HENRY B. HOTZ

818-400-6075
hbhotz@oxy.edu

SUMMARY:
Now doing independent consulting on cryptosystems and securing network services.

Created and maintained the central authentication service for JPL identities in a DevOps environment. Provided it with cryptographically strong interfaces. Previous positions included testing and operating critical spacecraft activities, as well as managing several test and development facilities.

Expertise:
- System Architecting and Engineering.
- End-to-end Software Development Life Cycle from requirements to design to implementation, testing, deployment and support of systems.
- Resolving/optimizing conflicting requirements.
- Application of Commercial technology to traditionally custom development problems.
- Management and coordination of cross-organization activities.
- Enterprise Identity Management and Utilization.

Computer specific expertise includes knowledge of:
- Identification and authentication technologies, including all types of One-Time-Passwords, Kerberos, SAML, X.509, PKI, and smart cards.
- NIST and IETF Security frameworks and standards.
- Networking protocols.
- Identity Systems Integration (e.g. between Active Directory and Unix).
- Computer Systems Integration and Administration.
- Cryptography, computer arithmetic and numerical analysis.

Within the last few years I have directly worked with all of the following: MacOS, Solaris, Linux (RedHat and Debian), LDAP, OpenLDAP, Sun/iPlanet LDAP, FreeIPA, NFS, AFS, Apache httpd, Tomcat, PHP, C, Java, JavaScript, Databases, MySQL, PostgreSQL, Git, OATH, HOTP, TOTP, FIPS-201/PIV/NIST 800-73/ISO 7816, OpenSC, RADIUS, Heimdal, MIT Kerberos, ASN.1, OpenSSL, TLS/SSL (with and without client certificates).

PROFESSIONAL EXPERIENCE:
Self-Employed
August 2014 to present, Consultant and Developer
Improving the security of network services, especially those which cannot be hidden by a firewall, or other network-level protections.

Jet Propulsion Laboratory, Pasadena, CA 91109
2003 to 2014 Senior Cyberidentity Engineer

Maintained a perfect 1.0 availability record for the service. Record was achieved with a combination of systematic pre-deployment testing, aggressive failure analysis, redundancy, and the design of comprehensive service monitors with automated responses.

Ongoing consultation on security issues for the Mars Exploration Rover project since 2011.

Provided customer support as needed for using JPL's authentication services. Contributed to the open source support for Kerberos and security in Web, database, email, and LDAP servers.

Separated the primary JPL electronic identification service from the AFS file service, upgraded it to current Kerberos 5 protocol levels, and integrated it with LDAP and RADIUS. Performed four subsequent bug-fix and enhancement upgrades. I was directly responsible for all process phases from requirements specification to implementation, testing, deployment, and maintenance.

- *PKI/Kerberos Integration*
  Published guides for using PIV (NIST 800-73) smart cards for authentication (Kerberos) and document signing (Adobe Acrobat), which reduced the need to support other PKI services.

  Completed smart card and PKINIT support in Heimdal and deployed to production. Provides support for PIV smart cards as an alternative to passwords.

  Author of the KX509 Internet RFC. PKINIT allows acquisition of a Kerberos ticket using an X.509 certificate on a smart card. KX509 allows the acquisition of an X.509 client certificate using a Kerberos ticket.

  Demonstrated PIV card provisioning using open-source tools. Recommended JPL stay with commercial products for better integration with other systems.

- *Critical and Flight Project Support*
  Expanded critical flight operations use of central identification services.

  Designed, and helped deploy, the combination of RSA tokens with Kerberos used by the Mars Science Laboratory project since before landing. It provides One-Time Password security for initial login, with single-sign-on ease of use thereafter.

  Evaluated how security is done for the ground support functions for JPL's flight projects, in order to bring them in line with FISMA/FIPS/NIST requirements. Support for PIV smart cards is being added as a result.

  Supported upgrades to JPL's spacecraft command system to use the central Kerberos service to authenticate the parties operating it, increasing the security of the system.

2002 to 2004 Ground Data System Test Engineer for Spitzer Project
Resolved ITAR and security issues necessary to use the South African tracking station at Hartebeesthoek via the open Internet. Managed testing of the entire downlink telemetry processing chain, including all off-site connections. Revalidated several delivered Ground Data System versions after the Launch version.

<u>2001 to 2002 Downlink System Engineer for SIRTF Project</u>
Resolved several long-standing problems with data content and delivery (through Firewalls).
Prepared downlink training video and process descriptions for personnel added later.

<u>Prior to 2001 at JPL</u>
Validated two of the twelve technologies (K-Band telemetry, and Beacon Monitoring) tested
during DS1s mission. Note that Beacon Monitoring is now in use by the Applied Physics Lab's
Pluto mission.

Primary engineer for the Demand Access Automation Continuous Improvement task for the
Deep Space Network which defined mission operations so no routine operations personnel and
minimum of tracking time were needed. The system was selected for testing and validation on
the DS1 Project.

Various positions with the Radio Science experiments on Voyager and other projects.

LORAL/Librascope Corp, Glendale, CA
<u>Scientist and Mathematician</u>
Lab Manager for Librascope's Advanced Technology Lab, a classified lab used to develop AI
software for Combat Control Systems for DARPA. Developed optimized target tracking
algorithms.

DEGREES:
B. A., Occidental College, Math/Physics double major.
M. S., University of Southern California, Computer Science.

HONORS: Nominee member of A. M. S., and Sigma Pi Sigma.
Space Act Award for Beacon Monitor Operations Software
Group achievement award for the "DS1 Rescue Team" following the star tracker failure.

SELECTED PUBLICATIONS:
RFC6717, *kx509 Kerberized Certificate Issuance Protocol*, http://tools.ietf.org/html/rfc6717.

Invited presentations at the MIT Kerberos Conference, 2009 and 2010.

Henry B. Hotz, "Introduction to HSPD-12 Smart Card Badges", *SAGE Presentation*, July 23,
2008.

Annual presentations at *AFS & Kerberos Best Practices Workshop*, every year it was held
(except 2009, due to a family health issue).

GSSAPI/Kerberos Support for PostgreSQL. March 2007, http://www.postgresql.org/message-
id/41EE2D08-CBC0-47AF-8380-EA0E7D26FD67@jpl.nasa.gov

R. Sherwood, J. Wyatt, H. Hotz, A. Schlutsmeyer, M. Sue, "Lessons Learned During
Implementation and Early Operations of the DS1 Beacon Monitor Experiment", *Third*

International Symposium on Reducing the Cost of Ground Systems and Spacecraft Operations, Tainan, Taiwan, March, 1999.

Earlier publications included several on the atmospheres of Venus, Mars, Jupiter, Titan, Saturn, and Uranus. Work done at Librascope was classified or proprietary.

CLEARANCES: NAC-I (National Agency Check with Interviews)
Secret, not currently active.

MEMBERSHIPS: IEEE
IETF

CERTIFICATIONS: CISSP