seclāb

SECURING MEDICAL DEVICES

WHITE PAPER • 2021

Securing Medical Devices

In the past few years **"Connected Healthcare"** has turned from a dream into reality but, as with any industry increasing connectivity, there are criminal gangs, nation state actors, or just mischief makers who will seek **to exploit this new connectivity** for financial gain, cyber warfare, or just to show they can

As well as this direct threat to the cybersecurity of medical devices, there is also a derived threat to other devices, as a breached or infected device may serve as the gateway, enabling the bad guys to disrupt more devices on that network.

In May 2017, the so-called WannaCry hack , shut down hundreds of thousands of computers around the world with messages from hackers demanding ransom payments. In the UK a third of NHS hospital trusts and 8pc of GP practices were affected. Around 1pc of all NHS care was disrupted over the course of a week and cost an estimated £92m.

By the end of 2019, healthcare-related data breaches in the US were expected to have cost the industry **$4 billion,** and before the current pandemic was declared, **estimates for 2020 were expected to be higher still.**

More recently, in March 2020, a large hospital in the Czech Republic responsible for running tests for coronavirus, said that a cyberattack had hit its computer systems prompting one security expert to say, “Even if the offline health care procedures work, reducing the capacity means that work might be slower than usual.”

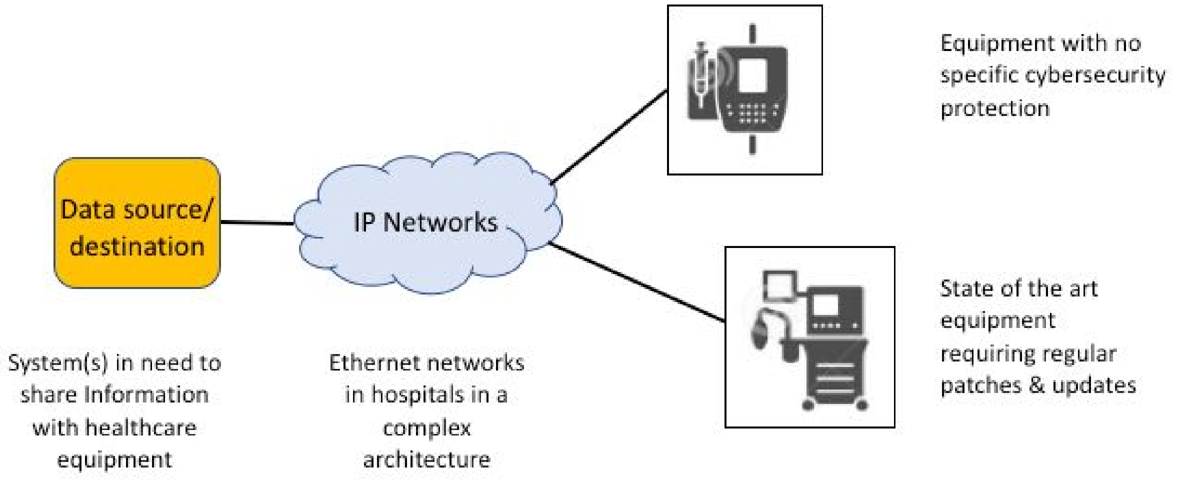
Despite increases in focus and funding, the root cause for this rising level of successful attacks against the hospital sector remains lack of budget for IT security infrastructure. That means new and outdated systems alike are vulnerable to attackers and may lead to, real, life-threatening incidents. Health care providers, like numerous industries, often run legacy systems on old hardware and/or using operating systems like MS Windows 95 or XP that can’t be easily updated but may be required to continue to operate for a few years more since replacing them would require a re-design of the complete architecture requiring substantial cost and resource.

Old systems frequently lack security. The hardware or the operating systems, including the TCP/IP stack, may be old and not updated when new vulnerabilities are identified, such as the VXworks ‘Urgent11’ or attacks like ‘Ripple20’ affecting millions of IoT devices including patient monitors or MRI scanners in June 2020. In these environments, the use of firewalls may not be sufficient, being software based and subject to compromise; Data diodes only allow one-way communication meaning that, due to the configuration of traffic flow, either updates can’t be done, or business information cannot be retrieved. A visit to site is often the only way to resolve the issue in this case, requiring resources to make things happen, and capacity to do it quickly where delay might put care at risk if things take longer than expected.

In short, the easiest option in these circumstances is “let’s not change anything”.

The problem is, to extend the useful life of these systems they may need to communicate with newer computers or systems, over networks carrying different flows of information, but which may also contain malware. The first challenge then is to isolate them while restricting the communication to limited sources or destinations. The second is to ensure that any data transferred between these old and new systems can be validated in a way that bad or malicious content can’t be exchanged.

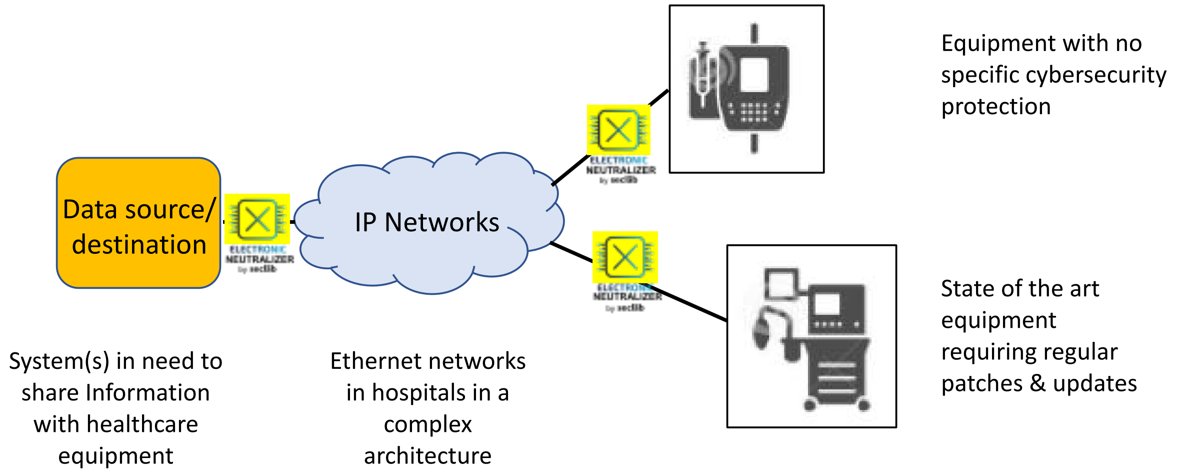
.

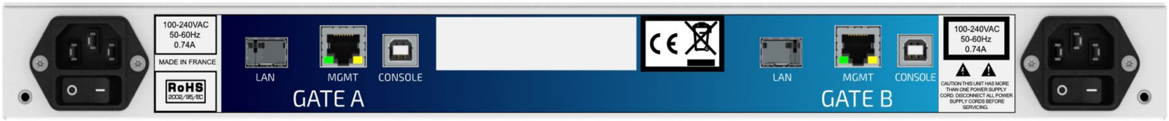

Equipment with no specific cybersecurity protection
Data source/ destination
IP Networks
State of the art equipment requiring regular patches & updates
System(s) in need to share Information with healthcare equipment
Ethernet networks in hospitals in a complex architecture

The solution? Using **SECLAB SEC-XN**, a unique 'hard-wired' security system, part of our **'Electronic Airgap'** technology range. This involves inserting a device that can't be compromised and allows only validated/certified content to be exchanged for a specific set of sources & destinations. The SECLAB Secure Xchange Network products allow file exchanges or application data flows without creating a network route between gates.

The benefits? Legacy systems can be connected without any need for a patch at the OS or network level! Information exchange can be made inside or outside of the Enterprise and without the need for expensive and time-consuming site visits. The valid communication flow can be 'hardwired' or made possible for change. In summary:

- Extending the life of the investment
- Reducing the capex and opex requirements
- Increasing the level of security and reducing the risk


Equipment with no specific cybersecurity protection
Data source/ destination
ELECTRONIC NEUTRALIZER by seclab
IP Networks
ELECTRONIC NEUTRALIZER by seclab
ELECTRONIC NEUTRALIZER by seclab
State of the art equipment requiring regular patches & updates
System(s) in need to share Information with healthcare equipment
Ethernet networks in hospitals in a complex architecture



KEY FEATURES

Installation	• **Simple** and **fast deployment** requiring only two IP addresses. • **Automated maintenance** (encrypted & signed packages by Seclab)
Security	• Sustainability of **security policies guaranteed** by the fixed factory configuration in **electronic components**, without on-site configuration. • **Complete protocol segregation**: only the transferred file passes from one gate to another. • Immunization to network attacks with only one ANSSI certified appliance. • Protection against all low-level layer network attacks. • **Integrity** and **traceability of files** via signatures verification. • Rejection of files without digital signature or with invalid digital signature.
File Transfer	• **Bidirectional** or **unidirectional** transfer. • Gates in client mode or **FTP/ FTPS/SFTP** server. • **Tracing of transmitted files** (name, size, fingerprint). • **File filtering** via digital signature.

For more information: Please contact us at info@seclab-security.com, +33 4 11 93 08 59