Journal of Information Systems Education

Volume 35
Issue 3
Summer 2024

Teaching Case

Security and Privacy Implications of Virtual Reality Applications in the Metaverse: A Case of Development, Security, and Operations (DevSecOps)

Ersin Dincelli and Alper Yayla

Recommended Citation: Dincelli, E., & Yayla, A. (2024). Teaching Case: Security and Privacy Implications of Virtual Reality Applications in the Metaverse: A Case of Development, Security, and Operations (DevSecOps). *Journal of Information Systems Education*, 35(3), 261-270. https://doi.org/10.62273/JMZA1065

Article Link: https://jise.org/Volume35/n3/JISE2024v35n3pp261-270.html

Received:	March 19, 2023
First Decision:	May 17, 2023
Accepted:	April 18, 2024
Published:	September 15, 2024

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Journal of Information Systems Education, 35(3), 261-270, Summer 2024
https://doi.org/10.62273/JMZA1065

Teaching Case
Security and Privacy Implications of Virtual Reality Applications in the Metaverse: A Case of Development, Security, and Operations (DevSecOps)

Ersin Dincelli
Business School
University of Colorado Denver
Denver, CO 80202, USA
ersin.dincelli@ucdenver.edu

Alper Yayla
Sykes College of Business
University of Tampa
Tampa, FL 33606, USA
ayayla@ut.edu

ABSTRACT

The availability of powerful head-mounted displays (HMDs) has made virtual reality (VR) a mainstream technology and spearheaded the idea of immersive virtual experiences within the Metaverse – a shared and persistent virtual world. Companies are eagerly investing in various VR products and services, aiming to be early adopters and create new revenue streams by taking advantage of the hype surrounding VR and the Metaverse. However, unique privacy and security issues associated with VR arise from the data collected by both VR applications and peripherals. Given that VR HMDs equipped with intrusive sensors designed to track eye movements, facial expressions, and other biometric data are already available in the market, it is essential to integrate security and privacy into the VR application development lifecycle. This study presents a hypothetical case that revolves around a team of programmers and cybersecurity experts tasked to develop new VR applications for a technology conglomerate that recently shifted its attention towards the Metaverse. Building on development, security, and operations (DevSecOps) practice, the case study tasks participants to consider secure software development, threat modeling, and adoption of security and privacy frameworks in the context of VR application development. This study contributes to IS education by emphasizing potential privacy and security issues associated with this rapidly evolving technology. Additionally, it demonstrates how the implementation of DevSecOps practices can effectively address potential security challenges throughout the software development process.

Keywords: Security, Privacy, Virtual reality, Metaverse, Threat modeling, DevSecOps

1. INTRODUCTION

The term "Metaverse" was originally coined in the 1992 science fiction novel Snow Crash (Stephenson, 1992). Coincidentally, with the 30th anniversary of Snow Crash, one of the world's biggest technology companies rebranded itself as Meta to reflect its new focus towards the development of the Metaverse. The Metaverse is a virtual reality (VR) environment where users can engage in various daily activities such as work, study, play, shopping, socializing, and more. Major technology companies are investing not only in the technologies necessary to build the Metaverse but also in developing digital products and services tailored specifically for it. For instance, Meta focuses on digital goods as a key revenue stream (Kovach, 2021). Similarly, Microsoft has begun integrating its existing collaboration tools into the Metaverse to enhance work productivity (Roach, 2021).

The Metaverse is a shared and persistent virtual space built on specialized hardware and software that provide the necessary computing power and networking capabilities to host virtual platforms, which enable the delivery of various content and services (Ball, 2021). On the software side, a game engine, such as Unity, Unreal, and Godot, creates a three-dimensional representation of a virtual environment. In this interconnected environment, users interact with objects, other users (i.e., avatars), and computer-generated characters (i.e., agents). Within the Metaverse, the virtual environment is both shared and persistent, setting it apart from standalone VR games or applications. On the hardware side, users require equipment to access and interact with the virtual environment. While this environment can run on various devices, including smartphones, computers, and gaming consoles, a fully

immersive experience is achieved using head-mounted displays (HMDs).

Beyond the hardware, software, and underlying infrastructure, creating a shared and persistent virtual world requires user data (Bavana, 2022). The Metaverse can become a personalized and intelligent environment that provides the envisioned fully immersive experience only through the utilization of user data. Alongside user preferences and activities, peripherals such as motion controllers, eye-trackers, sensors, and haptic gloves can collect a continuous flow of highly sensitive real-time user data. In fact, VR, through its implementation in the Metaverse, might be the first consumer technology that allows companies to concurrently collect both psychological and physiological data from users (Bavana, 2022; Dincelli & Yayla, 2022). Having access to such data (e.g., capturing customer emotions during virtual store visits or the blood pressure data of clients during business negotiations) would be invaluable for organizations but also highly invasive for users.

Developing robust and secure applications becomes even more critical as technology becomes increasingly interconnected and intrusive. This, in turn, leads to an increased demand for skilled professionals in development, security, and operations (DevSecOps) (Edmundson & Hartman, 2022). Addressing this growing industry demand requires engaging learning efforts aimed at fostering students' interest in DevSecOps. This teaching case builds on the potential security and privacy implications of VR and Metaverse applications through scenario-based learning (Dincelli & Chengalur-Smith, 2020). It aims to achieve the following learning objectives: Firstly, it serves as an exercise to enhance students' awareness of security and privacy. Secondly, it demonstrates how students can integrate the best security and privacy practices into the software development lifecycle. Thirdly, it highlights the differences between the security and privacy implications of data collection and underscores the importance of personal privacy and security in the context of emerging technologies. Lastly, it introduces students to industry best practices through well-established security and privacy frameworks.

2. CASE PROBLEM: SECURITY AND PRIVACY IN THE METAVERSE

Technology companies like Meta and Microsoft are aggressively pursuing VR as a new product market and a critical enabler of the Metaverse. Today, VR HMDs on the market already have the capability to collect highly intrusive user data, such as eye movements and facial expressions, to track users for a more personalized experience (Dincelli & Yayla, 2022). While all software development projects need to consider the security and privacy implications of the final information system product, the ability to track and collect highly invasive user data raises unique security and privacy issues (O'Brolcháin et al., 2016; Sutanto et al., 2013). Moreover, the amalgamation of such personal data with existing user profile information from social media and other online platforms provides technology companies tremendous insights into individuals, such as their consumption patterns, habits, lifestyle, and situational emotions (Kaspersky, 2022).

The data collected from intrusive VR HMDs and peripherals raises questions about the extent of data collection and potential compromise of user privacy in the process of developing the Metaverse. The excitement surrounding Web 2.0 and rich social media interactions preceded our sense of privacy (Dinev et al., 2009). Individuals have come to realize that technology companies continuously collect user data and profile users across various platforms. VR affords even more intrusive data collection capabilities (Nair et al., 2022). Therefore, it is imperative that security and privacy measures are integrated into VR technologies, products, and services from their early stages of adoption (Adams et al., 2018).

To provide an understanding of these practices, this case study introduces students to security and privacy frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity and Privacy Frameworks, along with cybersecurity practices, like DevSecOps, threat modeling, and software security. First, it delineates the importance of integrating security into software development lifecycle. It builds on the DevSecOps practice and provides a scenario that incorporates threat modeling into the NIST Cybersecurity Framework. Second, it highlights the distinctions between security and privacy concerning data collection and use. While security and privacy are interrelated, it is crucial to recognize that privacy violations can arise not only from security breaches but also from excessive data collection and processing (NIST, 2020). The teaching case considers these privacy violations using the NIST Privacy Framework.

3. BACKGROUND

3.1 Virtual Reality Technology and the Metaverse

VR is a computer-generated environment that imitates all or some aspects of the real world (Walsh & Pawlowski, 2002). Early VR applications date back to the 1960s and primarily consisted of research-oriented prototypes of VR hardware and virtual environments. The introduction of the Oculus Rift headset on Kickstarter in 2012 revitalized the interest in VR. More importantly, the accessibility of powerful consumer-grade HMDs elevated VR into the mainstream, and advancements in VR technology led to various applications for users and organizations. Figure 1 illustrates the wide variety of HMDs available to users over the past decade, ranging from basic smartphone add-ons to more sophisticated and expensive computer-tethered and non-tethered standalone variants.

Figure 1. Different Types of VR HMDs (Samsung Gear VR, Oculus Quest, and Valve Index)

Current VR technology enables a high level of immersion and an objective level of sensory fidelity (Slater, 2003) through HMDs and other associated peripherals (Figure 2). HMDs and peripherals play a vital role in creating the Metaverse as they are necessary for a sensory illusion of reality (Slater & Wilbur, 1997). Higher levels of immersion lead to higher levels of presence, which is the sense of being physically present in a virtual environment (Steuer, 1992). When users have higher levels of presence, they are more likely to behave in VR as they would in the real world (Slater & Wilbur, 1997). For successful

immersion, HMDs and peripherals collect and utilize intrusive personal data ranging from facial expressions to eye movements (Canales, 2021).

Figure 2. Examples of VR Peripherals (HP Reverb, Manus, bHaptics, HTC Vive Trackers, WorldViz)

While VR has been used to create standalone applications, organizations aim to further blur the lines between the real and virtual worlds through the Metaverse. The Metaverse is a shared and persistent virtual space, distinguishing itself from standalone applications by integrating VR technology with other emerging technologies, such as blockchain and nonfungible tokens (NFT) (Dincelli & Yayla, 2022). The Metaverse is expected to enable new disruptive organizational opportunities in various industries, from travel to education, retail, and medical (French et al., 2020).

3.2 Secure Software Development with DevSecOps

Cybersecurity attacks that exploit software vulnerabilities have increased significantly in the last decade (McAfee, 2020). The *SolarWinds* attack is an example of a software supply chain attack that impacted thousands of companies and several government agencies. According to the forensic analysis conducted by Microsoft, over a thousand hackers worked on this attack, which is considered the largest and most sophisticated cyberattack to date (Tung, 2021). Similarly, the vulnerability of the popular open-source tool *Log4j* is considered one of the most critical vulnerabilities identified to date. Attackers exploited this vulnerability to execute arbitrary code on servers and computers, affecting millions of devices and causing the leakage of sensitive information (Goodin, 2021). *Pegasus* spyware is another example that resulted from a software vulnerability. This spyware exploited vulnerabilities in mobile phone operating systems and was used for surveillance of activists, journalists, and political leaders in several countries. By 2020, it had already targeted over 50,000 "people of interest." Cybersecurity breaches cost companies millions of dollars (Swinhoe, 2020), and organizations are under increasing pressure from customers and legislative bodies to ensure the security of their IT assets (Gartner, 2020).

One strategy to mitigate software-based vulnerabilities is to integrate security measures throughout the software development lifecycle, from initial development to post-deployment phases. Detecting and addressing vulnerabilities early in the development process significantly reduces total development time and cost (Dawson et al., 2010; Hackbarth et al., 2016; NIST, 2002). With increasing cyberattacks due to software vulnerabilities, integration of not only the development and operations functions (DevOps) but also the security function (DevSecOps) has been suggested (IBM, 2020). While DevOps philosophy increases the efficiency and agility of software development by streamlining the work between the two functions, DevSecOps extends this philosophy by integrating security teams to address threats, vulnerabilities, and controls throughout the development process.

Security teams can contribute to the software development lifecycle through the evaluation of threats, source code analysis, security testing, and tracking security-related operational metrics. DevSecOps practices minimize vulnerabilities without impeding development and production workflows, mitigate the potential impact of vulnerabilities, address root causes of security issues, and ultimately increase the effectiveness and efficiency of development, security, and operations teams (Souppaya et al., 2022). DevSecOps teams can accomplish these goals by using the existing frameworks and best practices. For instance, NIST's Secure Software Development Framework (SSDF) (NIST, 2022) provides a comprehensive guideline for mitigating risks of software vulnerabilities. It recommends practices that prepare organizations for secure software development, protect all software components from tampering and unauthorized access, produce well-secured software with minimal vulnerabilities, and respond to residual vulnerabilities after the software release (Table 1). Similarly, Microsoft's Security Development Lifecycle (SDL) emphasizes integrating security and privacy measures across all development phases (Microsoft, 2016). These measures include providing initial core security training for the development team and establishing an incident response plan that considers threats and vulnerabilities after the release of the software.

3.3 Threat Modeling in Software Development

DevSecOps teams can also employ threat modeling throughout the development and operation cycles to enhance security. Threat modeling enables software architects to identify and mitigate security issues at early stages of development. For instance, Microsoft's STRIDE model is considered one of the most comprehensive threat models available (Shevchenko et al., 2018). STRIDE identifies seven distinct threat categories, detailed in Table 2, and provides DevSecOps teams with a structured approach to systematically assess and address potential security risks. DevSecOps teams can analyze relevant components of their software projects for susceptibility to these threats and take action to mitigate them during the development process.

During threat modeling, DevSecOps teams can focus on well-known software security risks to ensure robust security measures are in place. For instance, the Open Web Application Security Project (OWASP) periodically publishes the top ten most critical security concerns for web applications to raise awareness of emerging threats (OWASP, 2021). The OWASP Top 10 list represents a consensus on the most severe security threats to web applications, serving as a valuable resource that guides organizations to address these critical security concerns (Glisson & Welland, 2014). Table 3 lists the OWASP top ten web application security risks.

Practices	Tasks
Prepare the organization	- Define security requirements - Implement roles and responsibilities - Implement supporting toolchains - Define and use criteria for security checks - Implement and maintain secure software development environments
Protect software	- Protect all forms of code from unauthorized access and tampering - Provide a mechanism for verifying software release integrity - Archive and protect each software release
Produce well-secured software	- Design software to meet security requirements and mitigate potential security risks - Review software design to ensure compliance with security requirements and risk information - Reuse existing, well-secured software when feasible instead of duplicating functionality - Create source code by adhering to secure coding practices - Configure the compilation, interpreter, and build processes to improve executable code - Review human-readable code to identify vulnerabilities and ensure compliance with security requirements - Conduct comprehensive testing on executable code to identify vulnerabilities and ensure compliance with security requirements - Establish secure default settings for software configuration
Respond to vulnerabilities	- Identify and confirm vulnerabilities on an ongoing basis - Assess, prioritize, and remediate vulnerabilities promptly - Analyze vulnerabilities to identify their root causes

Table 1. NIST Secure Software Development Framework Practices (NIST, 2022)

Category	Description
Spoofing	Unauthorized access and use of a user's authentication credentials, such as username and password
Tampering	Malicious modification of data, such as unauthorized changes made to data within a database or network
Repudiation	Performing an action without other parties having any way to prove otherwise, such as performing unauthorized actions in a system that lacks the ability to trace operations
Information disclosure	Exposure of information to unauthorized individuals, such as reading a file without appropriate permissions
Denial of service	Denial of service to valid users, such as making a Web server temporarily unavailable
Elevation of privilege	Gaining increased privileged access, such as switching from a standard system user to an administrator level

Table 2. STRIDE Threat Categories and Descriptions (adopted from Microsoft, 2022)

Rank	Web Application Security Risk
1	Broken Access Control
2	Cryptographic Failures
3	Injection
4	Insecure Design
5	Security Misconfiguration
6	Vulnerable and Outdated Components
7	Identification and Authentication Failures
8	Software and Data Integrity Failures
9	Security Logging and Monitoring Failures
10	Server-Side Request Forgery

Table 3. OWASP Top 10 Web Application Security Risks for 2021 (OWASP, 2021)

The top twenty-five most dangerous software weaknesses, published by the Common Weakness Enumeration (CWE), is another valuable resource that can provide insights for developers (CWE, 2021). This list is compiled based on the most common and critical errors that may lead to software vulnerabilities. These weaknesses are generally easy to identify and exploit, eventually allowing hackers to take control of a system or obtain sensitive data. CWE employs a scoring system to assign a value to each vulnerability and prioritize vulnerabilities based on severity. Table 4 presents the CWE's top software weaknesses. These lists provide vital guidance to developers, administrators, and cybersecurity professionals, assisting them in understanding how to effectively mitigate security risks (Mahmood, 2021).

3.4 NIST Cybersecurity Framework

NIST is a non-regulatory agency of the U.S. Department of Commerce. NIST's mission is to promote innovation and industrial competitiveness in the U.S. while developing and utilizing a set of standards. Given the importance of cybersecurity to the nation's critical infrastructure, NIST published the Cybersecurity Framework (CSF) in 2014. The CSF provides voluntary guidance for organizations to better understand, manage, and mitigate their cybersecurity risks (NIST, 2018). The framework was revised in 2018 and has been widely adopted by both small and large organizations as a best practice for cybersecurity preparedness (Tracy, 2020).

The CSF provides structured guidance for achieving confidentiality, integrity, and availability of IT assets through five core functions, as outlined in Table 5. These five continuous and concurrent functions form a framework that provides a strategic view on cybersecurity risks. The associated 23 categories and 110 subcategories provide a granular view for the operationalization of cybersecurity efforts. Organizations are encouraged to address all five functions simultaneously and select activities from the categories and subcategories that align with their specific cybersecurity needs. It is important to note that the CSF does not mandate the importance or order of activities. Instead, it supplements existing cybersecurity risk management programs within organizations (NIST, 2022).

Rank	Software Weakness
1	Out-of-bounds write
2	Improper neutralization of input during web page generation (“cross-site scripting”)
3	Out-of-bounds read
4	Improper input validation
5	Improper neutralization of special elements used in an OS command (“OS command injection”)
6	Improper neutralization of special elements used in an SQL command (“SQL injection”)
7	Use after free
8	Improper limitation of a pathname to a restricted directory (“path traversal”)
9	Cross-site request forgery (CSRF)
10	Unrestricted upload of file with dangerous type
11	Missing authentication for critical function
12	Integer overflow or wraparound
13	Deserialization of untrusted data
14	Improper authentication
15	NULL pointer dereference
16	Use of hard-coded credentials
17	Improper restriction of operations within the bounds of a memory buffer
18	Missing authorization
19	Incorrect default permissions
20	Exposure of sensitive information to an unauthorized actor
21	Insufficiently protected credentials
22	Incorrect permission assignment for critical resource
23	Improper restriction of XML external entity reference
24	Server-side request forgery (SSRF)
25	Improper neutralization of special elements used in a command (“command injection”)

Table 4. Most Dangerous Software Weaknesses (CWE, 2021)

Security Function	Description	Categories
Identify	Develop an organizational understanding to manage potential cybersecurity risks to systems, people, assets, data, and capabilities.	- Asset management - Business environment - Governance - Risk assessment - Risk management strategy - Supply chain risk management
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services to support the ability to limit or contain the impact of a potential cybersecurity event.	- Identity management and access control - Awareness & training - Data security - Information protection processes and procedures - Maintenance - Protective technology
Detect	Implement appropriate activities to identify the occurrence of a cybersecurity event in a timely manner.	- Anomalies and events - Security continuous monitoring - Detection processes
Respond	Implement appropriate activities to respond to a cybersecurity incident to contain and mitigate its impact.	- Response planning - Communications - Analysis - Mitigation - Improvements
Recover	Implement appropriate activities to maintain resilience plans and restore compromised capabilities or services following an incident.	- Recovery planning - Improvements - Communications

Table 5. NIST CSF Framework Functions and Categories (NIST, 2018)

3.5 NIST Privacy Framework

Although privacy and security are often used interchangeably, they represent two distinct concepts. While the goal of security is the protection of IT assets, including private information, privacy focuses on the collection and use of private information (Dincelli et al., 2017). Similarly, data collected by organizations and governments create two distinct privacy challenges. First, the use of social media, digitalization of data, reliance on smart devices, and increased surveillance have resulted in a wealth of data on individuals. Over the past two decades, organizations have found various ways to harness this data for financial gains. However, the exploitation of extensive data collection has led to privacy violations (Wall et al., 2015), often without companies fully understanding the extent of privacy implications associated with the data they collect. Individuals may directly experience the impacts of these violations in the form of embarrassment, discrimination, and financial loss (NIST, 2020). For example, due to inadequate data handling practices, Target accidentally revealed to a father that his teenage daughter was pregnant (Duhigg, 2012). Such privacy violations resulting from excessive collection or inadequate data processing may have severe repercussions for organizations, including customer abandonment, loss of reputation, and noncompliance costs (NIST, 2020).

Second, the collected data is a valuable target for hackers. Personally identifiable information (PII), such as credit card numbers and social security numbers, along with protected health information (PHI), including health records, insurance, and payment details, have been frequently targeted by hackers. In fact, high-profile data breaches at Target in 2013 and Anthem in 2015 made cybersecurity a mainstream concern by highlighting the profound impact of private information loss. Targeted attacks on PII and PHI continue today. In the first half of 2019 alone, thousands of data breaches exposed over 3 billion records (Winder, 2019). Between 2005 and 2019, healthcare data breaches affected 250 million individuals (Seh et al., 2020), reaching an all-time high in 2021 (Landi, 2022).

Figure 3 illustrates the cybersecurity and privacy risks that organizations face today. The left circle represents cybersecurity risks, and the right circle represents privacy risks. Cybersecurity risk, area (a), includes security incidents that affect confidentiality, integrity, and availability of IT assets. Still, these incidents do not have privacy implications (e.g., denial of service (DoS) attack to a webserver). The intersection, area (b), captures privacy risks emerging from cybersecurity incidents – the second privacy challenge discussed above. The Venn diagram shows that cybersecurity risks do not encompass all privacy risks. That is, security can help organizations protect private information, area (b), but not alleviate the privacy risk arising from data collection and processing, area (c) – the first privacy challenge discussed above.

The NIST Privacy Framework (NIST, 2020) is a recent publication that organizations can use to evaluate the privacy implications of their systems, products, and services. While the core functions of the framework have similarities with the CSF, they are specifically defined for privacy. Table 6 summarizes these functions and the main categories within each function.

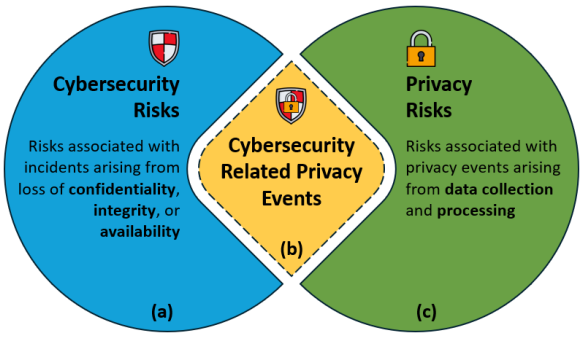


Figure 3. Cybersecurity and Privacy Risk Relationship (NIST, 2020)

4. CASE SYNOPSIS

Oasis is a hypothetical technology conglomerate that owns several social media platforms with billions of users worldwide. Its primary revenue source is advertising on these platforms. Recently, Oasis turned its attention to the Metaverse, a VR concept that encompasses a shared and persistent virtual world. The company owns a VR platform that hosts games, applications, and a marketplace with an integrated game creation system. The case study centers around a team of programmers assigned to create new Metaverse applications at Oasis. A cybersecurity expert is part of the programming team and assigned to accomplish several tasks that will ensure the security of the applications during development and post-deployment, while also considering the privacy implications of the data collected from these envisioned Metaverse applications.

The planned Metaverse applications will be mobile- and computer-based software and work with the current VR technology, such as HMDs and VR peripherals equipped with various sensors. Users are required to have an Oasis account to be able to use HMDs and have access to the VR marketplace. The VR marketplace is separate from the main Oasis social media platform. Users can create new accounts or use pre-existing Oasis accounts to access the marketplace. Considering that the goal of Oasis is to be part of the Metaverse - a shared experience with potential organizational applications - Oasis is planning to enable authentication through Amazon and Google and a single sign-on feature to create centralized access for business users. The planned Metaverse applications will focus on entertainment (games, sports, exercise, etc.) and productivity (collaboration, virtual meetings, training, etc.). The HMDs come with a standard heart rate monitor and can be enhanced by eye-tracking, motion controllers, and gamepads to increase immersion. In the near future, Oasis plans to manufacture new VR peripherals, such as haptic bodysuits and gloves, and will integrate these wearables into the existing ecosystem. The following section presents the case.

Privacy Function	Description	Categories
Identify	Develop an organizational understanding to manage potential privacy risk arising from data processing.	- Inventory & mapping - Business environment - Risk assessment - Data processing ecosystem risk management
Govern	Develop and implement a governance structure to enable an ongoing understanding of risk management priorities that are informed by privacy risks.	- Governance policies, processes, & procedures - Risk management strategy - Awareness & training - Monitoring & review
Control	Implement appropriate activities to enable organizations or individuals to manage data with sufficient granularity to manage potential privacy risks.	- Data processing policies, process, & procedures - Data processing management - Disassociated processing
Communicate	Implement appropriate activities to foster a reliable understanding and engage in a dialogue on data processing and its associated privacy risks.	- Communication policies, processes, & procedures - Data processing awareness
Protect	Develop and implement effective safeguards for data processing.	- Data protection policies, processes, & procedures - Identify management, authentication, & access control - Data security - Maintenance - Protective technology

Table 6. NIST CSF Framework Functions and Categories (NIST, 2018)

5. CASE TASKS AND QUESTIONS

This section presents various tasks related to the hypothetical case involving the DevSecOps team at Oasis. Students should read each task carefully and refer to the hypothetical case as they prepare detailed answers to the following questions. Most of the questions are designed for students to "recommend" a control and "identify" a risk among several potential options or activities suggesting there may not be a single correct answer. However, a "correct" answer needs to satisfy two conditions. First, students need to identify the best possible "choice," given the options. Some choices are certainly better than others. Second, students need to provide reasonable support for their choice in the context of the case. While there may be important cybersecurity risks or effective controls in the frameworks, not all of these are suitable for this specific case. Therefore, if necessary, students can undertake additional research on security and privacy issues in the Metaverse and VR HMDs with advanced tracking capabilities (Meta Quest Pro, HTC Vive Pro 2, Apple Vision Pro, etc.) to prepare a satisfactory response to the questions. Below is a brief introduction to contextualize the case tasks.

After months of extensive research and development, Oasis has successfully developed a cutting-edge VR application. This innovative application provides users a platform to immerse themselves in realistic virtual environments, engage in interactive experiences, and connect with others in the Metaverse. To ensure a seamless launch, Oasis forms a cross-functional team consisting of the company's top-tier software engineers, information systems analysts, UX designers, and cybersecurity experts. Each team member contributes their unique expertise to address various aspects of the VR application's development and deployment, ensuring that Oasis delivers nothing short of excellence.

As the cybersecurity expert on the team, you prioritize the implementation of robust security measures. You plan to conduct thorough threat modeling exercises, identify potential vulnerabilities, and craft effective countermeasures through various well-established frameworks. Data protection and privacy are at the forefront of Oasis' concerns as VR HMDs and peripherals come equipped with various sensors that can collect highly sensitive user data. Oasis expects you to implement industry standards to safeguard user information. You have a series of critical tasks that you need to complete before the launch:

5.1 Task 1 – STRIDE Threat Modeling

You chose STRIDE to conduct asset-based threat modeling. Your job is to explain what STRIDE is to your team. For each threat in STRIDE, provide (a) a short definition, (b) provide examples of how it relates to the new Metaverse applications developed for this case, and (c) rate each threat given the case information. Afterward, answer the following questions:

1. Are there any unidentified risks that you have not covered in the threat analysis? If yes, assign a rating for each one.
2. What is the potential impact of each identified risk?
3. What is one risk that you cannot afford to take?
4. How does STRIDE threat modeling apply to modern software applications, such as VR applications in the Metaverse?
5. Do you have any supply chain risks?

5.2 Task 2 – NIST Cybersecurity Framework

Your next task is to introduce the NIST Cybersecurity Framework to your team. Pick the most important subcategory for each category of the Protect and Detect functions in the NIST Cybersecurity Framework to ensure the security of the application during and after development. This part

encompasses security beyond code development and includes areas such as data security, access management, detection of attacks, and other related organizational issues. Refer to NIST Cybersecurity Framework v1.1 (NIST, 2022) and discuss how you will achieve the subcategories that you selected and note which STRIDE threat(s) you address. In this task, you will select a total of nine subcategories. Afterward, answer the following questions:

1. Would you recommend any additional subcategory that would support VR applications in the Metaverse? (Refer to pp. 29-40 of the NIST Cybersecurity Framework.)
2. It is important to understand the distinction between "security" and "secure" features, as it is possible to implement security features that are insecure. Explain the difference between security features and secure features to your team.

5.3 Task 3 – NIST Privacy Framework

Privacy has never been a big concern, like security for organizations or users, until now. Use the NIST Privacy Framework to outline the potential privacy risks of VR applications. Pick the most important category for each function in the NIST Privacy Framework to ensure privacy for VR applications in the Metaverse. Refer to NIST Privacy Framework v1.0 (NIST, 2020) and discuss how you will address each category that you selected. In this task, you will select four categories (Refer to pp. 19-27 of the NIST Privacy Framework). Afterward, answer the following questions:

1. Explain to your team how the goal of the NIST Privacy Framework differs from the goal of the NIST Cybersecurity Framework.
2. What other tasks would you consider in addition to the ones outlined above for preserving the privacy of users of the Metaverse and securing VR applications in the Metaverse?

5.4 Task 4 – Security and Privacy Metrics

Define two metrics for security and one metric for privacy as part of measurements of effectiveness and continuous improvement for VR applications in the Metaverse. Adapt the examples from the appendix of the NIST Performance Measurement Guide for Information Security to the case. Afterward, answer the following questions:

1. What is the name of the metric?
2. What are the goals of using the metric?
3. What does it measure?
4. What is the formula (quantify your metric)?
5. What is the frequency of measurement?
6. How will you implement the measure?
7. Where will you get the data?

6. CONCLUSIONS

The consumer demand for VR products and services is anticipated to grow rapidly (Luna-Nevarez & McGovern, 2021). VR HMDs and peripherals are instrumental in providing users with highly immersive virtual experiences and are predicted to shape the future of the Metaverse (Dincelli & Yayla, 2022). However, as VR technology advances, it also becomes more invasive to provide better immersive virtual experiences. The sensors and tracking features of VR HMDs and peripherals enable novel data collection capabilities, such as users' psychological and physiological data. Notwithstanding the benefits of this "new" personal data, it will also attract hackers and give service providers extensive information about their users (Adams et al., 2018). These elevated risks necessitate rethinking the software development process for Metaverse applications. This involves differentiating privacy and security issues and focusing on each risk individually (Di Pietro & Cresci, 2021). Additionally, organizations face a pressing demand for skilled cybersecurity professionals in DevSecOps due to an ongoing shortage in the field (Edmundson & Hartman, 2022). This workforce gap necessitates efforts to generate interest in DevSecOps practices.

In this study, we emphasize the importance of integrating cybersecurity expertise into the software development lifecycle. We introduce an intriguing case that suggests adopting industry best practices and frameworks to ensure security and privacy standards while fostering continuous improvement through identifying and measuring associated metrics over time. The case aims to enhance students' skills and nurture their interests in DevSecOps within the context of VR and Metaverse application development. By examining the intersection of emerging VR technology, privacy, security, and DevSecOps, this study also provides insights into safeguarding user data and promoting a secure and privacy-conscious approach to VR application development within the context of the Metaverse.

7. REFERENCES

Adams, D., Bah, A., Barwulor, C., Musaby, N., Pitkin, K., & Redmiles, E. M. (2018). Ethics Emerging: The Story of Privacy and Security Perceptions in Virtual Reality. *Proceedings of the 14th Symposium on Usable Privacy and Security (SOUPS)* (pp. 427-442).

Ball, M. (2021). The Metaverse Primer: Framework for the Metaverse. https://www.matthewball.vc/all/forwardtothemetaverseprimer

Bavana, K. (2022). Privacy in the Metaverse, *Jus Corpus Law Journal*, 2(3), 1-11.

Canales, K. (2021). The Metaverse Could Let Silicon Valley Track Your Facial Expressions, Blood Pressure, and Your Breathing Rates - Showing Exactly Why Our Internet Laws Need Updating. https://www.businessinsider.com/metaverse-silicon-valley-tech-data-collection-regulation-laws-need-updating-2021-12

Common Weakness Enumeration (CWE). (2021). CWE Top 25 Most Dangerous Software Weaknesses. https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html

Dawson, M., Burrell, D. N., Rahim, E., & Brewster, S. (2010). Integrating Software Assurance Into the Software Development Life Cycle (SDLC). *Journal of Information Systems Technology and Planning*, 3(6), 49-53.

Dincelli, E., & Chengalur-Smith, I. (2020). Choose Your Own Training Adventure: Designing a Gamified SETA Artefact for Improving Information Security and Privacy Through Interactive Storytelling. *European Journal of Information Systems*, 29(6), 669-687. https://doi.org/10.1080/0960085X.2020.1797546

Dincelli, E., Goel, S., & Warkentin, M. (2017). Understanding Nuances of Privacy and Security in the Context of Information Systems. *Proceedings of the Americas Conference on Information Systems* (pp. 1-5).

Dincelli, E., & Yayla, A. (2022). Immersive Virtual Reality in the Age of the Metaverse: A Hybrid-Narrative Review Based on the Technology Affordance Perspective. *Journal of Strategic Information Systems*, 32(2), 1-22. https://doi.org/10.1016/j.jsis.2022.101717

Dinev, T., Xu, H., & Smith, H. J. (2009). Information Privacy Values, Beliefs and Attitudes: An Empirical Analysis of Web 2.0 Privacy. *Proceedings of the 42nd Hawaii International Conference on System Sciences* (pp. 1-10). IEEE.

Di Pietro, R., & Cresci, S. (2021). Metaverse: Security and Privacy Issues. *In Proceedings of 3rd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)* (pp. 281-288). IEEE. https://doi.org/10.1109/TPSISA52974.2021.00032

Duhigg, C. (2012). How Companies Learn Your Secrets. https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Edmundson, C., & Hartman, K. G. (2022). SANS 2022 DevSecOps Survey: Creating a Culture to Significantly Improve Your Organization's Security Posture. SANS. https://www.sans.org/white-papers/sans-2022-devsecops-survey-creating-culture-improve-organization-security

French, A. M., Risius, M., & Shim, J. P. (2020). The Interaction of Virtual Reality, Blockchain, and 5G New Radio: Disrupting Business and Society. *Communications of the Association for Information Systems*, 46(1), 603-618. https://doi.org/10.17705/1CAIS.04625

Gartner. (2020). Gartner Predicts 75% of CEOs Will Be Personally Liable for Cyber-Physical Security Incidents by 2024. https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl

Glisson, W. B., & Welland, R. (2014). Web Engineering Security (WES) Methodology. *Communications of the Association for Information Systems*, 34(1), 1359-1396. https://doi.org/10.17705/1CAIS.03471

Goodin, D. (2021). As Log4Shell Wreaks Havoc, Payroll Service Reports Ransomware Attack. https://arstechnica.com/information-technology/2021/12/as-log4shell-wreaks-havoc-payroll-service-reports-ransomware-attack

Hackbarth., R., Mockus, A., Palframan, J., & Sethi, R. (2016). Improving Software Quality as Customers Perceive It. *IEEE Software*, 33(4), 40-45. https://doi.org/10.1109/MS.2015.76

IBM. (2020). What Is DevSecOps? https://www.ibm.com/cloud/learn/devsecops

Kaspersky. (2022). What Are the Security and Privacy Risks of VR and AR. https://www.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr

Kovach, S. (2021). Here's How Zuckerberg Thinks Facebook Will Profit by Building a 'Metaverse.' https://www.cnbc.com/2021/07/29/facebook-metaverse-plans-to-make-money.html

Landi, H. (2022). Healthcare Data Breaches Hit All-Time High in 2021, Impacting 45M People. https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people

Luna-Nevarez, C., & McGovern, E. (2021). The Rise of the Virtual Reality (VR) Marketplace: Exploring the Antecedents and Consequences of Consumer Attitudes Toward V-Commerce. *Journal of Internet Commerce*, 20(2), 167-194. https://doi.org/10.1080/15332861.2021.1875766

Mahmood, B. (2021). Prioritizing CWE/SANS and OWASP Vulnerabilities: A Network-Based Model. *International Journal of Computing and Digital Systems*, 10(1), 361-372. http://dx.doi.org/10.12785/ijcds/100137

McAfee. (2020). McAfee Labs Threats Report 2020. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-nov-2020.pdf

Microsoft. (2016). Security Development Lifecycle. https://www.microsoft.com/en-us/download/details.aspx?id=29884

Microsoft. (2022). Microsoft Threat Modeling Tool Threats. https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats

Nair, V., Garrido, G. M., & Song, D. (2022). Exploring the Unprecedented Privacy Risks of the Metaverse, *arXiv preprint arXiv:2207.13176*. https://doi.org/10.48550/arXiv.2207.13176

National Institute of Standards and Technology (NIST). (2002). The Economic Impacts of Inadequate Infrastructure for Software Testing. https://www.nist.gov/system/files/documents/director/planning/report02-3.pdf

National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology (NIST). (2020). NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management. https://www.nist.gov/privacy-framework/privacy-framework

National Institute of Standards and Technology (NIST). (2022). Secure Software Development Framework (SSDF) Version 1.1: Recommends for Mitigating the Risk of Software Vulnerabilities. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf

O'Brolcháin, F., Jacquemard, T., Monaghan, D., O'Connor, N., Novitzky, P., & Gordijn, B. (2016). The Convergence of Virtual Reality and Social Networks: Threats to Privacy and Autonomy. *Science and Engineering Ethics*, 22(1), 1-29. https://doi.org/10.1007/s11948-014-9621-1

Open Web Application Security Project (OWASP). (2021). OWASP Top Ten. https://owasp.org/www-project-top-ten

Roach, J. (2021). Mesh for Microsoft Teams Aims to Make Collaboration in the 'Metaverse' Personal and Fun. https://news.microsoft.com/innovation-stories/mesh-for-microsoft-teams

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, 8(2), 1-18. https://doi.org/10.3390/healthcare8020133

Shevchenko, N., Chick, T. A. O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). Threat Modeling: A Summary of

Available Methods. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=524448

Slater, M., (2003). A Note on Presence Terminology, *Presence Connect*, 3(3), 1-5.

Slater, M. & Wilbur, S. (1997). A Framework for Immersive Virtual Environments (FIVE): Speculations on the Role of Presence in Virtual Environments. *Presence: Teleoperators & Virtual Environments*, 6(6), 603-616. https://doi.org/10.1162/pres.1997.6.6.603

Souppaya, M., Ogata, M., Watrobsi, P., & Scarfone, K. (2022). Software Supply Chain and DevOps Security Practices. NIST. https://www.nccoe.nist.gov/sites/default/files/2022-11/dev-sec-ops-project-description-final.pdf

Stephenson, N. (1992). *Snow Crash*. New York, NY: Bantam Books.

Steuer, J. (1992). Defining Virtual Reality: Dimensions Determining Telepresence. *Journal of Communication*, 42(4), 73-93. https://doi.org/10.1111/j.1460-2466.1992.tb00812.x

Sutanto, J., Palme, E., Tan, C. H., & Phang, C. W. (2013). Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. *MIS Quarterly*, 37(4), 1141-1164. https://www.jstor.org/stable/43825785

Swinhoe, D. (2020). What Is the Cost of a Data Breach? https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html

Tracy, R. (2020). Small Business, Big Impact With NIST's Cybersecurity Framework. https://www.forbes.com/sites/forbestechcouncil/2020/07/15/small-business-big-impact-with-nists-cybersecurity-framework/?sh=6a44ef4171b6

Tung, L. (2021). Microsoft: SolarWinds Attack Took More Than 1,000 Engineers to Create. https://www.zdnet.com/article/microsoft-solarwinds-attack-took-more-than-1000-engineers-to-create

Wall, J., Lowry, P. B., & Barlow, J. B. (2015). Organizational Violations of Externally Governed Privacy and Security Rules: Explaining and Predicting Selective Violations under Conditions of Strain and Excess. *Journal of the Association for Information Systems*, 17(1), 39-76. https://doi.org/10.17705/1jais.00420

Walsh, K. R. & Pawlowski, S. D. (2002) Virtual Reality: A Technology in Need of IS Research. *Communications of the Association for Information Systems*, 8(1), 292-313. https://doi.org/10.17705/1CAIS.00820

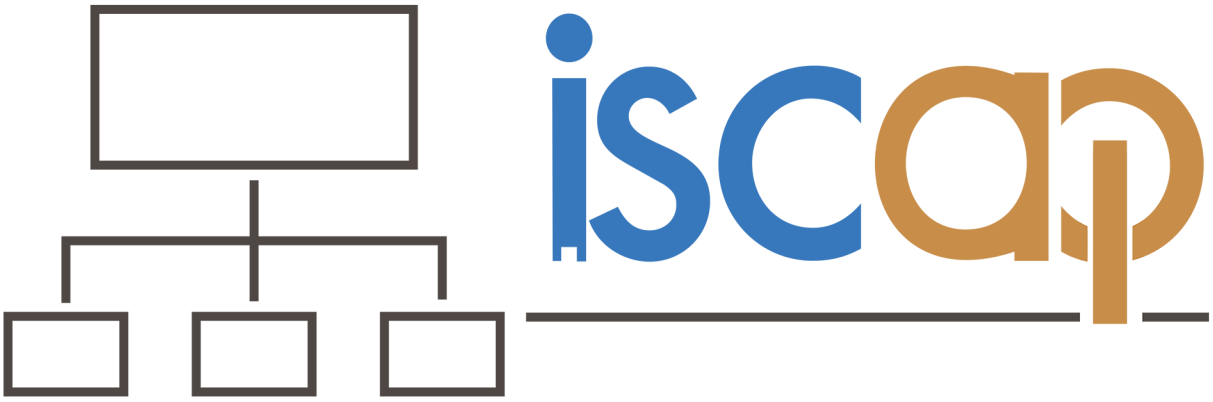
Winder, D. (2019). Data Breaches Expose 4.1 Billion Records in First Six Months of 2019. https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=394316c4bd54

AUTHOR BIOGRAPHIES

Ersin Dincelli is an associate professor of information systems in the Business School at the University of Colorado Denver. His research involves the behavioral aspects of information security and human-computer interaction (HCI). In particular, he studies individuals' decision-making processes and behaviors in the context of information security and privacy, privacy-invasive technologies, designing innovative security education, training, and awareness (SETA) programs, and HCI design for emerging technologies. His work has been published in academic journals, such as the *Journal of the Association for Information Systems*, *European Journal of Information Systems*, *Journal of Strategic Information Systems*, *Communications of the Association for Information Systems*, *Government Information Quarterly*, *Information Systems Frontiers*, *Behaviour & Information Technology*, and *IEEE IT Professional*.

Alper Yayla is an associate professor and the Director of the Cybersecurity Programs in the Sykes College of Business at the University of Tampa. His research interests include the impact of technology on organizations and individuals, with a focus on cybersecurity and emerging technologies. His work has been published in several academic journals, including *Decision Sciences*, *European Journal of Information Systems*, *Journal of Information Technology*, *Journal of Strategic Information Systems*, *Communications of the Association for Information Systems*, *International Journal of Electronic Commerce*, *Information Systems Management*, and *IEEE IT Professional*.

INFORMATION SYSTEMS & COMPUTING ACADEMIC PROFESSIONALS



STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)