A password you can swallow? Don’t hold your breath

Do you have trouble remembering all your passwords, PINs and identification codes? If you believe the hype, you could soon be swallowing away all your problems with a “password pill”.

But don’t hold your breath for this technology – better alternatives are already available.

News reports have suggested a swallowable device can beam user IDs and passwords to a smartphone or tablet. What they’re talking about is a component of Proteus Digital Health Feedback System, developed by Motorola.

How does it work?

The system has three components:

1. a phone app that you run on your smartphone
2. a wearable patch which monitors changes in skin tension (interpreted as pulse and activity or inactivity)
3. the “ingestible sensor” (aka “password pill”) - a digestible placebo pill containing a small radio transmitter which sends a fixed (and unique) string of 18 bits.

The phone app receives information from the patch by Bluetooth; the patch receives information from the pill by radio; and the pill slowly dissolves in your stomach, using galvanic corrosion (“just like a potato battery”) as a power source.

The pill could only store the equivalent of two keyboard characters. Image from shutterstock.com

But what does the pill send?

18 bits, which is the equivalent of two keyboard characters. So not a password or a medical history.

If we use the bits to represent numbers, 18 bits is equivalent to a bit more than a five-digit number, which would make a reasonably good PIN. Or it could be used as a key code in a remotely-located health database.

The pill was developed to monitor when patients actually take their medication, hence its original name: the ingestion event marker. When the radio signal is detected, the patch tells the phone app the patient has swallowed the pill. When the radio signal stops, the patch tells the phone app the pill has dissolved. That’s all.

Proteus is working on getting US Federal Drug Administration (FDA) approval for pills containing active ingredients. They could be used to detect when a patient has taken too many pills, thereby informing medical professionals of the potential for an overdose.

Image from shutterstock.com

But it’s still unclear how such a product would work. If each pill has a unique code, the patch would detect many signals. However, if all of the pills prescribed to a patient use the same static code, overdoses could go undetected. There may be radio collisions at the patch receiver, where many pills might prevent it from detecting the actual codes. Bad outcome.

The Proteus pill is designed to be digested. That means that it dissolves in your stomach, giving you minutes to use your “password”.

Proteus is also working on a pill which lasts longer – perhaps by adding an enteric coating (designed to resist
stomach acid until they reach the small intestine). Such pills could last up to four hours before they're digested. So the password pill might work in the morning, but after lunch it may be gone. If the 18-bit codes really are unique, you would have to re-key your access system twice a day.

If all the pills had the same code, this could leave consumers vulnerable to attacks. A malicious hacker could stand close to you, record the radio signal on another patch, get the code from the attacker’s own phone app and then use the code to open your car door, house, phone, and so on.

**Implantable chips**

Implantable radio frequency identification (RFID) chips, or microchips, could be a better solution to swallowable pills. The VeriChip, for example, stays in the body indefinitely, contains a 16-digit code and is powered by an RFID reader through a small antenna.

Implantable chips may be a better solution, but they're also vulnerable to attacks. Lightwarrior

But using a 16-digit code rather than a digital certificate, means they're still vulnerable to attacks.

RFID chips have a much larger range – typically one metre, and up to ten with a directional antenna on the reader – so the risk of attack is greater.

**Identity verification**

When security is really important, rotating or one-use-only keys are used to supplement passwords. One-use-only keys (also called one-time pads) are disposable passcodes synchronised with a server (at the place you want to communicate with). The server always knows the next code in the sequence, but it is different every time.

Rotating codes are a similar idea but recycle the codes after a while. Garage doors and some keyless entry systems (for cars) use these codes.

Tokens containing one-use-only keys may look like credit cards with a button and a screen, key fobs and USB plugs (YubiKey). They’re big (compared to Proteus’ grain-of-sand size), but they are reasonably secure, and they keep working for years. Best of all, you don’t have to swallow or inject them.

If that's too much for you, there are smartphone apps which pretend to be tokens. In the future, open authentication platforms such as Google Authenticator will allow many types of tokens to use a common infrastructure, so you only need to carry one device.

For the time being, consider the advantages of old-fashioned passwords: you can change them easily, they’re free, you can write them down (somewhere safe where people won’t find them), they’re always with you (in your mind), and they’re supported by more systems on the planet than any other method of authentication.