# The Extent of Biohacking and Its Security Implications

Ariel Serruya

December 13, 2017

## Abstract

While the human conceptualization of cyborgs and human enhancements has existed for decades, it is only as of the last few years that people have begun to normalize the idea and incorporate it into their quotidian lives. With the rise of this “do-it-yourself biology”, it is important to understand the modern innovations rising from biohacking and to analyze the security implications behind widespread cybernetics. This paper aims at informing and educating the lay person; it hopes to provide informative details about the extent of biohacking and what can be done to remedy certain faults and flaws in this exciting yet youthful sector of human enhancement.

### *Introduction*

Biohacking is often viewed as the first widespread technological step towards human augmentation and improvement. That being said, actually defining biohacking is difficult. Due to being a relatively new field, biohacking encompasses many different things, everything from the obvious RFID implants covered by the media to bioweapons and their international implications. The DEF CON Biohacking Village is a biotechnology conference that admits talks on "breakthrough DIY, grinder, transhumanist, medical technology, and information security along with its related communities in the open source ecosystem" [1]. This spectrum of do-it-yourself biology comes with exciting innovation as well as concerns, some justified and some based on misinformation. Biohacking is on the rise, with seemingly more and more *grinders,* the practitioners of the art in relation to cybernetics. In the past few months, biohacking has been seen, for the first time, in corporate settings. As a result of this unprecedented growth, it is important to better understand the field and the security implications it may entail.

### *To the Community*

I chose this topic because I think it is imperative that people understand both what biohacking entails as well as the dangers it poses. Biohacking has been used, for the first time in history, in a corporate environment, in which dozens of people received implants at the same time. Three Square Market, a company in Wisconsin, became the first company on American soil to offer its employees RFID implants. A few months earlier, a Swedish company by the name of Epicenter, had been the first company worldwide to offer its employees RFID implants [2]. With this rise in biohacking, media coverage has reached an all-time high. Unfortunately, a lot of this media coverage is singularly focused; in other words, these media outlets cover a very specific part of biohacking that often leads to misconceptions about the field. One of the top results on Google under biohacking is an article from 2012, published by The Verge. It is titled "Cyborg America: inside the strange new world of basement body hackers." The article introduces Tim Cannon, a relatively controversial figure on the forefront of biohacking [3]. This same mentality is what people like Jeffrey Tibbetts, one of the hosts of grindfest (the name seems self explanatory), are trying to dispel. Having done over 300 implants, Jeff is very familiar with the conditions of these procedures. At his talk , ironically titled "Biohackers die", at DEF CON 25 at the Biohacking Village, Jeff tells his audience that implanted devices have not led to any deaths thus far. He states that while people see the industry as a "basement hobby," many of the people involved are incredibly knowledgeable in their field, whether it be in lab safety, sanitation, or surgical procedures [4]. Much like Tibbetts, I think it is important to inform people and dispel misconceptions that they may have. Furthermore, it is essential that we understand the security concerns that may arise as a result of biohacking, which, as we will see, are oftentimes ignored.

### ***What to Know***

Nothing is more indicative of how extensive biohacking is than looking at all the sectors in which biohacking is applicable. I believe that understanding its different applications is essential to understanding biohacking as whole, both its good and its bad. We will attempt to delve, briefly if possible, into each different use. In doing so, understanding the security concerns behind biohacking will become much more intuitive.

While biohacking for personal convenience is useful, it is in this area that one finds the hobbyists that define, for better or worse, the biohacking community. It is in this sector that one sees RFID (Radio Frequency Identification) and NFC (Near Field Communications) implants. There are many companies that specialize in this, including but not limited to: Dangerous Things, Cyberize Me, Digiwell, and Grindhouse Wetware. Founder and employee of the Dangerous Mind podcast and university, C00p3r and Cur5or , explain the different uses of these implants well in their talk "Implant Show and Tell," at DEF CON 25. Main purposes include phone entry, keychain access, wallet control, travel cards, door/computer access, and so on [5].

Biohacking is also often associated with human augmentation on a sensory and perceptive level. Tess Schrodinger, a security engineer, was diagnosed with breast cancer. In her battle with cancer and chemotherapy, she learned of a phenomenon referred to as "chemo brain." Chemo brain encompasses the side effects of undergoing chemotherapy, including forgetfulness, memory lapses, and difficulty with simple tasks. In researching a remedy for chemo brain, Tess learned of ways in which biohacking can help. She learned of something called Serial Interception Sequence Learning. SISL allows one to play a game, much like Guitar Hero, in which one memorizes a 30 character string, oftentimes padded with 18 random characters (much like a key on an encrypted password). The person can not recall the password but can use it as necessary. Similarly, a group at Berkeley used an EEG machine to create passwords based on mathematical representations of electrical signals. By having someone think of a specific object or memory, and recording the associated electrical signals, one has a unique password impossible to duplicate [6].

Using the brain as the key component in human augmentation is not limited to Tess and her research. Trevor Goodman, at the same DEF CON, gave a talk appropriately titled "Hack your senses: Sensory Augmentation." He states that senses are "the mediatory between the mind and the outside world." By accessing the mind, one can adjust, change, or augment one's senses. This is often done, he tells us, as a result of neuroplasticity. The brain's ability to reroute connections after damage to certain areas allows people to walk again after a stroke, or to regain their sense of balance after an accident that may have damaged that part of their brain. Trevor quotes the previously mentioned Tim Cannon and states " the brain is a pattern recognition machine." The brain supersedes senses, which is why, Trevor explains, one falls for optical and auditory illusions. By using this knowledge, one can change the limitations of their senses. Examples of such include adding a sense of touch to a prosthetic arm in a woman at Case Western University or creating an antenna that allows a colorblind person to hear colors. By expanding our sensory bubble, we are, in effect, augmented. It is known that animals have different senses than humans, such as echolocation, infrared vision, and a magnetic north sense. By using animals as an example, humans have been able to duplicate such senses. Deaf people have been able to use a NEOsensory vest to allow for tactile feedback of soundwaves and blind people have been taught to echolocate [7]. Human augmentation, while sounding like an attempt at superhero powers, are as much selfless and helpful as they are innovative.

Lastly, in transitioning to discussing the security concerns behind biohacking, we analyze biohacking in the health and defense sectors. At DEF CON 25, Meow Ludo Meow Meow and Louis Auguste Jr discuss the uses of biohacking in bioweapons and in smart microscopes. While one is clearly more practical than the other, it is important to understand that both are equally feasible. Meow Ludo speaks to the simplicity in obtaining the materials necessary to create a bioweapon. Bioweapons include bacteria, viruses, and toxic agents, oftentimes in a gaseous form to provide easier and more widespread contamination [8]. These far reaching and self-regulating weapons can prove extremely deadly. Meow Ludo's talk, while informative, was clearly meant more as a precaution than a set of instructions. Louis Auguste Jr.'s talk however, was the opposite – it was extremely informative and interesting but lacking in all precautions whatsoever. Louis addresses what he calls “healthcare deserts,” areas in which suitable healthcare do not exist. In these areas, while there may be labs and microscopes, there are no professionals able to diagnose test results [8]. Louis and his team of engineers at NYU have developed an Internet of Things thing, essentially a smart microscope. He hopes to address the *travel* burden often found in rural or poor areas. Due to the distance between doctors, people are often diagnosed too late, or not diagnosed at all. In an attempt to combat the amount of lives lost due to this phenomenon, Louis’ team has created a camera based microscope that will upload your slides onto the cloud in which a medical practitioner in another city can easily, quickly, and cheaply diagnose a person. In his 20 minute long talk, however, Louis did not mention security once. In a talk about health records at DEF CON, Louis left out of one of the most important aspects of his product.

### *Security Implications*

Louis’s  omission is indicative of the mindset that leads to some of the worst and most intrusive hacks. The matter of the fact is that security is extremely overlooked and ignored, both by engineers and by policy makers. More so, biohacking is a relatively new field and the slow bureaucratic infrastructure in the United States is not conducive of dynamic and fast-paced legislation. Louis is not the only one, however, to be a victim of these shortcomings; a lack of policy or regulation in the biohacking community is illustrated perfectly by many of the aforementioned speakers. Meow Ludo Meow Meow made this gap in policy very clear. As a figure on the forefront of the biohacking community in Australia, he has found that policies have not yet been implemented and that biohackers find themselves helping officials in implementing these regulations. Meow Meow cites the ability of one group of researches to *legally* create a synthesized horsepox that met all national regulations [7]. He believes that, above all, there is a desperate need for international policies, especially considering the ease in which one can create a bioweapon. If health records and bioweapons don't seem relevant enough, C00p3r and Cur5or, previously mentioned, spoke about the lack of security in some of the implants people are getting, implants that use the same technology found in credit cards, fobs, and passports. They explain that bitcoin wallets and door/computer access keys are not very secure and provide no cryptography [5]. Tess, the security engineer that survived breast cancer, is clearly a proponent of EEGs being used to encrypt passwords and help forgetful people. That being said, she also explained the dangers of using such technology. Researchers found that using headsets similar to EEG machines could be used to steal private information. By using a malicious app PEEP to capture signals from a gaming headset, researchers were able to lessen the chances of figuring out a 4 digit password from a 1 in 10,000 to a 1 in 20 chance [6]. Jeffrey Tibbetts, the first character we encountered, stated that the 300 implants he gave were legal, followed by an "I think" [4]. The fact that he is uncertain, despite having given 300 implants, is equally as indicative of missing regulations.

While the future of biohacking may be as dire as it seems, it is important to have faith in overcoming these obstacles, and two people, once again, at DEF CON 25, stick out in trying to remedy the faults found in the biohacking community. Paul Ashley, the Chief Technology Officer of Anonynme, proposed the use of fake identities to the biohacking community as a remedy for the permanence of online communications [9]. John Nye attributes the flaws in security to our inability to address the root of the problem. He says that "we are all biased, it is an integrated part of our core selves," and rather than try to change these biases, it is important that we understand them. He elaborates that the most important node in any network is actually the human. “We are bad at decision making and by extension are bad at security.” We are subjective beings through and through, and “by default, the world does revolve around you.” Our best bet, therefore, is to change our assumptions. Never trust user input, people are not as rational as they seem. More so, educate in a relevant and powerful way, as opposed to simply throwing more technology at the users [10].

### *Conclusion*

It has become evident then, that biohacking is more than just an RFID chip to open your front door. Biohacking encompasses the emotional innovation we see in aiding disabled people. It encompasses bioweapons and progress in the health industry. It encompasses an entirely new way to store passwords, and a magnet in your fingertip. And while biohacking is both interesting and inspiring, it illustrates flaws in both the policies surrounding the tech-world and security concerns in the code itself. It is evident that with biohacking comes a new area of unexplored ethical and legal issues that demand being addressed. Do-it-yourself biology has reached a point of prevalence in a society ill-prepared for such innovation, and whether we adopt new identities or better educate people, something must be done to regulate this incredible technology capable of so much good.

# Bibliography

[1] "DEF CON Bio Hacking Village." DEF CON Bio Hacking Village, www.defconbiohackingvillage.org/.

[2] Astor, Maggie. "Microchip Implants for Employees? One Company Says Yes." *The New York Times*, The New York Times, 25 July 2017, https://www.nytimes.com/2017/07/25/technology/microchips-wisconsin-company-employees.html

[3] Popper, Ben. "Cyborg America: inside the Strange New World of Basement Body Hackers." *The Verge*, 8 Aug. 2012, https://www.theverge.com/2012/8/8/3177438/cyborg-america-biohackers-grinders-body-hackers.

[4] DEFCONConference. "DEF CON 25 BioHacking Village – Jeffrey Tibbetts – Biohackers Die." Youtube, 30 Oct. 2017, https://www.youtube.com/watch?v=nn0kglB46BU

[5] DEFCONConference. "DEF CON 25 BioHacking Village – C00p3r, Cur50r – Implantable Technology Show and Tell." Youtube, 30 Oct. 2017, https://www.youtube.com/watch?v=VyJftVIjDNo

[6] DEFCONConference. "DEF CON 25 BioHacking Village – Tess Schrodinger – Total Recall: Implicit Learning As Crypto." Youtube, 30 Oct. 2017, https://www.youtube.com/watch?v=lNs2TXUb33g

[7] DEFCONConference. "DEF CON 25 BioHacking Village – Trevor Goodman – Hack Your Senses: Sensory Augmentation." Youtube, 30 Oct. 2017, https://www.youtube.com/watch?v=mv-ensBMPIY

[8] DEFCONConference. "DEF CON 25 BioHacking Village – Louis Auguste Jr – Microscopes Are Stupid." Youtube, 30 Oct. 2017, https://www.youtube.com/watch?v=6VCj8MitA6M

[9] DEFCONConference. "DEF CON 25 BioHacking Village – Paul Ashley – The Future Is Fake Identities." Youtube, 30 Oct. 2017, https://www.youtube.com/watch?v=1Sft5aJ2Olo

[10] DEFCONConference. "DEF CON 25 SE Village – John Nye – The Human Factor Why Are We So Bad at Security." Youtube, 30 Oct. 2017, https://www.youtube.com/watch?v=MgXhjUzi_I0