The dangers of the digital age

Every year, millions of CT and MRI scans are done all over the world. The scanners are generally managed on an internal network, with a central server receiving and storing the images in readiness for analysis by the radiology department. However, networks that are not connected to the internet are still vulnerable to attack. A new, non-peer-reviewed paper from Israel shows the ease with which an external attacker could obtain and tamper with patient scans and trick experts into concluding that cancer is present or absent, when in fact the reverse is true.

The researchers on this study used machine learning techniques to establish an artificial intelligence model that could either remove cancerous nodules from a CT scan of a patient’s lungs, or insert cancerous nodules into images of healthy lungs. They tested a set of altered images on a team of three radiologists. For the scans in which cancerous nodules had been removed, the radiologists diagnosed the patient as healthy in 94% of cases. For the scans in which tumours had been introduced, they diagnosed the patient as having cancer in 99% of cases. The radiologists were then warned that the next set of scans they received would include faked images, but they still went on to misdiagnose 60% of the scans in which cancerous nodules had been removed and 87% of the scans in which nodules had been added.

This raises the question of how such malware could be introduced. To investigate, Yisroel Mirsky—one of the authors of the paper—went undercover at an unnamed hospital (admittedly with the permission of the hospital administrators). He sneaked into the radiology department after hours and connected a device that would allow him to intercept all data transmitted in the internal network. Mirsky completed his mission in an impressive 30 s.

“Machine learning is very accessible to the public these days; it is almost like plug and play”, Mirsky (Department of Information Systems Engineering, Ben-Gurion University, Beersheba, Israel) tells The Lancet Digital Health. Although this experiment pertained to cancer, the model could be readily deployed in other conditions. A criminal might install the malware, alter a series of images, and then demand payment to reveal the ones that have been affected. There is also the potential for health insurance fraud. If an individual can add a fractured vertebrae or small aneurysm to a scan, both of which are tricky to otherwise disprove, they could be eligible for a sizeable payout.

Malware could be used to sabotage clinical trials. A patient’s follow-up scans could be adjusted to show cancer spreading when in fact it is receding, or vice versa, which opens up the possibility of people receiving unnecessary treatment, or being deprived of vital treatment.

“So far, the health-care industry has not seen targeted attacks of this type, where a specific patient’s test results are tampered with or where there is the manipulation of a medical device”, says Kevin McDonald, Director of Clinical Information Security at the Mayo Clinic (Rochester, MN, USA). “On the other hand, this is not something care providers usually look for. If a patient has an unexpected outcome, there might be an autopsy or review, but health-care institutions typically do not examine the medical devices or the data that were used to treat the patient”, he continues. In other words, such events might have already occurred. The US Food and Drug Administration (FDA) has warned that intravenous infusion pumps might be vulnerable to hackers, and similar concerns have been raised over defibrillators and the temperature settings on hospital refrigeration units. In 2012, the US television drama Homeland included a storyline in which a character’s pacemaker was hacked to induce heart failure—any lingering doubts that such a scenario could occur in real life were dispelled 5 years later when the FDA recalled half a million pacemakers because of their vulnerability to cyberattack.

“Hospitals have tended to believe that because some components are segregated from the internet, they are therefore impervious to cyber-threats”, explains Mirsky. “But that is just not true—there are lots of ways malicious actors can break into the network, so you need be prepared for that.”

Securing internal networks by encryption of communications would make it more difficult for an attacker to intercept data, and having scanners add digital signatures to images would enable staff to verify that images have not been altered.

As with so much in cybersecurity, the precautions are straightforward and largely effective. Around 80% of the risks to health-care information systems can be mitigated by basic cyber hygiene—things like ensuring that operating systems are supported and updated and antivirus software is installed and functional. The consequences of neglecting such measures can be severe. In 2016, the WannaCry attack on the UK National Health Service (NHS) caused havoc. At least 81 trusts were affected and thousands of operations and appointments had to be cancelled. Yet the organisations who fell victim could hardly claim to have been taken by surprise. According to a report by the UK National Audit Office, trusts had been warned to stop using unsupported operating systems by the UK Department of Health and Cabinet Office and to patch their systems to prevent cyberattacks. The report added that “whether organisations had

Preparedness/planning/405d/
https://www.phe.gov/human-services
For the guidelines by the US Department of Health and Human Services see https://www.phe.gov/Preparedness/planning/405d/Documents/HCIP-Main-508.pdf
For the US Food and Drug Administration warning for medical devices see https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abotts-formerly-st-jude-medical
For the report by the National Audit Office see https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/
For the article by Mirsky and colleagues see https://arxiv.org/pdf/1901.03597.pdf
For the non-peer-reviewed article by Mirsky and colleagues see https://arxiv.org/pdf/1901.03597.pdf
patched their systems or not, taking action to manage their firewalls facing the internet would have guarded organisations against infection” (McDonald pointed out that in general, the picture is more complicated than simply installing a firewall, especially if the malware is sent by phishing or an individual opens a flash drive with a virus).

In 2018, the US Department of Health and Human Services (HHS), in conjunction with several industry partners, released a set of voluntary cybersecurity guidelines for health-care organisations. The guidelines focused on five major threats, which included email phishing attacks, which attempt to trick employees into providing access to sensitive information, perhaps by persuading them to click on an unsafe link; ransomware, such as that used in the WannaCry attack, which encrypts data on infected computers and then demands payment in return for restoring access; and data theft.

“The threat of a major shutdown is real. We keep thinking we are dodging the bullet, but we are seeing these precursor attacks, such as with the NHS, and we are not paying enough attention”, says McDonald. Ransomware has become a commercialised business. Attackers can demand payment in bitcoin, which is difficult to trace, and they need not even write the software themselves. “You can now buy all the infrastructure that is needed to make an attack”, points out McDonald. In 2016, a computer virus forced a network of ten hospitals and 250 clinics in the Washington, DC region to temporarily shut down.

In 2020, the Windows 7 operating system will no longer be supported, which means that the proportion of unsupported medical devices globally will jump from 30–40% to 70–80%. Many of these systems cannot be upgraded, so hospitals face the prospect of either keeping hold of unsecured equipment or spending large amounts of money on replacements. The average hospital in the USA has a net income of around US$11 million, so spending $1–3 million on a new MRI scanner represents quite an outlay, especially when the old machine is still operational. “Legacy systems are a key risk”, says Dan Jeffery of the NHS Digital Data Security Centre, which advises hospitals on matters of cybersecurity. “Medical equipment is a big capital investment, intended to last 10–15 years. It has not necessarily been designed with cybersecurity in mind”.

In 2011, 2000 patient x-rays were stolen from the Beth Israel Deaconess Medical Centre in Boston. This hospital now runs its own phishing campaigns to test staff awareness of cybersecurity. The NHS Digital Data Security Centre does something similar. Almost half of NHS providers of secondary care have undertaken training programmes with the National Cyber Security Centre. A separate multistage programme to improve the cybersecurity posture of NHS providers started last year, although it is too early to draw any conclusions on the success of the project.

Improving cybersecurity is a long-term process. It is already difficult to find trained information technology (IT) staff and the situation is likely to worsen. Cybersecurity Ventures, a research organisation, estimates that by 2021 there will be 3·5 million unfilled cybersecurity positions globally. “It is tough for smaller facilities in the USA to find and recruit talent”, says McDonald. “They are competing with the federal government and the finance sector.” Besides, there might not be the resources to fund a sizeable IT department, especially for community doctors and other primary care providers.

Health care has historically been slow to respond to evolving cybersecurity threats. The HHS report noted that US health-care organisations spend somewhere between 4–7% of their total IT budget on cybersecurity, compared with 10–14% in other industries. Yet data breaches cost the American health-care system over $6·2 billion in 2016. The overwhelming majority of physicians in the country have experienced a cyberattack. A combination of long-standing underinvestment, insecure technology, and lack of staff awareness have left hospitals all over the world vulnerable.

“Everything is becoming more and more connected, and medical records and data have an intrinsic financial value; that makes health care very attractive to criminal gangs”, says Mirsky. “Hospitals have to start following the standard, conventional security policies that most businesses perform; even ensuring a baseline level of security will be a major improvement”, agrees McDonald. “If you get the basics done, you have really protected yourself against many of the challenges, but at the moment we still have hospitals using systems that are old, vulnerable, and so poorly configured that you would not want to use them to do your home banking.”

Talha Burki
Copyright © 2019 The Author(s). Published by Elsevier Ltd. This is an Open Access article under the CC BY 4.0 license.