7 Evaluating Cyber Threats to the United Kingdom's National Health Service (NHS) Spine Network

Michael Gibbs

Abstract

This report serves as a brief review of United Kingdom's (UK) National Health Service's (NHS) information system infrastructure and the various security threats that could lead to potential breaches of personal health information hosted on the network. Specifically, the document will address details of the NHS Spine infrastructure and how its components, users, and security mechanisms have a great impact on the NHS' overall ability to provide quality service to the UK's healthcare customers. The report will also provide an overview of the NHS system, its sub-components, and how they are all connected via the Spine infrastructure to serve UK citizens seeking healthcare assistance. Lastly, the report will touch on recommendations for role-based access control and identity management.

Keywords

Cybersecurity · National healthcare system · NHS · Spine network · United Kingdom

7.1 UK NHS Information System Infrastructure

The UK originally established the NHS in 1948 as a way to provide health care for all citizens [1]. Today, the organization provides leadership for the strategy and implementation of all health care services to the UK. NHS has one of the world's largest workforces that number over one and a half million who strive toward providing services to approximately 54 million UKresidents [2]. NHS uses the NHS Digital organization to operate all networks, collect all user data, and ensure all security standards are enforced [3, 4].

The NHS falls under the Department of Health and is mostly comprised of approximately 211 clinical commissioning groups (CCG). The CCGs are the organizations providing most of the direct care to UK citizens. There are also other elements to include dentists, opticians, pharmacists, and trusts that fall outside any specific CCG [2].

NHS Digital operates a large backbone network known as Spine or N3 that interconnects 23,000 healthcare information technology (IT) systems used by 20,500 organizations [3, 4].

The Spine network infrastructure allows for all healthcare patients and providers to access databases that store personal health records, as well as a way to communicate health care planning across the entire country. To do this, Spine can be broken up into five major components.

The Legitimate Relationship Service (LRS) manages how health practitioners access patient records [5]. The National Care Record (NCR). This is where local health organizations store pertinent information allowing for staff to support customers [5]. The Personal demographics system (PDS) is where both customers and practitioners can access personal health information (PHI) [5]. The Spine directory service (SDS) database system houses all information associated with the healthcare organizations supporting the NHS [5]. The Transaction and Messaging Spine (TMS) component serves as the backbone routing element for all other systems through the use of the HL7 version three messaging standard [5].

The Spine network hardware consists of routers and switches that manage traffic paths across its thousands of systems. Additionally, Spine includes databases and application servers that provide access to patient and provider information. Because patients can also access personal information stored within the network, end users' devices such as desktop computers, laptops, and mobile devices might also be considered part of the network.

M. Gibbs (✉)
University Maryland University College, Evans, GA, USA

S. Latifi (ed.), *Information Technology – New Generations*, Advances in Intelligent Systems and Computing 738,
https://doi.org/10.1007/978-3-319-77028-4_7

The Spine network requires that systems use many flavors of software and operating systems, but all of them must be able to interface with HL7's Fast Healthcare Interoperability Resources (FHIR) message standard. The TMS uses FHIR to transmit messages across all databases, application servers, practitioners, and patients. FHIR does this using the Extensible Markup Language (XML) over the Hypertext Transport Protocol (HTTP) [5]. HTTP is an application protocol found at the seventh layer of the Open System Interconnections (OSI) model that uses the TCP/IP suite to transmit and control connections between clients and servers [6].

The NHS Spine relies on end user devices to be running fully patched operating systems as well as updated antivirus applications. Should end users become compromised due to failed security practices, hackers might then access NHS databases and application servers in an unauthorized manner. NHS Spine administrators should implement intrusion prevention systems (IPS) at core nodes to identify and mitigate malicious activities based on known signatures.

7.2 Threats

Due to the enormous number of systems that comprise the NHS network, the threat to its resources and data are equally large. Hackers would likely consider the NHS network a relatively easy target based on the volume of end users accessing the system on a regular basis. Should hackers compromise any of the end users' devices, they would be able to use the access to protected services in an unauthorized manner. Hackers might leverage the access to deny services or data to NHS end users by incorporating ransomware or dynamic denial of service (DDoS) tools into their attacks.

The NHS TMS network is based on transferring network messages via HTTP. Doing so creates a huge premium on web-based security protocols. Administrators must ensure that all web servers are properly patched and limit servers running processes not required for legitimate end user applications.

The insider threat poses the greatest risk to the network as it is usually the most difficult to identify and mitigate. Insiders normally have intimate knowledge of their employer's network systems and are privy to security protocols designed to limit unauthorized access. One of the best ways to stop this would be to log and audit all administrator actions on the network.

Healthcare practitioners can pose a security risk as they may become complacent with respect to cybersecurity since they are primarily focused their patients. These providers may ignore standard protocols designed to protect network components or even purposely subvert them if practitioners find them unduly restrictive or intrusive.

Motives driving intruders can span a range of reasons. One of the primary motives would be financial gain. Cyber criminals are always looking for ways to make money and one of the easiest ways is ransomware. NHS experienced a ransomware intrusion in 2017 and it served as an expensive lesson for NHS as some of its end users were not adhering to security protocols [7]. Another motive for insiders may be retribution. Disgruntled employees may seek to create financial hardships or cause public scrutiny against an employer at any point. Because of this, logging and auditing for critical positions should be mandatory.

To understand how breaches in the cybersecurity realm have become so prevalent, professionals charged with securing networks should maintain an awareness of hacking tradecraft. One of the most effective means of gaining unauthorized access to victims is through social engineering. These attacks prey on the psychological aspects of those they mean to exploit. Social engineering campaigns usually seek to take advantage of a potential victim's sense of fear, obedience, greed, or helpfulness [8]. Senior security staff should consider mandating training for all employees that provide education on how to spot social engineering attacks.

7.3 Vulnerabilities to Identity Management

One of the biggest threats to identity management would be end users losing their common access cards (CAC). These cards are instrumental in protecting the public key infrastructure (PKI) currently used to authenticate all users before they are granted access to network resources and databases [9].

Network administrators and senior security executives must ensure identify management is properly addressed. Currently, NHS employs the use of a PKI system that implements OAuth2 protocol authentication using tokens issued to end user devices. This construct helps to limit the possibilities of hackers gaining unauthorized access to network resources.

Authentication is handled through the PKI system and the OAuth2 database via the authorization server. End users must have a CAC and the correct credentials to successfully authorize themselves for access to resources.

After authentication, the authorization process affords the end users with access to those resources they are entitled based on their role. Patients should be restricted to only those services related to their personal information while practitioners should have access to all databases required for treatment. Managers and network administrators would also have different access to resources based on their jobs and responsibilities.

Table 7.1 Role-based access control recommendations

Role	Role-based controls	File-based controls	Access list controls	Database controls	Mobile-device controls
NHS Administrators	Allow access to all relevant files and network resources	Allow access to all files	Allow connections to all network resources	Allow connections to all databases	Deny mobile device access to critical files and network resources
Practitioners	Allow access to relevant files/resources, deny all else	Allow access to relevant files/resources, deny all else	Allow only connection to pertinent network resources	Allow only connection to pertinent database resources	Deny mobile device access to critical files and network resources
Patients	Allow access to relevant files/resources, deny all else	Allow access to relevant files/resources, deny all else	Allow only connection to pertinent network resources	Allow only connection to pertinent database resources	Deny mobile device access to critical files and network resources

Managing users' access to resources with the NHS network is critical to increasing the security of the entire organization. The following controls should be put in place.

NHS Spine core routers should be updated with access control lists that only allow connections coming from verified and trusted points of network infrastructure. As an example, the SDS should be restricted to only those IP addresses used owned by one of the CCGs.

User accounts should be assigned privileges based on their need for resources associated with their roles. Administrators should only be given administrator-level access to those systems they manage. Conversely, patients should be restricted to normal user permissions to those systems hosting personal information. These roles should be managed via the authorization server after authentication.

Much like server and database resources, sensitive files should be protected against unauthorized access. Administrators should restrict access to files and folders only to those roles needing to use them for official business. Examples might include router configuration backup files need to be restricted to those local administrators. Web-based services specific for a CCG would be locked down to only those computers within that same CCG network.

Database information is the lifeblood of the NHS and its ability to afford patients with quality care. Because they contain such sensitive data, administrators must restrict access to databases with regard to an end user's role. Patients should be able to access the PDS via approved web forms and approved application programming interfaces, but not others such as the NCR or SDS.

Mobile devices can pose threats to the network as they are not managed by the NHS and have a higher likelihood of risk. Patients and NHS employees with mobile devices should be limited to a small set of resources that are not critical to the overall functionality of the Spine. Enforcing these restrictions will drastically reduce the potential for unauthorized access to occur from a device that isn't managed by NHS administrators.

Administrators should also consider implementing a role-based access control construct to effectively manage risks to key infrastructure. The following chart provides recommendations for role-based access control measures (Table 7.1).

7.4 Identity Management Protection

Protecting NHS resources by way of authentication and authorization applications is useless if administrators are unable to ensure identity management is appropriately implemented across the network; for this password fidelity is instrumental to success. Administrators should enforce a password policy consistent with the latest suggestions from the cybersecurity field.

Properly constructed passwords significantly reduce the chances of successful password attacks. NHS should consider adhering to NIST's latest recommendations on enforcing password policies that prevent unauthorized access while also remaining palatable to end users. NIST now recommends that organizations simply enforce a requirement of eight characters or longer, but not mandate the use of the four types of characters [10].

Applications used for testing password strength can be helpful, but can also pose serious security risks to authentication systems. NHS should seriously consider this matter moving forward if it hopes to ensure it is limiting risk to patient data.

Password cracking tools can help security professionals if improper password choices are being chosen by end users. Finding weaknesses in password choice can result in policy changes that effectively increase authentication processes.

If used improperly, these tools could result in hackers or disgruntled employees acquiring access to end user account information and network resources.

7.5 Conclusions

The NHS Spine is a vast network that interconnects thousands of networks and millions of end users. Its availability and security is critical to UK citizens receiving vital healthcare. NHS Digital must enforce policies that ensure the network is reliable and secure. Most of the network traffic is handled by the TMS through the HTTP protocol and HL7 version three standard. NHS' authentication and authorization functions are managed through PKI and the OAuth2 database. To keep these elements secure, NHS should enforce a password policy requiring users to create passwords at least eight characters in length, as well as forbidding any NHS-managed computer to run password cracking tools. Taking these steps will help to severely reduce the threats that hackers or disgruntled employees pose to NHS' authentication and authorization systems.

References

1. T. Powell, The structure of the NHS in England. From NHShistory.net, (2016). http://www.nhshistory.net/Parliament%20NHS%20Structure.pdf
2. www.nhs.uk, The NHS in England. From www.nhs.uk, (2017). http://www.nhs.uk/NHSEngland/thenhs/about/Pages/overview.aspx
3. NHS Digital, Spine. From NHS digital, (2017). https://digital.nhs.uk/spine
4. NHS Digital, What is NHS digital. From digital.nhs.uk, (2017). https://digital.nhs.uk/article/219/What-is-NHS-Digital
5. R. Spronk, The Spine, an English National Programme. From Ringholm Whitepaper, (2007). http://www.ringholm.de/docs/00970_en.htm
6. B. Mitchell, Understanding the open systems interconnection model? From Lifewire, (2017). https://www.lifewire.com/open-systems-interconnection-model-816290
7. BBC News. NHS cyber-attack: GPs and hospitals hit by ransomware. From BBC Health News, (2017). http://www.bbc.com/news/health-39899646
8. A. Whipple, Hacker psychology: understanding the 4 emotions of social engineering. From Network World, (2016). https://www.networkworld.com/article/3070455/cloud-security/hacker-psychology-understanding-the-4-emotions-of-social-engineering.html
9. K. Mayfield, HL7 FHIR Plus OAuth2 in a NHS Trust. From Slide Share, (2015). https://www.slideshare.net/KevinMayfield/hl7-fhir-plus-oauth2-in-a-nhs-trust
10. Passwordping, Surprising new password guidelines from NIST. From Passwordping, (2017). https://www.passwordping.com/surprising-new-password-guidelines-nist/