This is the published version of a paper published in .

Citation for the original published paper (version of record):

Magnusson, L. (2012)
A New Authentication Paradigm?
ISC2 InfoSecurity Professional Magazine, 3(17): 24-24

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

Permanent link to this version:
http://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-77420
A New Authentication Paradigm?

WITH THE PROLIFERATION OF THE CLOUD, an old issue has resurfaced: seamless authentication and authorization to remote services. This concern has been around for many decades, with the development of protocols like Kerberos and tools such as IKE and AD. However, none of these protocols truly solved the overall problem.

User-ID/password is without a doubt the single most used and trusted method to achieve authentication and authorization. However, this method has proven to fail more than we would like to admit. Services offered by Microsoft, Google, Amazon and Facebook are increasingly revered by other Web services as trusted, using them as a sort of public key infrastructure (PKI), though all are based on user-ID/password. Why is this?

The answer is administrative simplicity. All other methods require more resources or a higher level of user complexity. The user-ID/password method, despite its unreliability and possibility of user negligence, is cheap—often zero cost, compared to other methods.

Central allocations and revocation are too complex, and the responsible security staffers simply hope the user will not misuse any access privileges. Still, statistics say 80 percent of all IT crimes are internal, reminding us that opportunity often creates the criminal.

In the age of the integrated cloud, perhaps it's time for a paradigm shift—a new multiplatform, authentication technology that would support system owners and allow administrators to maintain access control while utilizing the proper tools (without using external services).

How can this be done? Let's face it; the technology has been around for years, such as private/public keys and PKCS#12 certificates. We just have to tweak some protocols and tools to make this shift. For starters, we can use trusted certificate data to validate organizations. From there, individual keys can link individuals to the organization.

Can it be done? Yes, it can be done. In fact, it already has been done, though most of us don’t realize it. The model design for this type of tool is called Factorum. Factorum was the authentication and authorization process for the AT&T Plan9 Operating System (OS) from the early 1990s. Factorum works a lot like SSH and IPSec public/private key processes, but it’s not a part of the operating system. Rather, it sits on top of the OS, and controls a single user’s access to the complete system. Designed for a distributed, multiserver environment, it supports all protocols we can encounter, not just Web ones.

Plan9 and Factorum are no longer available, but by adding Factorum-like functionality to the current PKI/AD and allowing local and remote systems, as well as protocols like SAML2 to work with public/private keys instead of current identity parameters, we get a simplified functionality. This allows local system owners to control access by distributing public keys and revoking access by deleting the private ones.

By mimicking Factorum’s role-based authorization, we could give the user the right access in the same way local AD installation would be accessed. We could then have a trustworthy, boundless single sign-on authentication/authorization without multiple passwords or costly two-factor authentication tools.

Lars Magnusson, CISSP, is an information security manager in the Swedish automotive industry. He is based in Trollhättan, Sweden and can be reached at l.magnusson@home.se