Who Am I and Who Are You?

By Mark Johnson

Mark is a former military intelligence officer, drug enforcement agent, and global head of network fraud and security, now engaged by QA Consulting, the City of London Police, the National Police Chiefs' Council, CIFAS, the International Compliance Association, and MIS Training Institute as a cyber-crime and open source investigations (OSINT) trainer and consultant. He can be contacted at markj@trmg.biz.

I don't know who you are, but I am Mark Johnson. Why should you believe me? Perhaps because I am telling you who I am? Possibly because you are reading this in a trusted publication, sent to you from a trusted source? If I am a customer, an employee, a contractor, or a visitor at one of your sites, your identity and access management systems (IAM) might also tell you who I am, based on the credentials I presented on arrival. You choose to believe that I am Mark because, on the balance of probabilities, it's very likely to be true. But in identity management, few things are absolute. There is always room for error.

What Is an Identity?

Personal Identity. The concept of identity is evolving. One tends to think of people when the word is used, either as individuals, teams, nations, or those sharing common values and beliefs. But the requirements for authenticating people are changing, moving from photos and documents to biometrics and even DNA matching, and people are now only one of the items requiring an authenticated identity in the modern digital world.

Organisational Identity. As supply chain and financial services professionals well know, organisations have identities that require validation, sometimes on an ongoing basis. The recent furore over Huawei's involvement in new 5G network rollouts is one example of how questions about the ownership, culture, and frame of reference that applies to an organisation can affect how it is viewed by others. Before dealing with such companies, we want to authenticate them as being sufficiently like us and therefore trustworthy.

Technological Identity. Billions of machines, many operating without human control or interaction, are already a part of the world we live and trade in. Some of these machines have taken over the very act of trading, while others maintain the temperature in your house or serve as driverless vehicles or other robotic devices that are poised to take on many more roles. But who does this or that machine belong to? Who authorised its presence? Who configured it, who programmed it, who delivered it, and who maintains it? Who might have hacked it? The authentication of devices is a growing challenge that needs to be addressed urgently, before we find ourselves surrounded by increasingly intelligent and knowledgeable machines of dubious pedigree.

> When the state of one entangled particle is changed, the state of its entangled twin also changes instantly, apparently communicating with its pair faster than light speed, which promises new methods of quantum authentication that could prove unbreakable.

Attribution of Technology to a Human Identity. When a child commits a crime, the first question asked is normally, who are this child's parents or guardians? Parental responsibility is a well-established notion. The digital attribution challenge is no different. When a machine errs or acts maliciously, based on the errors or wishes of its owner or user, we will want to know who its parent is. Questions of this nature were among the first to arise during the 2018 drone incidents at one major UK airport; whose drone *is* this? If we fail to address the need for strong attribution between autonomous devices and their owners, we will pay a tremendous price.

Why Is Identity Management Business Critical?

Identity management is business critical because organisations cannot outsource accountability, regardless of what else they have outsourced. This is not a legalistic point; it relates to reputational harm and brand damage, a domain in which perception is reality. In the face of social media as a leading source of news, facts are now less important than memes.

In the same way that we have been forced to rethink the traditional outside-in "onion of security" approach to general security, where layers of protection surround an asset base and protect those assets from external threats, we also need to rethink the model for identity and access management. Yes, IAM will still be essential to ensure that only validated persons access your sites and systems, but IAM is now also required to ensure that your autonomous systems only go where they are supposed to go and only do what they are supposed to do.

Where Is Your Personal Identity Data?

The authentication of people is rendered more demanding as traditional authentication factors continue to leak out of digital storage systems and into the wider online world. One estimate puts the total number of user credentials (usernames and passwords) hacked and shared online to date at 10 billion. This is more than two pairs of credentials for each adult on the planet.

Corporate Databases. Corporate database hacks, often due to shocking failures of security and database administration, are the largest direct contributor to this disaster. Tesco Bank, Marriott, and TalkTalk are just some of the thousands of hacked organisations on the list, and the list is growing.

Big Data. At the heart of the data breach problem is the habit of collecting and storing as much personal and customer behaviour data as possible, rather than keeping only what is required to support specific business operations. This is because the concept of normal operations has been extended to cover relentless data analytics and marketing campaigns. A global failure of regulation and imagination is the underlying problem here, EU General Data Protection Regulation notwithstanding.

Governmental Databases. Surprisingly, a number of governmental systems are equally vulnerable, if not to hacking then to uncontrolled access. Anyone on the planet can, for example, access the UK's Companies House database and search for firms and directors. Because 75 per cent of UK small businesses use the director's home address as their business address, and because directors are often spouses or life partners, this unfettered access is a gold mine for fraudsters, social engineers, and foreign espionage agencies. Similar issues arise from the sharing of post office database records and land registry information with private firms that then make the information easily accessible online to anyone for a nominal fee.

Devices. Devices frequently store your data, and many of them either share this data with device and app developers or fail to protect it when on the device. If you have an iPhone with Siri active, there is a good chance that anyone with physical access to your phone can ask Siri to display your most recent calls, show your calendar, and even discover your home address by telling Siri, "Take me home." Similar issues are widespread and are indicative of a societal and regulatory failure to understand the common-sense fundamentals of good security and the vulnerabilities inherent in digital technology.

How Can Identity Data Be Misused?

Stolen or exposed identity data is exploited in various ways, with the focus usually being monetisation, turning data into cash.

Identity Theft and Fraud. Using stolen data to take over a victim's accounts or to create new accounts in the victim's name is a long-standing technique for monetising stolen credentials, and it continues to this day. What has changed is that an attacker can now create an entire online persona to support the fake account, including Facebook, LinkedIn, Twitter, and similar forms of online presence. Why is this so easy to do? Because sites like these fail abysmally to enforce effective identity access management systems of their own. Even in purely digital systems, IAM is about not only managing access but also validating identity. Social media providers have taken many years to get to grips with this simple principle.

Online Sale. Large sets of stolen credentials are sold online, sometimes via the darknet and also through clearnet sharing sites and social media pages. One Facebook page that featured in a UK investigation offered cloned credit cards for sale for a number of years without being detected or shut down. No attempt was made by the criminal to conceal the nature of his page, which included the phrase "cloned cards for sale" as well as images of cloned cards.

Lateral Movement. If a single username and password combination is exposed, it can sometimes be used to move laterally within the systems used by an organisation. This occurs when privilege access management (PAM) is weak. A good security system marries IAM to PAM in a harmonious relationship.

Credential Stuffing. Stolen credentials are also distributed across infected networks of computers (botnets). Each bot then tries using a small subset of credentials to log in once to a range of sites: Amazon, PayPal, Google, and so forth. Successful logins are reported back to the botnet controller. In this way, long lists of hacked credentials are tested and turned into shorter lists of usable credentials. These high-quality lists can be used by the hackers or sold to fraudsters.

Reputational Harm. Fraud aside, many people would blanch at the idea of every facet of their online lives being exposed publicly. Adult content represents 60 per cent of online searches, online dating is the new normal, and one's political views have never been more closely guarded. Reputational harm is now one of the main risks faced by anyone whose IAM credentials have been hacked and shared.

What Might the Future of Identity Look Like?

We have witnessed a long-term trend in which new factors of identification and authentication have emerged once criminals learned to forge or steal the older ones. There is no obvious reason to suppose that this process of evolution will not continue.

New facets of identity already in use or being tested, but perhaps not widely seen operationally, include the microchipping of humans, finger-vein scanning rather than fingerprint scanning, and new forms of memorable information, for example, a happy memory rather than your mother's maiden name. However, all of these will need to be digitised in some form for storage and processing, and while vendors of solutions are moving away from database storage, using advanced tokenisation, encryption, and/or hashing techniques in their place, no system is 100 per cent secure. Over time, we should expect to see new forms of breach occurring.

The Quantum Challenge to Authentication. One area of research and development well worth keeping an eye on is the application of quantum mechanics to cryptography, both to break existing cryptographic systems and to support new, more powerful encryption and authentication mechanisms. While conceptually simple, quantum approaches require an understanding of aspects of particle physics that can seem daunting to the layperson. We will explore these in an upcoming article, but two of the key features of the quantum world of relevance here are the proven property of particles to behave as both particles and waves, and the potential for particles to become entangled with one another and to maintain that entanglement over vast distances.

The ability of a particle to appear to exist on a spectrum of possible states (neither 1 nor 0 but somewhere between 1 and 0) allows it to be used to perform computing tasks in a way that has the potential to vastly out perform traditional binary computing systems in certain applications. This offers a mechanism for cracking the factorisation challenge upon which modern authentication systems, like RSA, are based. Meanwhile, when the state of one entangled particle is changed, the state of its entangled twin also changes instantly, apparently communicating with its pair faster than light speed, which promises new methods of quantum authentication that could prove unbreakable.

Crossover Threats

Constant change in the digital landscape demands the constant re-engineering of identity and access management solutions and processes. This is a message that loss prevention must convey to stakeholders and budget holders. An analogy is the subverting of keyless entry and ignition by car thieves. We do not want our manufacturing, shipping, warehousing, and distribution channels to suffer a similar fate.

But the loss prevention manager cannot properly assess his or her identity and access management controls if he or she is not already very well versed in how criminals steal identity and authentication data in the first place. This is a key point of crossover between physical and logical security; in today's digital era, all loss prevention professionals need to be comprehensively trained in current and emerging digital security threats and solutions, regardless of their technical background or lack thereof. The digital realm can now reach into your physical world and relieve you of your key assets. ■