All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Getting around authentication

One of the key components of authorized access, which we seek to facilitate, is determining whether the access is in fact authorized, and doing so quickly and efficiently without interfering with ease of use or slowing the smooth flow of commerce. This process is supported by authentication, the demonstration that a request is authentic (typically as in from an authorized act of an authorized actor).

How it works (in general) today

Starting with original identification, then through the creation of one or more identities to be used for identification, one or more methods of authentication are put in place so that when an act is to be authorized, it can be demonstrated to be from an authorized actor (an identity acts as a surrogate for the actor) by authentication to a desired level of certainty.

It is flawed

Here it is with flaws (and some counters) added:

- Original identification
  - The basis for original identification can be defeated by a doppelganger.
    - If in the hospital at birth or supported by a nation state or similar strong(er than you) actor, essentially impossible to defeat. Brought up as you own...
  - The basis for original identification may be forged or otherwise falsified.
    - It’s a contest of who does it better.
  - The systems/mechanisms of original identification may be bypassed (false positive or negative at use)
- Creation of surrogate ‘identitifiers’
  - Here we really run into trouble. Any surrogate can be faked, replaced, copied, altered, borrowed, or exploited in some way. Here are some examples:
    - User ID
      - Trivial to fake, copy, borrow, and get from all sorts of sources
    - Oops… Note that every other mechanism in general use today is essentially the same. Some sequence of symbols as a surrogate for an actual actor (human or otherwise)
- Association of identities with ‘authenticators’
  - More trouble arises here. Any authenticator can be faked, replaced, copied, altered, borrowed, or exploited in some way. Here are some examples:
    - Fingerprints

- You cannot change them, so once copied, it's all over
- Mechanisms for collection, storage, retrieval, and use readily bypassed
- Lots of false positives and negatives
- Are you willing to lose your finger to protect your Facebook access?

- Retinal prints
  - You cannot change them, so once copied, it's all over
  - Mechanisms for collection, storage, retrieval, and use readily bypassed
  - Lots of false positives and negatives
  - Are you willing to lose your eye to protect your Facebook access?
- Passwords (and phrases, etc.)
  - Mechanisms for collection, storage, retrieval, and use readily bypassed
  - Changing them makes it hard to use them and disruptive
  - The number of them needed to disaggregate risk of one taken may be large
- Voice recognition
  - You cannot change them, so once copied, it's all over
  - Mechanisms for collection, storage, retrieval, and use readily bypassed
  - Lots of false positives and negatives
  - What happens when you get a sore throat?
- Facial recognition
  - You cannot change them, so once copied, it's all over
  - Mechanisms for collection, storage, retrieval, and use readily bypassed
  - Lots of false positives and negatives
  - What happens when you have to wear a mask in a pandemic (or get in a nasty car accident and have to have reconstructive surgery, or have a black eye from a bar fight, or get stung by a bee, or change your makeup, or...)?
- Hardware devices
  - Easily stolen
  - You can be easily forced to use them (making them kidnap you)
- Behavioral characteristics
  - Footfall, how they talk, etc. are all seemingly good, but all can be readily forged against any automated mechanism.
  - Mechanisms for collection, storage, retrieval, and use readily bypassed
  - Lots of false positives and negatives

        - Stimulation and response
            - Sounds exciting, and may be able to differentiate characteristics that are inherent to a previously identified (and tested) individual. For example, color blindness can be detected (but it can also be faked).
            - You can change some of them by training. Which also means you can train someone else to fake it (in almost all cases).
            - Mechanisms for collection, storage, retrieval, and use readily bypassed
            - Lots of false positives and negatives
- Use of authenticators to demonstrate identity to the desired level of surety.
    - Here, we decide not to trust one authenticator (or identifier) and require more than one of different sorts at different times for different acts from different places, which means we have added inconvenience, and have all their flaws of each of the other mechanisms, but perhaps gain something by requiring the attacker to combine multiple attack mechanisms.
    - Or they could just decide to kidnap you and force you to do it for them.

Every time we need to authenticate again we also put the methods and mechanisms at risk. So the more we use them, the less effective they become.

Imperfection guaranteed

At the end of the day, the problem is not actually solvable (to a level of perfection) under any approach anybody has found to date. So the real question to ask (as usual) is what are the tradeoffs? So what are they (or should they be)?

- Horses for courses: Different situations call for different solutions.

Here are a few ideas:

- There are lots of cases where we just don't care about original identification. For example, to sell something to you, I don't have to know who you are. I just need to get paid, and you need to get what I sold you. Indeed you don't have to know who I am either.
- There are lots of cases where authentication as to identity is not really necessary. For example, in an amusement park, if you have to be so tall to be safe on such a ride, we can simply measure your height at the entrance to the ride. You are authorized!

Perhaps we can to start by eliminating the need for original identification wherever possible.

Perhaps we can decide when we really need to know who you are in favor of what you are.

In many cases, possession is all you need to spend money. That's called fiat currency. Paper and coins.

And perhaps we can have physical authentication – once you are there, you can do it. So we do what's necessary to get you authorized and authenticated into a place, and from there it's transparent and automatic. By the way, physical keys for doors are often good enough for protecting our most precious assets – our family members… just saying.

Some ways out?

None of these are new ideas, but perhaps they can start you on the way to understanding how to get out of the authentication problem to the desired required.

- **Your devices know you and each other.**
  - One interesting question is how many different things have to agree before it's good enough. I have a phone with multiple physiological factors it can sense. It also has a location and the mechanisms of the cellular provider(s) to authenticate the device and verify it's location. I can then enter a pattern before use for a higher valued transaction. It also connects to my earpiece using Bluetooth. I also have an electronic car key in my pocket, and proximity sensor capability to allow it to be detected by my car for engine start. At what point is this enough for what purpose? The car key is enough to start the car and get in and out. The phone plus my biometrics plus my earpiece plus my location are enough to do anything I allow it to do on that basis. Why is this not enough? What would I add for something better?
- **Over some thresholds multiple parties must agree.**
  - At some point, a financial transaction (for example) can be made to require multiple approvals. In most companies, there is an approval process with thresholds for spending (money out is limited, but money in is generally accepted in any amount). Specific people in specific positions can spend up to specific thresholds subject to specific approvals. It's part of the work flow. From a security standpoint, the same should be applied to any other potentially serious negative consequence, so for example, something that can disable a manufacturing system and cost the company $1M/hr should require approval by someone who could spend $1M/hr. Of course safety controls my stop the plant from operating automatically, but the surety level associated with those mechanisms should justify the associated consequences of false shutdowns and failure to make true shutdowns.
- **It's all public and a group decision.**
  - When it comes to really staggering amounts of money, the US Federal Government is an example of an approval process with multiple steps by multiple people that have to agree and are subject to punishments and rewards. Now you might not agree to the punishments and rewards associated with spending and not on this thing or that, but clearly it is tough to get things through this system, except of course lots of things get through that seem ridiculous to most of us.
- **Risk disaggregation.**
  - Even if I have $100M (which I don't by the way, so don't bother to kidnap my children for it), there is really no reason I need to be able to spend it all on a shopping trip to the grocery store. Limiting quantities over time with instruments and not putting all your eggs in one basket is the path to slowing the collapse of your empire. Authentication of more people from more places at more times makes it harder to rip the system off.

Conclusions

Horses for courses – many combinations – which one? Let's have a conversation...

