

History of SSO - a perspective from the original front lines.

John Haggard
Board of Advisors
Passfaces, Corp.
(www.passfaces.com)
John.haggard@passfaces.com
jhaggard1@leapmail.net



IMMEDIATE IMPACT
SingleSign-OnSummit™
Sponsored by Ping Identity™

My History Related to SSO

- 1982 August 16th join SKK's SSD MVS Team – ACF2/MVS
- 1983 Double DES 370 BAL implementation (evidently 1st to do it, didn't know better, & XDES earned NSA attention/review)
- 1987 my 1st Startup – ThumbScan (Fingerprint Auth), acquired Gordian Systems' Access Key product/patents, failed VC funding
- 1989-94 Product Owner for CA's SCA (ACF2, Top Secret, Examine, VMAN, Pan Audit)
- 65% of World Mainframe Market, Represented 67 Registered User Groups Internationally (1992)
- 1994-2000 – President, COO, & CTO VASCO Data Security (ThumbScan/Gordian)
- Currently Board of Advisors for Passfaces for Graphical Password Authentication

SSO - A Story of Extremes

The history of SSO is a story of extreme complexities, compromises, vulnerabilities, and unintended consequences.

SSO is a story of one simple objective - to “spin off” units of computation work to execute on behalf of an authenticated user without requiring the original user’s password.

First, Steve Martin

SSO is like Steve Martin's joke "So you want to be a millionaire? That's easy. First, you get a million bucks..."

This could easily be "So you want a secure SSO system? That's easy. First, you get an authenticated user..."

MEMORANDUM

To: Technical Directors
From: John Haggard
Date: January 12, 1994
Subject: CA's response to IBM's Secured Signon SPE (PassTicket)

... "Neither technology addresses the initial validation of a user's identity." ...

Comments Re: Strong Auth.

- *User remembered passwords simply do not count as “First you get an authenticated user.”*
- *Users, by their very nature, will compromise ANY reusable password*
- *SSO’s without strong authentication is begging for extreme vulnerabilities*
- *Phishing has always been completely avoidable – just ask ABN-AMRO Bank, SE-Banken, ING, and other EU Banking Institutions*

US Gov. Guidelines for Passwords

- *FIPS Pub 48 - “Guidelines on Evaluation Techniques for Automated Personal Information” 1977*
- *NEBS Special Publication 500-9, “The Use of Passwords for Controlled Access to Computer Resources” Helen M. Wood May, 1977*
(http://eric.ed.gov/ERICDocs/data/ericdocs2sql/content_storage_01/0000019b/80/35/7c/c3.pdf)
 - *P. 9, “There are three basic methods a person’s identity may be authenticated...”*
 - *P. 20 “All passwords and authentication data shall be stored in an irreversibly transformed state.” Bushkin, Arthur*
 - *P. 20, “R.M. Needham is credited with being the first to recognize the vulnerability of password lists.” Created “one-way cipher” concept*
- *DOD Password Management Guideline (Green Book) – Sheila L. Brand, Jeffrey D. Makey April 12, 1985*
 - *Sec. 3.0 Definitions – “System Security Officer (SSO)...”*
 - *Sec. 4.1.2.1 Preventing Exposure - “It is recommended...to prevent exposing a user’s ...password to the SSO.”*
 - *4.3.1 Internal Storage of Passwords - “reading it could result in disclosure of password...”*
- *FIPS Pub 112 – “Password Usage” May 30, 1985*
- *DOD Trusted Computer System Evaluation Criteria (Orange Book) – Sheila L. Brand December 1985*
- *NCSC Trusted Network Interpretation (Red Book) – July 1987 (Stephen Walker TIS & Gauntlet & Robert Morris , father of Robert Tappan Morris of Worm fame)*

Back to SSO Roots & SPA

- “... **one** simple objective - to “spin off” units of computation work to execute on behalf of an authenticated user **without requiring the original user’s password**”
- **Single-Point Authentication** would have been a better description at that time. **Single Sign On, implies interactive user signon process bypassed**
- “Units of computational work” referred to:
 - “batch jobs” then
 - today this would be SOA, or Web Services
- Same objective applies, “execute on behalf of ... user without user’s password”

SSO Historical Rational

- *Rational not born out of concern for:*
 - *Users*
 - *Administrators*
- *Rational was born out of concern for password disclosure*
 - *Passwords were being stored in JCL decks in partitioned data set (PDS) files*
 - *User passwords were desired to be left only in the heads of the user, never written down, never stored in a file (including the security system), and **NEVER** in resident system memory (core dumps)*
 - *Re-transmitting a password so it could be reconstructed or worse not reconstructed, was simply not acceptable*

1st Pass

Logonid Inheritance

- *In the ACF2/MVS world circa 1982, we used terms such as:*
 - “System Entry Validation” or SEV (SVCA for those oldies in the crowd)
 - “Spawning a job”
 - “Submitter’s ID”
 - “Propagated/Inherited”
- *In general terms, SSO was known as “Logonid Inheritance”*
- *The objective: submit a batch job (spawn) on a user’s (submitter) behalf (SEV inheritance) to run in a new MVS Address Space without a password being used (logonid inheritance)*
- *Goal Accomplished by ACF2 - “spin off” units of computation work to execute on behalf of an authenticated user **without requiring the original user’s password**”*
- *Passwords not compromised*

2nd Pass

Network Logonid Inheritance

- *“Units of work” (jobs) transmitted via NJE*
- *1983 ACF2 used NJE Headers (valid interface) to communicate identity of unit of work*
- *First use of one way password cipher text to replace clear text passwords for network validation*
- *First exploration of commercial strong authentication solutions due to rejection of “advanced” password enhancement requests from customer base*
 - *OTP (**Gordian**, Enigma Logic, SDTI), Retina, Fingerprint*
 - *EUA (Extended User Authentication) Exit Facility*
- *No compromises, but no takers on EUA facility*

3rd Pass

VTAM Session Managers (SM)

- *Mid 80's productivity tools arrived for enabling multiple concurrent "sessions"*
- *Typically not security minded, but productivity minded*
- *Scripted/replayed captured userid/password pairs*
- *Beginning of SSO as users knew it – sign on once and be "auto signed on"*
- *Compromises start to be made*
- *SKK's position on compromises – Exits and Usermods*

4th Pass

VTAM, SM, & 3270 Emulators

- *Late '80's and early '90's PCs provided platform for intelligent session management from the desktop (HLLAPI Interface for 3270 data streaming and "screen scraping")*
- *SSO assistance from:*
 - *CA's "Token" (1989) & CA's SECNET (1992)*
 - *IBM's APPC Persistent Verification (SNA LU 6.2) (1991)*
 - *OSF's DCE 1.0/1.1 (Kerberos & TGT) 1992*
 - *IBM's OpenEdition (POSIX with DCE) 1993*
 - *IBM's PassTicket (1994)*
- *3rd party vendors begin to emerge to address new Single Sign On (SSO) market*
- *Wheels getting wobbly on SSO integrity*

5th Pass

Multiplatform Access

- *Sysplex, LANs, WANs, and everything you can think of became connectable via Session Manager Products*
- *APPC (SNA LU 6.2) Persistent Verification (1991)*
- *Remote Dial-in (RADIUS) products backed up the system entry perimeter to NAS (Network Access Server)*
- *MVS isn't sole dominating business platform*
- *"Glass house" shattered*
- *Client/Server paradigm begins*
- *Depending on point of view, SSO either "got wheels" or the wheels fell off*
- *Everybody and every system is disclosing passwords*

6th Pass

HTML and Stateless Access

- *“Signed On” is not possible in stateless environment*
- *RADIUS Authentication Servers become important*
- *Authentication Servers in general become important (Kerberos)*
- *SSL re-establishes virtual session due to privacy concerns*
- *Cookies give users (de)illusion of a “session”*
- *PKI is born and promises SSO with SSL 3.0.*
- *Directories are born*
- *Identity Management is born*
- ***Time to rethink everything***

State of SSO Since mid - 90's

➤ Extreme Complexities

- *Scripting, Tickets , and proprietary “Tokens”*
- *Standards didn't have Standards – Kerberos V4 – V5 (OCSG → CyberSafe)*
- *Centralized, Decentralized, and Directories (DDB, CPF, etc..)*
- *POE, Source, and/or Path becomes source of major headaches*
- *Trust – what is “trust?” Source (geography), Path, Time of vouching (minutes of token issuance), Usage (one time tokens), Keys (symmetric/asymmetric)*

➤ Extreme Compromises

- *Buskin and Needham's irreversibility of passwords abandoned*
- *JCH January 12, 1994 “theoretically, CA's token processing can be attacked, however the effort to do so would be extremely expensive.”*
- *JCH “neither technology (IBM's & CA's) addresses the initial validation of a user's identity”*
- *End user convenience/pampering trumped security – especially in US*
- *“Pretty Good Privacy” actually was a catchy marketing name that was used – sign of the times*

State of SSO Since mid - 90's

➤ Extreme Vulnerabilities

- SSO without Strong Auth. is, and always will be, *simply nuts*
- Large (very large) financial institution rushed to close SSO induced exposures

➤ Unintended Consequences

- Passwords would be plastered everywhere - *by the trusted system(s)!*
- Password Management would get worse, not better (scale)
- SSO weakens, not strengthens integrity of computing systems
- "Something you know" was NEVER intended to be used this way
- Reliance on "something you know" verses systems generated credentials inhibited technology, such as SAML, from developing properly decades ago

SAML, SOA, and Viral

➤ SAML gets SSO right – finally

- *Web 2.0/SOA far too complex for password based credentials to keep up*
- *Existence of standardized dialect (XML) set stage far beyond PKI*
- *Peer reviewed as trusted*

➤ SOA or Web 2.0 Services is too lucrative/enticing to pass up, allows Federation of systems far beyond EDI

- *SaaS exposes different economic choices in computing services*
- *New Legal agreements/frameworks required anyway*

➤ SAML is Viral

- *Buy in begets buy in*
- *But, will enterprise vendors sour the standards via lock-in and/or poor R&D investment?*
- *Pure Play SAML vendor would be most likely to keep eye on the ball, without old code baggage*
- *Weight of SAML would become proportionally lighter with SOA infrastructures*
- *Alternative is to stay stuck and/or locked out of community*

Historical and Personal Comments

SKK far outpaced IBM's ability to innovate and lead in the enterprise security market precisely because SKK was a "pure play" that valued; independence, single focus, purity of security technology, and most importantly "love of the game." Simply put, we loved it.

Look for the same traits in your SAML providers and reward them. Also don't forget the joke.