MICHAEL STRÖDER

Klauprechtstr. 11
D-76137 Karlsruhe, Germany
Phone +49 721 8304316
michael@stroeder.com
http://www.stroeder.com/

OBJECTIVE

A contractor position as a consultant for planning and implementing identity and access management (IAM), security infrastructures (PKI, directory services) and related applications.

CAPABILITIES

- Planning / designing architectures and implementing mechanisms for secure usage of IT services (PKI, SSL, S/MIME, VPN, LDAP, Identity & Access Management (IAM), Single Sign-On, Firewalls)
- Designing, implementing and automatically installing/configuring (DevOps) secure software (e.g. web applications), object-oriented software design and programming (e.g. Python)
- System integration and user management in large and complex environments
- Training and workshops

EXPERIENCE

Transport / mobility group (11/2018..02/2019)

- Trouble-shooting / performance tuning of Samba file service and sssd integrated with MS Active Directory on CentOS
- Implemented ansible roles, modules and plugins for automated CentOS configuration based on group-wide security guide-lines (base OS, automated domain join, Samba, Apache HTTP server, DHCP server)
- Implemented OpenLDAP server as backend for DHCP with integrated authentication with MS Active Directory
- Configured LDAP integration of vCenter Server Appliance (VCSA)

IT Company (10/2018..11/2018)

- Compared four IAM products
- Created evaluation matrix and product overviews document

Implementation of free software project Æ-DIR (03/2018 .. today)

- Implemented various components with Python
- Custom NSS-/PAM service *aehostd* for Linux/Unix logins
- Specific hardening , e.g. with *AppArmor* profiles
- *ansible* roles for automated installation and configuration of all the components

International Internet Service Provider (12/2017..02/2018)

- Designed and implemented custom certificate authority issuing short-term SSH certificates for secure SSH logins
- Implemented HSM integration via PKCS#11 and integration of multi-factor authentication

IT Company (03/2016..12/2017)

- Identity and Access Management (IAM) for internal users and customers
- Setup and customizing Æ-DIR with multi-factor authentication (OATH-LDAP)
- Implemented various complex ansible roles

International Internet Service Provider (04/2012..11/2015)

- Setup a complex server infrastructure for a proprietary highly secure messaging system
- Installation and configuration of OpenDJ-based public directory service for customer data, later migrated this system to OpenLDAP
- Designed and implemented OpenLDAP server for authentication and authorization of system administrators, also used as backend for Samba and TACACS+ servers
- Designed special LDAP schema and set-based OpenLDAP-ACLs for fine-grained and highly secure access control for admins accessing various server groups
- Customized web2ldap for the maintenance of user, group, server and SUDO entries
- Set up various cryptographic systems for PKI, encryption and digital signature
- Implemented automated installation/configuration of the various services with Puppet 2.7
- Implemented various monitoring checks for a monitoring system based on check_mk
- Prepared security audits
- Designed data format for providers exchanging mail routing information for mandatory use of STARTTLS
- Designed and implemented internal PKI based on EJBCA
- Designed and implemented integrated 2-factor-authentication with OpenLDAP and yubikey (OATH-HOTP) for Linux login and various web applications/appliances
- International Logistics Group (01/2011..03/2013)
- Design and installation of OpenLDAP-based directory service for project-internal user management
- Designed and implemented various tools and small web applications with Python, customized web2ldap for administrating user, group and organizational LDAP entries
- Integrated various systems and applications with LDAP-based login and authorization (Jira, Confluence, Mediawiki, SharePoint, SVN)

Financial Institute in Frankfurt (06/2011..08/2011)

- Schema design and installation for OpenLDAP as a base for LDAP-based user login with CAS
- Implemented delta-synchronization of user and organizational data from Oracle DB to OpenLDAP in Python

National Government Agency in Germany (12/2010..07/2011)

- Design and installation for a migration from Novell eDirectory and DirXML to a solution based on OpenLDAP
- Implemented delta-synchronization of user data from Novell eDirectory to OpenLDAP in Python

International Logistics Group (10/2009..06/2011)

- Security consulting for proprietary messaging system with encryption and digital signature
- Coaching the developers, reviewed software
- Configuration of nCipher HSMs

National Government Agency in Germany (06/2009..10/2009)

- Design and pilot installation for a migration from Novell eDirectory and DirXML to a solution based on OpenLDAP
- Implemented pilot for user data synchronization from MS AD to OpenLDAP in Python

Financial Institute in Stuttgart (10/2007..03/2009)

- Designed Single Sign-On for web applications
- Implemented pilot installation of Central Authentication Service (CAS) with authentication based on MS Active Directory via SPNEGO/Kerberos or LDAP
- Implemented user account synchronization between PostgresQL database, MS Active Directory and Lotus Domino

Federal Government Agency in Baden-Württemberg (12/2005..today)

- Design, pilot installation and documentation of OpenLDAP-based directory service as central repository for abstract roles and application-specific authorization data
- Described processes, interfaces and use-cases for delegated user management

International Pharmaceutical and Chemical Group (02/2006..11/2007)

- Designed and installed a PKI tightly integrated with Lotus Notes for securing e-mails with S/MIME
- Pre-study for group-wide PKI for Windows Smartcard Logon and file encryption including cost estimation, milestone planning etc.
- Designed and installed concern-wide PKI
- Wrote a certification practice statement (CPS) compliant with RFC 3647 for public part of the PKI

Air Cargo company (02/2007..04/2007)

- Pre-study including conception and cost estimation for a single sign-on to web-based B2B-applications
- Documentation for existent applications

International Telecommunications Group (09/2005..04/2006)

- Re-design and pilot implementation of data synchronization processes for group-wide directory service.
- Evaluation and performance testing of LDAP server products (interoperability and performance tests)

International Logistics Group (09/2003..06/2005)

- Designed X.509-based PKI infrastructure enabling retail systems to use digital signature for secure archival of posting data
- Designed architecture for secure authentication and single sign-on at sales point systems using smartcards
- Designed concept for managing users of retail systems even when systems are offline most of the time including syncing with HR systems
- Resolved security-relevant topics related to accountancy with auditors

International Telecommunications Group (11/2002..09/2003)

- Designed registration, self-administration and recovery procedures for Entrust-based PKI architecture

- Documented experiences of integrating web and desktop applications with Entrust security architectures in a best-practice guide („cookbook“) for other projects following
- Integrated X.509-based single sign-on solution (Entrust TruePass) and the LDAP-based user management into a web application
- Coaching of Java developers, workshops for administrators

International Pharmaceutical and Chemical Group (09/2001..05/2003)

- Designed specific public-key infrastructure for issuing certificates used e.g. for SSL servers and machine entities. This work included defining the certificate profile, writing the PKIX compliant certificate policy (according to RFC 2527) and certification practice statement and designing the software.
- Evaluated PKI products (Entrust and RSA Keon) in pilot project for VPN, single sign-on, S/MIME e-mail.
- Designed, implemented and tested a corporate-wide LDAP directory (iPlanet Directory Server) for single-password user authentication. This system was designed as a central user store for internal and external users of web-based e-commerce applications and various other systems.
- Designed and implemented process for synchronizing user data stored on a mainframe with LDAP directory (DB2 on S/390, based DB2 Connect on Linux)
- Setup LDAP-backend for profile store of a web portal product, implemented synchronization process for user data stored in Domino/LDAP
- Conducted in-depth analysis of the security mechanisms of Netegrity Siteminder and integrated it with LDAP directory service of user management

Various activities since 04/2001

- Consulting for unified user management process and centralized user LDAP directory for internal and external users at an international textile group.
- Designed and implemented centralized, LDAP-based address book for the municipal administration of Karlsruhe. Integrated web content management system (ZOPE) with user management of Lotus Domino via LDAP.
- Held various LDAP workshops (basics, application-programming coaching).

emagine GmbH, Eschborn, Germany (10/2000 until 04/2001)

- Designed PKI-related software providing value added service to financial B2B applications (e.g. Identrus compliant applications).
- Designed concept for more general certificate workflow handling with arbitrary certification authorities for a *Registration Authority* server.

Propack Data GmbH, Karlsruhe, Germany (05/1996 until 09/2000)

- Introduced, planned, installed and maintained various Internet services for internal and external communication needs which highly improved the productivity by providing an integrated concept based on open protocol standards in a heterogeneous computing environment.
- Designed and set up a firewall which fulfilled the company's need for a highly secure internet connectivity.
- Established a public key infrastructure with an own certificate authority for securing the usage of Internet/Intranet services with encryption techniques (X.509, S/MIME, SSL, VPN).
- Installed a IPSec-based virtual private network (VPN) for reducing the communication costs by transferring the corporate IP traffic securely via the Internet.
- Introduced and deployed a directory service (LDAP) providing relevant corporate information (e.g. phone book, mail addresses, certificate data) and serving as a base for a single sign-on user

authentication system.

- Implemented several LDAP clients for using the LDAP directory in various services.

Various projects as software engineer for industrial automation and quality control (1992-1994)

OPEN SOURCE

Various free software projects are also used in customer projects:

- Æ-DIR - Authorized Entities Directory (see https://ae-dir.com/)
  Designed and implemented highly secure identity and access management especially for privileged access (IAM, PIM, PAM) based on OpenLDAP
- web2ldap (see https://web2ldap.de/)
  Designed and implemented a web-based LDAPv3 client for comfortable and secure access to LDAP servers with full support for sub schema, DNS SRV records, efficient group administration, etc.
- OATH-LDAP (see https://oath-ldap.stroeder.com/)
  Designed and implemented a OATH-based authentication system with LDAP server used as backend for HOTP / TOTP validation
- python-ldap (see https://python-ldap.org/) until 12/2017
  Developer and long-term maintainer of module package for LDAP programming with Python.

EDUCATION

Dipl.-Inform. (comparable to M.S. in Computer Science) at the University of Karlsruhe, Germany (Degree January 1999)

- Diploma thesis:
  "Introduction and Deployment of cryptographic Technologies for secure Usage of Internet Services at Propack Data GmbH"
- Relevant Courses:
  Telematics (Computer Networks, Distributed Systems), Interactive Systems, Performance Analysis, Automation Systems

TECHNICAL SKILLS

Data encryption and PKI standards:
SSL, TLS, S/MIME, X.509, PKIX, IPSec, OpenPGP, DKIM, DNSSEC/DANE

Authentication techniques:
Passwords including syncing passwords, OATH-HOTP/TOTP, Kerberos, SPNEGO, SASL, X.509 client certificates, PAM for Linux/Solaris, RADIUS, TACACS+

Security products:
Entrust Authority, Cybertrust UNICERT (formerly Baltimore UNICERT), Windows Certificate Services, Lotus Domino CA, RSA Keon CA, Netegrity Siteminder, OpenSSL, OpenSSH, Central Authentication Service (CAS), Thales nCipher nShield/netHSM, EJBCA, FreeRADIUS, FreeIPA, AppArmor

Directory services:
OpenLDAP, OpenDJ (OpenDS), iPlanet/Netscape/SunONE Directory Server, Novell eDirectory, MS Active Directory, MS ADAM, IBM/Tivoli Directory Server, CA eTrust Directory, Critical Path, Siemens DirX, Lotus Domino/LDAP, Fedora Directory Server

E-mail services: postfix, sendmail, qmail, fetchmail, dovecot

Web services: Apache, Tomcat, nginx, Squid, uwsgi, FastCGI, SCGI, WSGI

File server: Samba (SMB/CIFS), NFS

DNS & DHCP: PowerDNS, bind9, nsd, unbound, isc-dhcpd

Operating Systems:
Linux (openSUSE, SLES, RHEL, Debian etc.), Windows NT/2000/XP/2003/2008/2012, Solaris, OS/2, MS-DOS

Software development and configuration management:
Python, Shell-Scripting, HTML/CSS, Version control with git, Subversion and CVS, Jira, Bugzilla, Trac, Pascal, Modula-2

DevOps / config management: Puppet, ansible

Documentation tools:
Confluence, Mediawiki, Trac, T-Wiki, Foswiki

Hardware: Knowledge of PC hardware and basic knowledge of embedded systems

Virtualization: VMWare workstation, Virtual Box, QEMU/KVM, libvirt

REFERENCES

Available upon request.