Securing the Airspace with DroneShield

Interview with John Franklin, Chief Scientist at DroneShield

Pilot Earphones
Translate Foreign Languages in Real-Time

Meet Naked, the World’s First 3D Fitness Tracker
EEWeb FEATURE
Pilot Earphones Translate Foreign Languages in Real-Time

Secure, Effective, Economical: The 8th Cross-Platform Programming Language

10

INDUSTRY INTERVIEW
Meet Naked, the World’s First 3D Fitness Tracker

Interview with John Franklin, Chief Scientist at DroneShield

16
This New Gadget Fits in your Ear and Translates Foreign Languages in Real-Time

Pilot earphones let two people who speak different languages understand one another.

It’s often frustrating trying to understand someone who doesn’t speak the same language as you. But thanks to a new piece of technology, that miscommunication will soon be a thing of the past.

Developed by Waverly Labs, a New York-based company, Pilot earphones are the first smart earpiece capable of translating between two languages. At launch, the device will translate between English, French, Spanish, and Italian.

Pilot works by being connected to two different people, both speaking two different languages, and translates what they are saying into the desired user’s ear. The development of Pilot occurred after one of the technicians at the company met a French girl whom he wanted to communicate with. While the first generation of the wearable works only between two people, Waverly Labs hopes to make one that will translate everything happening around users in a foreign country.

The company launched a crowdfunding campaign on Indiegogo, where those who want to be the first to try the new technology can currently pre-order Pilot for a donation of $199. Only 8500 devices are available at this discounted price. The device is expected to be available at retail for between $250 and $300 by May 2017.

Pilot also comes with an additional earpiece for wireless music streaming and an accompanying app that toggles between languages. The device doesn’t need to be connected to the Internet either; it works both offline and overseas.

The earphones will be available for pre-order in three different colors (black, white, or red) beginning May 25, 2016, on the Waverly Labs website for $199.
Over the past several years, the team at software start-up Aaron High-Tech developed and released a secure, cross-platform programming language called “8th.” It allows programmers to write program code just once, using that same code to produce applications that run on Windows, OS X, Linux, Android, iOS, and Raspberry Pi.
The idea behind 8th is to allow programmers to easily develop mobile, desktop, server, or embedded applications, and is particularly ideal for applications in which the user interface is non-standard. For each platform, there is an 8th “engine,” which provides the language interface to the specific platform. The programmer’s application code goes through a “build” procedure, which compresses, encrypts, and cryptographically signs the code into a binary package. That same package can be run on any of 8th’s supported platforms. At runtime, the 8th engine examines the binary package and verifies that it has not been tampered with. Then, it unpacks it and compiles the code to the native machine format and runs the application.

According to founder Ron Aaron, the impetus for the new programming language was his desire to write a secure personal-data storage application, such as an encrypted notebook, which would be the same on the various devices he uses daily, along with access to all his information, while keeping others out. “I had worked on other cross-platform projects and knew about various options, which would be the same on the various devices he uses daily, along with access to all his information, while keeping others out. “I had worked on other cross-platform projects and knew about various options, but nothing I could find really answered all the requirements I had for that project,” Aaron said. “So I started writing 8th to satisfy my own needs.”

When 8th was publicly released in January 2015, the original target audience were small-to-medium-sized development groups needing to support an application on more than one platform simultaneously. “We thought that the obvious advantages of having only one set of sources to maintain, and not requiring in-depth knowledge of each platform, would be a big win in terms of time-to-market and maintenance costs, and that therefore it would be a slam-dunk,” Aaron said. “We have since realized that mobile developers, in particular, are very much married to the specific tools they use, so we are refocusing on the embedded market.”

While Aaron and his team still believe the original target user is an appropriate one, they’re currently working to expand 8th into the embedded arena, meaning additional users could include embedded developers, particularly those interested in writing a mobile or desktop application to control or communicate with their embedded device. But, overall, 8th is appropriate for any developer concerned with the security of the product being developed.

Perhaps the most significant unique feature of 8th is the encryption of the runtime package. Because it utilizes AES-256-GCM encryption as well as RSA signature verification, it’s as tamper-proof as a software-only package can get, according to Aaron. The encryption also makes it difficult for a hacker to discover the developer’s trade secrets or private data.

As for future goals of their cross-platform programming language, Aaron and his team believe that if they can convince enough embedded developers to adopt 8th, the impact will be huge in terms of the ROI they see, as well as the stability and security of their applications. “In truth, our most enthusiastic users seem to be the ones with hardware experience, so embedded seems a natural fit,” Aaron said. For more information regarding 8th, click here.

The programmer’s application code goes through a “build” procedure, which compresses, encrypts, and cryptographically signs the code into a binary package.
Meet **Naked**, the World’s First 3D Fitness Tracker

Silicon Valley tech startup Naked Labs has created the world’s first 3D fitness tracker for consumers. Surprisingly, it isn’t a wearable, but a full-length mirror that takes a scan of your body to record exact measurements, fat percentages, and weight. Once collected, the data is sent to a smartphone or tablet app where you can see your progress through heat maps and a time-lapse model.
With a focus on health and wellness, the mission of this magic mirror is to flip the body measurement game upside down. Equipped with Intel RealSense Depth Sensors, it scans your body while the Bluetooth-connected scales double as a turntable. The result is a 20-second 3D scan of your body that lets you track changes over time, and the scanner’s heat map can accurately show where you’re growing muscle or gaining fat at that exact moment.

“We are excited to work with the Naked Labs team on their fitness body scanner for the home, utilizing our industry leading Intel processors and RealSense Technology,” said Josh Walden, senior vice president and general manager of the New Technology Group, Intel Corporation. “This product and application will offer greater insight and awareness to users, helping them check progress on a continuous basis as they work toward healthy body transformation.”

To pinpoint any changes, you must not be wearing any clothing, hence the product’s name, but you can also be dressed in a skin-tight outfit for an accurate scan. Even though a regular bathroom scale can tell you how much you weigh, it won’t always reflect the changes your body goes through day-by-day. And though it’s not the focus of the platform, the Naked 3D Fitness Tracker does come with a scale that works on carpet and hardwood floors.

When first stepping onto the high-tech scale, a circle on the mirror will light up to let you know that scanning has begun. There are no buttons and no readout screen included, but instead a laser pointer in the mirror will let you know where to place the scales for easy use.

“We believe the only fitness metric worth tracking is progress,” said chief executive officer and co-founder of Naked Labs, Farhad Farahbakhshian. “The Naked 3D Fitness Tracker is transformative in its ability to motivate people to achieve their health and fitness goals through visualizations of their progress on their 3D body model.”

Owning another piece of tech might seem cumbersome, but with its modern design, Naked’s fitness tracker can fit nicely into homes. The scale also docks at the base of the mirror to recharge, so that it can spin you for the scan, and the two connect to each other via Bluetooth while sending information to your phone or tablet through Wi-Fi.

But what if there’s more than one health-conscious person living in your household? Fortunately, more than one person can use the mirror, since the technology intuitively knows whose device to send the scans to based on body type.

The mirror’s companion app is available for free, but as expected, the sensor-packed mirror, along with the scale, won’t come cheap, with a current price tag of $699. Stay motivated, because the fitness tracker is scheduled to ship in March 2017.

**PCBWeb Designer** is a free CAD desktop application for designing and manufacturing electronics hardware. The tool supports schematic capture and board layout, including integrated “click-to-order” manufacturing.

[www.PCBWeb.com](http://www.PCBWeb.com)
In the last few years, drones have become increasingly available and affordable for the masses. As the availability grows, so too does the need for security against misused consumer drones. With solutions for prisons, airports, government, commercial venues, critical infrastructure and executive protection, DroneShield is leading the march against unwanted drone invasions with their acoustic-based technology. EEWeb met with John Franklin, Chief Scientist at DroneShield to discuss the cutting-edge technology used in DroneShield’s detection products.

Interview with John Franklin, Chief Scientist at DroneShield
What made you and co-founder Brian Hearing start this company? How did you decide to focus on drone security?

We were of a similar sentiment. We had worked in large companies within the industry, but both possessed an entrepreneurial streak. We bounced ideas off of one another, and this idea of drone security seemed to have some legs. There were a couple of things we saw coming together during those years. We had the military’s use of drones overseas, which was heavy in the public eye, and we had these multi-rotor drones, which are an entirely different technology. The multi-rotor drones were coming onto the scene at an affordable price. Consumers could purchase a drone with a camera that was easily controlled with an iPhone at a local electronics store and use them without many laws or regulations regarding privacy and security.

During this time of fast-paced market growth, a lot of public wariness surrounded the domestic applications of drones. While people didn’t need to worry about their government using drones to surveil them, they did need to worry about neighbors, acquaintances, and strangers flying drones outside their window.

We decided to go after the idea of drone security and identified acoustics as one of the most effective and low-cost means to do it. Since the consumer drone market has exploded, the market for drone detection and countermeasures has also exploded. And it’s not only people worried about their own privacy anymore. It’s prisons worried about contraband deliveries to prisoners. It’s government facilities concerned about surveillance and payload delivery. It’s airports concerned with safe flight operations. The list of concerns goes on and on.

I think the root of these concerns lies in the fact that for the longest time, security personnel at a facility have been able to think of their perimeters as a sort of two-dimensional line on a map. All of a sudden, this third dimension is added. Drones have been around since the 1970s, or at least the capability to fly a remotely controlled aircraft has been, but the barrier has been lowered considerably by modern technology. You now have solid state IMUs, satellite navigation, and other sensors feeding sophisticated autopilots running on miniaturized low-power computers. The same technology that goes into smartphones.

You mentioned that there are different types of drones. Since DroneShield’s technology is acoustics-based, what acoustics are you focusing on?

Right now we’re focused on commercially available multi-rotor drones. We are looking to continue refining our acoustic approach and also to expand the sensor portfolio to include other types of sensors that might help detect those more challenging targets.

What type of sensors does DroneShield currently offer?

We have two different types of acoustic sensors for sale right now. One is what we call the omnidirectional sensor, which has increased sensitivity in the front hemisphere, versus the rear hemisphere. The other model uses a parabolic dish that provides a lot of gain and increases detection range in a particular direction and also helps suppress noise sources off to the side. We can combine dishes into clusters to cover large areas from a single location.

Our acoustic sensors currently won’t show a drone’s location on a map. Instead, it will show a zone where the drone should be, based on sensors going off. If the omnidirectional sensor is going off, you have a pretty good idea of the drone’s location within 100 meters of that sensor, and if the long-range dish is alerting, it will give you the drone’s bearing, plus or minus 15 degrees. Overlapping lines of bearing from more than one long range sensor can also be used to localize the drone.
**Entrepreneurial Engineer**

DroneShield can deliver notifications to its clients a couple of different ways. Your products seem to be commercial quality and commercial cost products. Is DroneShield focusing more on commercial use in locations such as airports and prisons rather than personal home systems? Is there a large enough demand to invest in the home market right now?

The home market is something DroneShield is keeping a close eye on. However, we currently feel the biggest market right now lies in facilities rather than residences. Our hardware is commercial grade rather than, say, military grade. We’re big believers in commercial off the shelf, or COTS. One of the greatest mistakes I see early-stage companies make is to sink a large portion of their capital into customized enclosures and boards. You’re locked in, and you’ve invested a huge amount into designing a custom piece of equipment, and if any changes come up, you’ll incur additional costs. You’re paying a premium for low volume manufacturing.

This COTS versus customization is something we wrestled with early on. We also realized each product needed proprietary software. It’s the algorithms, the software that goes with the hardware, that sets you apart from anybody else, is that correct?

Absolutely. Well, that and our ability to think about the product from the end user’s perspective.

New products have many details to address. I’d say one of the biggest risks you run is you get something working well in your test environment, and then you don’t get exposed to the wider range of environments and conditions that your product is going to face until it’s too late. We’re lucky to have a number of early adopters who right away were testing both in rural Virginia and also in downtown Tokyo and everywhere in between. Really bringing the system out, figuring out what it could and couldn’t do.

**How does DroneShield alert its clients about drones within the vicinity?**

DroneShield can deliver notifications to its clients a couple of different ways. We have a browser-based interface, which seems to be the way people are creating user interfaces these days with no standalone application. Our browser-based interface is hosted on a server. It can be locally hosted in the network room, or we can host it in the cloud. You can go to the website and see the status of your system. There is a dashboard with the location of all your sensors. Within sub-second latency when the drone is detected, you’ll see an alert—an audible and visual notification of which sensor is detecting a drone.

If the system has internet connectivity, which is always the case with the cloud, alerts can also be distributed to security staff via e-mail or SMS notification. We also offer an API and dry-contact relays for interfacing with existing security systems.

The Infrastructure as a Service cloud market is making this all possible. As a small company getting started, we were able to be a lot closer to our clients than we physically were thanks to the cloud. We can have a data center in Tokyo without actually having to lease a brick and mortar building and install our equipment. Our services are therefore delivered effectively and with low latency all over the world.

**So clients can request geographical locations for the servers?**

Well, when a client wants to launch a service somewhere, we pick which region to launch it in to give them the best performance. There are websites where users can test latency in different regions to see which is most appropriate. They’re constantly adding new regions. One was recently added in South Korea, and another was upgraded in Brazil. They’re always improving it, so it’s only going to get better.

Has DroneShield created profiles for every type of drone? In other words, how do you know which type of drone you’re detecting?

What we found early on was that we were gathering all these signatures for different types of drones, we thought we were going to know exactly what type of drone was being detected. During this time of gathering information, we discovered instead that we have a lot of what we call signature collisions. We’ll get a new drone, setting off a signature that we developed previously through a different drone. It’s not uncommon to get a knockoff from an unknown manufacturer that sounds almost exactly like another model we already have a signature on file for. We’ve backed off from the claim that we can tell you exactly what kind of drone is out there.

If you were to go around and look at the different markets that utilize DroneShield’s technology, some of them would care more or less about whether drones are a different size. If you’re really worried about payload being delivered rather than say, privacy, then you’d be worried about bigger drones. If you’re worrying more about small payloads or privacy, then you’re also going to have to worry about the little drones.

**OUR SERVICES ARE DELIVERED EFFECTIVELY AND WITH LOW LATENCY ALL OVER THE WORLD.**
So you inform your clients that you can detect drones and can give them an idea of the type and size of drone. Does DroneShield have any deterrent or is that up for the client to decide?

Right—you detect the drone, now what can you do about it? The answer to that question depends on who you are and where you are. If you’re in the U.S., most of Europe and Japan, and I’m sure many other markets, there is not a lot you can do about the drone as far as active countermeasures are concerned. It’s someone else’s property flying in public airspace and even if it’s not supposed to be there, you as a private citizen or a company don’t have the right to interfere with it in any way. That’s something that law enforcement would do. There’s a lot of confusion out there. People have heard the term “expectation of privacy.” However, unless you have a ceiling over your yard, you do not have the expectation of privacy, and that’s been established in the courts. Anybody flying over your backyard in an aircraft or a helicopter could pull out their binoculars and see what you’re up to. Instead of active countermeasures, the client can adopt an appropriate response protocol. For example, prisons can clear the yard and alert local law enforcement to investigate likely launch locations based on where the drone came from.

But that’s half the world. There’s another half of the world and even government customers here who do have authority to take action against a drone. We have partners who are interfacing our system with counter-measures. If you’re a customer who can legally employ a counter-measure, DroneShield does offer solutions. Even then there are questions you must ask yourself: What is the collateral damage you’re willing to accept? What happens if you miss and hit something else? If you’re going to jam it, what are you going to do if you jam something good such as somebody’s cell phone call or your own, or the radios of your staff as they try to coordinate among themselves?

As DroneShield grows into new regions, we are constantly looking to follow different regulations. We have partners that handle interfacing with potential customers and regulatory constraints in local markets, and that’s been a really good model for us.