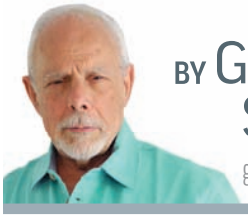
BREACHES SHOW IDENTITY IS KEY



BY GIDEON SAMID
gideon@bitmint.com

CAPITAL ONE IS KNOWN as the "Technology Bank" by its early adopters. It is the last bank at which someone would expect a massive breach. And, indeed, with its 77 million victims, Capital One's breach in March is not even among the top five breaches in the United States.

So why is it so alarming? We are all new migrants into cyberspace, where our identity is reduced to a string of bits. Stolen identity strings may harm us for many years hence, especially if the bits represent immutable data like Social Security numbers or a date of birth.

Financial databases store hundreds of millions of ID strings, and when they are breached it is a cyber catastrophe. So database administrators put a fence around their data. Alas, this fence is replete with gates.

Large financial databases field millions of transactions per day, and may have scores of bona fide user classes. Each user class has to have a tailored set of access rights to some and not other parts of the safeguarded data. To allow the proper users of all classes to have access to the data and keep all others out, the database administrator writes myriad sets of access rules, called protocols. These protocols are smart, elaborate, and represent the defense strategy of the database manager.

How does this strategy get articulated? The database administrator writes a series of (n) attack scenarios, reflecting every imagined way to compromise the data. Each of those scenarios is appraised as to its likelihood. If the likelihood is too high for a given scenario, the access protocols are adjusted to suppress this likelihood to acceptable levels. Security is about suppressing the likelihood of success for a given attack scenario.

The unrecognized truth is that often the hackers have more imagination than the database administrators. They carry out attack scenario (n+1). That scenario will defeat the protocols and lead to massive data theft.

Seasoned and scarred database administrators look beyond the protocol game to consider (i) hardware security, and (ii) de-incentivizing breaches. Hardware security emerged recently when it became clear that most breaches rely to some extent on an inside job. Some key data is then secured in a physical enclosure that either (a) cannot be tampered with without making the breach obvious (Patent #9471906), or (b) is self-destructing upon detection of tampering (Patent #15293352).

A more far-reaching strategy is to remove sensitive data from the digital grid (where hackers roam) and into a nanotechnology-manufactured lump, where the atomic structure reflects the data. That requires access to the physical device, which is pre-manufactured in limited numbers, and resists duplication (Patent #15898876).

A new US patent (#16228675) offers a conclusive way to prevent thieves from benefitting from their breach, discouraging them from breaching again. Here, the private data kept on the server is minutely different from the same data held in the customer's phone. This minute distinction plays no role in normal operation. But if the server is breached and the stolen data is fraudulently used, this minute distinction will implicate the identity thief. Next time, hackers will attack a database that does not use this "gotcha" protection.

Digital money will make a big difference in preventing data theft. Solutions like BitMint (Patent #6823068) fuse value and identity into a bit string, which then can be communicated (paid) cash-like, so no private information is required. Blockchain technology offers a dynamic view of identities to void the ongoing damage from a past breach.

Remember, identity is key. If identities are authenticated by a limited count of bits, someone has a chance to claim to be you. DT