JOURNAL OF APPLIED
COMPUTER SCIENCE
Vol. 24 No. 3 (2016), pp. 7-19

Medical-Grade Network Security - Air-Gap Isolation and Possible Weak Points

Daniel Arendt

Lodz University of Technology
Institute of Information Technology
Wolczanska 215, 90-924 Lodz, Poland
daniel.arendt@p.lodz.pl

Abstract. *Modern medical imaging devices (MID) are usually connected to the network. Transfer of digital data to the Picture Archiving and Communication Systems (PACS) and then to Hospital Information Systems (HIS) without the internal network is not technically nor economically reasonable. It is estimated that by the interconnection of medical devices and providing remote access to them, health care costs will be cut by $ 63 billion till 2030. Sharing MID's over public network by remote access can dramatically cut costs of medical care but creates risks well known from office networks. The firewall/IDS and the air gap isolation techniques are there applicable. Medical society ask for advice what to choose or what are the threats of network operation of medical devices. Here will be given description of known attacks on the security of air gapped networks and cases of disorder operation of systems and efficient data transfer from networks traditionally known as invulnerable and impermeable. Analyzing the presented cases of successful attacks allows to identify weak points of the air-gap mechanism. In conclusion opinion how to straighten security of isolated networks will be given, on the other hand an effective IDS has advantage and many strong points.*

Keywords: *network security, air gap technique, medical-grade systems.*

1. Modern medical devices and computer networks

Modern medical imaging devices are usually connected to the network. Because of its technical design they are in fact complex and distributed computerized data processing systems and often also the control systems. Communication based on standard computer network is natural solution from both technical and economic reasons. Transfer of the collected digital data to systems for the data collection, archivization, transmission and analysis of medical images, known as Picture Archiving and Communication Systems (PACS), other than by means of a computer network is not usually reasonable to Hospital Information Systems(HIS). Interconnection of medical devices and sharing remote access to them allow to reduce up tp one-third cost of hospital equipment. But this creates a extra risk well known from computer networks of various scale and extent or technical purpose. The good practices and standards known from office networks, industrial networks security should be applied. While in mission critical network systems air gapping and isolation is the standard procedure.

Using collection of standard solutions and data formats offers great benefits, but also created new threats well known from the office or industrial computer networks. Furthermore constantly are identified new types of threats and scenarios of the attack on the networks and computers. Some problem regarding medical imaging, radiology and network security problems were discussed in [1]. Hereinafter some of them and other will be presented with a special attention on air-gapping technique of isolating data systems to obtain expected and the highest or high enough level of security.

2. Security of computer networks - applied in health care

Application of the computer networks almost certainly increased the risk of operation of medical devices to the patient. The questions are:

If the information security in medicine is a separate issue or rather the subcase of information security in general?

Whether application of general good principles and practices is sufficient to ensure safety?

Why involve the networks if this negatively impact on security?

There are other risks so scale, how grave are network threats themselves? This allow to select proper solution and decide: connect to the net or not then share or isolate from public network?

It is estimated that by combining medical devices and providing remote access to them, one can reduce health care costs by $ 63 billion by 2030 and as much as one-third to reduce spending on hospital equipment [2]. The benefits are caused mainly possibilities of using remote diagnosis and reduce the time of hospitalization. Potential risks associated with the use of such techniques are: facilitated the ability to steal personal information, medical and deliberate adverse effects, including even directed against the patient by interfering with or influencing the operation of the built-in sensors [2]. It can therefore not be networked despite the savings? Here, however, there is no choice. Transmission of digital information from medical devices to the hospital PACS, RIS and HIS internal network is necessary because of the need for transfer and storage of huge amounts of data in a secure manner that is also reliable. The question remains: whether to connect further with a public network? It seems that there is no regulation. The document prepared by the Agency for Food and Drug Administration (FDA) is only a one-page, and a general recommendation [3]. Information systems in health care should be protected as well as similar systems of public administration or selected military systems. However, manufacturers of network devices make recommendations pointing to directed solutions such as Cisco [4].

3. Other types of risks associated with software devices

Before attempt to characterise network security aspect of medical device and systems let's turn attention to other risks associated with the use of medical computerized equipment. This will allow to assess the scale of computer network threats in the whole security or reliability of computers in health care. ‚According to the strategy of cyber security of Poland [5] computer networks are among other risks. Was pointed there the importance of access to the source codes of software systems for military and public administration, thus the medical software systems. It is also expressed in the said FDA recommendation [3]. This area is usually neglected or underestimated but wrongly, it is important area of threats and a serious challenge for manufacturers of high-tech equipment, especially including medical imaging devices, in which the algorithms of operation remain intentionally hidden and constitute and decide of the technological advantage over the competition. A number of cases confirms that device manufacturers leave intentionally stored permanently, hard typed superuser-password in order to facilitate the service in the future. Or just programmers add their own additional entries "backdoors" in order

to facilitate the testing or just because of the vanity, to leave own fingerprint in the device which has been prepared for the future . There are well known cases of the fraud or abuse, an example is Volkswagen emissions scandal in 2015, when the manufacturer intentionally programs algorithms changing working conditions at the time tests to gain a competitive edge at a low cost or to meet specific regulation only during certification. Such risks extremely difficult to detect and is currently the only effective way is to disclose and provide the manufacturer's source code to users.

4. Security of mission critical networks - Internet and private networks

Combining medical devices and in particular medical imaging devices operating on big datasets in network is a must They are in fact complex and distributed computerized data processing systems so there are no other options. However, the network of medical devices can remain private, isolated from the public network. This increases safety, but does not eliminate vulnerabilities of remote access completely. Today, two techniques for secure network from remote access are widely used to control network isolation from external threats. They are:

- IDS/IPS devices
  well known, even in SOHO networks Internet Protection Systems including firewalls and similar, although characterized by more complex method of hazard analysis and more intelligent activities then the said IPS, called Intrusion Detection Systems also called Incident Detection Systems characterized in the same abbreviation IDS known as Intrusion/Incident Protection Systems IPS.

- Air Gap
  a different approach is an air gap technique. Air gap, means, the physical isolation of the private network from the rest of the net or from the public network in particular. Air gapped network inserts the airlock in place of IDS/IPS and provides almost perfect security level. Internal network is inaccessible and data transfer if occasionally needed, must be organized manually.

The first solution leaves a private network in contact to the world allowing to share medical devices and send data to the outside, while the second is just a full

physical isolation at the level of transmission media. It seems that the technique of isolation provides excellent security for all devices inside the isolated private network. However, there are known simple and effective methods branch or jump over the air gap, as well as interesting and inventive cases where the insulating barrier was successfully crossed. Each year there are published new ideas presenting the opportunity to overcome the air gap [6, 7]. Some interesting and instructive examples will be described hereinafter. Analyzing presented, selected methods and attack scenarios can be postulated that the insulation itself is not satisfactory effective unless the the air gap not tight enough. Errors and Irresponsibility inf effective control of physical access to the isolated private network allows to form a bridge over insulating gap and break the security. What we need is to replace the air gap with the airlock control of people and devices that have access to the infrastructure of the protected private network.

5. How to gain access to physically isolated network - crossing air-gap case studies

The decision about air gapping, physically isolating internal network infrastructure from the public network means the loss of a number of advantages given by network connections. Cutting access to outside world and inability to provide access to the equipment and to share services to the outside. Inconvenience of moving data gives in return almost perfect security. There are reported numbers of known attacks on this type of security. Numerous cases of carrying abnormal or unstable operation of devices inside the air gap separated system are known. Also successful data transfer from networks or devices traditionally regarded as isolated so perfectly protected was reported.

To carry out the simplest but cost effective attack is enaugh to obtain direct access to the target network by connecting the attacker directly to the private network infrastructure. This is a kind of eavesdropping like tradicional bugging but applied to the network. This does not need affords in case of many of the medical care buildings in Poland. Accomplishing the task does not need more then find an unused, empty network outlet. The more affords needs getting access to the cable trays in the corridors and cutting for connecting own switch or repeater or only removing insulation to access bare wires. Tapping cable actions are relatively easy in hospitals or diagnostic medical facilities, where many people are on the move during business hours and internal network infrastructure crosses public

areas where there are freely accessible to the visitors. The scenario involving patient, well-meaning employee, staff person or cleaning and repair service is also very simple to imagine. One time, temporary cable access can be extended by leaving connected and hidden own rogue WiFi access point. Thus isolation of the network is tampered and the airlock crossed. Applying network access control on the port access level on on network switches is an effective preventive method in all cases based on the direct connection attack. The attacker can intercept data and eavesdrop network traffic but cannot transmit. However if the only intention of the attacker is just bugging network data port protection technique will be less effective or even useless. Regarding rogue WiFi access points, many wireless equipment manufacturers incorporate rogue access point prevention and detection functions for unattended and periodic scan of the covered area to facilitate to beacon and eliminate the said unauthorised connections. Nowadays, in security practice, this in assumption useful feature is hard to successfully implement in public areas where every smartphone can be turned to transmitting access point.

The effective solution against bugging is application of secure communication with strong data encryption. In local, private networks separated by air-gap airlock, application of secure communication is sometimes eliminated, as not applicable and redundant, but should not be because of eavesdropping danger.

Good results in the protection against tapping network wires and the eavesdrop can be obtained with fiber optics in place of copper cables. However, it is shown that folding optical fiber cable allows the flow of the radiant energy outside the fiber and the data can be tapped by the detector positioned outside. Effective application of that concept was presented using the device FCD-10B from EXFO. The device is intended to make a measurements of fiber optics cable and provide phone-like communication over fiber cable for installers. The "attackers" from EXFO opened and entered the telecommunication pit on the street near ATM machine, victim of the attack. After connecting the said cable bender with light sensor FCD-10B could read and record data transmitted to and from the nearby ATM. The data were open text data, not encrypted because according to old-rooted myth tapping and bugging in optic data transmission is not possible and secure data transmission is would be exaggeration, excess of care and redundant. One way to technically detect fiber tapping is tracing increased attenuation incidents introduced at the point of tapping. Some systems are able to trace and detect unexpected change of attenuation on a fiber link and inform the case. Some tappers, however, allow connection without notable increased attenuation.

Another spectacular case of penetrating the secured, air gapped network was worm named Stuxnet. The Stuxnet targets industrial computer systems incorporating specific type of industrial controllers while travelling on USB drives among personal computers. While spreading Stuxnet remain silent showing no symptoms. In Iran, in early days, close to 60 % of computers were infected. The Stuxnet malware after penetrated the network behind air gap separated industrial controllers in the system of uranium enrichment in Iran, was able to interfere with the operation of centrifuges for separating nuclear material. It is still not clear whether the case was filed by mistake of a careless employee or intentionally implanted by secret service /citegoodman15. Similar behavior and similar task are carried out nowadays with malware worms belonging to groups Flame or Duque. The worm, wanders on USB drives, collects data from computers, even isolated, from the network. After encountering a computer connected to a network with Internet access sends the collected data. Well-described mutation, worm called ACAD / Medre.A, resides on a USB drive, and when it detects an Internet connection sends e-mails with the collected data to servers in China. The name comes from the special interest of the malware to collect files from technical projects prepared in AutoCAD. Inside targets are Excel spreadsheets and other documents, but in the case of finding new CAD and lack of storage space will delete documents potentially less valuable and interesting for business intelligence.
After penetration next step is branching forming a bridge over the gap. The search for new ways is still ongoing for develop or improve new and effective sometimes unusual methods for crossing network isolation barrier. Two ingenious solutions are presented in [8, 6]. It was shown that it is possible to create a network of computers that use the microphone and speaker for communication in the ultrasonic range. Computers "talk to each other" form a mesh network of connections [9, 10, 11]. You can connect in such a network approaching in the vicinity, place your device close isolated network while staying in public areas. Similar networks are used today to communicate submarines in the range of infrasound. In [12, 13] an experiment was described to use the scanner to transmit information to the network. The idea was presented in [14] based on obserwation that LED status indicators on data communication equipment, under certain conditions, are shown to carry a modulated optical signal that is significantly correlated with information being processed by the device. Many different sorts of devices, including modems and Internet routers, were found to be vulnerable. To accomplish a task of transmission and control from outside, the worm have to be placed on a computer in the target network. It activates in predefined period scanner and reading data. At-

tackers send modulated laser light beam shining on the scanner glass. Worm reads transmitted instructions sent from outside. The experiment was performed over a distance of about 1 km on the scanner while shining through the window into the room. In this scenario, the worm may stay asleep for a long time in hospital network waiting for specific data to activate and disrupt the operation of sensors and medical devices in accordance with the instructions transmitted remotely from the distances ranging several hundred meters.

Still they are being developed new sophisticated ways to overcome the air gap. The analysis described here shows that as a first step it was necessary to physically move and install malware on the insulated network using removable disks or implant a rogue network devices.

None of mission critical systems is safe. An interesting case was reported on infecting even space station. According to a report on ExtremeTech [15], as in 2008 a Windows XP laptop was brought onto the International Space station by a Russian astronaut infected with the malware known as W32.Gammima.AG worm. The warm quickly spread to other laptops on the station. The case shows that even mission critical networks even highly air gapped are could be targeted.

In recent years some researchers demonstrated how hackers could use USB connectors implanted with extra RF transmitters to infiltrate data from air-gapped computers. Such methods are based on a hardware modification of the USB plug or any USB device where a dedicated RF transmitter was implanted [9]. But also the software only version was demonstrated as a combination of the software that can generate controlled electromagnetic signals from the data bus of any standard USB connector. The working prototype of the receiver can read of this transmissions. Baudrates are still very low ranging 20 to 60 bps and the working range is not still very but depends on hardwire layout running from specific USB connector and serving as antenna. Further direction of investigation technical solution to branch a gap based only on existing hardware are:

DiskFiltration attack that can steal data using sound signals emitted from the hard disk drive (HDD) of the targeted air-gapped computer[10];

BitWhisper that relies on heat exchange between two computer systems to stealthily siphon passwords or security keys;[9]

AirHopper that turns a computer's video card into an FM transmitter to capture keystrokes;

Fansmitter technique that uses noise emitted by a computer fan to transmit data [11];

GSMem attack that relies on cellular frequencies[7].

6. IDS or air-gap

In general, researchers demonstrated that air-gap cross channels can be formed over a number of physical mediums, including [16]:

- acoustic and seismic,
- light,
- magnetic,
- thermal,
- radio-frequency.

The collection of new ideas rises and it's almost impossible to seal all possible gaps in air lock on the physical medium layer. It was shown that there is no need to make special hardware of the transmitter and only standard computer parts like: speaker/microphone, fan, LED's, video cards, USB connector etc. may be useful and effective.

When someone wishes to enter an air-gapped system, will face and have to solve three problems:

1. Connect own device or infect computer within the isolated network.
   To breach an air-gapped system, one can select approach of infecting existing computer or insert own bug. The attacker needs to infect at least one of the air-gapped computers with malware. This could be done by abusing an insider in the targeted firm or an outsider, such as a service man, consultant, who may be able to get access to the isolated area and use a malware-infected drive to compromise the computer. Target computers could also be infected in supply chain, where the computer's components are intercepted and tampered with during the manufacturing or shipping processes. Proven way includes USB drives with commecial materials shared as a gift.

2. Exfiltrating data from the compromised computer or network.
   Unless the attackers only wants to cause some damage, They'll need to find a way to exfiltrate the stolen data from the air-gapped network. This can be done with the USB also while working range of known branching technologies is still poor.

3. Sending commands to the compromised computer.
   Once a computer has been infected, the attacker has to send commands and updates to the malware. Normally, this would be conducted over the internet; however, anyone attacking an air-gapped system needs to replay of one of known solutions or create teh combination of it.

In conclusion the air gapping is a strong tool in security, popular in mission critical systems and also medical care information processing systems. But number of presented solution capables to branch the gap indicates that physical access control to the infrastructure of isolated network is crucial. The attacker should be stopped on the first of three discussed above. Infection of the air gapped network infrastructure element it common step in all presented cases. To avoid data exfiltration even in case of successful implantation of the bug secure communication and data encryption,even in isolated networks, hast to be applied as a rule. On the other hand IDS - Intrusion Detection/Prevention System placed on the edge of internal infrastructure is even stronger solution and does not break the link to outer world. In IDS solution there are still the same threats as in air gapped plus an extra way to Internet running through IDS system. Presence of the IDS opens new possibility, to early identify symptoms of system infection and beacon the infected device or hostile device dropped intentionally. Recalling the honeypot mechanism to detect, deflect and counteract attempts of authorised data access hostile devices or malware should not be switched off but controlled and observed to identyfy attacer of feed intentionally false data.

7. Good practice in security of health care computer network

Analyzing the presented cases of successful attacks allows to identify weaknesses of air-gap technique. Was proven that air-gap cross channels can be formed over a number of physical mediums. But in every analised case the attacker had to gain a direct access to the internal network even for a while in the past before successful attack or abuse gullible and unwary employees. In conclusion one need to note that the air gapping is a very powerful and highly efficient way to ensure safety of internal network but can be tempered in case of weak physical access control to internal network infrastructure and equipment. Access control should not exclude own staff and no device like USB drive shell pass the airlock without strict control.

In every case the use of data encryption and secure communication channels even in private or air gapped network should be the rule. It was discussed that is hard to accomplish the task of well sealing internal network infrastructure in case of medical care systems. The hazard from the use of the network are among the many that the patient is exposed to. The air gap helps but air gapping disables possibility of sharing medical imaging devices data over wide network. Always it is important to find a balance between the rules of safety and efficiency of the operation of the whole system and to treat the security as a continuous, neverending process not a single occasional action. Application of effective Intrusion Detection/Protection System on the border of the network gives better overall results over air gapping when data exchange is crucial. IDS allows also to early identify symptoms of system infection and beacon the infected device or hostile malware. After beaconing the intruder stopping its operation should be always the last choice. Good practice is to observe and analyze its activity to avoid placing another, trace connections or even feed with false data. Technologies developed to bridging the air gap to isolated network are clever and innovative and can be applied to support backdoor connection even in networks connected to Internet in classic way, hence reports should be traced and analyzed carefully.

References

[1] Arendt, D., *Bezpieczeństwo teleinformatyczne- transmisja danych i kontrola dostępu*, In: Konferencja Promieniowanie jonizujące w medycynie, PJOMED 2015, 1-2 June, Krajowe Centrum Ochrony Radiologicznej, 2015, pp. 58–63, ISBN 978-83-61856-07-8(in Polish).

[2] Healey, J., Pollard, N., and Woods, B., *The Healthcare Internet of Things, Rewards ad Risks*, The Atlantic Council of the United State, 2015, ISBN 978-1-61977-981-5.

[3] FDA, *Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication*, Tech. rep., U.S. Food & Drug Administration, 2013.

[4] Mah, C. and Higgins, S., *Cisco Medical-Grade Network (MGN) 2.0—Security Architecture*, No. EDCS-957250 in s1, Cisco Corp., 2012.

[5] Kozlej, S., *National Security Strategic Tasks of the Republic of Poland at the Turn of the Second and Third Decade of the Twenty-First Century*, Mysl Ekonomiczna i Polityczna, Vol. 3(54), No. 2081-5913, 2015, pp. 292–317.

[6] Hanspach, M. and Goetz, M., *On Covert Acoustical Mesh Networks in Air*, Journal of Communications, Vol. 8, No. 11, 2013, pp. 758–767.

[7] Guri, M., Kahlon, A., Hasson, O., and Elovici, Y., *GSMem: Data Exfiltration from Air Gapped Computers over GSM Frequencies*, In: 24th USENIX Security Symposium, 2015, pp. 849–864, ISBN 978-1-931971-232.

[8] Madhavapeddy, A., Sharp, R., Scott, D., and Tse, A., *Audio networking: the forgotten wireless technology*, IEEE Pervasive Computing, Vol. 4, No. 3, 2008, pp. 55—60.

[9] Guri, M., Monitz, M., and Elovici, Y., *USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB*, arXiv preprint arXiv:1608.08397, 2016.

[10] Guri, M., Solewicz, Y., Diadulov, A., and Elovici, Y., *DiskFiltration: Data E xfiltration from Speaker less Air Gapped Computers via Covert Hard Drive Noise*, arXiv:1608.03431, 2016.

[11] Guri, M., Solewicz, Y., and Elovici, Y., *Fansmitter: Acoustic Data Exfiltration from Speaker less Air-Gapped Computers*, arXiv:1606.05915, 2016.

[12] Schneider, B., *Jumping Air Gaps with All-in-One Printers*, 2014, [online] http://www.schneier.com/blog/ archives/2014/10 [accesed 2016.03.02].

[13] Constantin, L., *All-in-one printers can be used to control infected air-gapped systems from far away*, 2015, [online] http://www.itworld.com/ article/ 2835037/ all-in-one-printers-can- be-used-to-control- infected-air- gapped-systems- from-far-away.html [Accessed 2016.04.16].

[14] Loughry, J. and Umphress, D., *Information Leakage from Optical Emanations*, ACM Transactions on Information and System Security, Vol. 5, No. 3, 2002, pp. 262–289.

[15] Goodman, M., *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, Anchor Books, 2015, ISBN 978-0804171458.

[16] Powell, J.-P., *Mind the gap: Are air-gapped systems safe from breaches?* 2014, [online] https://www.symantec.com/ connect/blogs/ mind-gap-are-air-gapped-systems- safe-breaches [accesed 2016.02.02].