I've Got You, Under My Skin: Biohacking Augmentation Implant Forensics

Steven Seiden[1,2(✉)], Ibrahim Baggili[1,2], and Aisha Ali-Gombe[2]

[1] Baggil(i) Truth (BiT) Lab, Center of Computation & Technology, Baton Rouge, LA, USA
[2] Division of Computer Science & Engineering, Louisiana State University, Baton Rouge, LA, USA
sseide3@lsu.edu

Abstract. Recently, people have become interested in embedding technology in their bodies to augment themselves with new abilities. For example, a person may embed a chip in their hand to wirelessly lock and unlock a door. Subdermal augmentation implants, the implant technology that can add these new abilities to a user, are increasing in popularity. With this new technology comes a variety of new forensics and security challenges. In our work, we conceive a modified forensics approach for augmentation implants, which includes device discovery and its associated forensic acquisition and memory analysis. First, we explore three device discovery methods: implant chip reading, X-Ray detection and the use of metal detectors. We then share a case study by implementing an augmentation implant authentication system, acquiring and analyzing its memory. Our results show that when an implant is installed in raw chicken meat, that X-Ray scanners are capable of not only unveiling it, but revealing the exact type of implant to a trained analyst. In the case of metal detectors, only one of the implants were detected, and our results indicate deeply installed implants (1.5 cm or more below the skin) are undetectable. In the case of using RFID and NFC scanners to read compatible chips, we found we could detect the implants up to 1.6 cm and 1.0 cm respectively. We also examined the potential legal and ethical issues surrounding augmentation implant forensics, highlighting cases in which surgical removal could potentially be legally mandated.

Keywords: Biohacking · Implants · Forensics · Ethics

1 Introduction

Due to advancements of modern technology, biohacking, or the act of modifying one's body with the goal of adding an ability, is becoming popular. One of the more common ways that people are biohacking themselves is through subdermal implants. Currently, the most common types of subdermal implants are storage devices that employ one of two wireless technologies: Near Field

S. Goel and P. R. Nunes de Souza (Eds.): ICDF2C 2023, LNICST 571, pp. 315–332, 2024.
https://doi.org/10.1007/978-3-031-56583-0_21

Communication (NFC) and Radio Frequency Identification (RFID) (Matthews 2015). Surveys have shown that as biohacking technology becomes easily accessible, more people would consider it (Michael 2016). Reports showed that 13% of worldwide consumers are "extremely interested" in utilizing a subdermal implant as a form of payment, and 51% of European consumers would consider getting a subdermal implant (Shipper 2021, Marqueta 2021).

This paper examines the use of digital forensics techniques on subdermal implants. As these devices are implanted within a human's body, the process of discovering and potentially extracting them during an investigation can present unique challenges. Additionally, there may be legal, ethical, and procedural considerations that affect the validity of any evidence obtained through this process. To the best of our knowledge, no academic research has yet examined the impact of biohacking on the digital forensics field. We provide the following contributions:

- This is the primary study to explore the forensics of augmentation subdermal implants.
- We explore various device detection techniques on consumer available products using device scanners, metal detectors, and X-Ray technologies
- We explore the viability of memory forensics on an augmentation implant authentication system

To accomplish the aforementioned contributions, we tested the following hypotheses:

Hypothesis H_0(Scanner Hypothesis). We can discover augmentation implants using an NFC or RFID scanner.

Hypothesis H_1 (Metal Detector Hypothesis). We can discover augmentation implants using metal detectors.

Hypothesis H_2 (X-Ray Hypothesis). We can discover augmentation implants using X-Rays.

Hypothesis H_3 (Verification System Hypothesis). We can retrieve meaningful data from an augmentation implant verification system.

The remainder of this paper is organized as follows: the overview of biohacking via subdermal implants, including a survey of the emerging market, itemizing usage, acceptability, risk, and potential discovery and data retrieval is provided in Sect. 2. Section 3.1 describes the experimental setup, methodology, and tools required for subdermal forensic analysis. This section also dives into the modified forensics process we have conceived for augmentation implants. We then illustrate a forensics investigation involving a subdermal implant based on an authentication system case study in Sect. 4. This is followed by the discussion of our findings and the review of biohacking impacts in Sect. 5. Section 6 describes the related works on subdermal implants and similar products and the novelty of our research contribution. Section 7 describes our future plans, and Sect. 8 concludes the paper.

2 Background

Table 1. A List of the Current Retailers Offering Augmentation Implants for Humans.

Seller	Purpose
Bioteq	General Purpose NFC/RFID
Dangerous Things	General Purpose NFC/RFID
Dsruptive	Medical
I Am Robot	General Purpose NFC/RFID
VeriChip	Medical & Identification
VivoKey	Identification
WalletMor	Payment

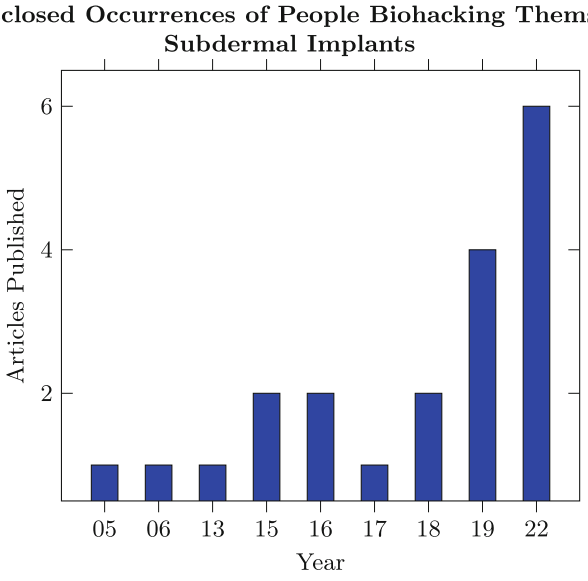

Fig. 1. The Number of Online Articles Describing an Individual Biohacking Themselves With Subdermal per Year Surveyed, Starting With 2005.

2.1 Implants in Practice

To understand how biohacking has emerged over the past few decades, we surveyed online documented cases of people utilizing biohacking on themselves. We found that these cases are growing, as shown in Fig. 1. A major part of today's biohacking involves employing subdermal implants – electronic devices embedded within one's skin that emit a wireless signal. These implants have a variety

of uses, such as unlocking doors, storing medical information, and acting as payment methods. While medical implants have existed for some time, the implants used for biohacking differ greatly in that they add additional features to the human body, rather than aiding or correcting existing ones. Thus, to make this distinction clear, we will be referring to these subdermal implants as *augmentation implants*. Amal Graafsta has made these augmentation implants much more attractive to the general population. Graafsta first implanted himself in 2006 with an RFID implant designed for pets, one of the first known cases in which an implant of this kind was installed in a human (TEDx 2013).

Today, several retailers sell augmentation implants designed for human implantation. As seen in Table 1, different companies produce implants for a wide variety of purposes. Some implants are designed for a specific purpose, such as storing medical information or payment methods, where as others exist for those who want to utilize the popular NFC and RFID however they chose.

2.2 Utilizing Implants in an Attack

Augmentation implants today are often used as an identification method. For example, an implant can be used to open a lock, start a car, or store another type of unique identifier (*Red XSIID bundle* 2022, Tanne 2004). As demonstrated by (Patel et al. 2018), it is possible to clone certain portions of the memory on these devices. As this practice becomes more commonplace, the risk of an attacker cloning an implant also increases. Due to the inaccessibility of surgically implanted devices, resolving an attack of this type can be difficult once the attack has been executed, especially for implants with read-only storage (Halamka et al. 2006).

There is also the possibility that in the future, these devices can store more than simple credentials, enabling the smuggling of sensitive data. To discover how an attacker can utilize an implant, we study the various ways a device can be discovered.

2.3 Implant Discovery and Retrieval

Utilizing materials that can represent human skin, we first explore the various methods for implant discovery (Dąbrowska et al. 2016). By implanting several augmentation implants into these materials, we are able to create a realistic implantation scenario. From here, we are able to test different means of implant discovery, such as through an RFID/NFC scanner, X-Ray or metal detector.

Once an augmentation device has been discovered, the data will need to be retrieved. Due to the nature of surgical augmentation implants, this step in the forensic analysis process can prove to be difficult. While current implants feature wireless protocols such as NFC and RFID, direct access to the device via surgical removal may be required for an in-depth analysis in the future. This introduces a new dimension of legal issues over whether or not a surgical removal can be forced upon someone with an augmentation implant, which we will discuss further in Sect. 5.

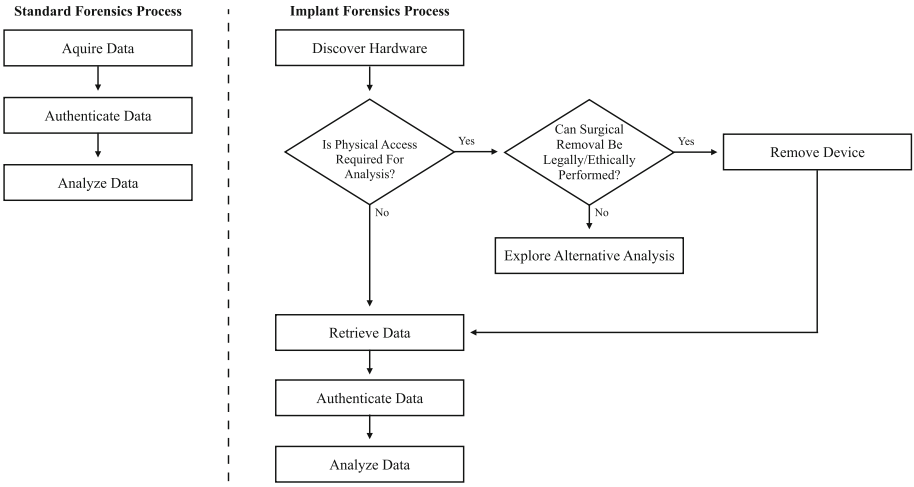

Fig. 2. Comparing Typical Forensics to That of Augmentation Implants.

3 Methodology and Tools

3.1 Augmentation Implants Forensics Process

To perform forensic analysis of augmentation implants, we first needed to devise our approach. A typical forensics process includes:

- The acquisition of hardware and data for analysis
- The authentication of the extracted digital data
- The analysis of the acquired data

With augmentation implants, the forensics process becomes convoluted. Therefore, to conduct a thorough forensics investigation, we devised a revised methodology. A comparison between the traditional forensics process and our modified implant forensic process is shown in Fig. 2. As shown in our modified process, the major setback will occur in the device discovery phase, as well as the physical extraction of the device through surgical removal. These additional steps add a new set of dimensions to the forensics process. We explore both of these challenges in detail in our studies.

In our work, we physically inspect several augmentation implants currently available on the market. After inspecting the implants, we performed our case study. This involves attempting to apply our modified forensics process (Sect. 3.1) to the implants. The first step of this process involves device discovery. We explore different detection methods and the use case scenarios of the discovery methods are determined. Next we study the process of device removal for the cases where this may be necessary, focusing on the process to legally and ethically do so. After this, we explore the methods of data retrieval from the implants. This allows us to perform data authentication and analysis. Our

methodology can be summarized as follows: 3.2) Materials Used 3.3) Device Implanting 3.4) Device Detection 3.5) Data Retrieval and Analysis and 3.6) Device Removal.

Table 2. Materials Used to Perform Our Study.

Device Type	Model	Usage
Implant	DangerousThings xSIID	NFC Implant
Implant	DangerousThings xEM	RFID Implant
Implant	DangerousThings flexEM	RFID-emulation Implant
Implant	DangerousThings flexDF2 DESFire EV2 8kB	NFC Implant
Writer	DangerousThings Proxmark	RFID Sniffer/Writer
X-Ray	Triumph II SPECT/CT	Device Detection
Reader	DangerousThings KBR1	NFC Device Reading
Reader	FlipperZero	RFID Device Reading
Metal Detector	Ranseners HTY1	Device Detection
Metal Detector	Garrett Pro-Pointer II	Device Detection

3.2 Materials Used

We used a variety of augmentation implants from implant retailer *DangerousThings*, as outlined in Table 2. The augmentation implants utilized either NFC or RFID technologies. The xSIID and xEM devices take one of the most common forms for augmentation implants, encasing the technology in a bio-glass cylinder (*Red XSIID bundle* 2022) (See Fig. 3). The flexDF2 and flexEM (See Fig. 3) implants, on the other hand, are encased in a thin flexible sheet of body-safe plastic. Both forms of implants were used during our studies.

3.3 Implant Installation

To conduct an augmentation implant detection study, we began with device injection. As human testing was impractical for this study, we simulated a real scenario by implanting the devices into synthetic, silicone skin, as well as raw chicken meat bought from a store. We employed both regular and boneless raw chicken legs. We follow the standard procedure for product installation, injecting the implants into the different mediums. This installation process can be seen in Fig. 4, in which a needle is used to inject an implant underneath synthetic skin.

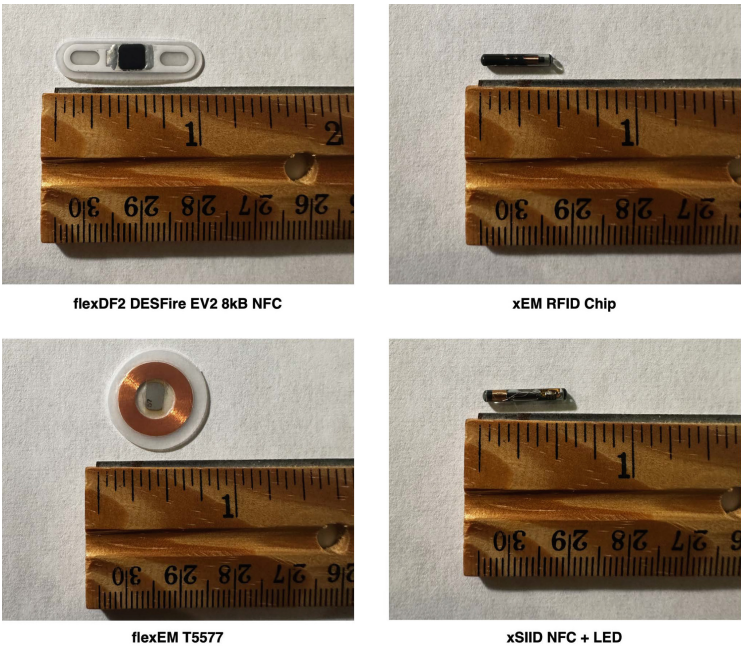

Fig. 3. Examples of Augmentation Implants.

3.4 Implant Detection

A major concern of ours is the detection of augmentation implants. Due to the nature of subdermal implants, the technology can be easily smuggled in a person's body, undetectable by visual analysis. If an adversary is utilizing one of these implants, it first needs to be discovered before it can be examined. Therefore, we introduce several methods in which subdermal implants can be detected. Many of these implants use NFC and/or RFID technologies, which means using an NFC or RFID scanner should allow an examiner to easily detect a device embedded in one's skin. This can be demonstrated in Fig. 4, in which an xSIID implant inserted below synthetic skin is responding to an NFC scanner.

Table 3. The Various Ways to Discover and Locate Implants in the Human Body.

	Pros	Cons	Use Case
Ultrasound	No Radiation Implant Easy to Identify	Needs Physical Contact Limited Scanning Area Scans Are Slow	Searching Single Individual High Accuracy Needed
X-Ray	Scans Are Fast Broad Scanning Area	Radiation Dosage Implant Harder to Identify	Searching Many People Medium Accuracy Needed
Terahertz Scanner	No Radiation Scans Are Fast	Implant Not Always Identifiable	Searching Many People Low Accuracy Needed
Metal Detector	No Radiation Scans Are Unobtrusive	Very Low Detection Rate	Searching Most People Lowest Accuracy Needed

Fig. 4. Injecting the xSSID Implant Into Synthetic Skin and Scanning the Implant From Within the Skin.

However, this method features many flaws. The first flaw is in the extremely limited range of NFC and RFID technologies, in which a scanner has to be within a few centimeters of a chip in order to receive a signal from an implant. The second flaw is that these scanners can only pick up on NFC or RFID signals if the implant is located close to the surface of the skin. Thus, if an attacker wanted to employ this type of implant to smuggle data, they could merely implant the device deeply enough as to not be able to read data without removal. To combat these concerns, we surveyed several technologies that can aid in implant discovery.

The first issue we tackled was finding alternative means of detecting subdermal implants. Matthews (2022) discussed how ultrasound technology could be used in scenarios in which an individual has been identified as a suspect of smuggling an implant. X-Ray technology could be used for searching a large group of people, in potentially more secure environments where accuracy is more important. Terahertz technology could also be applied in searching through large groups, though it may have more trouble detecting deeply implanted devices than the first two methods. Table 3 summarizes each of these technologies and the benefits and drawbacks to each.

3.5 Data Retrieval and Analysis

The next step in forensic analysis is data retrieval. We employed several augmentation implants to study the process of retrieving data from said devices. There are two primary ways to access the data from these devices. The first method is using a scanner such as the Proxmark (See Table 2). The Proxmark scanner supports reading a wide variety of wireless technology and can be used to read

data from many augmentation implants on the market today. Once the data is read, it can be either used for analysis or written to another chip in order to impersonate an individual. The same copying approach may be used in future digital forensics investigations to preserve a copy of the evidence.

The second method of acquiring data from augmentation implants is through their companion applications. Implants with specific features for health monitoring or payment can come with a companion smartphone application *(Walletmor* 2021, Dsruptive 2021). These smartphone applications can be used to read data from the implants, as well as write data to them. Other, more generic augmentation implants are meant to work with authentication systems. These systems read data from the augmentation implants to verify if a user is authorized for a specific action like unlocking a door. By analyzing the data read by these authentication systems, we can reveal data stored on the implants, as discussed further in Sect. 4.4.

3.6 Device Removal

During the digital forensics process, physical access to hardware is often critical as it allows for data to be acquired, authenticated and analyzed. However, this requirement can be challenging when attempting to pull data directly from implantable devices because physical access requires surgical removal.

Current augmentation implants can be analyzed by simply reading their data wirelessly. In the future, however, this is likely to change with the advancement of augmentation implant technology. Thus, in the future, a scenario in which one's augmentation implant will need to be removed is increasingly likely.

This brings into question many ethical and legal questions. We can examine existing laws and rulings to infer how augmentation implants will be treated in the future. When someone is defending themselves in court in the United States, they are given certain ethical rights. For example, the rights to medical privacy are granted unless a warrant is provided (Ramirez 2020). People also have protection from unreasonable search and seizure (Team 2022). These protections disallow general body searches, which would encompass searching for an augmentation implant. However, once a warrant is generated, these protections are no longer in effect.

At the same time, however, there are laws in place that allow for a full investigation to ensue unimpeded. In the future, the same rights could be applied towards subdermal augmentation implant removal. This could mean that not only removing the devices, but searching for them entirely, could be disallowed. In past rulings it has been decided that if deemed necessary a defendant could be mandated to take medication to properly represent themselves in court. Therefore, the same could potentially be applied to the removal of biohacking devices (Lieberman 2006).

4 Studies and Results

Our case study included discovering and performing a forensic analysis on augmentation implants available at the time of writing. Our work included two studies. The first was experimenting with three major ways of discovering augmentation implants. The second a proof-of-concept memory analysis of an NFC authentication system that employs the DangerousThings KBR1 alongside a simple authentication program to verify the identifier of scanned augmentation devices.

Fig. 5. An X-Ray of an xSIID Implant Within a Bone-in Chicken Thigh.

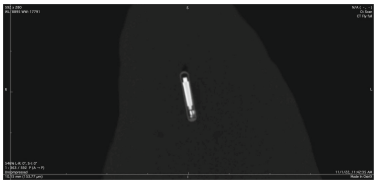

Fig. 6. An X-Ray of an xEM Implant Within a Boneless Chicken Thigh.

Fig. 7. Testing The flexEM T5577 Implant Being Embedded at Different Depths.

4.1 NFC/RFID Reader Analysis

Table 4. Results of Scanning for the flexEM T5577 Implant using the FlipperZero RFID Reader (left) and Scanning for the flexDF2 DESFire Implant using the DangerousThings KBR1 NFC Reader (right)

0.5 cm	Detected
1.0 cm	Detected
1.3 cm	Detected
1.4 cm	Detected
1.5 cm	Detected
1.7 cm	Undetected

0.3 cm	Detected
0.5 cm	Detected
0.7 cm	Detected
1.0 cm	Detected
1.3 cm	Undetected
1.4 cm	Undetected

To test hypothesis H_0, we embedded various implants into the synthetic silicone skin and attempted to detect them with the DangerousThings KBR1 RFID and FlipperZero NFC readers. All of these implants became undetectable by their respective readers once they were embedded below a certain depth beneath the skin. For this experiment we tested embedding two implants, the flexEM T5577 RFID implant and the flexDF2 DESFire NFC Implant. As seen in Table 4, the flexEM T5577 and flexDF2 DESFire were detectable (meaning no pressure of the metal detector on the skin was required) until embedded at 1.7 cm and 1.3 cm, respectively.

4.2 Metal Detector Analysis

Table 5. Results of Scanning for the flexEM T5577 Implant Using the Garrett Propointer II.

0.5 cm	Detected
1.0 cm	Detected
1.2 cm	Detected
1.4 cm	Detected
1.5 cm	Undetected
1.8 cm	Undetected

To test hypothesis H_1, we performed device discovery using a similar method to our scanner detection, but with the Garrett Pro-Pointer II and Ranseners

HTY1 handheld metal detectors, as shown in Fig. 7. Discovery via metal detectors proved difficult. The Ranseners HTY1 failed to detect all of the implants, even before they were implanted into a medium. The Garrett Pro-Pointer II failed to detect all but the flexEM T5577 implant. The flexEM T5577 augmentation implant was detectable when implanted under the synthetic silicone skin up to about 1.4 cm below the surface, as shown in Table 5.

4.3 X-Ray Analysis

To test hypothesis H_2, we employed a three dimensional X-Ray computed tomography imaging system as one method of device detection. Analyzing the images produced by this system clearly revealed that an implant existed within the meat (See Sect. 3.3), regardless of whether or not bones were present. This is shown in Figs. 5 and 6 and a trained analyst may be able to distinguish between the different types of implants based on the X-Ray. Therefore, it can be presumed that X-Ray technology is feasible to reveal augmentation implants when needed.

4.4 Forensic Case Study

To date, one of the most common applications for augmentation implants is controlling door access. In such a system, an NFC or RFID reader is present. This reader reads data from an implant and verifies whether or not the implant's unique ID is present within an allow-list stored on a server that the scanner communicates with. If the ID is determined to be valid, the user will be successfully authenticated; otherwise, the user will be rejected by the system.

Additionally, certain high-security access points control access through smart cards with NFC and EMV technology. Certain implant retailers, such as DangerousThings, offer to convert EMV cards into implants. Due to the inability to clone EMV chips, these retailers must outfit the original chip to create an implant (Madhoun et al.(2018), *Making payments with an implant* (2017)). This inability to clone these chips is significant because it means that an EMV implant is guaranteed to be the original implant, and not a clone, if successfully verified. Because authentication systems verify the unique augmentation implant ID, this system has the ability to reveal at what time an individual was attempting to authenticate. A forensic analysis of this data may be vital for an investigation, which is what we study below.

To test hypothesis H_3, we constructed an implant authentication system simulating standard door access control. An overview of this system is shown in Fig. 8 with the high-level code in Listing 1.1. For the implementation, we utilized the flexDF2 implant. This system also used the KBR1 NFC reader to read the ID from the implant. By creating a Python program, we built an access controller that reads the device ID from the implant and uses this to authenticate a user. To proceed with a forensics study of this scenario, we ran the program in a VMware VM, and connected the KBR1 NFC reader to the VM. We then presented the implant to the reader, asking the program to authenticate the device. An example of this program running is shown in Fig. 9. After the program

had successfully authenticated the device, we analyzed the memory dump of the machine. In Fig. 10, the device ID for the flexDF2 implant can be found in the memory of the machine. Therefore, if one has an implant, especially one that is guaranteed to be an original, such as an implant with EMV technology, it can be shown at what time a specific person was present at a reader. Because of the difficulty in removing and implanting these devices, it is highly unlikely that the physical implant has been stolen or traded. This shows the feasibility of being able to acquire forensically relevant data from these systems and augmentation implants in real-world scenarios.

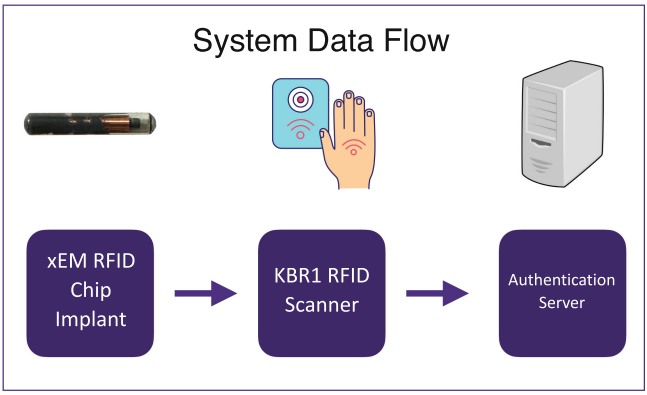

Fig. 8. An Overview of Our Implant Verification System.

```
[redacted]@research-vm:~$ python3 auth.py
Ready to scan device.
04561F1ABE5B80
Access granted to key 04561F1ABE5B80 at 18:46:59 04/19/23
Ready to scan device.
```

Fig. 9. An Example of a Program Used to Authenticate NFC Chips Being Run.

5 Discussion

By devising our augmentation implant forensics process, we were able to successfully apply the digital forensics process to the emerging field of augmentation implants. This process first involves determining several methods of device discovery. We then created a realistic scenario in which we could approach device discovery through x-rays and metal detectors. Utilizing x-ray technology successfully revealed that an implant existed, illustrating the feasibility of a method that could be used to discover a device. Utilizing metal detectors largely failed and most likely could only detect larger augmentation implants embedded closer to the surface of the skin.

```
p4g...  . g...  .-.. ..|.4g...    g...
                                          .hU...  poe...  p.a...
  j...  pUb...  ...       ..      ...     p..
Access granted to key 04561F1ABE5B80 at 18:46:59 04/19/23 .#> 43
..HM.FA- .    K..R2Q G. (.. =D?.  .*.% .. J&  $. .. . 01<../ C..
8 .; .!PE).  '7I9.N .T. , ..+ ....O.... ...Y .e 0.j...  ..f...
```

Fig. 10. The Memory Dump From a Virtual Machine Running the NFC Authentication Program. The ID of the Scanned Implant Is Highlighted.

Listing 1.1 . Authentication System Code

```
1  waitForInput()
2  // Device is presented
3
4  allowDevice = scanDevice()
5
6  if allowDevice equals TRUE
7      authenticate()
8  else
9      restrict()
```

After detecting an implant, one important aspect is device removal. By reviewing past legal and ethical decisions of similar cases, we were able to estimate how the process of augmentation implant removal could be treated. We found that while suspects are often granted the right to medical privacy, this can be navigated around if deemed necessary to conduct a criminal investigation. For example, blood can be tested without requiring a warrant (*Mitchell v. Wisconsin* 2019). Of course, surgical removal is much more invasive than simply drawing blood. We can examine one case in which surgical removal occurred; in a case in New Orleans, Louisiana, a suspect had been shot by a store clerk in self-defense. The injury was non life-threatening, leading the bullet to stay lodged within the suspect. A judge had decided that the bullet would provide meaningful evidence, issuing a warrant mandate surgical removal of the bullet (*Hughes v. United States* 1981). Thus, we can assume that there is a good possibility that one may need to have an augmentation implant surgically removed if it is deemed that the implant can provide meaningful evidence and is not dangerous to remove.

We then evaluated the various means of data retrieval. The amount of data available to be retrieved is currently limited by the technology available with today's augmentation implants. In the future, we expect this technology to become more advanced, meaning that a physical analysis will become much more important. Therefore, rather than attempting to physically gather data from a device, we focused instead on gathering data from a typical implant verification system. In our forensic analysis we were able to reconstruct the ID of an implant, from a computer's memory, when a user presents their implant to a reader for

authentication. This would also reveal the date and time a user attempted to authenticate. This information is forensically relevant, and is just one example of the data that can be pulled from state of the art augmentation implants.

6 Related Work

Previous research on these subdermal implants by (Kiourti 2018) primarily focused on studying the feasibility of incorporating NFC and RFID in internal medical devices. Previous research has also covered other types of medical implants, such as the VeriChip, which solely exists to store a serial number linking doctors to peoples' medical data (Tanne 2004). Another device, made by Dsruptive, can store patient information directly on the device (Dsruptive 2021). Research on these devices has explored the privacy and human rights violations that could come along with these implants (Foster & Jaeger 2007), (Sharpe 2008). As biohacking technology improves, the potential for abuse of said technology increases. In this paper, however, we study how this technology can be leveraged by an attacker, the process of discovering biohacking devices and acquiring data for a forensics investigation, analysis of the recovered data, and how these devices may change in the future.

6.1 Forensics of Related Devices

Past work has achieved forensic analysis on a wide variety of mobile devices and applications (Al Mutawa et al. 2012, Bader & Baggili 2010, Hassenfeldt et al. 2019, Husain et al. 2011). Many smart devices can be exploited for forensic analysis through their companion application (Moffett 2019, Awasthi et al. 2018). Certain implants, such as the Walletmor, utilize a companion application of their own (*Walletmor* 2021). Like other devices, forensic analysis can be applied to these companion applications to reveal important data.

Forensic analysis has also been applied to various medical devices, including medical implants (Schmitt 2022). (Grispos et al. 2019) demonstrates the ability to apply forensic analysis to implantable medical devices that communicate with smartphones. While this differs from our study of augmentation implants, the idea of applying forensics to wireless implants is similar.

The forensics process has also been applied to more uncommon electronics, such as mobile phone SIM cards and wireless carkeys (Savoldi & Gubian 2010, Bates 2019). Forensic Analysis has also been applied to the NFC recievers on mobile phones (Lakshmanan & Nagoor Meeran 2017) and wearable devices (Baggili et al. 2015). Forensic analysis has even been applied to Java Card applets a technology that certain implants utilize (Lanet et al. 2014, *VivoKey Apex* 2022).

However, no prior work has focused on biohacking. In our work, we performed forensic analysis on subdermal augmentation implants that people have biohacked into themselves. We evaluated how this analysis differs from that of other devices, and demonstrate how this analysis would take place in a realistic scenario.

7 Future Work

The augmentation implant field is rapidly changing as technology improves. Therefore, the forensic process applied to these implants will need to continuously improve to stay applicable. Future work should evaluate the changes within augmentation implants over time and the security impact that these changes make. For example, as these devices gain more computing power, physical analysis is expected to become more important. If these implants gain sophisticated computing power, wireless analysis of a device could only reveal some of the data required to conduct a thorough forensic analysis. Future work should also study other means of augmentation implant discovery. Our work primarily focused on device discovery through wireless scanners, X-Rays and metal detectors.

Lastly, since our work was limited to the analysis of memory, future work should explore other forensic sources such as companion devices, network, storage and cloud artifacts that may be applicable to augmentation implants.

8 Conclusion

As an emerging field, augmentation implants have the potential to make a major impact on the cybersecurity field, and may create new challenges for digital forensics. A major aspect of these devices is the possibility to be used to smuggle data. This is due to the hidden nature of the devices. We demonstrate the methodology for not only discovering these devices but acquiring data from both the devices themselves and systems that integrate them. In doing so, we are able to streamline a forensics process that will allow for the forensic analysis of augmentation devices.

References

Al Mutawa, N., Baggili, I., Marrington, A.: Forensic analysis of social networking applications on mobile devices. Digit. Investig. **9**, S24–S33 (2012)

Awasthi, A., Read, H.O., Xynos, K., Sutherland, I.: Welcome Pwn: almond smart home hub forensics. Digit. Investig. **26**, S38–S46 (2018)

Bader, M. Baggili, I.: iphone 3GS forensics: logical analysis using apple iTunes backup utility (2010)

Baggili, I., Oduro, J., Anthony, K., Breitinger, F. McGee, G.: Watch what you wear: Preliminary forensic analysis of smart watches. In: 2015 10th International Conference on Availability, Reliability and Security, pp. 303–311 (2015)

Bates, E.A.: Digital vehicle forensics (2019). https://abforensics.com/wp-content/uploads/2019/02/INTERPOL-4N6-PULSE-IssueIV-BATES.pdf

Dsruptive: Using implants for storing COVID vaccine certificates (2021). https://dsruptive.com/using-implants-for-storing-covid-vaccine-certificates/

Dąbrowska, A., et al.: Materials used to simulate physical properties of human skin. Skin Res. Technol. **22**(1), 3–14 (2016)

Foster, K.R., Jaeger, J.: RFID inside. IEEE Spectr. **44**(3), 24–29 (2007)

Grispos, G., Glisson, W.B., Cooper, P.: A bleeding digital heart: identifying residual data generation from smartphone applications interacting with medical devices. arXiv preprint arXiv:1901.03724 (2019)

Halamka, J., Juels, A., Stubblefield, A., Westhues, J.: The security implications of VeriChip cloning. J. Am. Med. Inform. Assoc. **13**(6), 601–607 (2006)

Hassenfeldt, C., Baig, S., Baggili, I., Zhang, X.: Map my murder: a digital forensic study of mobile health and fitness applications. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, pp. 1–12 (2019)

Hughes v. United States (1981)

Husain, M.I., Baggili, I., Sridhar, R.: A simple cost-effective framework for iPhone forensic analysis. In: Baggili, I. (ed.) ICDF2C 2010. LNICST, vol. 53, pp. 27–37. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19513-6_3

Kiourti, A.: RFID antennas for body-area applications: from wearables to implants. IEEE Antennas Propag. Mag. **60**(5), 14–25 (2018)

Lakshmanan, D., Nagoor Meeran, A.R.: NFC logging mechanism—forensic analysis of NFC artefacts on android devices. In: Dash, S.S., Vijayakumar, K., Panigrahi, B.K., Das, S. (eds.) Artificial Intelligence and Evolutionary Computations in Engineering Systems. AISC, vol. 517, pp. 93–101. Springer, Singapore (2017). https://doi.org/10.1007/978-981-10-3174-8_9

Lanet, J.-L., et al.: Memory forensics of a Java card dump. In: Joye, M., Moradi, A. (eds.) CARDIS 2014. LNCS, vol. 8968, pp. 3–17. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-16763-3_1

Lieberman, E.C.: Forced medication and the need to protect the rights of the mentally ill criminal defendant. Cardozo Pub. L. Pol'y Ethics J. **5**, 479 (2006)

Madhoun, N.E., Bertin, E., Pujolle, G.: An overview of the emv protocol and its security vulnerabilities. In: 2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ), pp. 1–5 (2018)

Making payments with an implant (2017). https://forum.dangerousthings.com/t/making-payments-with-an-implant/643

Marqueta: The European payments landscape in 2030 (2021). https://resources.marqeta.com/c/report-european-payments-landscape?x=hj28Ub&submissionGuid=95961be5-2b0b-4858-9459-d312087827a0

Matthews, D.: I got a computer chip implanted into my hand. Here's how it went.. (2015). https://www.vox.com/2015/9/11/9307991/biohacking-grinders-rfid-implant

Matthews, K.L.: Personal communication. Email correspondence (2022)

Michael, K.: RFID/NFC implants for bitcoin transactions. IEEE Consum. Electron. Mag. **5**(3), 103–106 (2016)

Mitchell v. Wisconsin (2019)

Moffett, O.: The digital forensics of internet-of-things devices, PhD thesis, Utica College (2019)

Patel, J., Das, M.L., Nandi, S.: On the security of remote key less entry for vehicles. In: 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), IEEE, pp. 1–6 (2018)

Ramirez, A. (2020). https://www.aclu.org/news/privacy-technology/police-need-a-warrant-to-collect-dna-we-inevitably-leave-behind

Red XSIID bundle (2022). https://dangerousthings.com/product/red-xsiid-bundle/

Savoldi, A., Gubian, P.: Embedded forensics: An ongoing research about sim/usim cards. In: Handbook of Research on Computational Forensics, Digital Crime, and Investigation: Methods and Solutions, IGI Global, pp. 396–423 (2010)

Schmitt, V.: Medical device forensics. IEEE Secur. Priv. **20**(1), 96–100 (2022)
Sharpe, V.A.: Ethics and indemnification regarding the verichip. Am. J. Bioeth. **8**(8), 49–50 (2008)
Shipper, D.: Beyond cards and mobile phones: Payment form factors of the future (2021). https://aite-novarica.com/report/beyond-cards-and-mobile-phones-payment-form-factors-future
Tanne, J.H.: FDA approves implantable chip to access medical records. BMJ **329**(7474), 1064 (2004)
Team, W.D.: Unreasonable search and seizure (2022). http://law.cornell.edu/wex/unreasonable_search_and_seizure
TEDx: Biohacking - the forefront of a new kind of human evolution: amal graafstra at tedxsfu (2013). https://www.youtube.com/watch?v=7DxVWhFLI6E
VivoKey Apex (2022). https://www.vivokey.com/apex
Walletmor (2021). https://us.walletmor.com/pages/how-it-works-us