

The GPS Dot and Its Discontents

Privacy vs. GNSS Integrity



Professor Langdon, played by Tom Hanks, examines a GPS dot in Sony Pictures' 2006 movie, The Da Vinci Code.

What is the predictable endpoint of the trend toward ever cheaper, ever smaller, and ever more sensitive GPS receivers? It's the GPS dot: a miniature GPS tracking device that we'll buy in bulk and stick on almost everything of value that we own. But the dot has a dark side: the capability it enables for secret and potentially malicious tracking of others. The need to protect ourselves from invasive tracking will motivate use of subversive tools such as GPS jammers and spoofers. A rise in the use of these illicit tools has the potential to wreak havoc on the «good» GPS receivers – those built into our critical systems and infrastructure. The result: A looming showdown between privacy and GPS integrity.

TODD HUMPHREYS

DEPARTMENT OF AEROSPACE ENGINEERING AND ENGINEERING MECHANICS, THE UNIVERSITY OF TEXAS AT AUSTIN

Over the last few years, several of us in the GNSS community have done our best to convince our colleagues, policymakers, and the general public that unsavory characters with GNSS jammers or spoofers are a genuine threat to GNSS and an orderly society.

“But who would want to use a jammer or spoofer?” people ask.

My response? Hackers, because they can. Thieves planning to snatch expensive cargo. A moonlighting employee in the company car. Worse yet, state actors or terrorists targeting our national infrastructure.

I have until now tended to avoid any mention of upstanding citizens or upright motives. But a sober examination of the trends in GNSS innovation has led me to believe that there are perfectly legitimate reasons why otherwise law-abiding citizens could be sorely tempted to use a GNSS jammer or spoofer.

Indeed, the set of rogues who might wish to employ these devices could well include people we respect; it might even include you and me.

To understand why, let's roll back the clock by 12 years.

Down to the Millimeter

Something happened in the early morning hours of May 2, 2000, that had a profound effect on the way our society operates. That morning, U. S.

President Bill Clinton ordered that a special switch be thrown in the orbiting satellites of the Global Positioning System. Instantaneously, every civilian GPS receiver across the globe became 10 times more accurate. Positioning errors that had been the size of a football field turned into errors the size of a small room (**Figure 1**).

It is hard to overstate the effects of this improvement in accuracy. Before the selective availability switch was turned off, there were no in-car navigation systems giving us turn-by-turn directions. Civilian GPS couldn't tell you which block you were on, let alone which street.

For practical geolocation, accuracy matters . . . a lot.

Over the last decade, GPS accuracy has only improved. With today's GPS

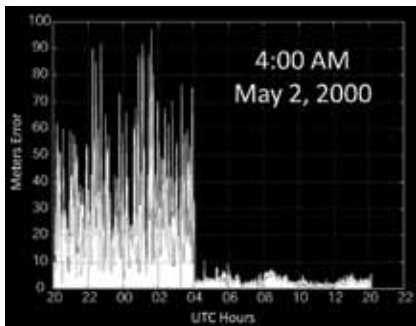


FIGURE 1 GPS positioning errors before and after selective availability was switched off.



FIGURE 2 The coming revolution in geolocation accuracy.

reference stations, better algorithms, and better receivers, stand-alone civil GPS can now identify not only the street, but which side of it you are on.

This level of accuracy has kindled a firestorm of innovation. Sophisticated in-car navigation systems have become the norm. Paper maps are becoming obsolete.

We're now on the verge of another revolution in geolocation accuracy. The three-meter accuracy that our iPhones and portable navigation devices give us is primitive compared with what we could be getting.

For some time now, we have known that, by exploiting the carrier phase of GPS signals and an Internet connection, we can achieve centimeter-level, even millimeter-level positioning.

So why don't we have this capability on our current smartphones? Only, I believe, for a lack of imagination.

Manufacturers haven't built carrier-phase differential techniques into cheap GPS chips because they're not sure what the general public would do with geolocation so accurate that it could pinpoint the wrinkles in the palm of your hand (Figure 2).

But it's not hard to see the potential of this next revolution in accuracy. Imagine, for example, an augmented reality app that overlays a virtual world to millimeter-level precision on the physical world.

In a few months' time, my students at the University of Texas Radionavigation Lab plan to demonstrate this augmented reality concept by hosting an art show that features virtual,

three-dimensional works of art created by Austin community artists with carrier phase-based GPS as the artistic medium. I expect that within the next few years this type of hyper-precise GPS, which has until now been limited to surveyors and other high-end users, will become ubiquitous and cheap — with fantastic consequences.

The GPS dot is precise positioning's Holy Grail. In the 2006 Sony Pictures' movie, *The Da Vinci Code*, the hero's accomplice explains that the GPS dot (see accompanying photo) is a tracking device accurate within two feet anywhere on the globe.

But we know that the GPS dot is impossible in the real world, right? For one thing GPS doesn't work well indoors. For another, complete GPS devices can't be quite so small, especially when they have to relay position measurements back over a communications network.

These objections were perfectly valid a few years ago, but things are changing. Since the first commercial GPS receiver was introduced in 1981, a strong trend has moved product development toward miniaturization, better sensitivity, and reduced price.

Five years ago, a GPS tracking device looked like the clunky box to the left of the keys at the top of Figure 3. Compare this to the latest GPS tracking device, released just months ago (second from top in Figure 3), which is the size of a small key fob. And when one looks at the state-of-the-art for a complete GPS receiver, which is less than a centimeter on a side and more



FIGURE 3 The GPS dot is the predictable endpoint of the current trend toward smaller, cheaper, and more sensitive GPS devices.

sensitive than ever (second from bottom in Figure 3), one realizes that the GPS dot will soon move from fiction to non-fiction.

Imagine what we will do with a world full of GPS dots! We will never lose our keys or our wallet — or our children at Disneyland — ever again. We'll buy GPS dots in bulk and stick them on everything we own worth more than a few tens of dollars. I



FIGURE 4 The Wave Bubble: an open-source GPS jammer.

couldn't find my shoes one recent morning, and, as usual, had to ask my wife if she had seen them. But I shouldn't have to bother my wife with such a triviality. I should be able to ask my house where my shoes are!

Those who have made the switch to Gmail remember how refreshing it was to go from organizing our email to searching it. The GPS dot will do the same for our possessions.

Dark Side of the Dot

Of course there is a flip side to the GPS dot. A few months ago, a woman — we'll call her "Carol" — called my office in a panic. She explained that an ex-boyfriend from California had found her in Texas and was stalking her. I was sympathetic but puzzled — why would she be calling me?

The case turned out to have a technical twist. Whenever Carol's stalker showed up — at the most improbable times and in the most improbable locations — he was holding an open laptop.

Over time, Carol began to suspect that he had hidden a GPS tracking device on her car, and she was calling to ask for my help in locating and disabling it.

"Perhaps you should go to a good mechanic and have him search your car," I suggested.

"I already have," she replied, "he didn't see anything obvious and said he'd have to take the car apart piece by piece if I really wanted to find the tracker."

"Then you had better go to the police."

"I already have. They're not sure it rises to the level of harassment and they're not set up technically to find the device."

"What about the FBI?"

"I talked to them too, same response."

We discussed a visit to the Radio-navigation Lab so that my students and I could perform a radio sweep of her car, but that wasn't a sure solution either. Some tracking devices are configured to transmit only when they are within a designated safe zone or when they sense that the vehicle to which they are attached is moving.

So there we were. I could only suggest that Carol trade cars for a week with someone bigger and meaner than she.

Carol wasn't the first and certainly won't be the last person to be left with no escape from this kind of frightening invasion of privacy. As I looked into her case, I discovered to my surprise that what the ex-boyfriend did is not clearly against the law in many states and locales.

The U.S. Supreme Court ruled in January that the police must obtain a warrant for prolonged GPS tracking of someone's vehicle. But as privacy law expert Orin Kerr of George Washington University has pointed out, the law isn't clear about civilians using GPS to track one another.

So it's not only Big Brother we have to worry about, but also Big Neighbor.

Illicit Tools

Tracking victims do have one effective, if illegal, option: a GPS jammer.

Figure 4 shows one such device, the so-called Wave Bubble, designed by open-hardware movement leader Limor Fried. Fried, an electrical engineer who earned her master's degree at MIT, calls it a "Tool for Reclaiming our Personal Space."

With the flip of a switch, the device creates a protective bubble around the user that drowns out all GPS signals. Fried designed the Wave Bubble in part because, like my caller, she felt threatened by GPS tracking. She pub-

lished her design on the Web. Those who don't have time to build their own Wave Bubble can simply buy an equivalent: Despite a recent Federal Communications Commission campaign to shut down U.S.-based Internet websites offering such products, enterprising online businesses sell nearly identical devices for less than \$50.

From one point of view, the Wave Bubble seems like a great idea. It would certainly be handy if someone ever puts a tracking device on *your* car. But use of the Wave Bubble is very much illegal in the United States.

Why? It's not a "bubble" at all. Its jamming signals don't stop at the edge of your personal space or at the edge of your car. They go on to jam innocent GPS receivers for miles around.

If you're only trying to protect your privacy, it might not feel wrong to use a Wave Bubble, but, in fact, turning one on could be disastrous.

Imagine that you are the captain of a cruise ship trying to make its way through a thick fog. A passenger onboard turns on a Wave Bubble. The ship's GPS navigation system goes blank. Now it's just you, the fog, and whatever you can pull off the radar. (Operational lighthouses and foghorns are in steep decline and LORAN, the only suitable maritime backup to GPS, was discontinued just over a year ago in the United States.)

Our modern society has an almost blind reliance on GPS. It's built deeply into our systems and infrastructure. Some call it the invisible utility. In this environment, turning on a Wave Bubble or any GPS jammer could be deadly.

Frankenstein's Monster

Dangerous as jammers are, an even more potent and subversive "privacy" technology exists that threatens GNSS reliability: the GPS spoofer. The idea behind a spoofer is simple: instead of jamming GPS signals, you fake them. If done properly, the target GPS device doesn't even know it's being fooled.

Inside the victim receiver's digital circuitry, a clear correlation peak is

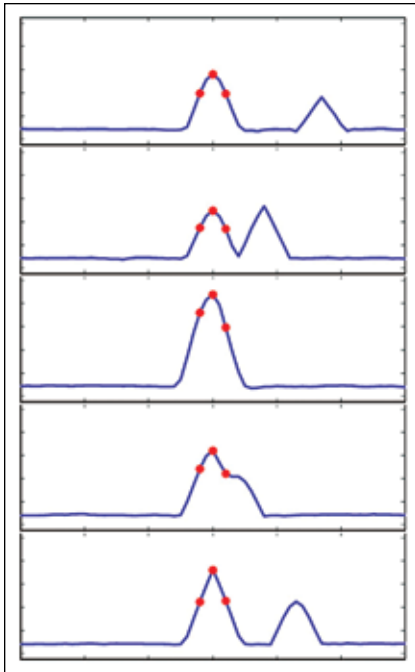


FIGURE 5 A civil GPS spoofing attack from the perspective of the victim receiver's correlation taps.

associated with the authentic GPS signal. The red dots in **Figure 5** represent tracking points that try to maintain themselves centered on this peak. If you send in a fake GPS signal, another peak pops up, and when these two peaks become perfectly aligned, the tracking points can't tell the difference. The stronger counterfeit peak hijacks the tracking points and forces the true peak off.

At this stage of the attack, the game is over (see the bottom panel of **Figure 5**). The fake signals now have complete control of the victim receiver.

So is this scenario really possible? Could someone manipulate a GPS receiver's timing and positioning just like that with a spoofer?

The short answer is yes. Non-military GPS signals are completely open. They have no encryption and no innate method of authentication. Civil GPS is the most popular unauthenticated protocol in the world.

Even so, up until recently few people worried about GPS spoofers. The general reasoning was that it would be too complex or too expensive for some hacker to build one. But I didn't see it



FIGURE 6 Stills from the spoofer's first successful test run.

that way and neither did Brent Ledvina, a friend from graduate school. Our training in software-defined GNSS had taught us that it wouldn't be so hard.

We decided to build a spoofer in order to get out in front of the problem, better understand the threat, and develop defenses against civil GPS spoofing.

I remember vividly the week it all came together. Ledvina and I built it at my home, with help from my three-year-old son. At first, the spoofer just looked like a jumble of computers and cables, though we eventually were able to fit it inside a small box.

The Dr. Frankenstein moment, when the spoofer finally came alive

and I got a glimpse of its awful potential, came late one night when I tested the spoofer against my iPhone. (**Figure 6** shows several still frames from footage of that first experiment.)

I had come to completely trust the little blue dot on my iPhone screen showing my location. Its reassuring blue halo seemed to speak to me, saying "Here you are, and you can trust me." So, something felt very wrong about the world — almost a sense of betrayal — when that blue dot, after I fired up our spoofer, started from my house and went running off toward the north without me.

What I then saw in that little blue dot was the potential for chaos. I saw



In-home construction of the first civilian-owned civil GPS spoofer.

airplanes and ships veering off course, with the captain unaware until it was too late. I saw the GPS-derived timing of the New York Stock Exchange being manipulated by hackers.

Indeed, we can scarcely imagine all the mischief that a knowledgeable person could do with a GPS spoofer. No wonder, then, that broadcasting a spoofing signal is very much illegal.

Nonetheless, the GPS spoofer has one redeeming feature: it is the ultimate weapon against an invasion of GPS dots of the Da Vinci Code variety.

Think about it: if you discover you're being tracked, you can play your tracker for a fool. You could pretend to be at work when you're on vacation . . . or even lure Carol's stalker to an empty parking lot where the police are waiting to nab him.

Bagful of Dots

I am fascinated by this looming conflict between the need for privacy on the one hand, and the need for a clean radio spectrum on the other. We simply cannot tolerate jammers and spoofers, and yet, given the lack of effective legal means of protecting our privacy from the GPS dot, can we blame people for wanting to use them?

My hope is that we will resolve this conflict with some yet undiscovered technical innovation.

Meanwhile, grab some popcorn, because this is going to get interesting.

Within a few short years, many of you will be the proud owners of a GPS dot. Maybe you'll own a whole bag full of them. You'll never lose track of your belongings again. The GPS dot will fundamentally re-order your lives.

But will you be able to resist the temptation to track your fellow humans? And will you be able to resist the temptation to turn on a GPS jammer or spoofer to protect your own privacy?

As usual, what we see just beyond the horizon holds both promise and peril. It will be fascinating to see how this all plays out.

Acknowledgment

This article is an adaptation of the keynote address given February 22 at the 2012 GNSS Vulnerability conference hosted by the National Physical Laboratory in the United Kingdom.

Additional Resources


[1] Fried, Limor, "Wave Bubble — A design for a self-tuning portable RF jammer," <<http://www.ladyada.net/make/wave-bubble/index.html>>

[2] Kerr, Orin, professor of law, George Washington University, <<http://volokh.com/2011/10/27/my-view-of-the-second-question-presented-in-united-states-v-jones-the-fourth-amendment-gps-case>>

[3] University of Texas RadionavigationLab <<http://radio-navlab.ae.utexas.edu>>

Author



Todd E. Humphreys is an assistant professor in the Department of Aerospace Engineering and Engineering Mechanics at the University of Texas at Austin. He directs the university's Radionavigation Laboratory, where software-defined GPS receivers are developed as a platform for GPS technology innovation and study of the ionosphere and neutral atmosphere. His recent focus has been on defending against intentional GPS spoofing and jamming. In 2008 he co-founded Coherent Navigation, a startup that hardens GPS by, among other things, exploiting telephony signals from the Iridium satellite constellation. Humphreys received a B.S. and M.S. in electrical and computer engineering from Utah State University and a Ph.D. in aerospace engineering from Cornell University. His research interests are in estimation and filtering, GNSS technology, GNSS-based study of the ionosphere and neutral atmosphere, and GNSS security and integrity. 



The Institute of Navigation

Your source for 24/7, anytime, anywhere access to objective, credible and trusted technical information!

JOIN TODAY!

Positioning | Navigation | Timing

The world's premier professional organization for the advancement of positioning, navigation and timing.

www.ion.org

