Editorial

Identity is Coming

Leith H. Campbell
Managing Editor

Abstract: This editorial includes some comments on identity management, a necessary addition to the Internet and World Wide Web and a topic of recent discussion in Australia. The editorial also introduces the content of the June issue.

Keywords: Editorial, Identity management

Identity on the Internet

The first Internet Protocol (IP) packets landed in Australia, according to Geoff Huston, in June 1989, so we have now had 35 years of the modern Internet in Australia. With the coming of the World Wide Web and widespread public access, the country has benefited greatly from new services and major advances in business productivity. We have seen the rise of "social media" as a new phenomenon. Along with this, we have also seen a new culture of online abuse and, increasingly, new forms of criminality, such as online scams and identity theft for financial gain. In response, there have been new regulatory actions, such as the Australian Competition and Consumer Commission's Scamwatch and the introduction of an eSafety Commissioner supported by the Australian Communications and Media Authority.

The ease with which the Internet and Web can be used for crime reveals some fundamental flaws in their design. Both started in environments where the expectation was that users, both machine and human, could be trusted. Trust, unfortunately, cannot be assumed in a wider sphere. This has led to numerous "bolt-ons" for security and regulation – but the underlying design issues remain.

A major design flaw in the Internet is the lack of robust identification and access controls. Vint Cerf, an acknowledged parent of the Internet, supports this view:

> "According to Cerf, the biggest flaw in the original design of the TCP/IP protocol was allowing computers to communicate without verifying trust and authenticity of the users attempting to communicate" ("Internet Security", 2019, quoting a Washington Post article from 2015).

Verified identity is not always necessary. If you are an adult just browsing for information – like every speech by Vint Cerf – your identity may not matter. If, however, you are a child using a browser, the fact that you are underage could be used to shield you from inappropriate websites.

When a verified identity is necessary, it is important that the other party in a transaction only receives the information it needs and that other unnecessary information is not passed on. For example, a bank should know that a person is, in fact, the genuine customer it expects; or a social media site should know that a user is under 13 years of age. In these examples, other characteristics, like gender, marital status and employment, are not relevant and should not be part of the transaction.

On the Internet, a user will have one or more identifiers. An identifier may or may not carry real identity information. That is, an identifier is not an identity. Using identifiers carefully can preserve anonymity (or "pseudonymity"), where appropriate, while passing on identity data when necessary (Cerf, 2015). Identity mechanisms, whether for verification or communication, need not, and should not, compromise privacy.

Identity verification methods exist and are being deployed. They may not always be fit for purpose (see, for example, the UK experience at Public Accounts Committee UK (2019)). Whatever their status, these methods will require constant vigilance to keep them up to date when flaws are identified – an inevitable but unfortunate aspect of all software systems. Sadly, flaws are often identified through security breaches with adverse consequences for users and overall trust.

Identity verification will always involve a trusted third party that holds real identity data. This may often be a government. In Australia, the federal government has moved to update the online verification of passports etc. See, for example, Australian Senate (2023) for a discussion of the Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023. In this discussion, identity verification services are defined as:

> "a series of automated national services offered by the Commonwealth to allow government agencies and industry to efficiently compare or verify personal information on identity documents against existing government records, such as passports, driver licences and birth certificates" (Australian Senate, 2023, para. 1.19).

It is important to note that, in addition to identity verification, all transactions within the Internet must be secure, as explained in Cerf (2015). A popular framework for implementing security is Zero-Trust Security. For a description of various levels of maturity in implementing Zero-Trust Security in a specific context, see Ali *et al.* (2022).

In summary, the framework and early applications for providing identity management to make the Internet and Web more secure are now available. Fit-for-purpose identity management is coming. There may be stumbles on the way, but it will provide a more robust platform for network security. It is a necessary transformation to make the Internet and Web better support the digital economy and society.

In This Issue

As usual, the June issue covers a wide variety of topics.

In the Public Policy section, we publish a contribution to the debate on updating the Universal Service Obligation in Australia, *Universal Service for the Twenty-First Century*.

In the Digital Economy & Society section, there are five papers. *Perceived Value and Adoption Intention for 5G Services in India* looks at how environmental awareness affects the take-up of 5G services. *The Effects of Social Media Content on a Firm's Book-Based and Market-Based Performance* considers what is known from the literature on how a firm's online presence affects its performance. *Innovation in Compensation Payments: What Does the Future Hold for Compensation in Cryptocurrency?* identifies factors influencing the acceptance or rejection of salary payments in cryptocurrencies. *Enhancing Customer Relationship Management with Data Analytics: Insights from Retail Survey* uses a survey of retail customers to examine the role of data analytics in customer relationship management systems. *Archery Analytic Workflow in a Web-Based Application* describes a system for analysing player performance in the sport of archery.

In the Telecommunications section, there is one paper, on *Evaluating Signal Quality and System Performance in NB-IoT Communications* with the detailed measurement of narrowband communications in the Internet of Things.

In the Biography section, we publish two items: *Vale Doug Campbell (1939–2023)*, an obituary of Doug Campbell, a senior manager in Telecom Australia and Telstra; and a heartfelt appreciation of *John Costa's 35 Years of Contributions to this Telecommunications Journal*.

Finally, in the History of Telecommunications section, we continue the subject of the Australian East-West Radio Relay System in 1971, this time with a reprint of papers on the topic of *The Australian East-West Radio Relay System Revisited: Thermal Design of Repeater Shelters*.

As always, we encourage you to consider submitting articles to the *Journal* and we welcome comments and suggestions on which topics or special issues would be of interest. Feedback on the current issue would be welcome.

References

Ali, B., Hijjawi, S., Campbell, L. H., Gregory, M. A., & Li, S. (2022). A Maturity Framework for Zero-Trust Security in Multiaccess Edge Computing. *Security and Communication Networks*, *2022*(1), 3178760. https://doi.org/10.1155/2022/3178760

Australian Senate. (2023). Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023 [Provisions] Report. Parliamentary Business, Senate Standing Committees on Legal and Constitutional Affairs. Available at https://www.aph.gov.au/Parliamentary_Business/Committees /Senate/Legal_and_Constitutional_Affairs/IDVerificationBills23/Report. Accessed June 24, 2024.

Cerf, V. (2015). Strong Authentication and Pseudonymity on the Internet. RSA Conference US 2013 Keynote. Available at https://www.youtube.com/watch?v=ZYAJaOVuyxI [Video]. Accessed June 24, 2024.

"Internet Security: How Vint Cerf Might Do It If He Could Start Over". (2019). Byos. https://www.byos.io/blog/network-security-design-vint-cerf. Accessed June 24, 2024.

Public Accounts Committee UK. (2019). Government flagship digital identification system failing its users. UK Parliament, Public Accounts Committee. Available at https://committees.parliament.uk/committee/127/public-accounts-committee /news/98272/government-flagship-digital-identification-system-failing-its-users. Accessed June 24, 2024.