Identity in the Internet Age

By Michael Dargue and William Wadsworth

The traditional password model of identity management is no longer fit-for-purpose. Increased security risks and growing consumer frustration have prompted a number of alternatives: multi-factor authentication, biometrics, and federated identity. Online media giants have been quick to enter this market, but opportunities exist for other players to differentiate and capture value.

September 2013
Identity Management: An Inadequate Status Quo

Around the world, consumers, businesses and government are moving more of their transactions and interactions online. Online services can have transformative benefits in efficiency and convenience – for suppliers of goods and services and their customers alike – but weak security practices create a growing risk of identity theft and fraud, increasing the need for secure and reliable identity management.

The familiar model of a unique username and password has its roots in a pre-Internet era, where many users had only one computer to log in to. Such a model may be appropriate for local computers, but it quickly became insecure at Internet-scale, as end-users and system admins have found to their cost. The average user today has 26 online identities, but shares just five passwords across them.¹ If the security of one site is breached, then all accounts using the same password are compromised: the “break once, break everywhere” problem. Worse, many users are choosing simple passwords which are trivial to guess or break through a dictionary attack; one dataset suggests that over 11% of passwords appear on the list of the five most commonly used (see Figure 1).²

With the annual cost to businesses from consumer cybercrime estimated at $110B annually, and 63% of US citizens reporting denied access to an account because of forgotten authentication details, the need for an alternative solution for the Internet age is clear.³,⁴

Why Do We Need Identity Mechanisms?

Before discussing potential solutions to these challenges, it is useful to first consider the objectives of security mechanisms: authentication, authorization, and accountability.

- **Authentication**: Establishing user identity
- **Authorization**: Permitting only authorized users to access protected content and services
- **Accountability**: Establishing a record of an event or transaction

Getting this “AAA” triplet right is essential for consumers – protecting their online bank account, for example – and also for suppliers of online services, who can face considerable reputational risk in the event of security breach, and may also rely on authentication for revenue protection, for example by controlling access to content behind a pay-wall. The level of security provided, and corresponding benefits, will always have to be balanced against the associated costs:

---

¹ Experian, July 2012
² Mark Burnett “10,000 Top Passwords” (http://xato.net/passwords/more-top-worst-passwords/#.UIVaLDZeYpo)
³ Nok-Nok Labs Consumer Attitudes On Online Authentication study, 2012
⁴ Symantec, September 2012
Figure 2: Costs and Benefits of a Secure Identity System

<table>
<thead>
<tr>
<th>Costs</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consumer</strong></td>
<td></td>
</tr>
<tr>
<td>• Inconvenience</td>
<td>• Protection of personal content</td>
</tr>
<tr>
<td>• Loss of anonymity</td>
<td>• Defence against impersonation</td>
</tr>
<tr>
<td><strong>Supplier</strong></td>
<td>• Protection of content and services</td>
</tr>
<tr>
<td>• Implementation costs</td>
<td>• Establishes greater trust in the service</td>
</tr>
<tr>
<td>• Operating costs</td>
<td>• Non-repudiation of transactions</td>
</tr>
<tr>
<td>• Potential barrier to user adoption</td>
<td></td>
</tr>
</tbody>
</table>

Solving the Password Problem

A recent survey found that 38% of people would rather fold laundry and scrub toilets than come up with new passwords. A number of approaches exist to mitigate the risk from password re-use, including multi-factor authentication, biometric identification, and federated security.

Multi-factor Authentication

Multi-factor authentication schemes strengthen security by combining something the user knows (the password) with something the user has (such as a token) and/or something the user is (see biometric identification, below). Pseudo-random code generating devices have been used in this regard, however the inconvenience of carrying and using a code generator (such as a key fob) has limited adoption. While popular in secure enterprise environments, consumer use thus far has been limited: users will only tolerate the hassle when accessing those services needing the highest security, such as online banking. More recently, code generators have been implemented as smartphone apps. The extent to which this promotes wider use remains to be seen.

Biometric Identification

Biometric identification may be used as a component of multi-factor authentication, or on a standalone basis. Examples of biometric signatures include fingerprint, iris pattern, facial recognition and heartbeat. Fingerprint-based technology has been readily available for many years, being featured in laptops from manufacturers such as HP, Lenovo and Sony, while ING Direct Canada, an online bank, has issued customers with computer mice equipped with fingerprint recognition system. Until now, the technology has largely remained a novelty feature outside niche markets – perhaps due to hardware costs and imperfect, unreliable execution. However, Apple’s inclusion of fingerprint authentication in the iPhone 5S could mark the beginning of biometric authentication’s move to the mainstream.

---

3 Harris Interactive: “The 2012 Online Registration and Password” study
Password Management and Federated Authentication

Similarly poised to address the identification needs of the mass market are providers of password management and federated authentication services. Password management applications such as LastPass and RoboForm allow subscribers to recreate the single-password experience of those early computing days: once logged in via a master-password, the application will auto-fill log-in details for all other authenticated sites. Established security service providers have launched similar services, with Symantec bundling “Norton Identity Safe” services at no extra cost as a means of adding value to its anti-virus products.

Federated security approaches such as OpenID enable existing online accounts to be used to sign in to new authenticated-access websites. Online media giants such as Facebook and Google have moved to leverage their vast user-bases (1.11B and 425M respectively) to offer such “federated authentication” services.\(^6\)\(^7\) This model helps the third-party websites lower the barrier to user-adoption by removing the need for yet another password, while the media companies enjoy increased knowledge of user behaviour, enabling yet more targeted advertising to be served to individuals. Such monetisation of identity could almost be said to add a “fourth A” – advertising – to the “AAA” triplet.

The Future of Identity

Federated security and password management are being adopted enthusiastically – with over 50,000 websites accepting OpenID for logins, and RoboForm reporting “millions” of active users – but these services are not yet suitable for providing the high-security, high-reliability authentication demanded by services such as online banking and public services.\(^8\)\(^9\) For such “high-end” services, trusted service providers such as financial institutions, governments and mobile operators may be well-placed to offer identity management services by becoming “aggregators” within their domain, and potentially beyond.

Financial Institutions

Mint.com, a division of accountancy software maker Intuit, offers credit monitoring and personal budgeting services, relying on centrally-authenticated access to all of a user’s online bank and credit card accounts to aggregate transaction and balance information across the user’s financial estate. In the UK, Internet bank First Direct offers a similar service with its “Internet Banking Plus” feature. In future, such portals could be developed to facilitate full access to all of a user’s online banking, credit card, and insurance accounts.

Financial services companies – including banks, providers of credit, and credit score providers – are well-positioned to offer such services given their existing security infrastructure assets and processes, and a “trusted service provider” brand status.

---

\(^6\) Facebook, March 2013
\(^7\) Number of Gmail users, Google, June 2013
\(^8\) OpenID, accessed September 2013 (http://openid.net/get-an-openid/what-is-openid/)
\(^9\) RoboForm, accessed September 2013 (http://www.roboform.com/about)
Government

In the wake of the scramble to move public services online, governments have been working to rationalise their identity management estate. The Netherlands’ “DigiD” service now provides single-password to access over 500 local and national public service organisations, while the US government is working to allow all federal services to be accessed by passwords from approved third parties, such as Google or PayPal, through the “Federal Cloud Credential Exchange” programme.

Other governments – such as Germany, Italy, Spain, Pakistan and Morocco – have adopted the “Electronic Identity Card” or “eID” format: a physical identity card with embedded microchip, allowing both virtual and physical authentication. The world’s first electronic parliamentary elections were held in Estonia in 2007, powered by the Estonia eID card. The European Union’s “STORK” programme (“Secure idenTity acrOss boRders linked”) is working towards a “digital single market by 2015”, allowing recognition of national electronic identity (eID) across the European single market.

A unified, user-friendly approach to public-sector identity not only reduces IT operating costs across numerous government departments, but also drives adoption of online public services, which are often cheaper to provide than their offline equivalent (e.g. a physical or telephone helpdesk).

Mobile Operators and Manufacturers

The mobile phone represents an under-used security asset which is already in the hands of billions of users worldwide. The Subscriber Information Module (SIM) allows Mobile Network Operators (MNOs) to authorize access to services and bill for use, providing a crypto-graphically-protected unique identifier for each subscriber. SIM-based security combines many of the benefits of federated identity, multi-factor authentication, and even biometric authentication, as illustrated in Figure 3.

The revenue potential is considerable.

Turkish operator Turkcell charges 5 Turkish Liras (£1.56, or $2.74) per month for its “Mobil imza” application, which it launched in 2007 to facilitate secure, legally-binding consumer and enterprise transactions. This represents ARPU uplift of 25%. Although adoption is currently low in absolute terms, it has been growing at 80% per year.10

---

10 GSMA, 2012: “Mobile Signature in Turkey”
MNOs and MVNOs are not the only players to be able to take advantage of mobile identity: the latest smartphones contain an embedded secure element, providing SIM-like security, beyond the control of the MNO. This creates opportunities for the likes of Apple, Google, Samsung and Microsoft to develop wider Identity Management capabilities.

**Identifying Opportunities**

For companies looking to monetise their assets beyond their historical core competency, then, Identity Management offers an intriguing strategic option: not only generating new revenue streams, but also increased customer loyalty and brand status. Financial institutions, government, and MNOs are all regarded as “trusted service providers”, and benefit from large user-bases and strong customer-service systems: the ideal foundations on which to build an Identity Management service.

As an increasingly cynical consumer body becomes wary of ceding more control of their identities to media companies who track and monitor their actions to sell adverts, perhaps the world will look to today’s banks, governments, or phone operators to manage the next generation of identity.
Cartesian is a specialist consulting firm of industry experts, focused exclusively on the communications, technology and digital media sector. For over 20 years, Cartesian has advised clients in strategy development and assisted them in execution against their goals. Our unique portfolio of professional services and managed solutions are tailored to the specific challenges faced by executives in these fast-moving industries. Combining strategic thinking and practical experience, we deliver superior results.

Contact us to find out more about how our services can take your business forward in the Identity Management field:

- **Opportunity assessment**: Customer insight, opportunity sizing, competitive assessment
- **Business case development**: Financial modelling, entry option analysis, scenario planning
- **Go-to-market strategy**: Market proposition, pricing, partner and distribution strategy
- **Technical execution**: Business requirements, solutions design, implementation and assurance
- **Data analysis**: Award-winning Ascertain® data analytics platform

[www.cartesian.com](http://www.cartesian.com)

For further information, please contact us at cartesian@cartesian.com