Communities of Things

Column: Bits versus Electronics

Communities of Things

Bob Frankston
Microsoft Corporation

■ **When I want** to go to a website, I just type in the URL, and I am there. Sure, we had to get a subscription from a service provider and set up our devices, but that was a one-time thing. As we move into a world of many connected devices, it is no longer a one-time thing.

Today, creating connected devices and services requires thinking about all the mechanics and networking and onboarding and providers. In designing products, we need to think outside the physical network and think about communities (social networks) of devices.

Today, to provide access to a printer we must connect it to the right network. We then need to use SSIDs to mimic the physical boundaries for the network in the absence of a wire. SSID once meant Service Set Identifier, but today we just accept it and do not recognize that it is bringing forward a legacy kludge.

In fact, mostly we think about connectivity reflects an accidental history. We accept that we cannot "just connect" devices. Implementors need to think the quirks of IP (and TCP), USB, Bluetooth, Zigbee, Z-Wave, etc. We should be able to just assume connectivity.

GETTING DISCONNECTED

Initially, each endpoint on the Internet had its own IP public address. You could easily make a connection between any two endpoints. Typically, the endpoints were large mainframes which required logins for users, both remote and local. Personal computers did not have a problem since they were isolated or only on local networks.

The advent of computer and home networks presented a challenge. I remember getting my first cable modem and I found I could look at files on my neighbor's computers.

I chose to use NATs as a temporary work-around for the limits of IP addresses for home networks. One consequence is that the machines on the local network are not visible to the outside world unless special efforts were made to make them visible using techniques such as forwarding. I expected that the limitation on visibility would be removed once we had IPv6 with encrypted connections and that new applications would be written to be careful about which connections they trusted.

Instead, the limitations of the NAT were rebranded as features with the firewall being treated as a security perimeter. This is problematic for several reasons. One is that it only provides the illusion of security because if any device inside the network is compromised, all other devices that trusted the perimeter are easily compromised. This has been the source of high-profile attacks.

Firewalls represent a simplistic model of authority at odds with a real world in which you may be a member of multiple communities. The

Digital Object Identifier 10.1109/MCE.2019.2953789
Date of current version 7 February 2020.

2162-2248 © 2019 IEEE
Published by the IEEE Consumer Electronics Society

Introduction

When I want to go to a website, I just type in the URL, and I'm there. Sure, we had to get a subscription from a service provider and set up our devices, but that was a one-time thing. As we move into a world of many connected devices, it's no longer a one-time thing.

Today, creating connected devices and services requires thinking about all the mechanics and networking and onboarding and providers. In designing products, we need to think outside the physical network and think about communities (social networks) of devices.

Today to provide access to a printer we must connect it to the right network. We then need to use SSIDs to mimic the physical boundaries for the network in the absence of a wire. SSID once meant Service Set Identifier but today we just accept it and don't recognize that it is bringing forward a legacy kludge.

In fact, much of the way we think about connectivity reflects an accidental history. We accept that we can't "just connect" devices. Implementors need to think the quirks of IP (and TCP), USB, Bluetooth, Zigbee, Z-Wave, etc. We should be able to just assume connectivity.

Getting Disconnected

Initially, each endpoint on the Internet had its own IP public address. You could easily make a connection between any two endpoints. Typically, the endpoints were large mainframes which required logins for users, both remote and local. Personal computers didn't have a problem since they were isolated or only on local networks.

The advent of computer and home networks presented a challenge. I remember getting my first cable modem and I found I could look at files on my neighbor's computers.

I chose to use NATs as a temporary work-around for the limits of IP addresses for home networks. One consequence is that the machines on the local network are not visible to the outside world unless special efforts were made to make them visible using techniques such as forwarding. I expected that the limitation on visibility would be removed once we had IPv6 with encrypted connections and that new applications would be written to be careful about which connections they trusted.

Instead, the limitations of the NAT were rebranded as features with the firewall being treated as a security perimeter. This is problematic for several reasons. One is that it only provides the illusion of security because if any device inside the network is compromised, all other devices that trusted the perimeter are easily compromised. This has been the source of high-profile attacks.

Firewalls represent a simplistic model of authority at odds with a real-world in which you may be a member of multiple communities. The people you work with and socialize with may overlap, but one is not a subset of the other. If you have a guest network in your home that is separate from your primary network, then how does a guest print on your printer (with your permission, of course)?

Rather than recognizing the limits of firewalls, the firewall mechanism has been treated as a necessity and extended by adding complex rules on each computer and at each point of interconnection. It becomes very difficult to make sure each setting on each device is tweaked just right so applications work. This works against the goal of simplicity.

A visitor plugging into a network jack, bypasses all the mechanisms, and has full access to internal systems. You might trust the visitor, but you can't know if the visitor's computer has been compromised. Even trusted employees might have their computers compromised when they visit other networks. Notice I used the word "compromised" rather than "infested with a virus" to avoid too much semantic overloading since so much of this approach is based on simplistic analogies with the physical world and ideas like finding safety in gated communities.

Having all these barriers makes the process of onboarding very difficult. And that has a direct effect on product acceptance and the cost of support. One reason one must authenticate to a Wi-Fi access point is to prevent untrusted computers from connecting to the physical network. Without wires, there is no simple boundary. This means going through a complex process of finding the appropriate SSID or using a physical button to establish access and then repeating this process for each network. I feel this acutely in my house in which I have over 200 devices with more than have wireless (many IP lights). I despair of ever having to change my SSID. Most users don't feel the pain now because people are at the dabbling stage and don't have many devices. I feel the pain that comes from trying to manage many devices. This will become an issue for most users as connected devices become the norm, and people aren't willing to live within the confines of a single provider, be it Alexa, or Google Home or Apple.

Other protocols such as Bluetooth, Zigbee, and Z-Wave have a version of this in having to pair with each device in each place. You rent a car and must pair your phone and then unpair.

Reconnecting

There is a major positive in the perimeter security model. It makes everything simpler. Websites obtain certificates to assure that if you type https://rmf.vc, you indeed reach a site with its name in the certificate. It doesn't really provide security – just encryption and name verification but calling it security is better marketing.

But what is the equivalent for devices? And how does one manage all the relationships? One can do one-time direct pairings, but that doesn't scale well. Or we can set the password in a new device but with my over two-hundred devices that becomes tiresome. That may seem like a lot of devices but just look around your house at each lightbulb, switch, door lock, thermostat, appliance, speaker, etc. Remember that now, with Alexa, each speaker is a smart endpoint. Those will all become intelligent over the next few years.

So today we generally punt and use open protocols for internal devices. It is wonderfully simple and, for now, works-well enough as long as you accept some risk that your light bulb may be compromised. More reason to assure that your main computer devices require some authentication.

Community Protocols

The power of the Internet is in its ability to let us address focus on what we are trying to accomplish without getting lost in the myriad details of mechanics of networking. At least in theory. In practice, users still have to concern themselves about which network they are connected to. The network is a community of devices and you must choose one and are either a member or not, there is no nuance.

We need to enable communities that aren't tied to any particular physical network. Devices and services can be part of multiple communities. For example, if you can choose to have your clothes dryer maintained as part of the manufacturer's community of devices as well as your apartment. If you are in an apartment you may also want to participate in a resource management plan for the building and run the dryer only when the price for electricity is low. A device may be in multiple communities.

The electronic equivalent of a membership card for the community is a shared secret. The actual implementation could be nuanced with different degrees of capabilities, but we want to allow for the simple case – one just as simple as to assume if two devices are plugged into the same network, they can trust each other.

Since you're not dependent upon which physical network you're connected to, you do not need an on-boarding process that involves connecting to the right access point. What we do need is open connectivity. One part of this can be achieved by having a public face on the standard router that provides access to the larger Internet as well as peer devices nearby.

Prisoners of our own Devise

Accepting this idea does require getting past the notion that you are "stealing" Wi-Fi if you are using someone's Internet connection. Xfinity already offers a form of this for its users – open access available on the access points it provides. Public policy should require having an open access option for APs even if only for public safety.

The idea of providing open connectivity goes against the traditional (legacy) business model of telecommunications that's built on the false idea that bits are expensive. This is

why I take pains to remind readers that bits are not electrons.

It also goes against the idea we need a physical security perimeter. The reality is just the opposite – once those walls are breached, there is no safety. And the onboarding process invites workarounds that create their own vulnerabilities. By having communities of cooperating devices independent of the accidental properties of the underlying physical network, we can have application-appropriate policies with meaningful trust. Compromising one device on a network doesn't affect other communities.

The Internet has been such a powerful force because it has allowed us to take advantage of any available connectivity and create our own solutions. You just type in a URL and arrive at the web page.

We're now ready to take the next step and enable peer connectivity among communities of devices. For programmers just naming the other device means you're effectively connected. No futzing with sockets and firewalls etc. This is even more true for users – their devices just-work anywhere without any setup.

The issue of communities and naming is fundamental even in something so simple as which light bulbs (light sources) are part of the living room (a physical place) or the Halloween scene (a logical grouping).

The ability to think in terms of communities rather than complexing wiring and networking issues is exciting and enables new classes of applications that have an even great impact on society than the web. The uses in healthcare alone can save many lives.

As we move into a world of connected devices the consumer industry can no longer accept the pain of onboarding and move to create great experiences for users,

ABOUT THE AUTHOR

Bob Frankston is best known for writing VisiCalc—the first electronic spreadsheet. While at Microsoft, he was instrumental in enabling home networking. Today, he is addressing the issues associated with coming to terms with a world being transformed by software. Contact him at IEEECE201911@bob.ma.