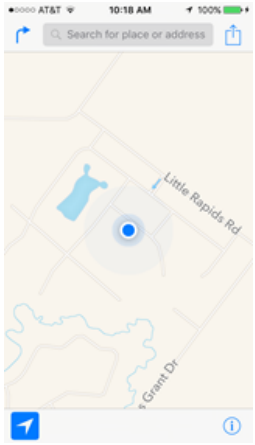
Choose ID over IP. Please.

Lori MacVittie, 2017-06-02

I take lots of pictures. Sometimes I'm using WiFi. Other times I'm out by the pond (fishing, if you must know) and using my cell connection. Same house. Same location.



And yet the geolocation information embedded into pictures taken in the same location vary based on whether I'm on Wi-Fi or cell. Sometimes I'm "near Wrightstown." Other times I'm not. When I'm on a wired machine, it gets even crazier. As I'm writing this, I'm pegged as being in Appleton, WI. Which is about 20 miles south of here. My iPhone, on the same desk, tells me I'm in the Town of Lawrence (correct). A photo I uploaded to Facebook says I'm near Wrightstown, some 5-10 miles away.

Needless to say, we're all aware that geolocation based on IP address can be as much art as science sometimes. Having worked in the GIS field (way back now, when I was still allowed to code) I'm well aware of the mathematical gymnastics required to map coordinates to place names accurately without introducing the questionable accuracy of an IP address. Consider this extraordinary situation encountered because of the vagaries of geocoding by IP:

> *MaxMind matches IP addresses, which are used to connect devices to the internet, to physical locations. It has said these are not meant to be precise.*
>
> *James and Theresa Arnold say it registered their home as the position of more than 600 million addresses.*
>
> *They say this has led many people to wrongly believe a host of crimes were committed at the property.*
>
> *"The first week after the Arnolds moved in, two deputies from the Butler County Sheriff's Department came to the residence looking for a stolen truck. This scenario repeated itself countless times over the next five years," documents filed with a Kansas court read.*
>
> http://www.bbc.com/news/technology-37048521

I'm glad I'm not the Arnolds*. And while this case is extraordinary, it does illustrate that dependence on IP address is not necessarily a sound idea – especially if you're using it, in part, to authorize access to applications.

We know many financial institutions, in particular, rely on IP address as much as they do device to ascertain validity of login attempts. That's a good thing if you're pretty much always using the same device from the same place because your IP address doesn't change all that much. But for mobile apps, which are increasingly "the way" folks communicate with customers, it could be problematic. My IP address changes as I roam, not to mention sometimes even when I don't thanks to limitations on the reach of WiFi outside my home.

IP address as a means of identification has long passed its usefulness, anyway. It used to be that everyone using that broadband connection had their own IP because they got it directly from the provider, via DHCP. But that went the way of the Dodo when devices connected to the Internet in a home outnumbered the people. According to recent surveys, "there are now 734 million in use within U.S. Internet homes, averaging 7.8 connected devices per home." That's twice the average 3.14 people per household in the US in 2015.

Which means the notion of one IP address per person (and now thing) is largely untenable an option, given the limited number of IPv4 public IP addresses providers have to dish out. Everyone's using just one public IP per household, generally speaking, and everyone else is being routed through that little black box.

IP, as a means of authoritative identification, is dead.

Credentials, whether they be tokens or username/password or some other heretofore undiscovered method, are the best means of identifying – and thus authenticating – users. It is also the best way to protect apps today, given the abuse of IP addresses in a variety of attacks. When I can spoof my IP as readily as I can my user-agent, it is not a good idea to consider it an authoritative source of information.

Nor it is appropriate to use for whitelisting or blacklisting, because honestly, IP addresses can be changed in a matter of seconds on the Internet. Tens of millions of IP addresses are routinely noted as taking part in DDoS attacks. Some intentionally, others by happenstance of visiting the wrong site or buying the wrong device. Blocking by IP address leads to headaches for consumers. Using IP reputation moving forward isn't going to be nearly as effective as it once was, back in the day, when the Internet was young and innocent and full of people with good intentions. Now that the Internet is old and jaded and rife with attackers who are as likely to abuse your devices as they are anything else, we've got to look to something else.

We need to move to identity as the new firewall, to secure the new perimeter that is the application. Whether it be through federation or traditional corporate identity management, we need to rely more on ID than on IP to secure our borderless business and provide access to an increasingly mobile set of users, both corporate and consumer.

* Interestingly, my mother's family are Arnolds. No relation, I'm sure, but then again…

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | wwww.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com