SPARK: Exposing Vulnerabilities in Collaborative Display Systems and Session-Key Exposure

Emerson Darlington, Marissa Gist, Sana Goyal, Isabelle Feigenberg, Fanxing (Amy) Fei, Claire Lu, Yige (Yoyo) Lu, Audrey Lawler, Stella Mrockowski, Laura Messamore, Rachel Mirin, Sabine Kim, Nikoletta Kuvaeva, Huanyan (Hanne) Li, Kyla Walker, Whitney Shissler, Hanna Shevade, Olivia Stankiewicz-Goldsmith, Yanzi (Ruby) Zeng and Thomas Heverin
The Baldwin School, Bryn Mawr, PA, USA

thomas.heverin@baldwinschool.org

Abstract: This study investigates the vulnerabilities of Solstice Pods, wireless collaboration devices often used in academic environments, focusing on universities with publicly exposed devices. We analyzed 22 universities, each with 10 or fewer Solstice Pods exposed on Censys.io, a platform for identifying publicly exposed devices. This subset was selected to emphasize vulnerabilities in smaller, publicly exposed systems, without excluding large institutions that may have only a few devices exposed. Our research centers on unauthorized access to device configuration pages and the retrieval of live session keys, which are critical for screen sharing. From 81 exposed Solstice Pods, we manually examined several IP addresses and found that critical configurations, including screen-key disabling, password changes, and session key retrieval, were accessible in some cases. To scale testing, we developed the Solstice Pod Access Retrieval Key (SPARK), a Python tool using SSL/TLS requests to interact with the devices' configuration pages. The SPARK tool successfully generated live session keys in 13 instances across 9 universities, while 68 attempts failed. Statistical analysis revealed that self-signed certificates (issued by Mersive, the Solstice Pod vendor) significantly reduced vulnerability to the SPARK tool, with a success rate of 8.33% for devices using self-signed certificates, compared to 63.89% for those with non-self-signed certificates. To assess the statistical significance of this difference, Chi-square and Fisher's exact tests were performed, yielding p-values of 0.0464 and 0.0231, respectively. Additionally, a proportions test showed a highly significant result with a p-value of 0.00077. This study underscores the risks of publicly exposed Solstice Pods and highlights the real-world consequences of these vulnerabilities. If exploited, these vulnerabilities could lead to unauthorized access to sensitive data, disruption of university operations, and compromise of ongoing academic collaborations. The findings call for stronger security measures, particularly the use of self-signed certificates, to reduce vulnerabilities and protect sensitive information in these devices.

Keywords: Solstice pods, Session key retrieval, Certificate configuration, Self-signed certificates

1. Introduction

In today's academic and organizational environments, collaboration tools such as Solstice Pods are crucial for facilitating real-time communication and data sharing. These wireless devices allow multiple devices to share content onto a central display and are widely used in meeting rooms and classrooms. However, with the increasing adoption of Internet of Things (IoT) devices, security concerns have become more prominent. Devices exposed to the public internet, especially those lacking robust security measures (such as encryption or self-signed certificates), are highly susceptible to cyberattacks, leading to unauthorized access and service disruptions.

While existing research addresses general university cybersecurity issues, a critical gap remains in understanding the specific risks facing smaller, decentralized deployments of IoT devices (such as classroom display systems) within academic settings. Universities often comprise numerous networks managed by diverse entities, many of which operate outside the direct oversight of central information security teams (Ulven, Bjørge, & Wangen, 2021). This decentralized management can lead to departments or individuals deploying devices independently, potentially without adhering to university-wide cybersecurity policies and best practices (Ghazvini, Shukur and Hood, 2018). Consequently, smaller deployments of devices like Solstice Pods, while individually seeming less significant, may collectively represent a substantial and often overlooked attack surface.

This study aims to address this gap by focusing on 22 universities, each with fewer than 10 publicly exposed Solstice Pods, examining their security vulnerabilities, particularly unauthorized access to configuration pages and the retrieval of session keys. The research employs a combined approach of manual examination and an automated tool, the Solstice Pod Access Retrieval Key (SPARK), to enhance testing efficiency. We acknowledge that the relatively small number of publicly exposed devices does not reflect the likely scale of total Solstice Pod deployments within these universities. Rather, these publicly accessible devices serve as a starting point for investigating potential vulnerabilities that may also exist within the larger, often less visible, internal

networks of these institutions. Our focus on these exposed devices allows us to establish a baseline for understanding the security posture of Solstice Pods in academic settings and to infer potential risks present in the broader deployments.

Our research is important because the exploitation of Solstice Pod vulnerabilities can have serious real-world consequences. If compromised, these devices could allow attackers to access sensitive data, disrupt critical university operations, and undermine academic collaboration. For example, unauthorized access to a Solstice Pod's configuration page could enable an attacker to hijack ongoing presentations or classes, compromising intellectual property, disrupting lectures, and affecting the quality of education. Additionally, the retrieval of session keys could lead to a broader breach, allowing malicious actors to view or manipulate sensitive content in real-time (Haney, Furman, and Acar, 2020; Kamenskih 2022). These vulnerabilities pose a direct threat to the privacy of students and faculty, potentially leading to data breaches that could damage the institution's reputation and erode trust within the academic community.

2. Background

2.1 Cybersecurity Risks in Higher Education

The increasing frequency and severity of cyberattacks targeting universities is a significant and growing concern. Universities hold vast amounts of sensitive data, including research findings, student records, and financial information, making them prime targets for cybercriminals (Ulven & Wangen, 2021). This susceptibility is further compounded by the very nature of university environments, which often prioritize open access and collaboration, sometimes at the expense of security protocols. The potential consequences of a successful attack can be devastating, ranging from the loss of valuable intellectual property to the disruption of critical university operations and the erosion of public trust.

Several factors contribute to the heightened vulnerability of universities. Phishing attacks, which exploit human error, remain a persistent and prevalent threat in educational institutions (Bandara et al., 2021). These attacks often target staff and students, attempting to trick them into revealing login credentials or other sensitive information. Furthermore, the rapid expansion of technology within universities, particularly the shift towards remote and hybrid learning models, has broadened the attack surface considerably. The increased reliance on IoT devices, such as Solstice Pods, and the use of personal devices on university networks introduce new vulnerabilities that can be exploited by malicious actors (Pósa & Grossklags, 2022). These devices, if not properly secured, can serve as entry points for attackers to gain access to sensitive university systems.

The integration of IoT devices in educational settings presents unique security challenges (Alexei & Alexei, 2021). The complexity of these systems, coupled with the often-limited resources available for cybersecurity management, can make it difficult for universities to effectively secure these devices. Unsecured networks, bring-your-own-device (BYOD) policies, and inconsistent security practices across different departments further exacerbate these vulnerabilities (Ulven, Bjørge, & Wangen, 2021). Often, these technical vulnerabilities are compounded by organizational challenges, including a lack of senior management support for cybersecurity initiatives, resistance to security measures within academic environments, and insufficient security awareness among staff and students.

These organizational shortcomings create opportunities for social engineering attacks, which exploit human psychology to bypass technical defenses (Bjørge & Wangen, 2021; Cheng & Wang, 2022). Attackers may impersonate trusted individuals or organizations to manipulate staff and students into divulging confidential information or performing actions that compromise security. The threat landscape also includes financially motivated cybercriminals, nation-state actors targeting intellectual property, and insiders with malicious intent (Ulven, Bjørge, & Wangen, 2021). Effectively addressing these multifaceted threats requires a comprehensive approach that encompasses robust technical safeguards, ongoing cybersecurity education and training, and strong organizational commitment to security best practices. Proactive security measures and continuous monitoring are essential to mitigate the risks posed by these evolving cyber threats (Pósa & Grossklags, 2022).

2.2 Cybersecurity Issues with Display Technologies

Classroom display screens, increasingly integrated into smart educational environments, present various security vulnerabilities that can compromise both user privacy and institutional data integrity. These vulnerabilities span several key areas, including network security risks, data privacy concerns, and physical security threats.

One significant vulnerability stems from the integration of classroom display screens into broader smart education ecosystems, which often rely on interconnected devices and cloud services. As Kamenskih (2022) highlights, the architecture of smart educational environments must carefully consider the interaction points between users and technology, as these interactions can expose sensitive information to unauthorized access. This risk is further compounded by a general lack of user awareness regarding the security implications of these technologies. Haney, Furman, and Acar (2020) note that users may not take necessary precautions to protect their data, a particularly concerning issue in educational settings where sensitive student information is frequently displayed or processed.

Network security is another critical area of concern. Classroom display screens are typically connected to local networks, which can be susceptible to various cyber threats. If these screens are not adequately secured, they could serve as entry points for attackers, potentially granting access to the broader network and leading to data breaches or unauthorized control over other connected devices (Haney et al., 2020). The vulnerabilities associated with smart technologies, including classroom displays, can be exacerbated by inadequate security measures and a lack of transparency in device configurations, leaving users vulnerable to exploitation (Haney et al., 2020).

Data privacy is also a pressing issue. Classroom display screens may collect and display personal information about students and staff. The integration of cloud services in educational settings raises concerns about how this data is stored, processed, and shared. Kim, Yang, and Kim (2016) emphasize that reliance on cloud-based learning management systems (LMS) can introduce vulnerabilities if proper security protocols are not implemented. Furthermore, the potential for data interception during transmission poses additional risks, especially if sensitive information is displayed on these screens without adequate encryption (Kamenskih, 2022).

Physical security threats should not be overlooked. Classroom display screens can be physically tampered with, potentially leading to unauthorized access to displayed content or manipulation of the device itself. This risk is heightened in environments where multiple users have access to the same physical space. Cebrián, Martín, and Recalde (2020) discuss the importance of training educators on the secure use of smart classroom technologies. Without proper training and awareness, educators may inadvertently expose themselves and their students to security risks. Addressing these multifaceted concerns requires a comprehensive approach that includes robust security protocols, ongoing user education, and continuous monitoring of these systems.

2.3 Solstice Pods Overview

Solstice Pods are wireless collaboration devices that enable multiple users to wirelessly share content from various devices to a central display. These devices support several connectivity methods, including AirPlay, Miracast, Mersive's proprietary apps, and web-based sharing. Designed to simplify audio-visual (AV) systems in meeting rooms and classrooms, Solstice Pods facilitate real-time collaboration and enhance the efficiency of team-based environments. Figure 1 illustrates a typical setup involving the device.

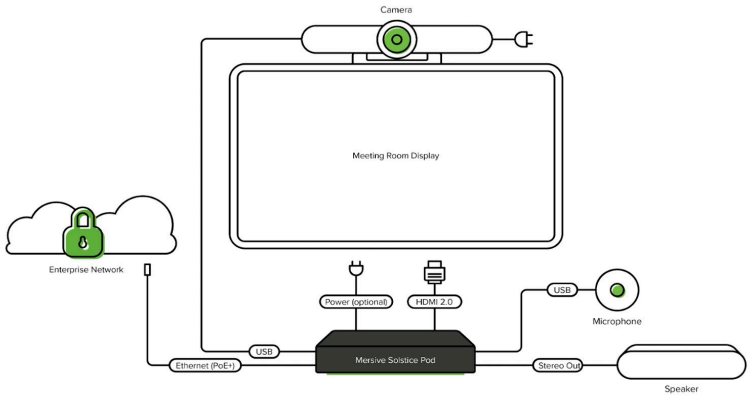

Figure 1: Typical set up of a Solstice Pod

Despite their advanced functionality, four vulnerabilities have been identified in Solstice Pods, which expose these devices to potential unauthorized access and exploitation. These vulnerabilities have been documented in various security advisories and the National Vulnerability Database (NVD), highlighting critical security concerns (NIST, 2025).

Existing research often focuses on large deployments or general IoT security risks, leaving a critical gap in understanding the vulnerabilities specific to smaller, decentralized deployments. These smaller deployments, often managed independently by individual departments or staff, may lack the resources or oversight necessary for robust security measures. This gap is particularly concerning because, while smaller deployments like those with fewer than 10 devices may seem less significant, they can collectively represent a substantial attack surface. By focusing on these less visible, yet highly vulnerable, systems, this research aims to uncover risks that are often overlooked in broader studies of higher education security.

3. Methodology

This research adhered to a structured and systematic approach, following best practices outlined in the Penetration Testing Execution Standard (PTES). The methodology was divided into several phases: identifying exposed devices, performing manual testing, developing the SPARK to automate the testing, and analyzing the results through statistical tests.

3.1 Identification of Exposed Solstice Pods and Test Set

The first phase of the research involved identifying exposed Solstice Pods using Censys.io. Censys is an internet intelligence platform that indexes publicly accessible devices, providing detailed metadata about the services they offer. Using the search term "solstice", we identified over 1,600 Solstice Pods exposed across the internet.

We narrowed the focus to universities with exposed Solstice Pods, filtering out large deployments based on the Autonomous System Numbers (ASN) associated with the devices. ASNs define network groups under a common routing policy. We analyzed these groups to identify universities with smaller, publicly exposed deployments. We found 26 universities with publicly accessible Solstice Pods, and many universities had 10 or fewer devices exposed. After excluding institutions with more than 10 exposed devices, we focused on 22 universities, leading to a total of 81 Solstice Pods across these institutions, which formed the test set for this research.

3.2 Manual Testing of Exposed Devices

After identifying the 81 exposed Solstice Pods, a subset was selected for manual testing. This phase followed the “Vulnerability Analysis” component of PTES (2014), focusing on determining whether the exposed configuration pages of these devices could be accessed and manipulated without authentication. We connected to the devices over Port 8443, which provided access to configuration pages on many devices.

These pages allowed unauthorized access to critical settings, such as:

- Device passwords
- Session key configurations
- Screen sharing controls

In some cases, we successfully manipulated these settings and retrieved session keys—critical components for content sharing between users and the Solstice Pod. These findings were crucial for understanding how easily these devices could be exploited by attackers if exposed on the public internet.

We found that self-signed certificates, which are self-signed by Mersive, are the default configuration for Solstice Pods per Mersive’s documentation (https://documentation.mersive.com/). These certificates provide internal validation but are not trusted by external parties. This self-signed configuration was tested alongside devices using non-self-signed certificates that are signed by external Certificate Authorities (CAs), such as Sectigo, for enterprise deployments.

3.3 Development of the Solstice Pod Access Retrieval Key (SPARK) Tool

To streamline vulnerability testing, we developed a Python-based tool, SPARK, which automates the retrieval of exposed data, including session keys and configuration information. Manual testing was time-consuming, so SPARK was created to expedite this process by sending automated requests to the devices. The tool uses SSL/TLS requests to interact with Solstice Pods over HTTPS, ensuring secure communication and minimizing detection risk.

SPARK employs a custom-built "SSLAdapter" class that specifies the SSL/TLS version and disables hostname verification. This allows the tool to bypass SSL/TLS errors caused by misconfigured certificates, which is crucial for data retrieval. The tool appends relevant strings to IP addresses to automate testing for vulnerabilities such

as session key retrieval. By using threading, SPARK enables concurrent testing of multiple IP addresses, which reduces testing time and allows for the analysis of a larger set of devices. Each thread sends a GET request to the Solstice Pod's API endpoint to retrieve session keys. If a key is found, it is printed; otherwise, the tool reports its absence.

This automated approach aligns with the "Exploitation" phase of PTES (2014), where tools like SPARK are used to identify and exploit vulnerabilities at scale. The ability to query devices concurrently enables a more efficient, comprehensive vulnerability assessment.

3.4 Ethical Considerations and Responsible Disclosure

We adhered to ethical hacking guidelines, following the “Post-Exploitation” and “Reporting” phases as outlined in PTES (2014), and followed responsible disclosure protocols which allowed institutions to take corrective action (CISA, 2020). Our primary goal was to identify vulnerabilities, and no attempts were made to exploit them for malicious purposes. Upon confirming vulnerabilities, detailed reports, including proof of concept and recommended mitigation strategies, were shared with the affected universities and Mersive for further analysis and remediation. This approach reflects our commitment to cybersecurity best practices and the protection of sensitive information while facilitating prompt resolution of identified risks.

4. Results

4.1 Identification of Exposed Solstice Pods

Our initial search on Censys.io revealed over 1,600 exposed Solstice Pods. After filtering for universities with publicly available devices and reviewing ASNs, we narrowed down our focus to 26 universities. We focused on universities with fewer than 10 publicly exposed Solstice Pods, as smaller, decentralized deployments of IoT devices, often independently managed by departments or individuals, can represent a significant but overlooked attack surface. The final test set consisted of 81 Solstice Pods from 22 universities, all of which had 10 or fewer exposed devices.

Figure 2 presents the distribution of exposed Solstice Pods across the 22 universities, highlighting the number of devices exposed by each institution.

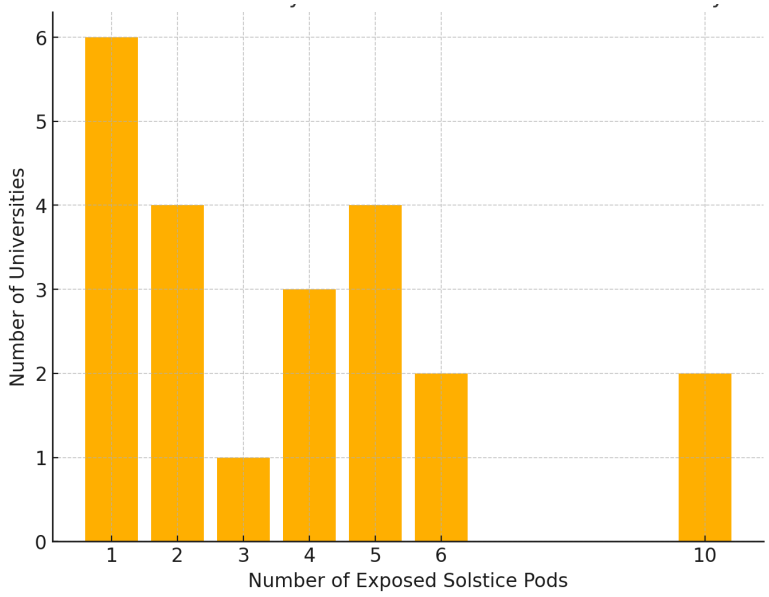

Figure 2: The number of Solstice Pods distributed across universities

4.2 Manual Testing Results

Further manual analysis showed that many devices had unprotected configuration pages that could be accessed without any authentication. The exposure of these pages allowed unauthorized modification of device settings, including disabling the screen key, changing device passwords, and altering display settings. Figure 3 shows the main page of a targeted Solstice Pod, while Figures 4 to 7 show other pages accessed with no login required.

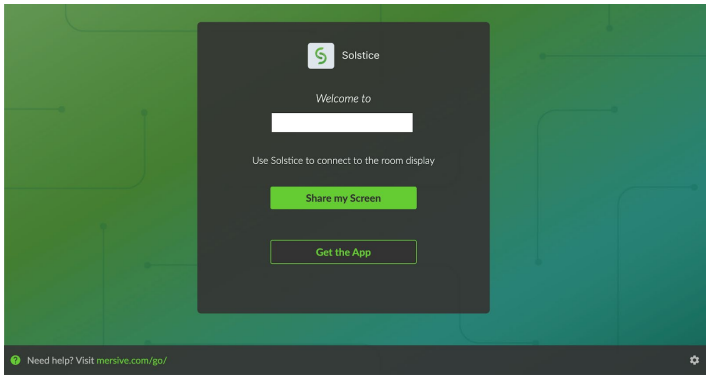

Figure 3: Main page of a targeted Solstice Pod

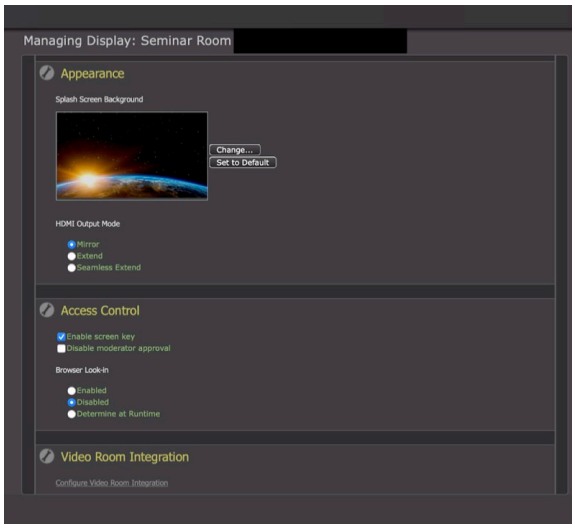

Figure 4: Appearance, access control, and video room integration settings exposed on a vulnerable Solstice Pod

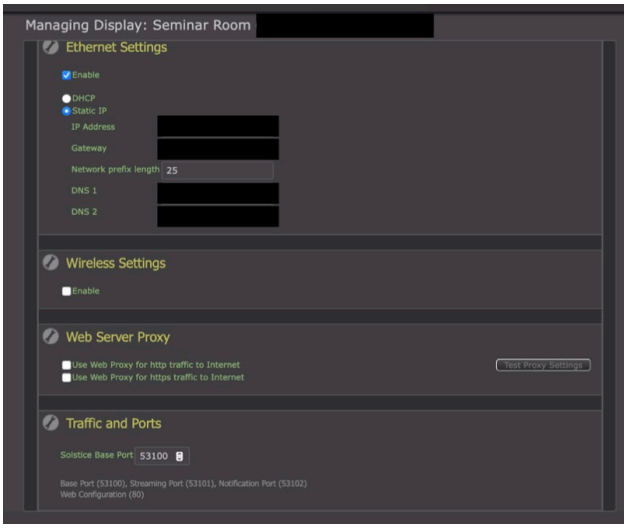

Figure 5: Ethernet, wireless, web server, and network traffic settings exposed on a vulnerable Solstice Pod

By appending specific text to the IP addresses of the exposed Solstice Pods, we successfully retrieved dynamic session keys used for screen sharing. These keys are for sharing content between users and the Solstice Pod. Our findings showed that session keys could be retrieved without proper authentication, which allowed for unauthorized access to ongoing presentations or meetings.

Figure 6 shows the screen that appears to enter the session key for a targeted Solstice Pod.

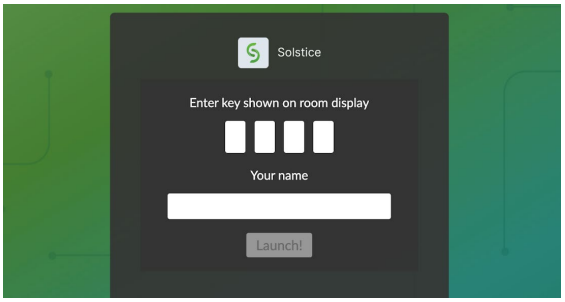

Figure 6: Display screen for entering live session key to access screen sharing

After appending specific text to the end of the IP address and locating the live session key, we were able to fully compromise many Solstice Pod display screens across universities. Upon compromising Solstice Pod screens, we were able to display a hacking logo as shown in Figure 7.

Figure 7: The Baldwin Ethical Hacker's logo is displayed on compromised Solstice Pod display screens

4.3 Automated Testing with SPARK

SPARK testing results across 81 Solstice Pods can be summarized with the following data. The automated tool successfully retrieved session keys from 13 of the 81 devices (16.0%). In contrast, 68 devices (84.0%) were resistant to the attack, showing that not all exposed devices were vulnerable to session key exploits. Notably, 50 devices (61.7%) used self-signed certificates, while 31 devices (38.3%) used non-self-signed certificates. It was found that devices with self-signed certificates were less likely to have their session key retrieved.

4.4 Statistical Analysis of Key Generation Success

We conducted various statistical tests to determine statistically significant associations, relationships, and differences.

The Chi-Square Test of Independence was performed to determine if there was a significant association between certificate type (self-signed vs. non-self-signed) and the outcome of the SPARK testing (whether session key retrieval was successful or not). The chi-square statistic returned a value of 3.97 with a p-value of 0.0464. This p-value is below the typical threshold of 0.05, indicating that there is a statistically significant relationship between the certificate type and the likelihood of a successful key generation. This suggests that Solstice Pods with non-self-signed certificates are more vulnerable to session key retrieval attacks compared to those with self-signed certificates.

To further confirm the results from the chi-square test, we conducted the Fisher's Exact Test. The test produced a p-value of 0.0231, also below the 0.05 significance threshold. This confirms that the observed relationship between certificate type and vulnerability is not due to chance and further supports the finding that non-self-signed certificates are more likely to allow session key retrieval.

Finally, we conducted a Proportions Test to compare the success rate of key generation between Solstice Pods with self-signed certificates and those with non-self-signed certificates. The self-signed certificates showed a success rate of 8.33% in generating session keys, whereas non-self-signed certificates had a significantly higher success rate of 63.89%. The p-value from the Proportions Test was 0.00077, indicating a statistically significant

difference between the two groups. This suggests that devices with self-signed certificates are much less vulnerable to session key retrieval attacks, emphasizing the protective role of self-signed certificates in enhancing the security of Solstice Pods.

5. Discussion

5.1 Summary of Statistical Findings

The results from all three statistical tests consistently indicate that self-signed certificates (through Mersive) significantly reduce the vulnerability of Solstice Pods to session key retrieval attacks. Specifically:

- The Chi-Square Test yielded a p-value of 0.0464, indicating a statistically significant relationship between certificate type and vulnerability.
- The Fisher's Exact Test produced a p-value of 0.0231, reinforcing the significance of the relationship.
- The Proportions Test confirmed that non-self-signed certificates have a higher rate of successful key generation (63.89%) compared to self-signed certificates (8.33%), with a p-value of 0.00077.

The self-signed certificates by Mersive likely limit exposure, thus reducing the risk of successful attacks. Devices with non-self-signed certificates are significantly more vulnerable to key generation exploits, which can compromise the confidentiality of shared content in collaborative environments. This is particularly significant because Solstice Pods are widely deployed in academic settings where sensitive data, such as student information and proprietary content, may be shared. Universities must recognize the potential risks posed by publicly exposed devices.

Additionally, Haney et al. (2020)'s assertion that many IoT devices—including those used for collaboration—are inadequately secured, thus amplifying the risks in environments where the security of shared content is paramount. Unauthorized retrieval of session keys allows attackers to hijack presentations or view sensitive content, which aligns with previous literature emphasizing the need for secure protocols in collaborative technologies (Kamenskih, 2022; Haney et al., 2020). This supports Cebrián et al. (2020), who argue that vulnerabilities in smart devices like collaboration tools can lead to significant risks if not properly secured.

5.2 Implications for University Cybersecurity

The findings highlight the critical role of device configuration in securing Solstice Pods and similar collaborative technologies. Given the results, we recommend that institutions prioritize the use of self-signed certificates or ensure that certificates are properly configured with robust security measures to minimize exposure. This recommendation aligns with Kamenskih (2022), who advocates for self-signed certificates as a potential solution to secure smart education technologies. Additionally, universities should take a proactive approach in conducting regular security audits of all publicly exposed devices to identify and address vulnerabilities before they can be exploited.

5.3 Limitations of the Study

While this study provides valuable insights into the security risks associated with publicly exposed Solstice Pods, there are several limitations. The focus was specifically on publicly exposed devices through Censys.io, which means that the results may not fully capture vulnerabilities in devices behind firewalls or within more secure internal networks. This limitation echoes the concerns raised by Haney et al. (2020) regarding the underreporting of vulnerabilities in internal networks, particularly those devices that are not publicly exposed but still vulnerable within closed environments.

Future studies should aim to assess the internal network vulnerabilities of Solstice Pods, as well as explore potential risks in devices that are not publicly exposed but remain susceptible to attacks within the network.

Additionally, other security risks such as attacks on device firmware or wireless communication that could further compromise the security of collaborative devices were not explored.

5.4 Recommendations for Future Research

This study lays the groundwork for further exploration into the security of collaborative display technologies, particularly in environments where sensitive data is shared. Given the success of the SPARK in automating testing, future research could further develop SPARK to expand testing to a broader range of collaborative devices and device configurations. We recommend that future studies focus on the following areas:

- The internal vulnerabilities of Solstice Pods, especially those in more secure environments that are less likely to be publicly exposed but still susceptible to internal attacks.
- A broader analysis of device configurations and security protocols beyond certificates, considering other vulnerabilities such as firmware exploits and authentication flaws.

Furthermore, as the deployment of IoT devices in academic and professional environments continues to rise, there is a growing need for multifaceted security strategies that combine both technical defenses and user education to address security vulnerabilities. This is in line with Kamenskih (2022)'s call for integrated solutions that not only improve device security but also raise awareness among users about the risks posed by insecure devices. This also corresponds call for effective security policies (Ghazvini, Shukur and Hood, 2018) and for a large-scale approach to university protection (Cheng and Wang, 2022).

6. Conclusion

This study highlights the significant cybersecurity vulnerabilities of IoT devices like Solstice Pods, particularly in environments where these devices are publicly exposed, such as universities. Our analysis revealed critical weaknesses that could allow attackers to access sensitive data and disrupt collaboration sessions by exploiting poorly configured devices. With the SPARK tool, we demonstrated how these vulnerabilities can be efficiently tested, enabling the automated retrieval of live session keys and showcasing the risks of unauthorized access to configuration pages. These findings underscore the urgent need for universities and organizations to adopt more rigorous security practices, particularly in academic environments where sensitive information is frequently shared. Moreover, our results highlight the importance of using strong encryption methods, such as self-signed certificates, to mitigate vulnerabilities. As IoT devices continue to play an integral role in academic and organizational functions, ensuring their security is essential to protect privacy, safeguard intellectual property, and maintain operational continuity.

References

Alexei, A., & Alexei, A. (2021). Analysis of IoT security issues used in higher education institutions. *International Journal of Mathematics and Computer Research*, 9(5).

Bandara, I., Balakrishna, C., & Ioraş, F. (2021). The need for cyber threat intelligence for distance learning providers and online learning systems. *INTED2021 Proceedings*.

Cebrián, G., Martín, R., & Recalde, J. (2020). The smart classroom as a means to the development of ESD methodologies. *Sustainability*, 12(7), 3010.

Cheng, E., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, 13(4).

CISA. (2020). Coordinated vulnerability disclosure process. https://www.cisa.gov/coordinated-vulnerability-disclosure-process

Ghazvini, A., Shukur, Z., & Hood, Z. (2018). Review of information security policy based on content coverage and online presentation in higher education. *International Journal of Advanced Computer Science and Applications*, 9(8).

Gill, S., & Vij, P. (2020). Security ambiguity and vulnerability in G2C e-governance system: Empirical evidence from Indian higher education. *Indian Journal of Science and Technology*, 13(34), 3515-3520.

Haney, J., Furman, S., & Acar, Y. (2020). Research report: User perceptions of smart home privacy and security. National Institute of Standards and Technology.

Kamenskih, A. (2022). The analysis of security and privacy risks in smart education environments. *Journal of Smart Cities and Society*, 1(1), 17-29.

Kim, D., Yang, S., & Kim, S. (2016). Advanced smart learning using cloud service-based LMS. *Advanced Science and Technology Letters*, 134, 29-34.

National Institute of Standards and Technology. (2025). *National Vulnerability Database*. U.S. Department of Commerce. https://nvd.nist.gov/vuln/search

Penetration Testing Execution Standard. (2014). *Penetration Testing Execution Standard*. http://www.pentest-standard.org/

Pósa, T., & Grossklags, J. (2022). Work experience as a factor in cybersecurity risk awareness: A survey study with university students. *Journal of Cybersecurity and Privacy*, 2(3), 490-515.

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, 13(2), 39.