Likewise®

LPC 2010 - LINUX MULTI-TENANT FILE SERVERS | 03-Nov-2010

Gerald (Jerry) Carter

<gcarter@likewise.com>, <jerry@plainjoe.org>

- Director of Engineering, Likewise Software
- USENIX Association Board of Directors (’08 – ’10)
  - Instructor from ‘98 – present
- Former Samba developer (‘98 – ‘09)
- Past companies include VA Linux and HP
- Authored books for O’Reilly and SAMS Publishing
- Musician, Runner, Gamer, blah blah blah …

Outline

- Define the problem – What is multitenancy?
- Overview of the Likewise File Server and Security Authority
- Multi-Domain State Management
- Remaining and future work

Multitenant Use Cases

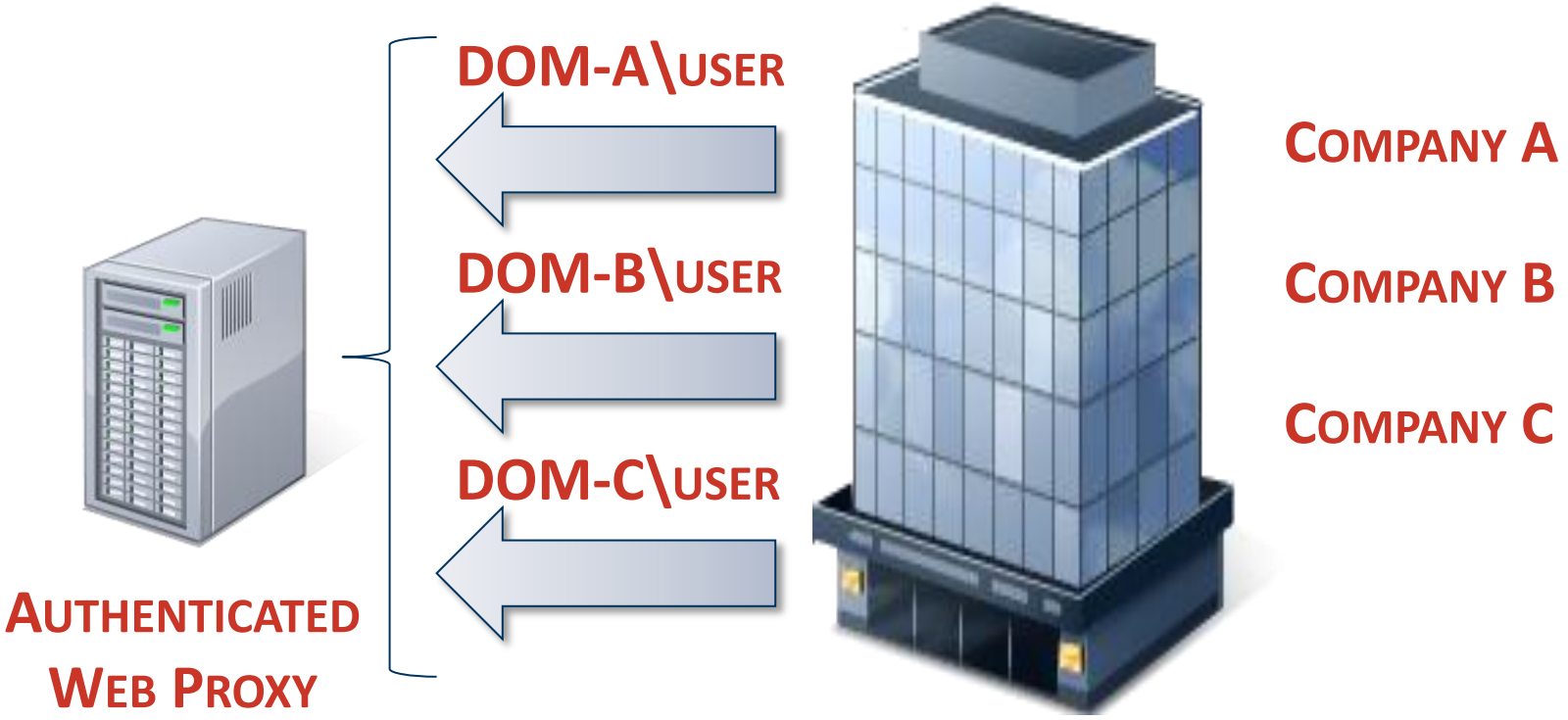
- Use case #1
  - Network device required to lookup and authenticate users from multiple, non-trusting Active Directory domains.
- Use case #2
  - File server required to lookup and authenticate users from multiple, non-trusting Active Directory domains.
- Use case #3
  - File server consolidation. I.e. virtual servers.
- Use case #4
  - IP based file server configuration and migration within a cluster.

Multitenant Solutions

- Solution #1
  - Join device to multiple AD domains and route requests to the correct provider instantiation.
- Solution #2
  - Provision a multi-homed host and bind each NIC (or VIP) to instantiated computer account with AD.
- Solution #3
  - Server consolidation roots using MS-DFS.
- Solution #4
  - Full configuration and instantiation abstraction

Multi-Domain Example

Authenticated Web Proxy



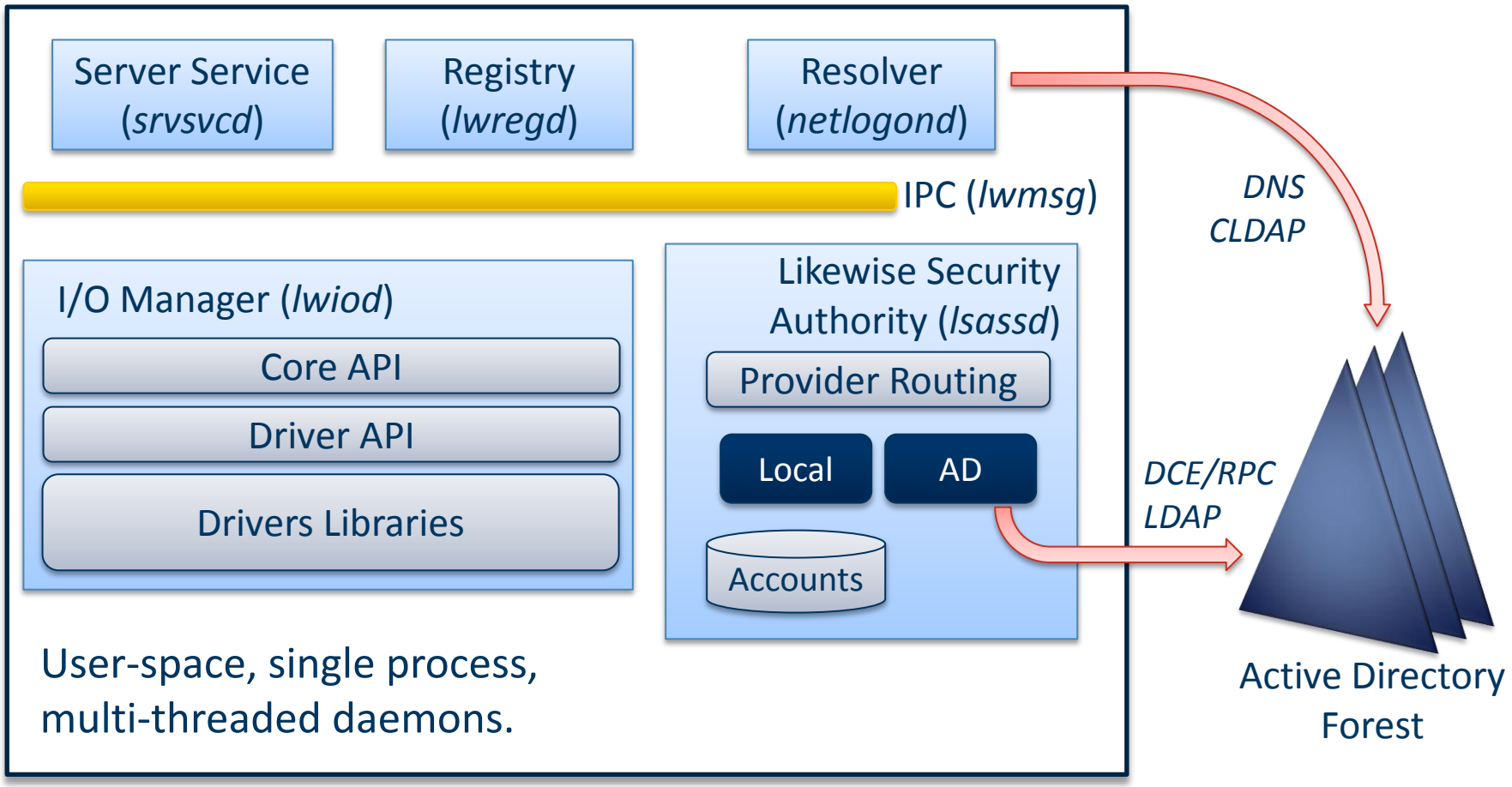
LIKEWISE BACKGROUND

http://www.likewiseopen.org/

- *Likewise Open Project* is the umbrella project sponsored by Likewise Software to provide an interoperability platform for non-Microsoft hosts in MS OS dominated networks.
- *Likewise Open* (product) refers to the open source authentication & Active Directory integration suite
- *Likewise Identity Services* is the AD bridge component
- *Likewise Storage Services* is the file server software stack
  - Formerly known as *Likewise-CIFS* (SMB/SMB2)
  - Additional protocols in development
- Dual-License: Commercial or GPLv2+/LGPLv2.1+
  - Single code base

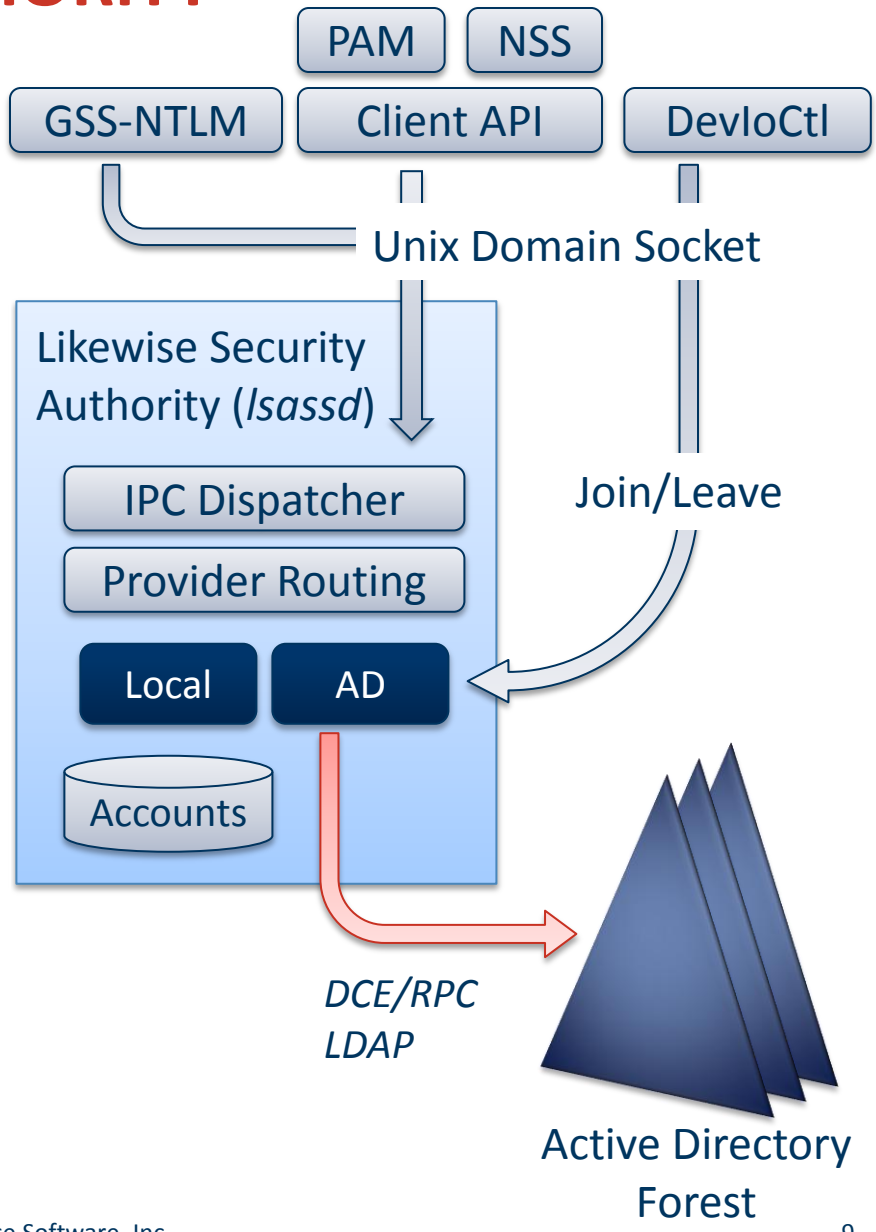
LIKEWISE COMPONENTS

Likewise Identity and Storage Services

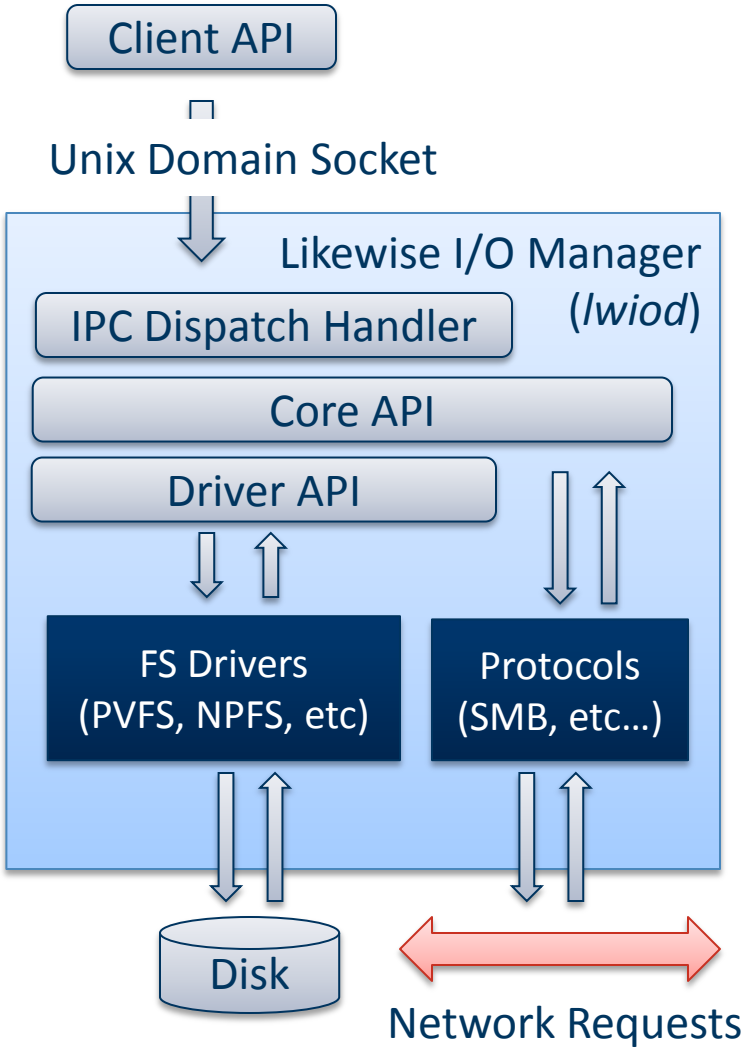


Likewise Security Authority

- Authentication
  - Kerberos, NTLMv1, NTLMv2
  - Privileged local user management
- Identity management
  - Unprovisioned domains, Forest naming scope, etc…
- Domain member services
  - Site affinity
  - Caching
  - Offline authentication
  - Automatic machine password and ticket updates



LIKEWISE I/O MANAGER



- Kernel based I/O Subsystem ported to user-space
- Driver-oriented architecture
- I/O Request Packet Model
  - 20 unique IRP_TYPEs
- Core API similar to the Windows NT Kernel I/O Subsystem
  - ZwCreateFile(), ZwQueryInformationFile(), ZwReadFile(), etc…

Joining an Active Directory Domain

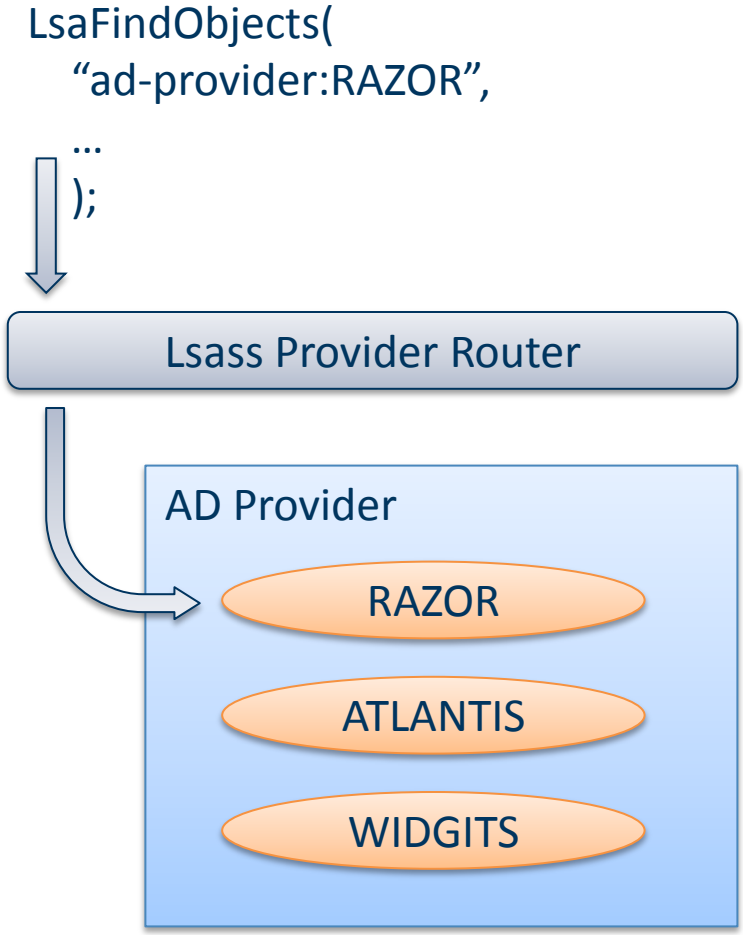
Two step process

- Establishing the computer identity
  - If necessary, creates the computer object in AD
  - Establishes the shared secret between the host machine and AD
  - Creates entries for long term keys in system keytab file
  - Updates DNS with A and PTR records for host
- Host system configuration
  - Add appropriate entries to PAM and NSS files
  - Enables GSS-API enabled applications for SSO (e.g. sshd)
  - …

Multi-Domain Lsass

Design

- Abstract run-time and persistent state to a context structure
  - Configuration details grouped under a per-domain key in the registry
  - Machine credentials internally isolated per domain
- Support multiple provider instances using a secondary routing decision
  - Allow client side API to target a specific "*provider:instance*" when opening a provider handle
  - One "*provider:instance*" is designated as the default for backwards compatibility



Multi-Domain Lsass – Run Time State

lsass/server/auth-providers/ad-open-provider/adstruct.h

```
typedef struct _LSA_AD_PROVIDER_STATE
{
    PSTR pszJoinedDomainName;

    struct {
        BOOLEAN bIsInitialized;
        pthread_mutex_t Mutex;
    } MachineCreds;

    ...
    LSA_AD_CONFIG       config;
    PAD_PROVIDER_DATA pProviderData;
    PLW_HASH_TABLE pAllowedSIDs;
    LSA_DM_STATE_HANDLE hDmState;
    LSA_MACHINEPWD_STATE_HANDLE hMachinePwdState;
    LSA_SCHANNEL_STATE_HANDLE hSchannelState;

} LSA_AD_PROVIDER_STATE, *PLSA_AD_PROVIDER_STATE;
```

Multi-Domain Lsass – Persistent State

$ lwregshell

```
[HKTM\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin]
  "Default" REG_SZ           "RAZOR.LIKEWISEOPEN.ORG"

[HKTM\...\DomainJoin\RAZOR.LIKEWISEOPEN.ORG]
[HKTM\...\DomainJoin\RAZOR.LIKEWISEOPEN.ORG\DomainTrust]
[HKTM\...\DomainJoin\RAZOR.LIKEWISEOPEN.ORG\DomainTrust\RAZOR]
  "ClientSiteName"           REG_SZ          ""
  "DNSDomainName"            REG_SZ          "razor.likewiseopen.org"
  "Flags"                    REG_DWORD       0x00000001 (1)
    ...
[HKTM\...\DomainJoin\RAZOR.LIKEWISEOPEN.ORG\ProviderData]
[HKTM\...\DomainJoin\RAZOR.LIKEWISEOPEN.ORG\Pstore]
  "ClientModifyTimestamp"    REG_DWORD       0x4cc99ff1 (1288282097)
  "CreationTimestamp"        REG_DWORD       0x4cc99ff1 (1288282097)
  "DomainDnsName"            REG_SZ          "RAZOR.LIKEWISEOPEN.ORG"
  "DomainName"               REG_SZ          "RAZOR"
  "HostDnsDomain"            REG_SZ          "razor.likewiseopen.org"
  "HostName"                 REG_SZ          "CF-LAPTOP"
  "MachineAccount"           REG_SZ          "CF-LAPTOP$"
  "SchannelType"             REG_DWORD       0x00000002 (2)

[HKTM\...\ \DomainJoin\RAZOR.LIKEWISEOPEN.ORG\Pstore\MachinePassword]
```

Remaining & Future Work

- Current functionality
  - Programmatic joining to multiple domains and targeting specific "*provider:instance*" accounts.
- Remaining Lsass work
  - User accessible Join/Leave application (CLI & GUI)
  - Integration with the GSS-NTLM mechanism
  - ETA – Dec, 2010
- Remaining file server work
  - Abstract SMB/CIFS configuration (e.g. shares) on a per VIP basis in the registry
  - ETA – Q1 2011

Test Drive

Administration/User guides at http://www.likewise.com/

- Simple build system for Linux & FreeBSD
- Step 1: Download the source code
  - git clone git://git.likewiseopen.org/likewise-open
- Step 2: Build the likewise-open components
  - build/mkcomp [--noincremental] [--debug] all
  - Installs all pieces to “staging/install-root/”
- Step 3: Generate RPMs/DEBs (Linux only)
  - build/mkpkg [--debug] cifs
  - Creates package in “staging/packages/”

GERALD CARTER

GCARTER@LIKEWISE.COM

HTTP://WWW.LIKEWISE.COM/

HTTP://WWW.LIKEWISEOPEN.ORG/

GIT://GIT.LIKEWISEOPEN.ORG/LIKEWISE-OPEN

QUESTIONS?

LPC 2010 - LINUX MULTI-TENANT FILE SERVERS