anima Working Group
Internet-Draft
Intended status: Standards Track
Expires: 13 January 2022

M. Richardson
Sandelman Software Works

12 July 2021

Involuntary Onwership Transfer of IoT devices: problem statement draft-richardson-iotops-iot-iot-01

Abstract

This document details a problem statement relating to ownership of IoT devices.

The problem details is that of changing ownership or possession of a device when against the consent or knowledge of the device and/or manufacturer.

Examples relating to outer door control are used to illustrate the problem statement in an intuitive scope.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 13 January 2022.

Copyright Notice

Table of Contents

1. Introduction

Much has been written about how to secure IoT devices against both physical attacks and those that are done through network protocols. (Insert survey articles)

In most cases, the goal of the security mechanisms is to make sure that the device remains under control its lawful or intended owner. One example of such a definition of this control could be to mean that the device accepts commands only from that owner and that the device provides information only to destinations that the owner specifies.

This document explores the problem of what happens when the physical or legal ownership of the device does not correspond to the logical ownership of the device.

There are many ways to explain, scope, and illustrate the general problem. It is much easier to understand with concrete examples, and in this example the front-door lock scenarios are used an easy to understand way to connect to real life intuition. It is believed that most other IoT authorization and ownership problems are probably subsets of the situations outlined here.

2. Door Locks

Most people live in some kind of dwelling with at least one door. When there is more one door, one of them is usually the front-door. This is the primary method of entry and exit, and it usually connects to the street and thus to the rest of the world. It is where both strangers and friends arrive and depart, while other doors (side, garage, balcony, basement and back doors) may lead only areas from which further egress may be impossible, difficult, or deadly.

The door lock is among the simplest of IoT actuator: after potentially many layers of system, there is a single output pin from the lock microcontroller which operates some kind of solenoid. When the solenoid is operated, the door unlocks.

Of course, some doors may be much more complicated with automatic opening or closing motors, sensors to make sure there is clearance before opening, and that the door is clear before closing. Some doors may slide, lift, rotate or perhaps in the future, modulate to alternate dimensions in order to create an opening. None of those details matter to this document.

Also irrelevant to this document are the mechanical details of the door lock itself. While the physical characteristics of the lock are terribly important to actual lock design, it is assumed in this document that the mechanical aspects of the lock is of sufficient quality to resist the expected amount of brute force that is anticipated to be applied to it.

The history of physical door locks is frequent tussle between lock makers who attempt to make locks more resistant to attack, vs thieves who use ever more sophisticated methods to attack the locks. There is an obvious relationship to cryptography and cryptoanalysts, and it is hardly surprising that many cryptographers and cryptoanalysists are also competent lock pickers. [blazepicking]

2.1. Human Relationships to Doors and Door locks

Homes and apartments come with a complex set of ownership conditions, often via laws established over many centuries. Many places have very ancient laws about when and how a Hotel may evict people.

2.1.1. Single owner

The simplest situation is that of a freestanding dwelling, owned by a single individual.

2.1.2. Family home

To the single individual one adds a spouse, some children of a variety of ages, grandparents, sisters, brothers, neighbours, cat-sitters, etc.

Some members of the household may be trusted to open or close the door from the inside only. For instance a younger child might be allowed to open the door when inside, and only when there is someone else in the house.

The child would not be allowed to leave the house and lock the door, and preventing such an young child from locking themselves out might a useful feature.

Many homes choose to have deadbolts which require a key to lock the door when leaving. Pulling the door shut is insufficient to lock the door.

Other owners prefer that the door lock itself when pulled closed, and so might use a spring-bolt lock.

Still others have double deadbolts which require a key in the inside in order to lock or unlock the door. People prefer these if they are concerned that a thief will enter their home through a window, and then will go out the front door with their stuff. The double deadbolt requires a key to unlock from the inside. The downside of the double deadbolt is that in the event of a emergency, it is not possible to use the door without the key. As a result, many homes with a double deadbolt will have a key hanging nearby, but not within reach of a window.

2.1.3. Roomates

One scenario where there are multiple unrelated individuals in a dwelling is when it is shared by roomates. Each roomate will have co-signed the lease and will have an equal right to be in the apartment. It would be inappropriate for any roomate to have the power to lock out the other roomates.

This is constrasted with a owner (or renter) who sublets one or two rooms to other people. In that case, this primary owner should have more power over who can enter and exit, subject to some legal restrictions. The degree to which subletter have legal rights varies by jurisdiction.

Can any of these individuals give a "key" to girlfriend/boyfriend? This is definitely a complexity of the situation which is usually not seen in the family home.

2.1.4. Apartment building

An apartment building consists of many dwellings with some common space. (This is distinguished from a multi-tenant building where each tenant has their own front-door.)

Residents of an apartment buildings must pass through a common front door. Historically access to such buildings was via a kind of guard, the door-man. This has now been replaced with some kind of master-key on the front-door, which a telephone mediated system that allows visitors to "buzz" up to the appropriate apartment. The resident of that apartment then activates a circuit to unlock the front door.

Historically, these telephone systems were hardwired private handsets present in each apartment. This meant that anyone who was in the apartment could let anyone else in.

More modern system are tied into the public telephone system, and a DTMF tone is used to unlock the front door. With such a system, if the phone number attached to the apartment is a mobile phone, then a resident can buzz themselves while outside the apartment, and then buzz themselves in.

The modern apartment system does not usually provide for multiple numbers to be attached to the system, and a guest in such an apartment would be unable to, for instance, let medical people in, if the primary resident took ill.

2.1.5. Rented or Leased Dwellings

Many dwellings are owned by one person, but occupied by another person based upon a rental agreement.

Historically such agreements were based upon leases of many months to years, but intermediation of the relationship by a number of dotcom companies have reduced the lease time to days, and the same rental systems are expected to accomodate what is more like a Hotel relationship. That situation is handled in the Section 2.1.6 section.

In many cases the owner (or property manager) of the home has a legal right to enter, under certain circumstances. For instance to effect repairs, to show the dwelling to a new potential tenant, and in emergencies, to do things like shut off water or gas to avoid damage.

Notice is often required for most activities, most laws allow a landlord to enter without notice during emergencies to do things like shut off water when there is a leak. A landlord can also be compelled to open the door for a police warrant, and in cases where the police suspect harm, they often will enter without a warrant.

This situation is even more complex in apartment buildings, even where the apartments are owned (and occupied by the owners). There is still a building manager, and there are still water leaks.

There is additionally, many common areas to which many people should get access. Some areas like common rooms are multi-access, but during a reserved time, are exclusive to the person who made the reservation.

Additionally, there are secondary areas that are private to each residents, such lockers for bicycles and parking spaces.

2.1.6. Hotels

Placeholder.

2.2. Rented Automobiles

Automobiles have doors, locks, and ignition locks. There are sometimes different keys for the different locks. The valet key for instance, allows the driver door to be opened and the car to be started, but does not provide access to the glove compartment or the trunk.

Automobiles are rented in a variety of ways: from hourly rentals by car-sharing companies (e.g., [communauto], [zipcar], [tribecar]..), to traditional daily rentals by well-known companies, to yearly car leasing.

During the valid period of rental, the motorist probably needs to have complete control of the vehicle. If any other party had any control of the vehicle, it might significantly change the legal liability for activity done with the vehicle.

This is usually done by giving them a key which they must insert into the ignition.

Some car sharing companies have schemes involving lockboxes (with master physical keys!) to share the car-specific key. (This is rather akin to Kerberos tickets: one key is used to unlock another key)

Increasingly automobiles are going "keyless", and it is sometimes sufficient for the "fob" to be just near the vehicle, but the fob is essentially still a key.

Many manufacturers are now using the individual's smartphone to unlock the car via Bluetooth or NFC, and once inside the vehicle, the phone serves as the "fob", authorizing the vehicle to run.

Integration with the smartphone has a transaction cost to it: the phone/car connection must be onboarded in some way, and is therefore only suitable for car owners, or longer-term leases.

Shorter term leases may transition to use of a smartphone, but today, they are mostly based upon passive RFID FOBs or physical keys. Today, when used via smartphone, there is a satellite or LTE based care security system that the drive interacts with via the Internet. There are reports of people being stranded in the woods for days, because the were too far away from the LTE tower, and the vehicle would not unlock or start without authorization.

At the end of the rental period, the access for the motorist must be revoked. This is akin to getting rid of roomate (Section 4). But there are some caveats: there has to be some kind of grace period or interlock with the renting agency, as the vehicle might not yet have been returned properly. They could just be late. The vehicle could stall meters from the proper location and need to be restarted. Once at the proper location, the motorist might still need to access the trunk or other compartments to retrieve their belongings.

But, once properly returned, the vehicle should no longer be accessible to the original renter.

The next renter may be standing waiting, particularly if the vehicle is late. The transition from one renter to another needs to have a standardized ceremony.

For long-term leases the process may be more complex at the end. While some significant grace period (compared to rental period) is appropriate for short-term, for longer term leases, the owner likely needs to be able to disable the vehicle some few number of days after the end of the lease. But, never before.

2.3. Additional Third Parties who need access

In addition to this obvious arms race, there are specific third parties that bring their own interests to the locks in the front-door lock scenario, e.g. law enforcement or fire departments.

In some places there are locks which accept keys carried by fire, police or postal personnel. For instance, the service key in a building allows the fire department to override the elevator controls. The electrical panels and gas systems in the buildings may also be accessible by the fire department in order to cut off electricity or gas during a fire.

The mailboxes of an apartment (and the outer door to get to the mailbox) can be opened by the postal carrier in order to deliver the residents mail. The French PTT T-10 key is an example of such a key, and there is a law and regulation around it as well.

This is an example of a master key necessary in most multi-tenant buildings.

It is hardly surprising that there was significant concern when the fire/police "master key" for the city of New York was being openly sold on ebay. (see [huffpostkey] and [fdnymaster])

A digital door (and elevator control) key that could be safely deployed as a replacement for this physical key would be a significant improvement over the physical keys. It would be easier to add new users and revoke old users, and an audit log of who used what key in which building could be easily generated.

3. Death of a Home Owner

Start from a single freestanding dwelling, owned by a single individual, and ask what happens when the individual dies. How do the inheritors (or the executors of the estate) take possession of the property? Prior to electronic door locks, a physical key can be used, and if one is not available, then a locksmith can be engaged. This may require a legal statement from an appropriate authority, at which point the locksmith may make use of a drill, or maybe even some other implements such as saws or battering rams.

The same techniques can probably be used against electronic door locks that do not use keys, but can this technique be used against, for instance, smart toasters, furnaces or automobiles?

Repairing a hole in a front door is a nuisance. Replacing a furnace or other large appliances due to a death is unacceptable.

In particular, automobile locks are usually designed to resist significant amounts of force as they are often the target for thieves. The vehicles are left unattended in public parking lots among many other automobiles for many hours at a time, and it is even a common occurance that a person legitimately walks up to the wrong automobile (having forgotten exactly where they parked) an attempts to unlock it.

Any tool or protocol that the locksmith can employ against the automobile could also be employed by a malicious attacker. Any mechanism that the automobile maker includes in the system to allow a locksmith (or legal court) to open the vehicle would be the target of attackers. This is fundamentally why security protocols do not include back doors ([RFC1984]).

4. Multi-person Dwelling: how to kick that that deadbeat roomate out?

The situation above was for a single dwelling. Many dwellings are occupied by multiple people, often jointly.

Should any of the occupants be allowed to change the locks, that is, change the entry authorization for other occupants? Under normal circumstances, the answer should probably be no. Under the situation of a legal injunction, the answer may be yes. How can the door lock system know? How can the party which is asking for the injunction know that the door lock has no other secret authorizations?

If the legal system must be a party to this activity, how does the home owner, not involved in such a process know that the legal system's computers haven't itself been compromised? This is one of the major arguments against official escrow: the escrow system is now a very high value target.

5. Getting rid of the abusive Spouse

The situation where a couple separate under duress requires that access to the original home be restricted. That is, the door locks must be rekeyed. Digitally, this means removing the access to the abusive spouse.

Is this different than the case of roomates? Not really: multiple people had access to the door lock before, and one must be removed. For the case of roomates, each had a legal right to access, and no roomate should be allowed to revoke access for the other roomate.

Now, in the case of separation, the remaining "roomate" must now be permitted to revoke access for the other "roomate"

6. What is ownership

One technical definition of ownership might be that the device has an identity certificate from the owner. This is a good definition, and it is currently what is used in [RFC8995], [MATTER], and many other similar systems.

In the security space, the vernacular term, "p0wned" is often used to refer to a device that is no longer under the control of the legitimate owner. That is, an attacker has taken control of the device, usually through some security vulnerability, and now the attacker controls what code the device will run.

So a deeper notion of what it means to own a device is that it could involve control of what software a device runs. Whomever controls the software in a device controls what the device does, and whose commands it obeys. This can generally be expressed in the form of an authorization from a Trust Provisioning Authority (Section 7 of [RFC9019]).

Control and access decisions are not usually changed by changes to the firmware of the device. (Not withstanding the dispute between the FBI and Apple: [applefbi]) For good or bad, all devices of a particular type run the same firmware that the manufacturer has provided. The decision as to who is in control of the device is determined by the firmware based upon the identities of the parties.

All of the challenges in the previous section boil down to finding a way to express the question as to whether an identity is allowed control.

7. Questions and Opportunities

While the example of the front door lock was used as an exemplar, essentially the same question applies to pretty much all forms of actuator. Access to some sensors may be significantly simpler, but other sensors will be as complex as any actuator.

A primary question is whether the front door problem is a superset of all other problems. If so, then a solution to the front door ownership can provide for all other actuators.

Or, if there some other physical world interaction which is more complex, then the front door may be a subnet of it. Alternatively there may be some other master pattern which does not overlap with the front door and it would provide a different model. Some actuators might be a subset of these two models.

The various modes of front door interaction need to be named. Based upon the above description, these would include: roomates, spouses, ex-spouses, renter/owners, tenant/superintendant, fire-department, police officer, young-children/parent, adult-children/seniors...

The automobile, personal or medical device interactions are mostly variations on the front door. Instead of superintendant, substitude mechanic, leasor or ER doctor. Instead of child, substitute neighbour-who-borrows your tools.

The IETF has created a number of authorization systems. This starts with SPKI [RFC2393], OAUTH2 [RFC6749], Authorization in Constrained Environment [RFC7744], SAML ([oasissaml] and [RFC7522]). There are many others: most are based on the providing virtual access to a virtual resource (computer, web resource,etc.) rather than authorizing physical access to a physical resource.

Can the required policies be representing in the existing frameworks? If so, are the frameworks we have sufficiently small as to live within a front door lock? Perhaps a better question is: what is the price point that society is willing to pay for a front-door system which satisfies the various needs of the multitude of stakeholders involved?

8. Privacy Considerations

There is a significant tussle between having policies which are clearly asserted (and auditable) and having privacy for the individuals or groups named.

For instance, it may be entirely appropriate for a front door to make it clear who is allowed access in the event of emergency, such that those people can easily be found. On the other hand, it may be inappropriate for the front door to list one’s current romantic interests as having access. (Such access might even be "aspirational")

A significant mix of abstract identities ("The Superintendant of the Building"), along with pseudonymous identities will be required.

9. Security Considerations

This entire document is about a proposed set of authorization systems.

10. IANA Considerations

This documents makes no IANA Requests.

11. Acknowledgements

Hello.

12. Changelog

13. Informative References

[applefbi] "Apple, Americans, and Security vs. FBI", n.d., <https://www.eff.org/deeplinks/2016/02/apple-americans-and-security-vs-fbi>.

[blazepicking] Blaze, M., "Notes on Picking Pin Tumbler Locks", 7 November 2003, <https://www.mattblaze.org/papers/notes/picking/>.

[communauto] "Communauto Car Sharing", n.d., <https://www.communauto.ca/>.

[fdnymaster] Schneier, B., "Schneier on Security: Master Key", 10 January 2012, <https://www.schneier.com/blog/archives/2012/10/master_keys.html>.

[huffpostkey] Huffington Post, "Daniel Ferraris, Retired Locksmith, Sells NYC Master Keys On eBay", 10 January 2012, <https://www.huffpost.com/entry/daniel-ferraris-new-york-master-keys_n_1928826>.

[MATTER] Alliance, C.S., "Connected Home over IP Specification", 1 July 2021, <https://buildwithmatter.com/>.

[oasissaml]
"OASIS Security Services (SAML) TC", n.d.,
<https://www.oasis-open.org/committees/
tc_home.php?wg_abbrev=security>.

[RFC1984] IAB and IESG, "IAB and IESG Statement on Cryptographic Technology and the Internet", BCP 200, RFC 1984, DOI 10.17487/RFC1984, August 1996, <https://www.rfc-editor.org/info/rfc1984>.

[RFC2393] Shacham, A., Monsour, R., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 2393, DOI 10.17487/RFC2393, December 1998, <https://www.rfc-editor.org/info/rfc2393>.

[RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <https://www.rfc-editor.org/info/rfc6749>.

[RFC7522] Campbell, B., Mortimore, C., and M. Jones, "Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants", RFC 7522, DOI 10.17487/RFC7522, May 2015, <https://www.rfc-editor.org/info/rfc7522>.

[RFC7744] Seitz, L., Ed., Gerdes, S., Ed., Selander, G., Mani, M., and S. Kumar, "Use Cases for Authentication and Authorization in Constrained Environments", RFC 7744, DOI 10.17487/RFC7744, January 2016, <https://www.rfc-editor.org/info/rfc7744>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

[RFC9019] Moran, B., Tschofenig, H., Brown, D., and M. Meriac, "A Firmware Update Architecture for Internet of Things", RFC 9019, DOI 10.17487/RFC9019, April 2021, <https://www.rfc-editor.org/info/rfc9019>.

[tribecar] "Tribe Car", n.d., <https://www.tribecar.com/>.

[zipcar] "ZIP Car", n.d., <https://zipcar.com/>.

Appendix A. Personal Devices

There is an increasing number of devices that a person might have on their person or around them. The list is endless, and goes from step trackers, to watches, to recreational (exercize) heart monitors, shoes, shirts with displays (for fun or for the disco), to intimate devices that might be worn at unusual times.

Some devices may belong only temporarily to a person. For instance, a tread-mill or weight-lifting machine, or even a kitchen appliance. After the user is finished with the device it may need to reset to be ready for the next user.

A kitchen appliance (a blender or microwave) might have only a small number of legitimate users (the members of the household), but when one person is using it, it might remain exclusive.

The same appliance, however, might also be purchased for use in a workplace kitchen, and so the number of legitimate users might range in the hundreds. The users will want the appliance to remember their personalized settings.

The names of the previous users should not be easily divulged, but at the same time, the name of the person who used it should be available to a privileged user (owner), for the case the finding out who broke the device. In this case, it might seem obvious that the device has a privileged owner, and may also have just users. But this interaction may be quite complex, and is subject to a wide variety of locally significant social compacts.

In addition, devices get lent. This could be akin to thinking about there being users vs owners, with the owner always being the one responsible for the device. However, passing on a coffee maker to one’s child who is moving to another city is not always a loan, and not always a gift. Which one it is may not be obvious to the people involved until later on. The parent may forget about it, thinking they have given it away, while the (adult) child might pass it on to a friend. Only when the friend tries to "own" the device, do they find out that the parent is still the owner. Now what? Does the device have to be returned to the parent to physically give away ownership?

If the answer to the above question is no, then does this in essence enable theft? Is this a kind of theft that we need to care about? Does it matter if this is a $50 coffee maker, vs a $600 espresso machine? Or can we even set a meaningful threshold? Theft of a $600 espresso machine might not be a problem for some people, while the loss of a $50 coffee machine might be a rather big problem.

Author's Address

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca