Brewing a User-Centric Electronic Identity Solution (abstract)

Kal Toth, Ph.D, P.Eng, May 1st, 2015, submitted to PNSQC 2015

The growing popularity of mobile apps, the “bring your own device” (BYOD) phenomenon, cloud computing, and big data, seem to have created the perfect storm for traditional identity technologies and solutions. Service providers - and certain users too - are increasingly aware that the features and benefits offered by an identity solution are worth nothing if a crafty attacker breaks through critical design elements, exposes secrets and private information, and thereby facilitates user impersonation and fraudulent transactions. This paper provides a synopsis of the identity problem (as I see it), discusses essential weaknesses of certain traditional solutions, and proposes what I believe to be critical design requirements for next generation identity solutions. I also highlight the role of software quality engineering in the development of such solutions.

For some time now, I have advocated and refined a user-centric model [21-24] for personal identity to counter certain weaknesses of server-centric identity solutions. Rather than allocating the responsibility for storing and managing personal identities to service providers and applications in the cloud, I have suggested that next generation identity solutions enable individuals to embed their identifying information into their personal devices such as their smart phones, smart cards, tablet PCs, and laptops. Naturally, such an approach opens up many new challenges for the software quality engineer.

Although privacy laws oblige enterprises to safeguard private and identifying information of customers and employees, their record has not been stellar. 2014 was not a good year for big targets like Target, Home Depot, JPMorgan Chase, Athenahealth [1]. We have plenty of evidence that the server-side of the web is rapidly losing ground in its battle against hackers, malware and other forms of electronic abuse.

I believe the root of the problem is that enterprise servers and server farms are, by definition, massively complex, collectively containing virtually all of the identities and private data of our global population. It is no wonder that servers are the primary targets for online hacking, breaches, identity theft, and fraudulent use of identities. In comparison, end-users, numbering 270M in the US alone [3], are collectively much more numerous, are widely dispersed, and are mostly low-yield targets. With the exception of notables like Bill Gates and Warren Buffet, the average return-on-hacking effort against individuals will be much less than that realized by attacking enterprise and service provider repositories. Shifting from a server-centric to a user-centric identity model that strengthens user control over their identities, while reducing opportunities for exploit on the server-side, could turn the tide. Such models have merit and should be widely discussed.

This paper proposes to briefly cover the following topics, relating each to the objective of creating a new identity model that will rely inevitably on best software quality engineering practices:

- Impersonation attack vectors
- How identity assurance relates to authentication assurance
- Weaknesses of traditional password/PIN authentication
- Potential and limitations of single-sign-on and identity federation
- Strengths, weaknesses and potential of public/private key encryption, PKI, and PGP
- Role of multi-factor authentication including biometrics
- Benefits of out-of-band Authentication schemes
- Benefits and limitations of Fast-Identity Online (FIDO)
- Relevance of effective identity proofing and attestation
- Role of trusted execution, trust zones and trusted platform modules
- Role of software quality engineering
- Proposed critical attributes of next generation identity solutions.
References

[15] Gary Blair, SMS-delivered two-factor authentication will be dead in three years, 2007
[29] Fast Identity Online (FIDO) specification: www.fidoalliance.org
[30] FIPS PUB 201-2, Personal Identity Verification of Federal Employees and Contractors
[34] Elliptical Curve Encryption: see http://en.wikipedia.org/wiki/Elliptic_curve_cryptography