LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Medical Device Image Tampering

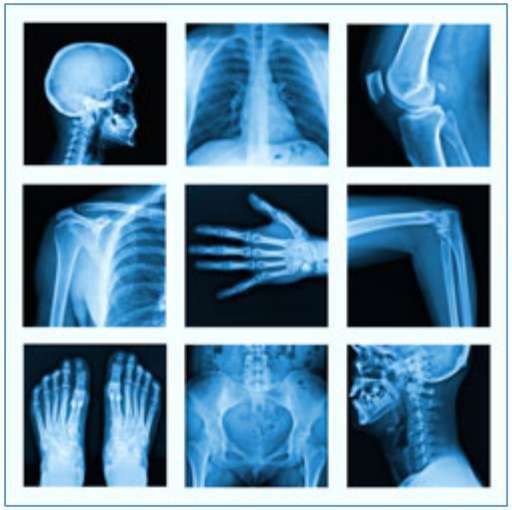
07/11/2019

Report #: 201907111000

Agenda

Software Subversion

- Overview
- Medical Image Devices
- CT GAN Framework
- Realism
- Attack Vectors
- Attack Methods
- Implications
- Test Scenario
- Vulnerability Findings
- Mitigations
- Conclusion
- References



Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

- Researchers have developed software that can tamper with CT and MRI scanning equipment to produce false results.
- Developed by Yisroel Mirsky, Yuval Elovici, Tom Mahler, and Ilan Shelef at Ben-Gurion University, Israel.
    - The intent was to explore security weaknesses both in medical imaging equipment and networks transmitting those images.
    - Using the software, researchers were able to manipulate CT and MRI scanning equipment.
- The attack utilizes a neural networking technology that learns to create more convincing fake images.
- The implications of using the exploit range from medical fraud to causing harm or death.
- The exploit can be performed utilizing a number of attack vectors in a typical lab with medical scanning equipment and a supporting network.
- Researchers demonstrated the exploit by performing a penetration test at a participating hospital.
- The fake images created by the attackers were able to pass assessments by trained radiologists.
- The demonstration highlights the lack of sufficient encryption in medical imaging enterprises.

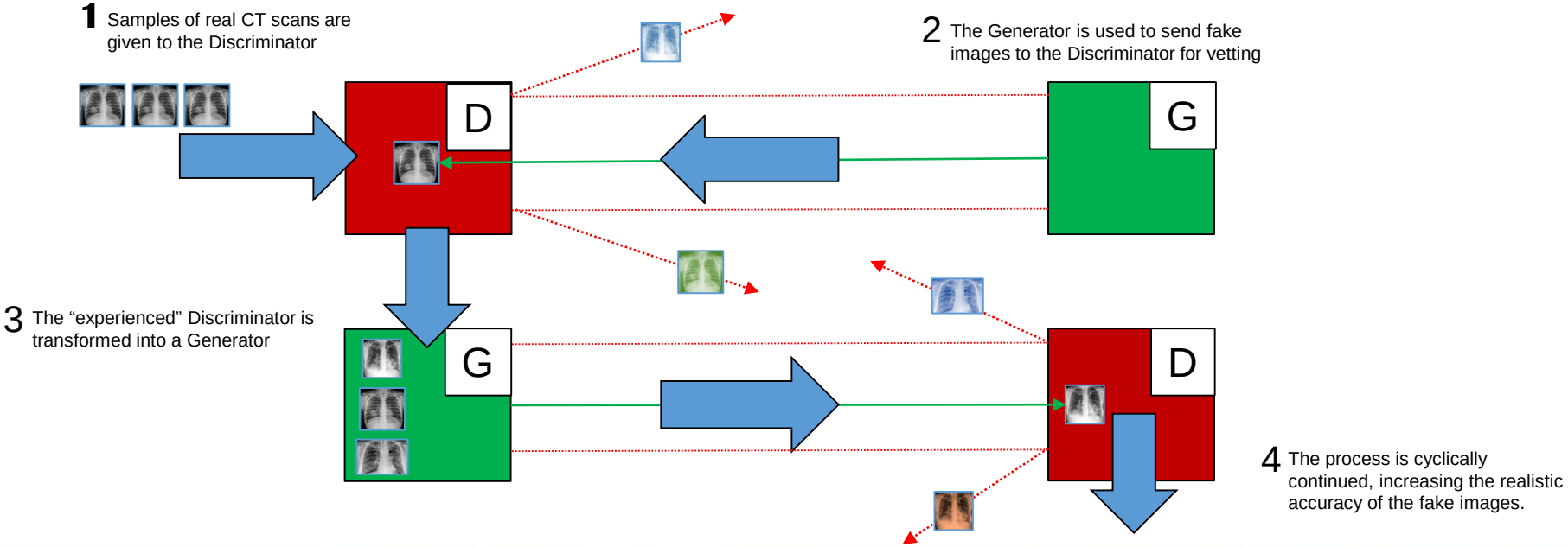
The attack would work for brain tumors, heart disease, blood clots, spinal injuries, bone fractures, ligament injuries and arthritis, - Mirsky.

Medical Image devices

- The exploit developed by researchers was used to alter images created by MRI and CT scanners.
- MRI and CT scanners create 3D images by taking many 2D scans of the body over the axial plane (from front to back) along the body.
  - MRIs use powerful magnetic fields to diagnose issues with bone, joint, ligament, cartilage, and herniated discs.
  - CTs use X-Rays to diagnose cancer, heart disease, appendicitis, musculoskeletal disorders, trauma, and infectious diseases.
- Today, CT and MRI scanners are managed though a picture archiving and communication system (PACS).
  - A PACS is an Ethernet-based network involving a central server which:
    - receives scans from connected imaging devices.
    - stores the scans in a database for later retrieval.
    - retrieves the scans for radiologists to analyze and annotate.
    - The digital medical scans are sent and stored using the standardized digital imaging and communications in medicine (DICOM) format.

CT-GAN Framework

- Generative Adversarial Network (GAN) is a type of deep neural network.
- The neural network can be specifically focused on CT images. (CT-GAN Framework)
  - GAN consists or two neural networks which works against each other.
    - **Generator (G):** creates fake samples, trying to fool the discriminator.
    - **Discriminator (D):** learns to differentiate between real and fake samples.
  - The Generator images become more realistic as it learns from trial and error, vetting from the Discriminator.



Realism

- 70 Computerized Tomography (CT) lung scan images were altered.
- Each altered image was evaluated by 3 individual Radiologists and 1 Artificial Intelligence Program.

Aggregate Results

Fabricated Cancer Nodules


= 1%

Healthy Diagnosis


= 99%

Cancer Diagnosis

Real Cancer Nodules Removed


= 94%

Healthy Diagnosis


= 6%

Cancer Diagnosis

A second set of scans were given to the radiologists after being informed of the modifications:

Fabricated Cancer Nodules


= 60%

Cancer Diagnosis

Real Cancer Nodules Removed


= 87%

Healthy Diagnosis

Conclusion: Altered scans were highly effective at deceiving both medical professionals and AI programs

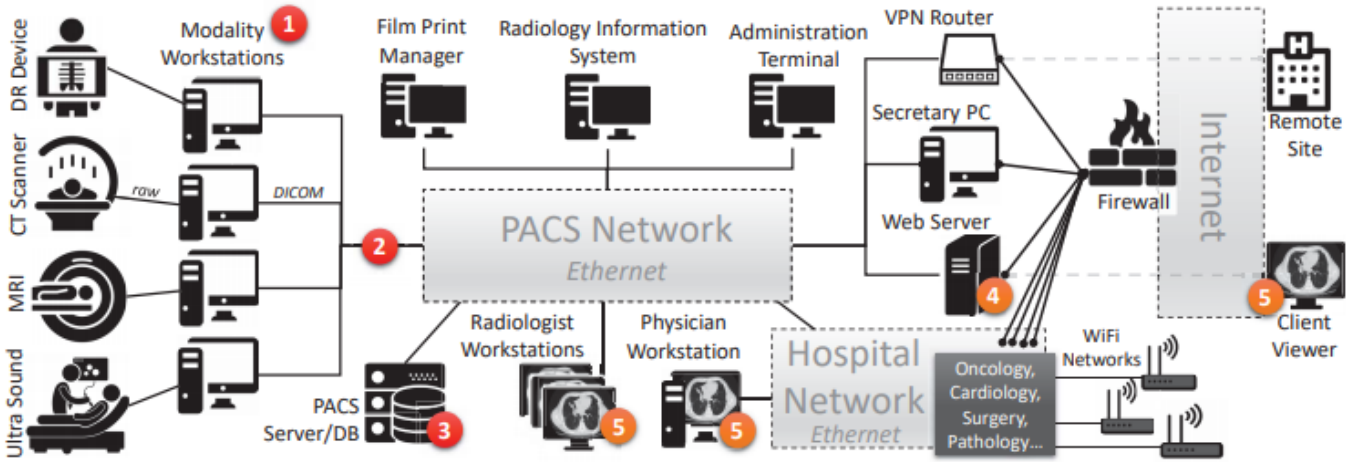
Attack Vectors

Attacker can tamper with all scans

1. **Modality Workstations:** Used by technicians to configure and capture scanning images. Can also send images to PACS server for storage.
2. **Data in transit:** Data moving from the modality workstations to the PACS server (man-in-the-middle attack).
3. **PACS Server/DB**: Responsible for storing, organizing, and retrieving DICOM imagery.

Attacker can tamper with a subset of scans

4. **Web server:** Enables viewing of the stored medical images via web browsers, mobile applications, or web API's.
5. **Radiologist/Physician Workstation:** Allows physician to retrieve scans from various locations (can include the physician's personal PC and/or mobile device.
5. **Client Viewer:** PCs used by the patient to view medical scans.



PACS Network Topology

Attack Methods

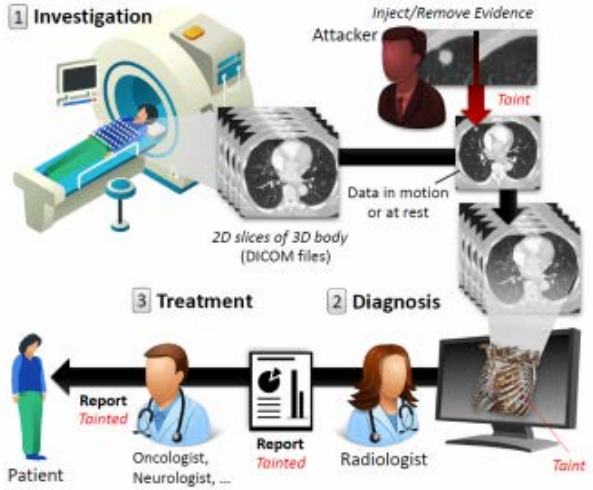
- In general, the attack vectors involve either remote or local infiltration of the facility's network

Remote Infiltration. The attacker may be able to exploit vulnerabilities in elements facing the Internet, providing the attacker with direct access to the PACS from the Internet.

- *Social engineering attacks:* Attackers can use social engineering methods such as spear phishing and backdoors to infect the PACS network with malware.
- *Personally-owned equipment:* Employee laptops and phones can serve as a target of opportunity if the attacker knows the technician/doctor analyzes cans on his/her personal device.
- *Remote site:* Attacks can target a remote site (e.g., a partnered hospital or clinic) which is linked to the hospital's internal network.
- Lateral Movement: If the PACS is not directly connected to the Internet, attackers can focus on infiltrating the hospital's internal network, then move to the PACS internally.
    - PACS are usually connected to the internal network (using static routes and IPs), and the internal network is connected to the Internet (evident from the recent wave of cyber-attacks on medical facilities.

Local Infiltration. The attacker can gain physical access to the premises with a false pretext, hire an insider or even be an insider. Once inside, the attacker can plant the malware or a back door by connecting a device to exposed network infrastructure (ports, wires, etc.) by accessing an unlocked workstation.

- *WiFi access points*: Attacks can gain access to the PAC through WiFi access points, using existing vulnerabilities such as 'Krack' or 'BleedingBit'.
- *Directly Compromising the PACS:* Once access to the PACS has been achieved, attackers can exploiting misconfigurations, use default credentials or leverage known software vulnerabilities.



Implications

There are a number of examples in which malicious actors can utilize these exploits:

Public Figures/VIPs: An attacker can manipulate a medical diagnosis of a political or business adversary, forcing them to step down or focus a significant amount of energy on the "medical issue".

Ransomware: A hacker can pursue monetary gain by holding medical images hostage; altering scans then demanding payment for revealing which scans have been affected.

Fraud: An individual could manipulate their own medical scans in order to receive money from insurance companies or to get approval for prescription drugs.

+ : Add Evidence − : Remove Evidence ± : Either ● : Target Effect ○ : Side Effect			Goal								
			Steal Job Position	Affect Elections	Remove Leader	Sabotage Research	Falsify Research	Hold Data Hostage	Insurance Fraud	Murder	Terrorize
Motivation		Ideological			+						±
		Political		+	+					−	
		Money	+		+	+	−	±	+		
		Fame/Attn.	+		+		±				
		Revenge	+		+					−	+
Effect	Physical	Injury	○	○	○		○	○		○	●
		Death						○		●	●
	Mental	Trauma	○	○	○			○		○	●
		Life Course	●	●	●	○			○	○	●
	Monetary	Cause Loss	○		○	●		○		○	●
		Payout	●			○	●	●	●		
Attack Type		Untargeted				X		X			X
		Targeted	X	X	X	X	X		X	X	

Attacker motivations and goals for attacking 3D medical imagery

Other Implications

Falsifying research evidence, sabotaging another company's research, job theft, terrorism, and indirect bodily harm.

Test Scenario

- Tool used: One Raspberry PI 3B and one Ethernet-USB adapter
- Installation time: 30 Seconds
- Distance when connected: 20 meters
- Performed with full permission from participating hospital

Artifacts from the penetration test

Execution

1. Performed a man-in-the-middle attack on the CT scanner using the Raspberry Pi 3B.
2. Raspberry PI was configured as a passive network bridge and a hidden Wi-Fi point.
3. 3D logo of the CT scanner's manufacturer and glued to it – less conspicuous.
4. Attackers waited at night until cleaning staff opened the doors.
5. Found the CT scanner's room and installed the Pi-bridge between the scanners workstation and the PAC's network.
6. Hid the Pi-bridge under the access panel in the floor.

Pen Test Video Link

Raspberry PI 3B

Effects

- Attackers were able to intercept scans and move laterally to other PAC subsystems. (real-time scan intercepts were tested)

- Obtained usernames/passwords of 27 staff members and doctors due to multi-casted Ethernet traffic sent in cleartext.

Vulnerability Findings

PACS Vulnerabilities

Researchers have highlighted the lack of encryption within many PACs as a major factor in making medical systems and networks vulnerable to attack.

- Examples include: Centricity PACS (GE Healthcare), IntelliSpace (Philips), Synapse Mobility (FujiFilm), and PowerServer (RamSoft).
- It is often erroneously thought that there is no need for security measures, such as encryption, due to not being directly connected to the internet.

- After discovering the vulnerability in the pen-tested hospital, the software provider (with over 2000 installations worldwide) commented that their hospitals do not enable encryption in their PACS because “it is not common practice.”
  - Provider also admitted some of the PACS “don’t support encryption at all.”
    - Health-care policies often focus on addressing data privacy (access-control) but not data security (availability/integrity).
    - Hospitals often have old components (scanners, portals, databases, etc.) which do not support encryption.
- Using Shodan, a quick search 667 medical image (DICOM) servers and 102 PACS servers in the U.S. exposed to the Internet.

Mitigations

Prevention

Prevention of medical image exploitation relies on secure both the data-in-motion (DiM) and the data-at-rest (DaR).

Data-in-Motion: To secure data-in-motion, admins should enable encryption between the hosts in their PACS network using proper SSL certificates. Enterprises should utilize network access control systems and network segmentation to further secure data-in-motion.

Data-at-Rest: Servers and anti-virus software on modality and radiologist workstations should be kept up to date, and admins should also limit the exposure which their PACS server has to the Internet. End point devices should also utilize full disk encryption capabilities to protect data on medical devices.

Detection

Digital Signatures: The DICOM image file standard that allows users to store signatures within the file's data structure is one of the best options to detect this attack. If enabled, admins should check that valid certificates are being used and that the radiologists' viewing applications are indeed verifying the signatures.

Digital Watermarking: A hidden signal embedded into an image can provide a means for localizing changes in a tampered image. and can provide a means for localizing changes in a tampered image. However, they add noise to images which may harm the medical analysis.

Machine Learning: It is possible to utilize machine learning models that are "trained" on tampered images to detect a potential compromise of this type.

Reference Materials

References

- Y. Mirsky, T. Mahler, Y. Elovici, “CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning.”, Dept of Information Systems Engineering, Ben-Gurion University, 6 June 2019, accessed 17 June 2019. https://arxiv.org/pdf/1901.03597.pdf

- N. Cohen, “Can Attackers Inject Malice into Medical Imagery? Fake Growths here and there” Tech Xplore, April 6 2019, accessed 17 June 2019; https://techxplore.com/news/2019-04-malice-medical-imagery-fake-growths.html

- Kim Zetter, “Hospital viruses: Fake Cancerous Nodes in CT scans, created by malware, trick radiologists”, The Washington Post, 3 April 2019, accessed 17 June2019 https://www.washingtonpost.com/technology/2019/04/03/hospital-viruses-fake-cancerous-nodes-ct-scans-created-by-malware-trick-radiologists/?utm_term=.d26fb486f47e

- Siau-Chuin Liew, Siau-Way Liew, Jasni Mohd Zain, “Reversible Medical Image Watermarking For Tamper Detection And Recovery With Run Length Encoding Compression, 2010, accessed 10 June 2019; http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.309.3206&rep=rep1&type=pdf

- Christiaan Beek. “Mcafee researchers find poor security exposes medical data to cybercriminals, mcafee blogs. 11 March 2018, accessed 17 June 2019; https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-researchers-find-poor-security-exposes-medical-data-to-cybercriminals/

Questions

Questions

Upcoming Briefs

- Iranian Threat Brief
- Healthcare Malware Update 2019

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.

Contact

Health Sector Cybersecurity Coordination Center (HC3)

(202) 691-2110

HC3@HHS.GOV