442170

1 INTRODUCTION

More than two decades ago, two seminal papers in cybersecurity, "Why Johnny can't encrypt" [81] and "Users are not the enemy" [1], were published that influenced the community to focus on the underlying human factors in order to adopt a user-centered design approach. Since then, plenty of Human-Computer Interaction and Security (HCISec) research papers have examined these factors through surveys, interviews, and lab experiments [2, 31, 33, 34, 56]. Similarly, a growing body of research has investigated human economic behaviors that impact cybersecurity decision-making (for an overview, see [61]). This growing recognition of human factors has facilitated a paradigm shift in cybersecurity, so much as to consider it an art as well as a science [7]. However, while an increasing body of literature in computer science has incorporated philosophical aspects [4, 9, 16, 55, 75], little work has tested the philosophical concepts the notion of security presupposes.

In this paper, we take up Jacques Derrida's writing about deconstruction [24] to present a series of philosophical arguments showing the applicability of deconstruction to security research. We argue that deconstruction allows us the theoretical means to detail the instability of a host of concepts that are latent within discourses of security and are increasingly being unearthed by a growing body of research conducted under the umbrella of "a holistic approach to cybersecurity". While deconstruction is notoriously difficult to define due to its insistence that concepts are not stable, an element we do not seek to break with for reasons we present below, here we offer the reader some description that should help in making sense of the rest of the paper. Deconstruction aims to show how concepts and the discourses built around them are inherently unstable and ultimately insecure; it shows that at a philosophical and practical level, security is ultimately built on and requires insecurity. In doing so, deconstruction could be thought of as analogous to "philosophical hacking" (in the sense of being able to make a system function in ways it was never intended to) on multiple grounds:

- It is an activity that can be taken up with a diversity of goals, including malice, research, or to discover vulnerabilities in order to attempt to deal with them.
- What exactly it means or what falls under its purview is not fixed, especially as both technology and conceptual apparatuses change; early security researchers likely never could have imagined the breadth of vulnerabilities we confront now.
- What it may discover to be insecure or vulnerable can always be surprising, demonstrating through various means the insecurity of even those systems we believed did not require security; both deconstruction and hacking have a way of discovering insecurity where we least expect it.

To this end, we take as our starting point a shift from "security" discourse to "insecurity" discourse – that is, a discourse centered on instability and contradiction. We explain the larger stakes of deconstruction to identify these instabilities and contradictions, and the ways it calls into question the very idea of security or at the very least the primacy of security over insecurity.

Deconstruction provides a language and a means to explore the complex set of practices that are involved in cybersecurity and

NSPW '20, October 26–29, 2020, Online, USA

ACM ISBN 978-1-4503-8995-2/20/10…$15.00
https://doi.org/10.1145/3442167.3442170

thereby adds to literature that has overcome the definition of security as a trade-off [66, 73]. Deconstruction argues that the meaning of security is not fixed or unconditional, rather it is constructed through acts of speech or inscription. One of the central tenets of deconstruction is that writing, and with it all communication, is fundamentally insecure as a result of finitude – that is paper can be destroyed, letters forged, memories forgotten, and intentions misunderstood [22, 24]. Moreover, much of deconstruction is dedicated to showing how attempts to fix, preserve, or make secure end up creating new insecurities; Derrida's discussion of speech and writing could be summarized by explaining that much of European philosophy [67, 69] has thought of writing as simultaneously a cure for the insecurity of speech (i.e., writing solves the impermanence of speech by inscribing it on a physical medium) and a vulnerability in so much as it is significantly harder to authenticate writing than speech given by a known speaker [22, 24]. In sum, not only does security produce insecurity, but security requires insecurity as its very precondition (one could think here of the added security provided by writing information down such that it will not be forgotten simultaneously producing all sorts of new insecurities including the paper being destroyed, modified or read – these new insecurities are structurally part of the very benefits writing provides). In this way, the concerns of deconstruction are, perhaps surprisingly, very close to those of cybersecurity.

But, deconstruction goes further, and in this way we believe it has much to offer to the field of cybersecurity. Not only are systems necessarily insecure, but the very concepts through which we think them are given over to the same forces of vulnerability and insecurity. In short, deconstruction is capable of bringing to the fore the instability of concepts and structures such as systems, users, calculable trade-offs, security, etc. Additionally, deconstruction helps us view (in)security not only in relation to adversaries, but in a larger context of finitude (i.e., no form of inscription from writing to computers lasts forever and can always be forged, advances in the cost and speed of computation have outpaced older methods of cryptography [51], etc.).

Thus for us, "insecurity" takes on a much broader sense than is usually meant in cybersecurity discourse, but can still be thought of in terms of integrity (i.e., as outlined in the triad of confidentiality, integrity and availability). In this way, insecurity and security for us also encompass the integrity of concepts and of meaning; anywhere that concepts are contested – say for example, the meaning of a citizen or who should vote – speak to a lack of integrity of meaning and hence insecurity, but one that cannot be simply excised or firmly decided once and for all.

In order to demonstrate the ways in which deconstruction can illustrate the insecurity of concepts and thus aid in cybersecurity research, we explain some of the general principles of deconstruction in relation to security with four concrete examples drawn from four different areas in cybersecurity:

(1) Digital rights management: We discuss the Sony Rootkit scandal [38] and show how attempts to create one type of security, or security for a specific organization, can end up creating other types of insecurity. In light of Derrida's concept of autoimmunity [27], we take this incident as an example to highlight the importance of examining the philosophical and political assumptions inherent in cybersecurity decision-making.
(2) Cyberwar: Using cyberwar as an example of deconstruction [47], we explain how largely societal questions like truth, democracy, etc. – that have all been the subject of various works [19] dealing with deconstruction – are central to larger questions of cybersecurity but are themselves inherently insecure.
(3) Software vulnerability: We use buffer overflows to demonstrate an idea central to deconstruction that it can never be known with absolute certainty where a message will arrive [21] and this is precisely what goes wrong with a buffer overflow: a programmer expects data of a certain length but the data overflows the intended variable, leaving potentially malicious commands elsewhere in memory.
(4) User Authentication: We borrow the concepts of auto-affection and hetero-affection [28, 29] from deconstruction to destabilize the notion that the user is a stable, singular, and well understood individual. We argue that heterogeneity and temporality are two important factors of user identity that need to be addressed when designing an authentication paradigm.

Next we do a cross-case analysis to highlight the key concepts at stake and show the similarities and differences across the cases. We further extend our discourse on user authentication and connect it with the notion of ontological security [36] to demonstrate the ways in which centering insecurity can provide meaningful insights. We address Giddens' concept of ontological security [36] and juxtapose it with Croft's construction of ontological insecurity [18] to show how deconstruction can be used as a helpful lens for design and research pushing the design of systems to account for and plan for the instability of their very concepts.

In summary, our work offers insights to interpret the nature of cybersecurity in a postmodern world. We manifest that cybersecurity writ large cannot be extricated from larger philosophical, social, and political questions, and argue for the relevance of deconstruction as an analytical orientation that can help to unearth unarticulated philosophical assumptions in security discourse. We also outline further opportunities for the exploration of deconstruction in relation to cybersecurity. Our aim is to show that any system, whether conceptual or material, is ultimately insecure. This is in large part because it can never secure or stabilize the context in which it functions. For example, fundamental questions about the nature of democracy or the difference between data and instruction are always shifting and determined outside of the systems that use them such as a voting system or a database system. While much more can and should be said about both the relevance of deconstruction's underlying claims to cybersecurity and each of these examples, we outline them briefly in this paper to suggest the importance of this approach and to lay out a possible research agenda for future work. To the best of our knowledge, our study is the first of its kind to apply deconstruction directly to the analysis of digital security systems. We believe that our work contributes significantly to the growing discourse around conceptualizing cybersecurity as a holistic discipline [43] that incorporates art, science, economics, technology, society, politics, and philosophy.

2 BACKGROUND AND RELATED WORK

In this section, we first briefly introduce deconstruction and the associated concepts that are relevant to our examples in the next section. Next we discuss the application of Derrida's deconstruction in other domains outside cybersecurity in order to suggest the ways deconstruction can be applied to concrete questions. Finally, we give a brief overview of the related cybersecurity literature that questions the foundation of security.

2.1 Deconstruction

Deconstruction, originally described by the French philosopher Jacques Derrida [24], is a difficult concept to define, this is in large part because what it aims to "deconstruct" is the very insistence on clarity, transparency, and the simple presence of meaning to understanding. It has been conceived, both by Derrida and others, alternatively as a method of reading, a philosophical project, and a form of criticism (our focus will be on it as a method of analysis). In its most popular and straightforward rendition, deconstruction is the process of overturning systems and hierarchies, usually by showing that the minor term of a hierarchy is in fact central and then in a second move by erasing the very distinction between the two terms [22]. For example, in one of Derrida's most well known texts, *Of Grammatology* [24], he traces the history of the relationship between speech and writing, especially as they are presented in Plato and Rousseau, both of whom presume that speech is more authentic, clear, and meaningful than writing [67, 69]. He argues that the history of Western philosophy has been founded on privileging speech – which is understood to be a form of presence where the speaker can explain herself – over writing that has been imagined to be lifeless with its intended meaning always absent. He then shows how writing is in fact the central term, and that both writing and speech are forms of what he calls "writing in general", stressing the absence and insecurity of all forms of language. For instance, while a speaker is present in speaking, the speaker pulls from concepts, texts, and the entire history of a language that are all absent in the moment of speech. Throughout his extensive body of work, Derrida picks up many concepts from Western philosophy and demonstrates their internal contradictions and instabilities [22, 24].

Despite significant uptake and interest in deconstruction, in many fields this work is now thought of as esoteric and philosophically outdated. Moreover, both during Derrida's career and recently, commentators having taken issue with deconstruction and the larger philosophical movement of postmodernism, claiming that deconstruction has undermined the solidity of Enlightenment concepts such as understanding, truth, science, politics, and humanity [19]. Some have gone so far as to blame this work relatively little read outside humanities, for current problems with so called "fake news" and "post-truth politics" [19].

While we will not directly address these debates, we argue and demonstrate that deconstruction offers an especially helpful set of insights for cybersecurity. As deconstruction demonstrates how to carefully trace the instabilities in concepts questioning their foundations, it can help show the vulnerabilities in these concepts that are all too often taken for granted. Moreover, while the terminology may differ, deconstruction's focus on text, "writing in general", and their instability closely mirrors cybersecurity's interest in the integrity and security of information. Thus, we understand deconstruction not as a cause of any denial of truth but rather a means of confronting and dealing with the inevitable difficulties of any philosophical concept. In our minds, to blame deconstruction for any erosion of collective truth would be analogous to blaming cybersecurity researchers for the existence of the vulnerabilities they discover. While respecting the debates about what deconstruction is and is not, we see it potentially as a processes of questioning fundamental concepts, especially the very idea of security, that can help guide security research.

In this light, we can offer a definition, or perhaps more of a working hypothesis on what deconstruction could be for cybersecurity. Deconstruction can be understood as the tendency of systems or ideas to fall apart and undermine themselves. Therefore, in terms of cybersecurity, deconstruction can be understood as a principle of insecurity: namely that all systems and philosophical principles are at some level insecure and that they must inevitably confront that insecurity. In the world of cybersecurity, this is usually in the form of someone discovering the vulnerability, either maliciously or preventatively. So, throughout this paper, we use the term "system" in a much broader sense than is usually used in regards to computation. Following Derrida and his discussion, especially of structuralism, we use system to mean any arrangement of either concepts or structures that have some intended function or explanatory power [20]. Thus, software, machines, and democracy are all systems that rely on certain concepts and structures in order to function.

A second element can be added beyond this notion of insecurity: deconstruction can also name the process of finding and exploring the nature of this insecurity, mainly by testing the very philosophical concepts a system presupposes. Any attempt to secure a system must presuppose that we have some agreed upon definition of security; that we can identify security in contrast to insecurity. In general, computational systems allow some information to change, be shared and accessed; while other types of information should be maintained, kept confidential or inaccessible. In actually existing systems, the distribution of these attributes will depend on all sorts of philosophical, economic, and social categories such as legal personhood, citizenship, rights, ownership, sender, recipient, message, etc., that are often brought along unintentionally. These concepts are not neutral or completely stable. We aim then to show how their instability can be a necessary cause of insecurity that deconstruction can help in clarifying. Such a definition offers a helpful starting point and distills the one offered by Joque in "Deconstruction Machines" [47], where he argues that cyberwar should be understood as a form of deconstruction in both senses: the vulnerability of systems being exploited and the tracing of these vulnerabilities as a form of securing systems.

In this way, as mentioned above, deconstruction appears as analogous to philosophical hacking, especially if we think of it as a method for doing security analysis or at the very least as an approach that can inform security analysis. Deconstruction is thus what takes place when vulnerabilities are brought to light either by researchers or the functioning of some system or text in the world. By closely reading texts and analyzing concepts as they are used, deconstruction allows us to discover conceptual and philosophical

insecurity where many may assume nothing is amiss. Like hacking, deconstruction is not a single method, a formula or checklist that could be applied to every situation, rather its method depends on the system that is being analyzed and what is discovered there. Moreover, just like hacking, such discovery can be used both maliciously or in order to improve systems. Indeed, Sloterdijk describes the project of deconstruction as an attempt to build "a survival machine" that could somehow outlast the inevitability of insecurity that deconstruction discovers nearly everywhere [71]. While we do not necessarily share Sloterdijk's optimism about the possibility of creating systems that would be totally undeconstructable or completely secure, it still points towards a reading of deconstruction that would aid in the construction of more secure systems through the identification of otherwise unnoticed philosophical insecurities.

Deconstruction was developed throughout Derrida's extensive work and career, in which he utilized a whole host of terms to delineate and explain the ways in which deconstruction operates across domains. A number of these terms we will use below – e.g., autoimmunity and hetero-affection – but these terms all tend to speak to the instability of language and the subject that perceives it, and as such are both slippery and even resistant to simple definition. Thus, it is easier to explain these concepts in the context of the examples in the next section rather than attempt to provide a definition that fails to capture their nuance.

2.2 Derrida in Different Domains

Deconstruction began as a philosophical project but quickly found homes in a variety of disciplines. Recounting some of these "applications" of deconstruction can provide guidance into how deconstruction could be explored in relationship to cybersecurity. One of the first fields to take up deconstruction, especially in the United States, was literature studies. The scholars in this field built on Derrida's extremely close reading of texts to turn deconstruction into a method for analyzing literature, often turning texts against their traditional understandings [49]. A number of other fields in the humanities and humanistic social sciences adopted deconstruction in a variety of forms, including political science [76], visual arts [11], and history [62].

One example that can suggest the ways in which deconstruction has been adopted is in the fields of geography and cartography as exemplified by Harley's "Deconstructing the Map" [40]. He argues that in regard to cartography, the purpose of deconstruction is to promote "an epistemological shift in the way we interpret the nature of cartography. For historians of cartography, I believe a major roadblock to understanding is that we still accept uncritically the broad consensus, with relatively few dissenting voices, of what cartographers tell us maps are supposed to be. In particular, we often tend to work from the premise that mappers engage in an unquestionably 'scientific' or 'objective' form of knowledge creation", and concludes that "it allows us to challenge the epistemological myth (created by cartographers) of the cumulative progress of an objective science always producing better delineations of reality". From such a description, we argue that the purpose of deconstruction in cybersecurity should be similar: it should work to fully dislodge the assumption that the concept of security is scientific or objective [42]. Instead, deconstruction allows us to be attentive to the ways in which security is negotiated and socially produced.

One field that has done well considering deconstruction while still using it to inform decisions that could potentially provide inspiration for cybersecurity is law. Critical legal theorists and others have explored deconstruction as a means to better understand law and its similarly unstable and insecure foundations (for example: [14] [78] [48] [37] [68]). While there is always a danger that deconstruction turns into a completely nihilistic enterprise simply negating all concepts, these varied fields suggest the ways in which the close attention to philosophical foundations offered by deconstruction can ultimately be beneficial. Deconstruction provides a means for sharpening analysis and questioning moments of over-reliance on established concepts, especially in this context the idea of security, which necessarily smuggles with it a long history of philosophical ideas about people, governments, writing, truth, and permanence.

2.3 Foundation of Cybersecurity

Although our approach is different, we note that questioning the foundation of cybersecurity already began a few decades ago [60]. Landwehr argues that security research is at a rudimentary stage of an observational science [52], and efforts have been limited to offering taxonomy and basic concept specifications [3]. More recently, in their long-running influential agenda on making security research more scientific, Herley and Oorschot have recognized that there is a lack of clarity on what "scientific" means in the context of security research [42]. Similar to Landwehr [52], they identified different potential approaches and remarked that the community has yet to reach a consensus on the very nature of science of cybersecurity. As cybersecurity is still in its early days and it has been facing issues that are historically well-known in other scientific disciplines, they recommend that researchers in this area learn from past mistakes and adopt more scientific methodologies [42].

From the vantage point of philosophy, we call for a similar awareness about the instability and fallibility of cybersecurity but warn against any attempts to interpret cybersecurity as a discipline that could ever become completely objective or "scientific", at least in the sense that would require a complete and final definition of security. In their important work, Palen and Dourish point out that having a conceptual interpretive framework is important to unpack privacy for a networked world. They frame privacy as a dynamic process and discuss the associated tensions from a broader sociotechnical perspective [65]. We adopt a similar approach to unpack the complex dynamics of digital rights management and cyberwar.

In their work, Jackson et al. propose the "broken world thinking" perspective by bringing the discourse of repair and maintenance to the fore [44, 45], which is often undervalued compared to designing new and innovative technologies. By acknowledging the importance of repair and maintenance, they advocate thinking with insecurity rather than security and highlight the importance of considering not only the first user, but also the last one. Our work proposes a similar perspective by emphasizing instability and insecurity. However, our approach is different because we focus

on analyzing how meaning and concepts are created and communicated, whereas they focus on the practical side of repair and maintenance activities.

Especially notable for our concerns around notions of identity and user experience, Baumer and Brubaker have argued that while the concept of "the user" has been beneficial, it has limited usability researchers in certain extent to addressing situations in which a unitary user is the intended subject of a system and its design [6]. They outline a number of philosophical and practical levels at which the concept of the user breaks down, especially in the case where someone affected by a system is not considered a user (e.g., a photo of someone who does not have an account is posted to social media by someone else). In response, they argue for "post-userism", which they state does not necessarily help solve problems, but helps frame problems more inclusively. Our work is informed by all these different approaches that question the foundational concepts of cybersecurity.

3 DECONSTRUCTING CYBERSECURITY

In this section we offer four instances of insecurity and suggest the ways in which deconstruction can provide a frame to understand the stakes.

3.1 Digital Rights Management

Our first example uses the Sony rootkit scandal and the Derridean concept of autoimmunity to attempt to show how the multiplicity of actors and understandings of security complicate any attempt to calculate ideal trade-offs. In 2005, it was discovered that Sony BMG had included a rootkit on approximately 22 million CDs [38]. When inserted into a computer, the CDs modified the computer's underlying operating system in order to prevent copying of the CD. The software also sent data on the user's listening habits back to Sony and exposed the computer to additional malware from unrelated attackers. The intent of the software, which was ostensibly a form of digital rights management, was to protect the copyright of the music, but it is clear in hindsight that there were many unintended consequences of the way in which this was approached.

Many security researchers have acknowledged that security is always a question of trade-offs [70] and trade-offs are important considerations for cybersecurity risk management as well. For example, NIST Special Publication 800-37 – a popular risk management framework – recommends considering trade-offs as potential inputs for preparing risk management strategy and statement of risk tolerance [64]. For the Sony rootkit case, security for one group (the recording industry) was produced at the cost of insecurity for other groups (music listeners). Deconstruction, however, goes further than this concept of calculable trade-offs, especially the idea that we could make "sensible" trade-offs. The entire notion of "sense" and the ability to evaluate and calculate these trade-offs require that one could step outside of the system and evaluate it objectively. But, this is precisely what digital insecurity calls into question. The ability to calculate these trade-offs requires one start from a secure experience of calculation and computation.

While this may seem abstract and perhaps belie the common sense notion that we can in fact determine what trade-offs are worth making, this suggests how complex this is in practice and the extent to which these calculations are complicated by the sheer number of actors, with very different goals, involved in any process of computing. It is highly unlikely that most purchasers of these CDs or the creators of their machines or operating systems even considered the possibility that Sony would include a rootkit and thus such a trade-off could never be properly calculated for the vast majority of actors involved in making a whole host of security decisions around their machines and their design and use.

A central concept of Derrida's later work, autoimmunity, is especially helpful in showing what is at stake here [27]. Derrida describes this process as "that strange behavior where a living being, in quasi-suicidal fashion, 'itself' works to destroy its own protection, to immunize itself against its 'own' immunity" [27]. For Derrida, this concept is not an exclusively biological one and takes on a deeper philosophical meaning, of which he states, "It is not some particular thing that is affected in autoimmunity but the self, the ipse, the autos that finds itself infected" [27]. That is the very coherence of the system as a system is at stake in autoimmunity.

What at first glance appears as the simple act of listening to music appears after further analysis to require taking into account the entire history and social structure of intellectual property relationships. Thus, the very concept of security is contested and dependent on the context in which one designs a system to be secure; moreover attempts at securing a system always run the risk of creating even more insecurity. Deconstruction often works by adding additional terms for consideration [25]. Similarly to hacking, additional contexts, considerations, inputs, use cases, etc., are added in order to allow a system to do something that it was not designed to (or to show that it was already doing something it was not supposed to like leaking data or in this case adding additional vulnerabilities). So, deconstruction allows us to see and explore what might at first glance seems agreed upon, fixed and stable, including even our understanding of what security is, or how it relates to insecurity.

In a perhaps unexpected way, security requires insecurity; for a perfectly secure, hermetically sealed system can only be one that does absolutely nothing – any interactivity is a type of insecurity. In instances where attempts to secure one portion of a system (e.g., copyright) undermine some other component of security (e.g., exposing a computer to malware), it is not simply a question of trade-offs but the very nature of what it is that the system is "supposed" to do. The multiplicity of actors means that such systems always have a multitude of interpretations of what they are supposed to do and what is valued.

3.2 Cyberwar

The ways in which both insecurity and deconstruction challenge conventional notions of security, especially as a paradigm of evaluating trade-offs, is even more apparent in regards to cyberattacks, especially the types that have been associated with the 2016 US presidential election [41]. These types of attacks are demonstrative for three interrelated reasons:

(1) They offer a prescient example of exploiting human and social factors to attack digital systems; that is, to say that voting systems can be attacked both through the computational infrastructure that tallies votes and through the information

systems (e.g., media, government, etc.) that surround the process of voting.
(2) Attempts to confront these larger social issues through the framework of cybersecurity suggest the difficulty of considering security without its social context.
(3) To fully accept the importance of social, political, and economic structures means recognizing that in context, even the meaning of "security" is contested and thus insecure. In this way, these sorts of cyberattacks both provide an example of adversaries applying the principles of deconstruction (i.e., destabilizing concepts) and of how deconstruction can aid in security analysis.

For example, writing about these types of attacks, which they term "soft cyber" attacks, Farrell and Schneier argue for understanding governments as information systems whose vulnerabilities can be addressed by analyzing attack surfaces [32]. They further argue that political knowledge can be understood as either common political knowledge or contested political knowledge, and that various forms of government distribute what is and can be contested differently. Thus for them, democratic systems of government "are vulnerable to information attacks that widen contested political knowledge so that it spills over into disagreements over the common political knowledge that democracy needs to operate" [32].

The problem with such an approach, and one that deconstruction can help to explain, is that this division between common and contested political knowledge is always politically and historically determined. That is, to say that there cannot be a universally correct answer to how these should be divided, instead their very division is contested through politics. For example, Farrell and Schneier offer among their possible solutions to these vulnerabilities that common political knowledge should be defended. They suggest the Census as one place this should be done, trying to prevent attempts at "excluding portions of the population" [32]. But, one only has to look to the most general account of history, such as the infamous Three-Fifths Compromise where the enslaved Black population of the American South was only counted as three-fifths of a person, or the 1870 Cremieux Decree which granted Jews in Algeria French citizenship and its 1940 revocation by the pro-Nazi Vichy regime, to appreciate that who constitutes the population and how they should be counted have always been fundamentally political and contested questions [57]. Moreover, beyond the Census, exactly how votes should be counted and who should be allowed to vote have long been politically contentious. Arrow's impossibility theorem even brings mathematical rigor to the challenge of converting individual preferences into democratic force [35].

It is precisely in relationship to these questions of democracy that Derrida develops the concept of autoimmunity, tracing the ways in which many of the attempts to "secure" democracy are simultaneously anti-democratic. For example, ending the recount of the 2000 US Presidential election (an election where Al Gore won the popular vote [5]) can appear either as an attempt to secure and protect common political knowledge or a gross negation of the rule of law. Derrida states this directly: "one will never actually be able to 'prove' that there is more or less democracy in granting or in refusing the right to vote to immigrants, notably those who live and work in the national territory, nor that there is more or less democracy in a straight majority vote as opposed to proportional voting; both forms of voting are democratic, and yet both also protect their democratic character through exclusion ... One electoral law is thus always at the same time more and less democratic than another; it is the force of force, a weakness of force and the force of a weakness; which means democracy protects itself and maintains itself precisely by limiting and threatening itself" [27]. These questions of democracy cannot be reduced to technical analysis and are always fundamentally political and philosophical questions.

We should not be surprised then when Farrell and Schneier conclude that there is ultimately a tension between attempts to secure common knowledge and allow other knowledge to be contested. There is operative here something of an ouroboros – that ancient symbol of the snake eating its own tail – of security and insecurity. What must be secured is the very possibility of insecurity itself (i.e., political contestation). We do not pretend to offer a complete account of how this tension should best be managed. In the case of these attacks against democratic governance, it is possible to see simultaneously the inability of traditional notions of security to account for the deep philosophical unmooring these attacks portend and the extent to which the language of autoimmunity and deconstruction can address the stakes. While deconstruction offers little guide for how to answer these questions, we believe it provides a powerful framework to ask them and to trouble some of the assumptions that often follow technical analyses into socio-political realms, as cybersecurity must be understood by its nature to be both political and philosophical [13].

Such concerns very quickly expand beyond cybersecurity to the nature of democracy, yet it is telling that Farrell and Schneier both feel compelled to address "soft cyber" attacks at all and that they propose these attacks can be understood within a framework of information security. Thus, while their article attempts to expand information security approaches into the realm of politics, we suggest the opposite lesson should be learned from the attacks on the 2016 election: namely, that cybersecurity is always a philosophical, political, and social question. Exclusively securing voting machines cannot provide any meaningful security if the rest of the process is wholly compromised. While researchers are well aware that election security is now a question of international politics and security, that securing machines is not merely enough [8], deconstruction allows us to see that the very notion of security is exposed to philosophical questions and the necessary insecurity of autoimmunity that deconstruction entails [27]. In short, it is not possible to simply set aside politics and philosophy or to bracket and address only security questions; this ouroboros cannot simply be disentangled.

3.3 Software Vulnerability

Next we offer buffer overflow as a significantly more constrained example of how deconstruction can provide a means to explain a common vulnerability by showing how the focus on writing and the variability of interpretation can affect security– and conversely how issues of cybersecurity can show what is at stake in deconstruction. To put it simply, a buffer overflow happens when more data is written to a variable than there is space in memory and the additional data overflows into surrounding memory [15]. If this is a result of an accident, it can cause a program or system to crash,

but it can also be exploited purposefully to deposit malicious code, which will then be run on a targeted machine, potentially giving adversaries complete access to the machine.

One recent example suggests how important a single buffer overflow vulnerability can be. In May 2019, WhatsApp – the very well used encrypted messaging and call software that is now owned by Facebook – reported that a buffer overflow vulnerability in its VoIP (Voice over IP) stack had been exploited to install software that could monitor targets' phones [53]. The vulnerability allowed attackers to deliver the payload simply by calling the target and not even require the target to pick up the phone.

While technical solutions to buffer overflows are well known (e.g., checking inputs, using languages and libraries that protect against these vulnerabilities) [15], legacy code and failures to implement these protections still leave a relatively large number of systems and software vulnerable to buffer overflows. Their functions can help demonstrate the relevance of deconstruction to digital security. Crandall and Oliveira describe buffer overflows as fractures in interpretative frames as information flows across boundaries in abstractions (e.g., programming languages, locations in memory, etc.) [17]; thus what buffer overflows represent is a mismatch or insecurity of abstract concept – information that in one place is supposed to be data but somewhere else is instruction.

One of the central elements of deconstruction is the necessity of being open to the unpredictable arrival of what is "other", what is unexpected [26] and misinterpretable. In Derrida's later work, this takes on a nearly ethical meaning, but it also describes a technical fact of insecurity. This is ultimately what makes writing, and with it all technology and language, fundamentally insecure but also productive. Writing always exists outside of the author, secured in one way against forgetting, but insecure in another, exposed to destruction, rot, forgery, etc. What can happen to writing is due simultaneously to its exposure to others and to time. Through this philosophical discussion of the message, we can understand the centrality of insecurity to deconstruction; if all messages were completely predictable, if they told us nothing new, they would be utterly meaningless. This is in many ways the same problem we face with computer security, computers are powerful information processing machines because they can process arbitrary inputs. While doing the exact same task over and over again may be beneficial for the processing of physical material in a factory and in individual computations where we need results to be accurate and replicable, but at the level of entire computational systems or software, we require them to be able to create novel outputs on inputs we do not directly plan for.

Furthermore, for deconstruction, one of the central elements of language is that its meaning is never fixed and texts can always be turned against themselves and their authors' intent because language is neither hermetic nor static. Derrida states, "The writer writes in a language and in a logic whose proper system, laws, and life his discourse by definition cannot dominate absolutely" [24]. Language can always be destabilized by reproducing it in unexpected contexts.

This is precisely what we see happening in buffer overflow vulnerabilities: what ultimately makes the von Neumann architecture-based digital technology so powerful is the co-location of data and instruction [79]. That is, to say that memory can hold both instructions and data and read one as the other. In essence, a buffer overflow vulnerability arises because a programmer expects the user to input only data but instead receives a surplus of data along with instructions that are deposited into unexpected locations in memory. It is ultimately the very flexibility and openness, which makes computers so powerful, that leaves them vulnerable to these accidents of language and address. Thus, what constitutes a buffer overflow in this philosophical language is an inability, often due to accident, of the programmer to foresee the input (i.e., the exploit of the buffer overflow vulnerability) that would turn the program against itself.

It is worth mentioning the philosophical ramifications of the halting problem here [77]. According to the halting problem, a program's output fundamentally cannot be predicted without running it, which essentially means that it is not possible to predetermine all "safe" and "unsafe" actions because new bugs will constantly be found as new states are further explored. Ultimately, buffer overflows are indicative of a larger deconstructability of computers and programming in general; of the fact that their openness means that software and machines can be used in unexpected ways, exposed to unexpected inputs, that challenges any system that assumes it can predict all possible messages or usages. In short, computers address not something permanent and fixed but an address in memory whose contents can always be other than what is expected. While of course it is possible to prevent specific buffer overflows, and this is a worthwhile goal, this analysis suggests the impossibility of ever doing away with the vulnerabilities inherent in combining data and instruction (in von Neumann architecture) and allowing users to input arbitrary strings of data – two elements that are arguably necessary for computing to be worthwhile. Again, we see here the potential value of deconstruction in its ability to expose and clarify the very limits of security.

What deconstruction explains here offers no easy way out; we confront a paradox wherein the very conditions of computation (and writing in general for deconstruction) are causes of insecurity. Moreover, there is no ideal balance that would allow us to optimize for just the right amount of insecurity and security. By decentering the stability of information and writing, deconstruction again can show what we may hope to secure is never actually secure, but rather always fleeting and pointing elsewhere. It is ultimately through recognizing this inherent and incalculable instability, rather than ignoring it, that better systems can be designed.

3.4 User Authentication

Our final example turns to the concept of the user, especially in regards to authentication, in order to show how the deconstruction of the subject (which played a central role especially in Derrida's early work) relates to cybersecurity. While user-centered design has allowed the usability community to consider and design for the ways humans actually use computers, it is based on a concept of the user that does not necessarily account for the complexity of human life and the philosophical challenges contained therein. In the case of authentication, the user is not simply someone who uses a system but someone who uses a system again; that is, the system is designed such that the user can be re-authenticated to resume their work. We are thus dealing with an individual who

has some legitimate claim to use a system and who persists across time – who in short maintains this legitimacy through time. This ability to maintain oneself through time is central to the philosophical concept of identity, and a major target of deconstruction's critical apparatus. Identity sits at the center of many European philosophical concepts [54], especially in so much as it provides a supposedly stable site from which the individual can contemplate and understand the world. We can see the operation of identity at play in the privileging of speech over writing mentioned in the earlier section, for what makes speech appear fully present is that the speaker can maintain their identity and hence fully explain themselves, whereas with writing the word and the individual who wrote them can potentially be separated.

It is here that we can approach the deconstruction of auto-affection and hetero-affection [28, 29]. The concept of auto-affection (also known as self-affection) traces its origins to Kant [50], and names one of the basic operations of European philosophy, namely the processes of reflecting upon oneself [12]; in essence being simultaneously the object and subject of thought. Auto-affection is a very important concept in Derrida's work as its deconstruction can be understood as at work in many of the other concepts he seeks to deconstruct.

Auto-affection occurs when an individual affects herself, when the affecting is the same as the affected; or put otherwise when the thinker is also the object of thought. An intuitive example of auto-affection is speaking to oneself, where one may believe that there is nothing external between hearing and speaking, and where there is a negligible amount of time differentiating the act of speaking and hearing [29].

Derrida argues that despite this perception, the individual does not auto-affect herself in this strict sense; rather her acting upon herself is always on the other that she is. Derrida terms this actual process a hetero-affection [28], and explains that this process of affecting one's self, of thinking about one's self "is not something that happens to a transcendental subject; it produces a subject. Auto-affection is not a modality of experience that characterizes a being that would already be itself (autos). It produces sameness as self-relation within self-difference; it produces sameness as the nonidentical" [29]. Thus, the entire process of self-contemplation makes one other than oneself. One contemplates oneself through language, history and society, and through this is affected by all of these elements that exist outside of oneself. The very process by which we imagine ourselves to be the same is in the final analysis that makes us differ from ourselves.

The user is not a singular entity that sets herself a clear task and carries it out, all the while reflecting exactly what she wants to do. She is instead pulled in multiple directions: forgetting passwords, reusing passwords, giving a password to an acquaintance so they have access to a streaming service, etc. This is already well-known and understood as the purpose of user-centered design. Yet, this deconstruction of identity and auto-affection calls us to go further. It calls us to ask how this process of self-reflection, especially in regard to the user's desire for security, produces these actions and values in the user. As mentioned above, according to Derrida, this process of self-reflection does not happen to an already existing subject (or user) but rather produces a subject. This resonates with the arguments presented by Vuorinen and Tetri in their work on ontology of information security [80]. They claim that everything that is connected to security, including user and information, also becomes subjected to it and explains how individual users become modified by this subjection.

Malabou further explains this phenomenon: "The other who is affected in me and the other who is affecting me are definitely not one and the same ... the feeling of existence is thus never present to itself, but always disarticulated. It is not the feeling of my existence, but of the other's existence in me. The temporal difference that lies at the heart of the 'I' is the difference between me and the 'intruder', the other of me in me" [59]. Malabou here draws out two points that are critical for our present concerns. First, her use of the term "intruder" to describe this other is notable in that it immediately suggests the ways in which hetero-affection is directly an issue of security. Hetero-affection is the primary grounds upon which we betray our best intentions when it comes to security. It is always this other that we are that makes the user such a difficult concept.

Second, the issue of hetero-affection bears an important relationship with temporality. We could say that one of the primary elements of the experience of hetero-affection is the experience of time in a way that is similar, or perhaps the inverse side, of the temporality of authentication: namely, the user who returns to be re-authenticated is different in so much as time has affected them. Each and every user likely tells themselves to remember their passwords, but over the course of time many fail to listen to themselves.

So, for instance, when Bonneau et al. state, "we assume that ordinary users won't necessarily follow the often unreasonably inconvenient directives of security engineers, such as never recycling passwords, or using randomly-generated ones" [10], or Haque et al. measure the level of comfort when constructing a strong password [39], the question of why this happens becomes more complicated than simply convenience. Perhaps more accurately the point becomes that this very concept of convenience is cross cut by the entire field of the subject's hetero-affection and the complex temporality that founds it, all the while subjecting the subject to insecurity.

To summarize, deconstruction problematizes any simple notion of identity, especially across time. This deconstruction of identity suggests that the concept of the user is more complicated in two critical ways: first, as we have just argued, in so much as the heterogeneity of the user and their self-understanding bring insecurity to the fore of our analysis and, second, this temporal hetero-affection implies that the user who returns always holds within it a kernel of difference. That is, time affects the user such that the user who returns is not wholly synonymous with the user who arrived in the first instance. While researchers have begun to question the usefulness of the concept of the user [6], through deconstruction we arrive at a more fundamental and unsettling conclusion: the subject, or user, just like systems are at their root, ultimately insecure. The very possibility of security is founded upon and circumscribed by an originary insecurity. The subject's interaction with the world requires its exposure and risk, and hence insecurity. Most importantly, this means that there is not some originally secure subject who risks themselves, just as a usable system requires insecurity in the form of interactivity, the very concept of the self is struck

through with its insecurity. Deconstruction can thus help to show how radical insecurity truly is.

4 CROSS-CASE ANALYSIS

Each of the above examples takes up different elements of security and deconstruction, ranging from the actual code and data stored in memory to the individual and political context in which computers are used. In all of these cases, both deconstruction and insecurity appear in perhaps significantly different guises, but what unites them all in their breadth is a non-fixity and insecurity of critical concepts. That is, to say that even inside these systems, key concepts take on multiple and contested meanings, which are further convoluted by the variety of actors who both want and understand things differently. The multiplicity of actors and elements that should be secured (e.g., intellectual property rights, listener's computers, competing notions of citizenship, etc.) in the case of digital rights management and cyberwar makes calculating trade-offs incredibly complex and tied to a host of legal and economic systems. Likewise, with buffer overflow vulnerabilities, the unpredictability of messages and the necessity of always bounding memory and checking inputs complicate attempts to keep software secure. Finally, in user authentication, we see that even the bounds of the individual user are not fixed and hence contested and insecure.

In each of these examples, critical concepts upon which any notion of security rests already admit a level of alterity and unpredictability; they all function by way of folding something insecure, contestable, and unpredictable into their functioning: rights, citizenship, input, users, etc. For these systems to function in a meaningful way, they must include these elements, but these elements guarantee their insecurity and instability. Moreover – and this is the most important point – their meaning must be negotiated and contested internal to the system; there does not exist some wholly external and stable place from which their meaning can be derived. While, of course, one can and must look elsewhere for the meaning of these terms (e.g., in the case of the US, to the constitution, laws, and court rulings for the meaning of citizenship), those concepts are not fixed there either; instead they are mutable, contestable, and insecure there as well, introducing further vulnerabilities into the system. For example, in the case of elections, the outcome of any given election can affect citizenship laws that will then affect future elections. These generally assumed outside places of stability become vulnerable through the very systems that rely on them.

Deconstruction then provides us a means of tracing these instabilities, these conceptual insecurities. Like hacking, this can either be used to actively undermine systems, simply better understand what is happening and how a system works or to help design better systems by recognizing the limitations and insecurities inherent in the systems we are working with. It is in this latter use of deconstruction that we feel it can be most helpful for security research.

Example	Key Concepts at Stake	Key Ideas from Deconstruction
Digital Rights Management	Security; Trade-offs	Autoimmunity; Intertextuality
Cyberwar	Political Knowledge; Trade-offs	Autoimmunity
Software Vulnerability	Address; Memory	Message; Arrival from elsewhere
User Authentication	User; Identity	Auto/hetero-affection

Table 1: Cross-case Analysis

5 DECONSTRUCTION AND ONTOLOGICAL SECURITY

Much of the discussion of cybersecurity, along with national and personal security, assume an inviolate subject (whether the user, nation, or corporate entity) – one who is ontologicaly secure. Here we use ontology not in the traditional computer science sense of a definition of sets of categories, things and relations, but rather in the philosophical sense of a theory of what exists and what its essence is. The concepts of ontological security and insecurity offer a fruitful lens to understand the ways in which deconstruction can help move away from the presumption of a stable user or system and our ability to analyze security more generally. Ontological security was originally proposed as a concept by Giddens to describe the psychological need for one's world, or reality, to appear consistent and have meaning [36]. So, ontological security is a perpetual process of securing reality, not only in its existence but in its meaning and its predictability. To offer a possibly mundane example, one daily expects to be able to successfully login to their email account; and if for some reason they are unable to do so, this can be disorienting and possibly even frightening (especially in the case where one may suspect their account has been hacked). Thus, much of what we consider cybersecurity is a form of ontological security: we expect the data that we store digitally to act in predictable ways and be accessible when we need it.

While the value of ontological security is clear, the presumption that insecurity should be seen as a brief interruption in an otherwise secure experience is less so. Croft, in tracing the period since 9/11, demonstrates the ways in which the state and other social forces engaged in a process of ontological insecuritization of British Muslims, largely through treating the Muslim community as a security threat outside of the rest of the population [18]. Likewise, Noble, while not directly using the term ontological insecurity, demonstrates the ways in which anti-immigrant sentiment in Australia has undermined ontological security among migrants [63]. Just as in the case of democracy above, and its attendant questions of who counts and how, this work makes it clear that ontological security is not a given and that there is a tendency to insecuritize certain groups, especially along ethnic, racial, and religious lines as well as based on the place of birth. Moreover, what these examples make evident is that the very notion that security is a trade-off risks constructing an approach which ignores the ways in which that framing predetermines the economy under which these trade-offs are evaluated; that is, that the security of certain elements is prioritized almost guarantees the insecuritization of others. For example, in the case of the Sony rootkit, the framing of the problem from Sony's perspective around copyright produced

other forms of insecurity. That is, to say that it overlooks the ways in which security systems tend to be auto-immune; risking greater insecurity through the very process of attempting to secure.

Thus, to put the insights of deconstruction as directly as possible, it could be said that many of the discourses around security that treat security as a set of trade-offs still assume the basic condition we confront is one of ontological security. Even if something like absolute security is impossible and trade-offs must be made, the standard approach tends to assume that ontologically secure designers design systems for ontologically secure users. But, deconstruction flips this, arguing that the condition from which we should understand systems and their security is from the level of ontological insecurity. While one may be able to build a system that provides some level of predictability and consistent functioning, for deconstruction, vulnerability, accident, and insecurity are the rule rather than the exception. As Derrida famously states, "A letter can always not arrive at its destination" [21].

More generally, deconstruction allows us, through the process of close reading and philosophical reflection, to test some of the key concepts that underlie any security system or approach to cybersecurity, such as trade-offs, the user, etc. Still, a deconstructive approach to cybersecurity almost necessarily has a few key limitations. Two key misreadings or dangers of deconstruction are immediately apparent and should be addressed. First, as explained above, deconstruction resists being translated into a specific program or agenda. On the other side of the same equation, there is a risk that deconstruction appears too clearly and succeeds in becoming a method, especially one that would be equated simply with thinking critically about concepts. While there is no reason to oppose such critical thinking, the field is already engaged in thinking critically about security. Thus, such a reduction to critical thinking would likely result in deconstruction providing little additional benefit.

6 DISCUSSION

This is the first study to date that we are aware of that specifically applies deconstruction to the analysis of digital security systems. We have utilized numerous readings of Derrida to deconstruct different concepts in cybersecurity. We now present a few guidelines in regard to the use of deconstruction in cybersecurity.

First, for deconstruction to be beneficial for cybersecurity, it must avoid two poles: refusing either to be a mere reflection that provides no guidance nor an empty method of critical appraisal. Rather, it must provide a means of closely reading and examining key philosophical assumptions that otherwise would go unnoticed and unexamined. Thus, its real power and promise is that it can help draw our attention to the insecurity of those concepts we use but are most likely to overlook.

Second, the basic insights of deconstruction are, perhaps surprisingly, closely aligned with the work of cybersecurity. Deconstruction stresses the centrality of finitude, misunderstanding, loss, and insecurity in order to demonstrate how fragile many of our assumed philosophical principles are. One of the central concerns of deconstruction is the insecurity of writing and the impossibility of anyone completely mastering it; in this telling, writing and with it all language is always a trace, never completely present and thus always capable of saying something that was not intended. While deconstruction is often written in a dense philosophical language, this fundamental insight is central to nearly every question of cybersecurity. As much as we may draw distinctions and differences between physical writing and digital systems, at a deep philosophical level, the challenge of cybersecurity is ultimately founded on the fact that writing is uncontrollable and insecure (e.g., a letter can be spoofed, a message can fail to arrive, writing can be altered without its owner or author knowing, etc.).

Third, recognizing temporality and finitude, in short insecurity, not only at the level of systems but also at the philosophical level of basic concepts allows us to see insecurity where we otherwise may not. We are then left with a question of what security can mean and whether or not it continues to be a useful concept. We still believe that the notion of security is helpful, but that if we admit the insights of deconstruction, what becomes notable is that "security" can only be defined within the coordinates of a system or process; moreover, that definition will always rely on concepts, systems, individuals, etc., that lie outside of those coordinates. That is to say that security itself can be helpful in articulating aims and purposes, but that it's very definition is both contextual, insecure, and shifting.

This insight, in turn, will help us to better design systems to handle this insecurity. The notion of security can help to define and communicate our goals, but it is essential to recognize that it is never closed nor settled. Moreover, such recognition opens up potential avenues of research that consider how we may proactively imagine these concepts, such as that of the user, otherwise. Furthermore, while deconstruction offers few answers and instead calls us towards a constant process of questioning, we still believe that it can help guide the process of creation and design.

For example, the user could be considered a function of time to address the discrepancy between hetero-affection and security. By stressing user's heterogeneity and tendency to change over time, more usable systems could be designed for repeating security or privacy tasks such as authentication, installing security updates, or posting sensitive contents on social media.

Finally, despite deconstruction's insistence on the instability of writing and identity, it does not call for a complete nihilistic destruction of these concepts, rather it also shows how these concepts can and do still function despite their deconstruction. Thus, deconstruction in general, alongside the writings of Derrida and others committed to this work (e.g., Catherine Malabou [58], Gayatri Spivak [72], Barbara Johnson [46], Bernard Stiegler [74], etc.), offers a host of insights into the fundamental insecurity of existence and technology that are directly relevant to cybersecurity. In this paper, we have focused all too briefly with a few examples, but many other concepts such as system [20], memory [30], translation [23], etc., have been explored within deconstruction and its literature in ways that are directly relevant to cybersecurity research.

Beyond these guidelines for cybersecurity, our work has broader implications for usability in general. Our deconstruction of user identity and authentication reveals the heterogeneity of the user in each instance and across instances. This destabilizes the notion of the user as a singular and well understood individual and highlights the insecurity of the user-centered design approach on a philosophical level. We thus propose augmenting the user-centered

design approach – which both asks what users want and in a way produces a certain type of user – and begin exploring what else a user could possibly be. Moreover, we see these brief examples and explorations as the foundation for a long term research project that would attempt to bring the philosophical insights of deconstruction to answer many theoretical and practical questions of cybersecurity.

Thus, while it is important that deconstruction not be reduced to some sort of checklist that could be reviewed as an element of security analysis, it can also serve a directly productive role. Especially if we think about deconstruction as analogous to a form of philosophical hacking, it can serve as a means to continually test our systems and assumptions. If in this context we were to imagine a sort of "applied deconstruction", it might look something like a process of continually testing the concepts and language we use to describe and do security work, never assuming that any concept we may use is fundamentally secure: user, identity, system, trade-off, citizen, memory, message and especially the idea of security itself. Instead, we should ask after each concept, what does this concept do and what stable points of reference does it rely on? Then, if we admit alterity, insecurity, and contestation into that concept, how does that reformulate both the understanding of a given system's security and what else could the system possibly do? In this way, deconstruction becomes exactly what the name suggests: a way to carefully take things but especially ideas apart, ask how they work, and allow us to see if perhaps there may be some different ways for them to be put together, while recognizing that no arrangement will be stable or secure forever.

7 CONCLUSION

In this work, we adopted deconstruction as an analytical orientation to understand the challenges in cybersecurity on a philosophical level. By making a shift from "security" discourse to "insecurity" discourse, we focused on instability and contradictions to show the relevance of deconstruction in cybersecurity for important areas such as digital rights management, software vulnerability, cyberwar, and user authentication. We used ontological insecurity to stress the ways in which identity and concepts tend to fall apart rather than hold together in order to argue that we must confront insecurity as the basic condition of things and security as the exception. Taken together, we believe deconstruction contributes significantly to the advancement of philosophically-informed research in cybersecurity.

ACKNOWLEDGMENTS

We would like to thank our shepherds, Laura Kocksch and Tom Walcott, who provided valuable feedback in the development of the current version of this paper. We are also grateful to the anonymous reviewers for their thorough review of our work.

REFERENCES

[1] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (December 1999), 40–46.
[2] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. 2015. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Seoul, 3523–3532.
[3] Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr. 2004. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing* 1, 1 (2004), 11–33.
[4] Jeffrey Bardzell and Shaowen Bardzell. 2016. Humanistic HCI. *Interactions* 33, 2 (2016), 20–29.
[5] Larry M. Bartels and John Zaller. 2001. Presidential vote models: A recount. *PS: Political Science and Politics* 34, 1 (2001), 8–20.
[6] Eric PS Baumer and Jed R Brubaker. 2017. Post-userism. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 6291–6303.
[7] Matt Bishop. 2018. *Computer security: Art and science*. Addison-Wesley, Boston.
[8] Matt Blaze. 2019. Testimony of Prof. Matt Blaze. https://www.mattblaze.org/papers/blaze-homelandsecurity-20191119.pdf
[9] Mark Blythe. 2014. The hitchhiker's guide to ubicomp: Using techniques from literary and critical theory to reframe scientific agendas. *Personal and Ubiquitous Computing* 18, 4 (2014).
[10] Joseph Bonneau. 2012. The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes. In *IEEE S&P*.
[11] Peter Brunette and David Wills. 1994. *Deconstruction and the visual arts: art, media, architecture*. Cambridge University Press Cambridge.
[12] Miles Burnyeat, M. J. Levett, and Plato. 1990. *The Theaetetus of Plato*. Hackett, Indianapolis.
[13] Myriam Dunn Cavelty. 2007. *Cyber-security and threat politics: US efforts to secure the information age*. Routledge.
[14] Drucilla Cornell, Michel Rosenfeld, and David Gray Carlson. 2016. *Deconstruction and the Possibility of Justice*. Routledge, London.
[15] Crispin Cowan, Perry Wagle, Calton Pu, Steve Beattie, and Jonathan Walpole. 2000. Buffer overflows: Attacks and defenses for the vulnerability of the decade. In *DISCEX*.
[16] Richard Coyne. 1998. Cyberspace and Heidegger's Pragmatics. *Information Technology and People* 11, 4 (1998), 338–350.
[17] Jedidiah R Crandall and Daniela Oliveira. 2012. Holographic vulnerability studies: vulnerabilities as fractures in interpretation as information flows across abstraction boundaries. In *Proceedings of the 2012 New Security Paradigms Workshop*. 141–152.
[18] Stuart Croft. 2012. Constructing ontological insecurity: The insecuritization of Britain's Muslims. *Contemporary Security Policy* 33, 2 (2012), 219–235.
[19] Matthew d'Ancona. 2017. *Post-Truth: The New War on Truth and How to Fight Back*. Random House, New York.
[20] Jacques Derrida. 1966. *Structure, Sign, and Play in the Discourse of the Human Sciences*. Routledge, London.
[21] Jacques Derrida. 1975. The purveyor of truth. *Yale French Studies* 52 (1975), 31–113.
[22] Jacques Derrida. 1981. *Position*. The University of Chicago Press, Chicago.
[23] Jacques Derrida. 1998. *Monolingualism of the Other, or, the Prosthesis of Origin*. Stanford University Press, Redwood City.
[24] Jacques Derrida. 1998. *Of Grammatology*. Johns Hopkins University Press, Baltimore.
[25] Jacques Derrida. 2004. *Dissemination*. A&C Black.
[26] Jacques Derrida. 2005. *Politics of friendship*. Vol. 5. Verso.
[27] Jacques Derrida. 2005. *Rogues: Two Essays on Reason*. Stanford University Press, Redwood City.
[28] Jacques Derrida. 2008. *The animal that therefore I am*. Fordham University Press, New York City.
[29] Jacques Derrida. 2010. *Voice and Phenomenon*. Northwestern University Press, Evanston.
[30] Jacques Derrida and Jeffrey Mehlman. 1972. Freud and the Scene of Writing. *Yale French Studies* 48 (1972), 74–117.
[31] Serge Egelman, Andreas Sotirakopoulos, Ildar Muslukhov, Konstantin Beznosov, and Cormac Herley. 2013. Does my password go up to eleven?: the impact of password meters on password selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Paris, 2379–2388.
[32] Henry Farrell and Bruce Schneier. 2018. Common-Knowledge Attacks on Democracy. *Berkman Klein Center Research Publication* 2018-7 (2018).
[33] Adrienne Porter Felt, Robert W. Reeder, Hazim Almuhimedi, and Sunny Consolvo. 2014. Experimenting at scale with google chrome's SSL warning. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Toronto, 2667–2670.
[34] Simson Garfinkel and Heather Richter Lipford. 2014. *Usable security: History, themes, and challenges*. Morgan & Claypool, San Rafael.
[35] John Geanakoplos. 2005. Three Brief Proofs of Arrow's Impossibility Theorem. *Economic Theory* 26, 1 (2005), 211–215.
[36] Anthony Giddens. 1991. *Modernity and self-identity*. Stanford University Press, California.
[37] Peter Goodrich, Florian Hoffmann, Michel Rosenfeld, and Cornelia Vismann. 2008. *Derrida and Legal Philosophy*. Palgrave Macmillan, New York.
[38] J. Alex Halderman and Edward W. Felten. 2006. Lessons from the Sony DRM episode. In *USENIX*.
[39] S M Taiabul Haque, Shannon Scielzo, and Matthew Wright. 2014. Applying psychometrics to measure user comfort when constructing a strong password.

In *SOUPS*.
[40] John Brian Harley. 1989. Deconstructing the map. *Cartographica: The international journal for geographic information and geovisualization* 26, 2 (1989), 1–20.
[41] Susan Hennessy. 2017. Deterring Cyberattacks: How to Reduce Vulnerability. *Foreign Affairs* 96, 6 (2017).
[42] Cormac Herley and P.C. van Oorschot. 2017. SoK: Science, security, and the elusive goal of security as a scientific pursuit. In *IEEE S&P*.
[43] Lance Hoffman, Diana Burley, and Costis Toregas. 2011. Holistically biulding the cybersecurity workforce. *IEEE Security and Privacy* 10 (2011), 33–39. Issue 2.
[44] Steven J Jackson. 2014. Rethinking repair. *Media Technologies: Essays on Communication, Materiality, and Society* (2014).
[45] Steven J Jackson, Syed Ishtiaque Ahmed, and Md Rashidujjaman Rifat. 2014. Learning, innovation, and sustainability among mobile phone repairers in Dhaka, Bangladesh. In *Proceedings of the 2014 Conference on Designing Interactive Systems*. ACM, 905–914.
[46] Barbara Johnson. 1994. *The Wake of Deconstruction*. Wiley-Blackwell, Hoboken.
[47] Justin Joque. 2018. *Deconstruction Machines*. University of Minnesota Press, Minneapolis.
[48] Peter Kalulé. 2019. On the undecidability of legal and technological regulation. *Law and critique* 30, 2 (2019).
[49] Peggy Kamuf. 1997. *The division of literature: Or the university in deconstruction*. University of Chicago Press.
[50] Immanuel Kant. 2017. *Critique of pure reason*. Cambridge University Press, Cambridge.
[51] Jonathan Katz and Yehuda Lindell. 2015. *Introduction to Modern Cryptography*. CRC Press.
[52] Carl Landwehr. 2012. Cybersecurity: From engineering to science. *The Next Wave* 19, 2 (2012), 2–5.
[53] Dave Lee. 2019. WhatsApp discovers 'targeted' surveillance attack. Retrieved July 21, 2005 from https://www.bbc.com/news/technology-48262681
[54] Gottfried Wilhelm Leibniz. 1989. *Philosophical papers and letters*. Springer, Berlin.
[55] Ann Light, Irina Shklovski, and Alison Powell. 2017. Design for Existential Crisis. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Extended Abstracts*. ACM, Denver, 722–734.
[56] Alexander De Luca, Alina Hang, Emanuel von Zezschwitz, and Heinrich Hussmann. 2015. I feel like I'm taking selfies all day!: Towards understanding biometric authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Seoul, 1411–1414.
[57] Staughton Lynd. 1966. The Compromise of 1787. *Political Science Quarterly* 81, 2 (1966), 225–250.
[58] Catherine Malabou. 2004. *The Future of Hegel: Plasticity, Temporality, and dialectic*. Routledge, London.
[59] Catherine Malabou. 2009. How is subjectivity undergoing deconstruction today? Philosophy, auto-hetero-affection, and neurobiological emotion. *Qui Parle* 17, 2 (December 2009), 111–122.
[60] John McLean. 1987. Reasoning about security models. In *IEEE S&P*.
[61] Tyler Moore and Ross Anderson. 2012. *The Oxford Handbook of the Digital Economy*. Oxford University Press, Oxford.
[62] Alun Munslow. 2006. *Deconstructing history*. Routledge.
[63] Greg Noble. 2005. The discomfort of strangers: Racism, incivility and ontological security in a relaxed and comfortable nation. *Journal of intercultural studies* 26, 1-2 (2005), 107–120.
[64] National Institute of Standards and Technology. 2018. Joint Task Force Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. Retrieved July 25, 2005 from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
[65] Leysia Palen and Paul Dourish. 2003. Unpacking "privacy" for a networked world. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, Ft. Lauderdale, 129–136.
[66] Wolter Pieters. 2011. The (social) construction of information security. *The Information Society* 27, 5 (2011), 326–335.
[67] Plato. 1952. *Duality*. University Press, Cambridge.
[68] Sara Ramshaw. 2013. *Justice as improvisation: The law of the extempore*. Routledge, London.
[69] Jean-Jacques Rousseau. 1966. *Essay on the Origin of Languages*. Frederick Ungar Publishing Company, New York.
[70] Bruce Schneier. 2006. *Beyond fear: Thinking sensibly about security in an uncertain world*. Springer Science & Business Media.
[71] Peter Sloterdijk. 2006. *Derrida, an Egyptian*. Wiley.
[72] Gayatri Chakravorty Spivak. 2012. *In Other Worlds: Essays in Cultural Politics*. Routledge, London.
[73] Jonathan M Spring, Tyler Moore, and David Pym. 2017. Practicing a science of security: a philosophy of science perspective. In *Proceedings of the 2017 New Security Paradigms Workshop*. 1–18.
[74] Bernard Stiegler. 1998. *Technics and Time: The Fault of Epimetheus*. Vol. 1. Stanford University Press, Redwood City.
[75] Norman Makoto Su, Victor Kaptelilin, Jeffrey Bardzell, Shaowen Bardzell, Jed R. Brubaker, Ann Light, and Dag Svanaes. 2019. Standing on the shoulder of giants: Exploring the intersection of philosophy and HCI. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems Extended Abstracts*. ACM, Glasgow.
[76] Lasse Thomassen. 2010. Deconstruction as method in political theory. *Österreichische Zeitschrift für Politikwissenschaft* 39, 1 (2010), 41–53.
[77] Alan Turing. 1936. On computable numbers, with an application to the Entscheidungsproblem. *Proc. London Math. Soc.* 2, 42 (1936), 230–265.
[78] Cornelia Vismann. 2005. Derrida, philosopher of the law. *German Law Journal* 6, 1 (2005), 5–13.
[79] John von Neumann. 1993. First draft of a report on the EDVAC. *IEEE Annals of the History of Computing* 15, 4 (1993), 27–75.
[80] Jukka Vuorinen and Pekka Tetri. 2012. The order machine – The ontology of information security. *Journal of the Association for Information Systems* 13, 9 (2012).
[81] Alma Whitten and J. D. Tygar. 1999. Why Johnny can't encrypt. In *USENIX*.