IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

Highly Compromised Health Records - Indian Healthcare Sector during CV19; Medical – CPS. Risk Assessment, Issues, Challenges and Recommendations

Mahesh Devarshi,
PhD Scholar, MS University

Introduction

The world has been battling the coronavirus for the last two years, a virus that has put extreme pressure on our healthcare system and has been able to exploit many of its weaknesses. And while our medical system is struggling to fight this biological virus, it is not the only virus it has to worry about. For the past two years, healthcare institutions worldwide have been seeing an increased assault from digital viruses, incidents of Ransomware attacks and other malware have risen by a significant amount, according to the report from HealthITSecurity ‘One in three healthcare organisations globally is being hit by ransomware in 2020’. For India, too, this has become an issue of great concern as the last two years saw approximate seven million cyber-attacks (CyberPeaceFoundation, 2021); this includes pharma companies and healthcare firms, along with hospitals and vaccine makers. A majority of these viruses here are ransomware, which is malware that employs encryption to hold a victim’s, in this case, healthcare providers, information at ransom. The ones most commonly used here are WannaCry, CryptoLocker, NotPetya. This study attempts at the threat analysis to identify what makes cyber-physical systems and data within the Indian healthcare system susceptible to such attacks.

Literature Review

Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health- The article, written by Menaka Muthuppalani and Kerrie Stevenson analyses the prevailing cybersecurity risks pertaining to global healthcare institutions, the article explains cybersecurity threats in the backdrop of the coronavirus pandemic and cites several incidents across the world that have experienced cyberattacks during the pandemic period. The article goes on to explain the core cybersecurity principles that healthcare institutions must adhere to in order to safeguard themselves from potential threats.

Cybersecurity in healthcare: A systematic review of modern threats and trends- This report by Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson, and Kyle D Monticone analyses how the adoption of technology in the healthcare sector have increased its vulnerability to cyberattacks. The article goes into identifying cyber risk trends including ransomware using searches through CINAHL and PubMed among other databases. The researchers identified several threats based on the industry lag in security. The article further commented on the necessity of proper guidelines and policies pertaining to maintaining the cybersecurity standards of healthcare institutions

State of Cyber-attacks: Indian Healthcare System

Cyber-attacks in India have risen significantly during the pandemic with as many as 16,43,169 cases reported by the CyberPeace Foundation using their simulated Healthcare sector-based Threat Intelligence Sensors Network. The research which looked at instances of malware or ransomware attacks towards healthcare institutions during the period of October 1 to November 25 showed a few trends revealing themselves in these attacks for instance, vulnerable exposed systems that were not monitored and faced the internet were among the most attacked system for the attackers. It further pointed out that the vulnerable internet-facing systems with remote desktop protocol enabled and old Windows server platform were among the most attacked. The report came after Microsoft reported cyberattacks from at least 3 nation-state actors that were targeting pharma companies and vaccine manufacturers The major attacking parties came from Russia and North Korea named ‘Strontium’ and ‘Zinc and Cerium’ respectively. Overall, it was reported that India saw a 45% spike in cyberattacks on healthcare organisations which makes it the most targeted sector by cybercriminals (Check Point Research, 2020).

A notable case of cyberattacks would be the October 22, 2020 attack on Dr Reddy’s Laboratories which lead to the company temporarily shutting down some of its production facilities, the attack, which was targeting user data using ransomware, came days after the company got approval The attack had come close on the heels of Dr Reddy’s receiving Drugs Controller General of India (DCGI) approval to conduct Phase 2/3 human clinical trial for Sputnik V vaccine, developed by Russia, in the country. A more unfortunate example came just weeks after the Dr Reddy incident with Lupin- the Mumbai based pharmaceutical company disclosing in November 2020 that an unknown entity was able to successfully carry out a cyberattack against it which affected many of its internal IT systems.

Such incidents have shown that attacks against the healthcare industry are increasing in India and that the success rate of these attacks has risen. The lack of investment in IT resources and poor management of existing infrastructure is partly to blame for the rise in such cases.

Medical Healthcare Application Scenario

When consider the Healthcare – CPS, Fig. 1 shows the features of our medical health care application scenario which encompasses basically of three main spots, like home, hospital and office surroundings. The key applicational value of Healthcare- CPS are to improve the QoL (Quality of Living) of people (especially elderly persons, Children or patients) whose close relatives are usually working offices in the daytime wanted to monitor their loved one’s health situation on real-time mode so as to save medical cost. In normal scenarios, the health conditions like physical or medical information are get to be monitored via Surveillance Camera, Biosensors, Micaz etc remotely stored in third party cloud (either in the hospital or main Labs) via an in-home WSN-Cloud Gateway. So that the real-time information could be monitored on regular basis and to take appropriate actions in no time delay. For instance, the healthcare professionals (Doctors/Nurses) could regularly verify such medical cloud records and advice / administer suggestions and to prescriptions medicine as well via wireless (or Wired) connection in an authenticated reliable way. H-CPS cloud data interventions can help in any urgent situations and immediate actions can be taken to help those who seeks very urgent medical attentions.

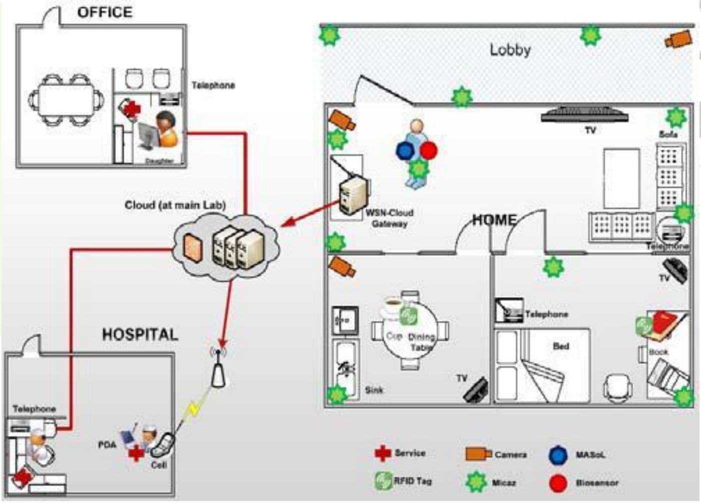

Fig 1. A medical healthcare application scenario

From the Fig. 1 it could be seen that it comprises components of typical H-CPS architecture. Here, both wired and wireless communication interchanging data through the is built different systems. The administration or computation can be realised both inside the cloud and the gateway (or even sensing devices). Data/information interchange is the crucial and vital activity between the communication devices on real time mode and scheduling and resource management authentically can be done inside the cloud with various security strategies.

At the hospital front, it is worth noting that different H-CPS application services can be so as to enhance the quality, reliability and accountability of health monitoring and care. In certain area wherein surveillance systems like camera may not be applicable, RFID tag or ZigBee devices like MicaZ can be used instead.

Cyber-physical systems are supposed to play an imperative role in the design of emerging engineering systems especially in the healthcare scenario with innovative and more powerful capabilities to counter measure today’s legacy applications. But still in its infancy, CPS has many research issues and challenges.

Identifying risk in the healthcare system

To identify what makes the healthcare system so susceptible to such attacks, we must first do a threat analysis on the many components that are vulnerable to cyberattacks.

Some of these issues have been traditionally documented as existing problems even before the pandemic, such as:

Fractured Infrastructure put under heavy stress: As mentioned earlier, the IT infrastructure and HCPS infrastructure present in the healthcare sector is often outdated and poorly maintained. A big reason this is caused is the lack of compulsion from state or security agencies to compel better maintenance the same way that banks, insurance companies and critical facilities have. The dependence on legacy systems and outdated or older technicians also adds to an entity not being able to advise it. With the pandemic forcing remote work, IT employees in healthcare institutes are at an even more disadvantageous position to support healthcare institutes.

Rogue devices**:** The use of remote monitoring cyber-physical systems have risen during the pandemic. But the subsequent mass purchase requirements meant that many off the shelf items were brought where quantity mattered more than quality. The use of such devices, which were mostly connected to local networks meant the system was suddenly introduced to several alien devices which has the ability to transfer sensitive data. Poor diligence in ordering and managing these devices, such as sticking with the default password makes them a major risk point in HCPS cyber security.

Telehealth: Remote health monitoring systems called Telehealth (aka Remote health), health apps and remote monitoring equipment have also grown rapidly during the past few years. The speed of adoption and the new opportunity in the market meant there wasn't much time to test these applications for risks and take proper precautions. In android OS, which is still the dominant operating system in India for a majority of mobile-based telehealth applications, this opened another potential risk as the linking of accounts and use of unnecessary permissions leads these applications to be able to access sensitive data.

Third-party risks: The Healthcare sector works with multiple 3rd party vendors- suppliers, such as government agencies, suppliers, universities and other organisations. Such a diverse supply chain opens significant risk since it is challenging to ensure the legitimacy of these organisations and their cybersecurity standards, this also opens an exploitable weakness. Even vendors specifically hired to assist with security operations can sometimes make mistakes with severe consequences.

Tired staff, weak security culture: A human component in the risk assessment is the professionals working in the industry. It is no surprise that the healthcare industry is one of the most physically taxing industries to work with, this leads to more room for human error compared to other sectors. Any IT-related risks that can happen here is a cause for concern to the entire system.

Apart from all this the Pandemic has introduced several more stressful factors that has led to jeopardising the sector even more. These are-

An increase in attacks Cyber-attacks: As Mentioned earlier, the number of cyberattacks towards healthcare industry has risen significantly, causes such as Lupin and Dr Reddy shows that such targeting attacks have a good chance of success even against well-funded private agencies. The failure to update the system proportionally to the attacks makes the sector weaker with each consecutive attack

Majority of attacks result in data breaches: Given the more aggressive types of ransomwares and other data-stealing malware, it's no wonder that nearly every successful cyber-attack now results in a data breach. The financial loss coupled with the loss of sensitive data puts many institutes at a very risky position. Incidents in the past have shown that many companies refuse to come forward with their incident as it has very detrimental impact on their business. As such the lack of reporting of such incidents leads to there not being enough data being available to investigate such issues thoroughly and identify proper patterns, moreover it incentivises hackers to target this sector more.

Recommendations

Generic saying like healthcare often said "prevention is better than cure", the same can be said of cybersecurity and as such many of the recommendations are preventive in nature.

Awareness and email security**:** Many cyber-attacks manipulate the human components at healthcare facilities. Better training and sensitisation will reduce their chances of downloading suspicious documents or clicking suspicious links as well as adopting better cybersecurity practices from the employees. There have been incidents of realistic phishing simulation targeting employees that weren't very difficult as such awareness and training should be the first course of action.

Protect internet-facing devices: Along with emails and messaging apps, another potential risk is the many software components that use the internet. Hardware and software vulnerabilities are often used in cyberattacks. Open ports and remote access protocols are not difficult to access in many scenarios and lead to potential risks at that point. As an IT hygiene issue this can be solved with better care and attention. Only necessary ports should be opened to the internet. Researchers found vulnerable RDP ports increase the likelihood of a successful ransomware attack by 37%(Sonic Guard, 2022). Today the black market hosts several platforms where RDP credentials can be sold or brought.

Prevent credentials theft**:** The theft of employee credentials is also a significant risk; hackers can use software such as Mimikatz that employs aggressive password spraying and other credentials stealing techniques to access servers and spread across the network. Having robust passwords and two-layer authentication will reduce the chances of these succeeding.

Implement endpoint security**:** Endpoints are the necessary means of entry to your network and assets. Having an advanced endpoint security solution on all endpoints and servers is essential to improving the healthcare organisation's cybersecurity resilience.

Conclusion

The ever-increasing threat of cyber-attacks on the health care sector is apparent. The negative impacts it has on society will be immense as the healthcare sector is battling one of the most significant biological crises on one front, we see them battling a similarly unprecedented attack on the virtual end. As the world is adopting more and more HCPS components, the value of healthcare information has also risen significantly. From Vaccine data to patient information, a wide range of components within the healthcare system has become vulnerable. This has incentivised one of the hackers to make this sector the most susceptible to cyber-attacks. A weak digital system coupled with outdated practices and a lack of security demands made the existing healthcare system quite vulnerable. The quick adoption of remote and digital HCPS also raises concerns as proper precautions are not practised industrywide. Therefore, it is essential that more awareness, investments, and actions be taken to create a more resilient digital infrastructure for healthcare organisations. The benefits of HCPS are more prevalent as the world adapts to a system of social distancing. This connects to the larger question of what society can do to ensure cybersecurity within cyber-physical components.

References

1. *A. K. Leichman, "Hospital cyberattack is the new pandemic; here's the cure," ISRAEL21c, 29-Nov-2021. [Online]. Available: https://www.israel21c.org/hospital-cyberattack-is-the-new-pandemic-heres-the-cure/. [Accessed: 28-Feb-2022].*
2. *"Indian vaccine makers, healthcare institutions targeted by cyber attackers: Report," CyberPeace Foundation, 02-Dec-2020. [Online]. Available: https://www.cyberpeace.org/indian-vaccine-makers-healthcare-institutions-targeted-by-cyber-attackers-report/. [Accessed: 28-Feb-2022].*
3. *M. Muthuppalaniappan and K. Stevenson, "Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to Global Health," International Journal for Quality in Health Care, vol. 33, no. 1, 2020.*
4. *S. Weiner, "The growing threat of ransomware attacks on Hospitals," AAMC, 20-Jul-2021. [Online]. Available: https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals. [Accessed: 28-Feb-2022].*
5. *Sonic Wall, Healthcare Cybersecurity in the Pandemic. Sonic Wall, Milpitas, California.*
6. *TMN Staff, "7 million cyber-attacks on Indian health sector in October and November: Report."*
7. Sha, L., Gopalakrishnan, S., Liu, X. and Wang, Q. (2008). Cyber-Physical System: A New Frontier. *the 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, 1-9.
8. *Tang, L., Yu, X., Kim, S., Han, J., Hung, C. C. and Peng, W. C. (2010). Tru-Alarm: Trustworthiness Analysis of Sensor Networks in Cyber-Physical Systems. the IEEE International Conference on Data Mining, 1079-1084.*
9. *Xia, F., Ma, L., Dong, J. and Sun, Y. (2008). Network QoS Management in Cyber-Physical Systems. the International Conference on Embedded Software and Systems, 302-307.*

10. *Xia, F., Kong, X. and Xu, Z. (2010). Cyber-Physical Control over Wireless Sensor and Actuator Networks with Packet Loss. in Wireless Networking Based Control, Springer, 85-102.*
11. *Zhang, Y., Gill, C. and Lu, C. (2008). Reconfigurable Real-Time Middleware for Distributed Cyber-Physical Systems with Aperiodic Events. the 28th International Conference on Distributed Computing System, ICDCS, 581- 588.*
12. *Pham, N. Abdelzaher, T. and Nath, S. (2010). On Bounding Data Stream Privacy in Distributed Cyber-physical Systems. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing.*