IoT Security in Schools

Application Security Article

Léo Gabaix - Francesco Mosanghini

Master of Cybersecurity 2023

Abstract

This document explores the dynamic interplay of IoT technology in the educational sector, particularly focusing on its applications, cybersecurity challenges, and regulatory considerations. IoT, by connecting 'smart objects' to the internet, revolutionizes various aspects of school operations, from resource management and energy efficiency to enhanced learning experiences through tools like smart boards and digital textbooks. However, the proliferation of these technologies brings significant cybersecurity risks, such as data breaches and network vulnerabilities, particularly in the context of schools. The document discusses the importance of robust security measures, including regular software updates, secure password practices, and network monitoring, alongside adherence to regulations like GDPR and FERPA. It also highlights real-world incidents like the Harvard Computer Society email privacy breach, underscoring the necessity for vigilance and proactive measures in securing IoT devices in educational environments.

Table of content

1. Introduction

1.1. Whats is IoT?

The Internet of Things (IoT) connects physical objects, or "things" embedded with sensors, software, and technology to exchange data over the internet. These "smart objects", ranging from household items to industrial tools, are expected to increase from over 7 billion today to 22 billion by 2025. IoT devices, including smart home devices, wearables, and sophisticated machinery, form a vast network that communicates and performs tasks autonomously. They enable diverse applications such as environmental monitoring on farms, traffic management with smart cars, factory operations, and resources management in schools.

1.2. Cybersecurity in IoT

Cybersecurity is critical in IoT, as a single threat could compromise the entire network, potentially giving cybercriminals full system access. In sectors like schools, IoT vulnerabilities can lead to serious data breaches or physical damage. Despite the benefits for businesses, governments, and healthcare, IoT's interconnectedness increases the risk of financial and security damages from hacks. More devices on a network mean more potential entry points for cybercriminals, posing significant threats to defense logistics and national security.

A major issue is that many organizations prioritize IoT's convenience and cost-efficiency, overlooking security risks, leaving overly confident and data-reliant organizations exposed to vulnerabilities.

2. Understanding IoT in Schools

2.1. IoT applications in education

The internet's integration into schools has led to significant advancements in e-learning and the application of IoT in education, revolutionizing safety, resource tracking, and information access in learning environments. Technologies like “smart lesson plans” are enhancing teaching methods. Schools like New Richmond in Ohio are saving significantly, approximately $128,000 annually, by using IoT for energy efficiency and operational cost reduction. The shift to reusable tech like computers and tablets could eliminate the hefty paper costs, typically around $200,000 annually, for schools. Additionally, IoT enables universities to monitor students, staff, and resources more efficiently, contributing to safer campuses and cost savings. Notably, technologies like SMART boards have transformed classroom interactions since 1991, moving away from traditional chalkboards.

2.1.1. Communication and Collaboration

IoT devices like intelligent whiteboards and tablets enable real-time interaction and collaboration among teachers and students, facilitating easier connection and cooperation, even from different locations.

2.1.2. Resource Management

IoT systems help in efficiently managing classroom resources and facilities, ensuring students have necessary materials and optimizing the usage of school facilities for cost savings and effective resource utilization.

2.1.3. Safety and Security

IoT devices improve the safety and security in schools by monitoring buildings, grounds, and buses, using technologies like IoT-enabled cameras and GPS systems for real-time tracking and securing school premises.

2.2. IoT devices commonly used in schools

2.2.1. Tracking Devices

To monitor students' whereabouts, IoT solutions like smart ID cards, school bus trackers, attendance trackers, and parking sensors are used. These systems enable efficient tracking of a large number of students, overcoming the limitations of manual monitoring.

2.2.2. Smart Boards and Textbooks

Interactive digital media such as smart whiteboards, augmented reality (AR), and virtual reality (VR) make learning more engaging and immersive. These tools not only enhance the classroom experience but also allow educators to collect and analyze data, helping them identify gaps in their teaching methods and tailor lessons accordingly. Digital textbooks provide students with up-to-date information, saving costs and being more eco-friendly.

2.2.3. Security Systems

For institutional security, IoT-enabled devices like wireless door locks, facial recognition technology, and surveillance cameras complement traditional security personnel. These advanced systems enhance the safety of students, teachers, and staff, offering protection against sophisticated threats.

2.2.4. HVAC

IoT devices in HVAC systems can significantly improve energy efficiency. By monitoring and analyzing the use of heating, ventilation, and air conditioning in real-time, these systems can adjust settings to optimize energy use. This is especially important for schools operating on tight budgets, as it can lead to substantial cost savings.

3. IoT Security Challenges

3.1. In IoT in general

The diverse ecosystem of IoT, characterized by a variety of devices and platforms each adhering to different standards and protocols, presents a significant challenge in implementing uniform security measures. This complexity is further compounded by resource constraints, as many IoT devices possess limited computational power and storage, thereby limiting the types of security measures that can be feasibly implemented. Additionally, the interconnected nature of IoT devices, often spread across extensive areas, adds another layer of complexity to network security, making it more challenging to secure these networks effectively.

3.2. in IoT for schools

In the realm of IoT in schools, the task of infrastructure management is pivotal, involving the development and maintenance of a secure network infrastructure capable of supporting a diverse array of IoT devices. This necessity, however, is often hampered by resource limitations, particularly budget constraints and a scarcity of IT staff, which can significantly impede the implementation of robust security measures. Compounding this challenge is the technical complexity inherent in managing a wide range of IoT devices, each with its unique security requirements. This technical demand necessitates a rigorous approach to policy and compliance, where establishing and adhering to policies and procedures that align with legal regulations, such as GDPR or FERPA, is critical for ensuring data privacy and security.

Moreover, the aspect of education and awareness plays a crucial role; it is essential to ensure that staff, students, and faculty are not only aware of but also actively adhere to the best practices for IoT security. In tandem with these measures is the issue of physical security, which involves safeguarding IoT devices against theft, damage, or tampering. A key component in maintaining the integrity of these devices is the practice of software and firmware management, which includes regularly updating and patching IoT devices to address new vulnerabilities and ensure their continued secure operation.

4. Risks and potential impact

4.1. List of risks

In the context of IoT in schools, infrastructure management risks are a significant concern. Outdated systems can leave schools struggling to keep their network infrastructure up-to-date, subsequently leading to vulnerabilities in the system. Moreover, inadequate support, characterized by insufficient maintenance or monitoring of the infrastructure, escalates the risk of security breaches. Alongside these challenges are the risks associated with resource limitations. Budget constraints may result in insufficient investment in security solutions, and a limited IT team may lack the necessary expertise to effectively manage and secure a diverse IoT environment.

Adding to these difficulties is the technical complexity involved in standardizing security across various devices, each with different requirements, making the process complex and time-consuming. Policy and compliance risks also pose a threat, with legal liabilities arising from non-compliance with regulations such as GDPR or FERPA, potentially leading to legal and financial penalties. Furthermore, inadequate policies may compromise the privacy of student and staff data.

Education and awareness represent another area of risk. A lack of awareness among students, staff, and faculty can lead to unintentional security breaches, and without proper training, the school community might fail to follow best practices for IoT security. Physical security risks also need to be addressed, as IoT devices are often vulnerable to theft, damage, or sabotage, particularly in accessible areas. Unauthorized access or physical tampering with these devices can lead to compromised network security.

Finally, software and firmware management risks are critical to consider. Outdated software or failure to regularly update and patch IoT devices can leave them vulnerable to exploitation. Additionally, new vulnerabilities might be exploited before patches are available, making devices susceptible to zero-day attacks. These multifaceted risks underscore the need for comprehensive and proactive measures in managing IoT security in educational settings.

4.2. Potential impacts

The impact of diverse ecosystem risks in schools includes system inefficiencies, where incompatibilities between various IoT devices can lead to operational inefficiencies in IoT system operations. This complexity also heightens the risk of increased security breaches, as managing a diverse range of devices makes it more challenging to safeguard sensitive data effectively.

Resource constraints present another significant risk. Devices with limited resources might fail to perform optimally, especially under security constraints, adversely affecting educational and administrative functions. Additionally, these devices are more vulnerable to cyberattacks due to their inability to support advanced security features, leading to potential data breaches and system disruptions.

Network security risks are particularly concerning. A breach in one part of the network can potentially compromise the entire network, affecting all connected devices and systems. This can lead to widespread system compromises and disrupt digital learning environments, impacting teaching and learning activities.

In terms of infrastructure management risks, schools face operational disruptions due to inadequate infrastructure, leading to frequent system downtimes. These issues also entail long-term financial costs, as rectifying outdated or compromised systems can be expensive.

Resource limitations also pose significant risks. Limited budgets and staff constraints may lead to inadequate security measures, leaving schools vulnerable to attacks. A small IT team might be overburdened with these challenges, potentially leading to oversights in security management.

The complexity of securing a diverse range of IoT devices poses technical challenges. This complexity can overwhelm IT teams, leading to potential security gaps. In terms of policy and compliance, schools face legal and financial repercussions for non-compliance with data protection laws, leading to potential legal actions and fines. Incidents of non-compliance or data breaches can also damage the trust and reputation among parents, students, and staff.

Education and awareness risks involve increased human error due to a lack of proper training, which can lead to security-compromising mistakes such as phishing attacks. Additionally, there might be cultural resistance to adopting necessary security measures without proper awareness.

Physical security risks include the loss of equipment due to theft or damage, which can be costly and disrupt school activities. Physical tampering can also pose threats to data integrity. Finally, software and firmware management risks include system vulnerabilities due to outdated software, which can leave systems exposed to newer types of cyberattacks. Responding to and recovering from attacks due to unpatched vulnerabilities can be resource-intensive and disruptive.

5. Regulatory and Compliance Considerations

5.1. Relevant data protection and privacy regulations

Data protection and privacy laws are a cornerstone in the context of IoT in schools. The General Data Protection Regulation (GDPR), effective in the European Union, establishes strict rules on data handling and privacy. This regulation is pertinent to schools that need to ensure IoT devices collecting data about students or staff comply with GDPR's provisions. These provisions include consent, data minimization, and ensuring the rights of data subjects are upheld.

In the United States, the Family Educational Rights and Privacy Act (FERPA) serves a comparable purpose. It protects the privacy of student education records. Just like GDPR, FERPA necessitates that schools manage IoT devices and systems to secure any collected data. It also requires adherence to regulations regarding the sharing of this data.

5.2. Compliance requirements for educational institutions.

Schools are responsible for ensuring compliance with not only GDPR and FERPA but also with other regulations like the Children's Online Privacy Protection Act (COPPA). COPPA is crucial as it regulates the collection of personal information from children under 13 by websites, apps, and IoT devices. Schools must be especially vigilant in ensuring that IoT devices used do not breach COPPA regulations, particularly when these devices are capable of collecting data from younger students.

Beyond these specific laws, educational institutions must also consider guidelines provided by the National Institute of Standards and Technology (NIST). NIST's cybersecurity framework, while not legally binding, offers valuable guidance for securing IoT devices and networks. By adopting these best practices, schools can significantly enhance their security posture.

Moreover, schools must be cognizant of state-specific legislation. Various states or regions may have unique laws regarding cybersecurity and data protection. It's essential for educational institutions to be aware of and comply with any local regulations that apply to their use of IoT. Overall, adhering to these diverse regulations and guidelines is critical for ensuring the security and privacy of data within the educational environment.

6. IoT Security Best Practices

6.1. Device and Software updates

In a school setting, it's crucial to regularly apply updates to IoT devices. Keeping the software up-to-date significantly reduces vulnerabilities, as outdated software is a common target for hackers. Schools should check for vendor-provided updates and frequently visit the manufacturer's website for the latest patches to ensure their IoT devices remain secure.

6.2. Password Management

Effective password management is essential for IoT security in schools. Each IoT device and the Wi-Fi network should have a unique, strong password. A robust password typically includes a mix of characters, symbols, and numbers, and should avoid easily guessable information like sequential numbers or personal details. This practice prevents cybercriminals from gaining easy access to multiple devices.

6.3. Router Security

Securing the router is a foundational aspect of IoT security. Schools should change the default name of their routers to prevent easy identification of the make or model, which can be a vulnerability. Additionally, using strong Wi-Fi encryption methods, such as WPA2 or later, helps safeguard the network against unauthorized access.

6.4. Guest Network

Establishing a guest network with strong encryption is a wise strategy for schools. This network should be used for visitors, as it helps to maintain the security of the main network by isolating guest traffic, which might include devices compromised or infected with malware.

6.5. Privacy Settings

Schools need to regularly review and adjust the default privacy and security settings of their IoT devices. This ensures that the settings align with the specific security requirements of the educational environment, safeguarding sensitive data against unauthorized access.

6.6. Feature Management

Disabling unused features on IoT devices reduces potential attack opportunities. In schools, where a variety of devices are used, it's important to evaluate and turn off unnecessary functionalities, thus minimizing the risk of cyberattacks targeting these features.

6.7. Multi-Factor Authentication (MFA)

Implementing MFA on IoT devices provides an additional layer of security. This practice is especially important in schools, where a variety of users access the network. MFA ensures that even if a password is compromised, unauthorized access is still prevented.

6.8. Network Monitoring

Regular monitoring of all devices connected to the school's network is crucial. This includes keeping an eye out for unusual activities and considering upgrades for older models that might lack advanced security features. Continuous vigilance helps in early detection of potential security threats.

6.9. Public Wi-Fi Caution

When managing IoT devices, it’s important to be cautious about using public Wi-Fi networks, as they can pose significant security risks. In a school context, using a VPN can provide an additional security layer, protecting data transmission over less secure networks.

6.10. Encryption and Secure Communications

Ensuring that data from IoT devices is encrypted is key in a school environment. This, along with the use of secure communication protocols, protects sensitive information from being intercepted or compromised. Managing cryptographic keys effectively is also a part of this process, balancing data protection with accessibility.

7. Incident examples

7.1. Cyber Risks in U.S. Schools

Since 2005, K-12 school districts and colleges/universities across the US have experienced 2,691 data breaches, affecting nearly 32 million records.

In recent years, the trend of cybersecurity threats towards the Educational/Research sector is sharply increasing. In fact, as stated by the company Checkpoint: hackers prefer to target schools as 'soft targets' due to the abundance of personal data stored on school networks, making both students and schools vulnerable.

The data is alarming, but even more concerning is that most of these attacks are carried out exploiting vulnerabilities detected in the IoT devices used by the schools themselves, now necessary for the proper conduct of lessons.

Another alarming fact is provided directly by the Government Accountability Office. In an article they published in 2022, the following is stated: “Cyberattacks on K-12 schools have increased. Not only do these attacks disrupt educational instruction and school operations, but they also impact students, their families, and teachers”. It immediately becomes apparent that most of the schools targeted by hackers are K-12 schools, which range from kindergarten to middle school. In this phase, the students attending the school are totally vulnerable and exposed, considering they do not exceed 12 years of age.

7.2. Analysis: Harvard Computer Society Email Privacy Breach

The Harvard Computer Society (HCS) email privacy breach involved the unintended public exposure of over 1.4 million emails, including sensitive information such as Harvard students' grades, financial aid details, and at least one individual's Social Security number. The breach occurred because the email lists managed by HCS, used by teaching fellows, resident tutors, college administrators, and undergraduates, were publicly accessible by default.

The privacy breach at the Harvard Computer Society (HCS) resulted in a significant security incident where over 1.4 million emails were exposed to public access. This breach revealed sensitive information, including private details such as BGLTQ undergraduate group memberships and financial data of student organizations. The situation was particularly concerning as it potentially violated the Family Educational Rights and Privacy Act (FERPA).

The root cause of this breach was the default setting of HCS's list archives, which was set to public. This setting inadvertently led to the public exposure of emails. Compounding this issue, many of those managing the lists, including college administrators and HCS leaders, were not aware that these lists were public. This lack of awareness affected a significant portion of the email lists, with over 5,500 out of approximately 7,000 lists in HCS’s online index being publicly accessible.

The issue first came to light through the reporting of The Harvard Crimson, which prompted HCS to take immediate corrective action. HCS responded by making the lists private and restricting access to the archives of all existing lists with private membership. Additionally, they sent out communications to all list administrators, reminding them to check and adjust their lists' privacy settings.

In response to this incident, HCS undertook several measures to prevent future breaches. They initiated a revision of the list creation process, placing a greater emphasis on the default public setting of email archives. Plans were made to reevaluate the default values for email list archives to enhance privacy. Furthermore, as a precautionary step, HCS temporarily disabled the email list directory to halt any further unauthorized access. These actions reflect HCS's commitment to strengthening their data security protocols and safeguarding the privacy of their digital communications.

This incident highlights the importance of default privacy settings and awareness among users and administrators regarding the public accessibility of digital communication platforms.

8. Conclusion

To conclude this document we can say that the integration of IoT in schools represents a paradigm shift in education, enhancing learning environments and operational efficiency while posing significant cybersecurity challenges. From tracking devices and smart boards to advanced HVAC systems, IoT devices offer numerous benefits, such as energy savings, improved safety, and interactive learning experiences. However, these advantages come with inherent risks, including data breaches, network vulnerabilities, and compliance issues with regulations like GDPR and FERPA. To mitigate these risks, schools must adopt best practices in device and software updates, password management, network monitoring, and education on cybersecurity. The Harvard Computer Society email privacy breach serves as a cautionary tale, emphasizing the need for stringent security measures and awareness in managing IoT devices in educational settings.

9. References

What Is the Internet of Things (IoT)?

What is the internet of things? | IBM

Cyber Security and the Internet of Things (IoT)

Applications of IoT technology in the education sector for smarter schooling

Top 6 Things You Should Know About IoT In The Education Industry

Benefit Of IoT In Education Industry In 2023

Internet of Things security challenges and best practices | Tips for Securing IoT

Navigating IoT Regulations and Compliance: A Guide

IoT Security Best Practices? How To Protect IoT Devices | Fortinet

The ultimate IoT security best practices guide

Internet of Things for education: A smart and secure system for schools monitoring and alerting - ScienceDirect

https://scholar.google.es/scholar_url?url=https://peer.asee.org/iot-privacy-and-security-in-teaching-institutions-inside-the-classroom-and-beyond.pdf&hl=fr&sa=X&ei=VhN-Zeb2F4SAmwGh2oCoAQ&scisig=AFWwaeaHL8BmmFcFXIhpYFzLCUv7&oi=scholarr

Education sector sees 34% increase in IoT attacks | SC Media

How Universities Can Mitigate IoT Security Risk | Asimily

Chicago Public Schools data breach blamed on third-party ransomware attack | The Daily Swig

Harvard Computer Society Email Privacy Breach

Georgia Tech Suffers Second Data Breach, Exposing Data of 1.3 Million People

Hackers Hit School District in Clark County, Nev.

Fall data breach at San Diego Unified worse than originally thought: District

Checkpoint:
https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector/#:~:text=The%20education%20and%20research%20sector,increase%20from%20the%20previous%20year

GOA.gov:
https://www.gao.gov/blog/cyberattacks-increase-k-12-schools-here-whats-being-done#:~:text=In%20recent%20years%2C%20cyberattacks%20on,their%20reliance%20on%20IT%20services

Data breaches Harvard:

https://www.linkedin.com/pulse/harvard-computer-society-email-privacy-breach-theon

10. Glossary

Abbreviation	Meaning
AR	Augmented Reality
COPPA	Children's Online Privacy Protection Act
FERPA	Family Educational Rights and Privacy Act
GDPR	General Data Protection Regulation
HCS	Harvard Computer Society
HVAC	Heating, Ventilation, and Air Conditioning
IoT	Internet of Things
MFA	Multi-Factor Authentication
NIST	National Institute of Standards and Technology
VPN	Virtual Private Network
VR	Virtual Reality