Linux/Unix - Windows Inter-operablity

Joseph Guarino
Owner/Sr. Consultant Evolutionary IT
CISSP, Healthcare IT+, LPIC, MCSE 2000/2003, PMP
www.evolutionaryit.com

Who is this dude?

- Joseph Guarino
- Working in IT for last 15+ years
- CEO/Sr. IT consultant with my own firm Evolutionary IT
- CISSP, Healthcare IT+, LPIC, MCSE, PMP, Toastmaster CL, ACS
- www.evolutionaryit.com
- social.evolutionaryit.com

evolutionaryIT™
BEST PRACTICE IT

Place Nice!

Objectives

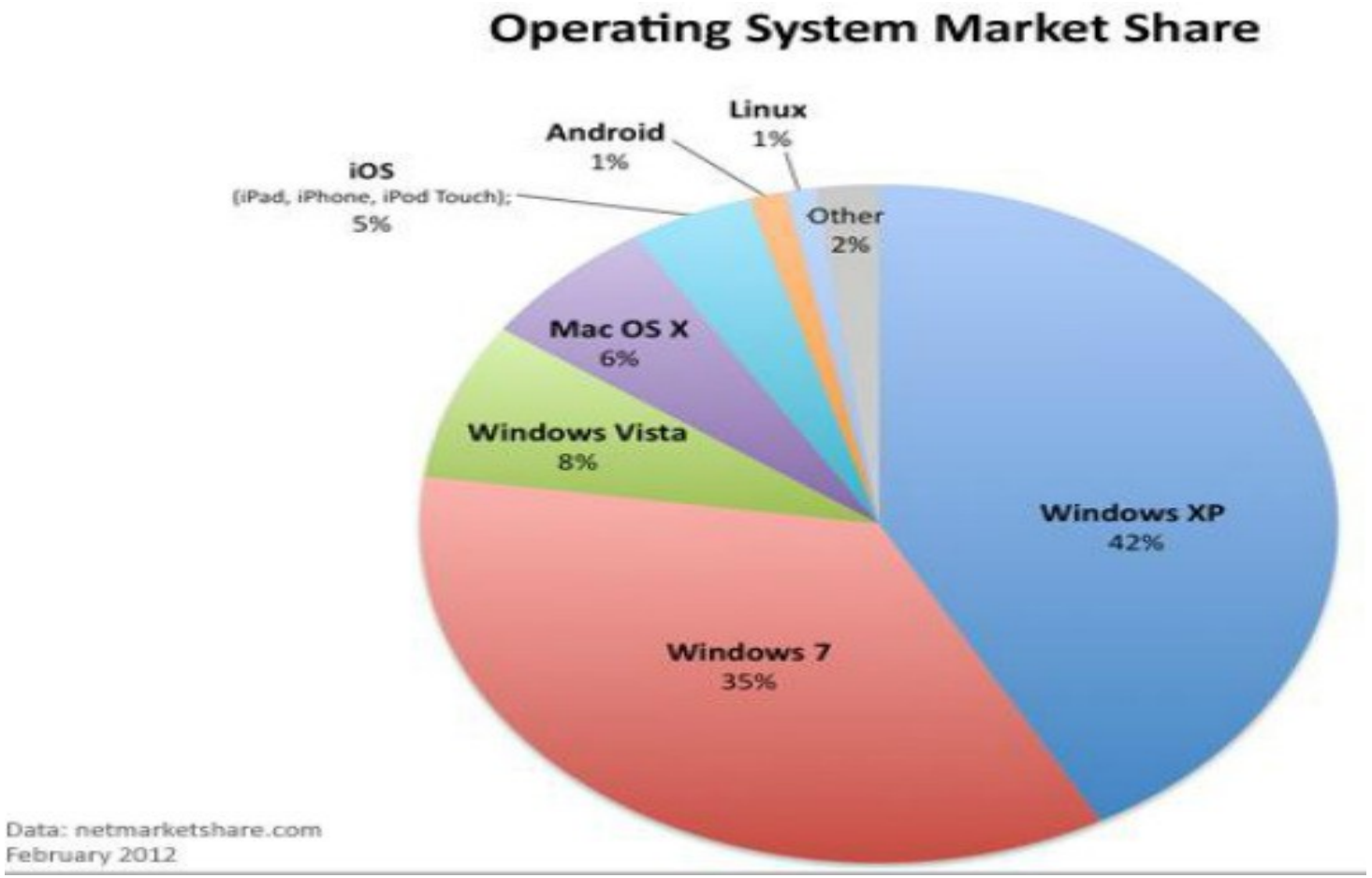
- State of the union *for everyone*
- Why is this relevant?
- FOSS Options
- Commercial Options

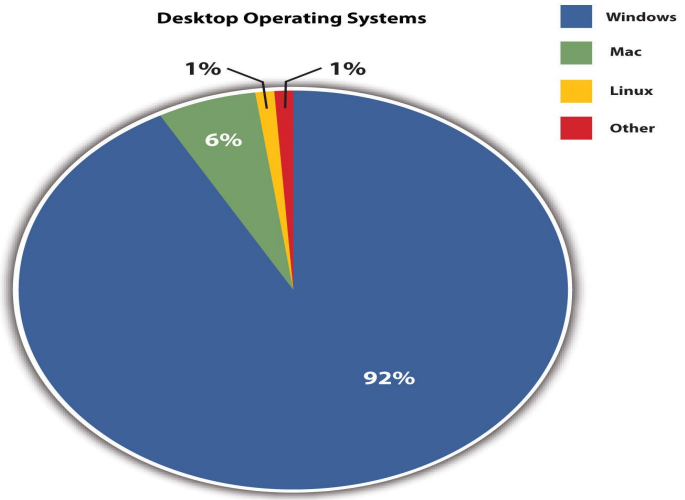
Inter-operablity Imperative

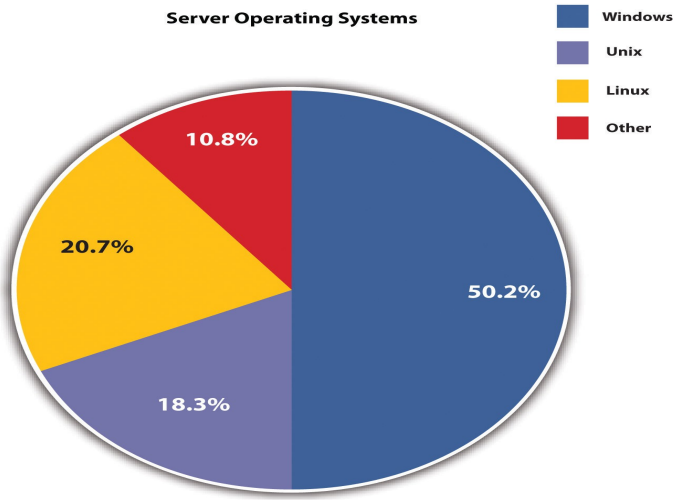
- Windows is 65%-90% of enterprise desktop market
- Linux and Unix are growing presence
- Very few environments are homogeneous
- Inter-operablity isn't a nice to have option

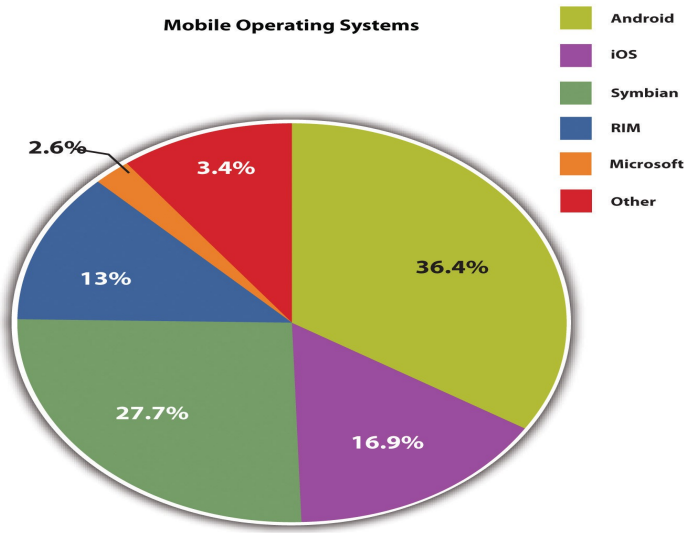
Homogeneity

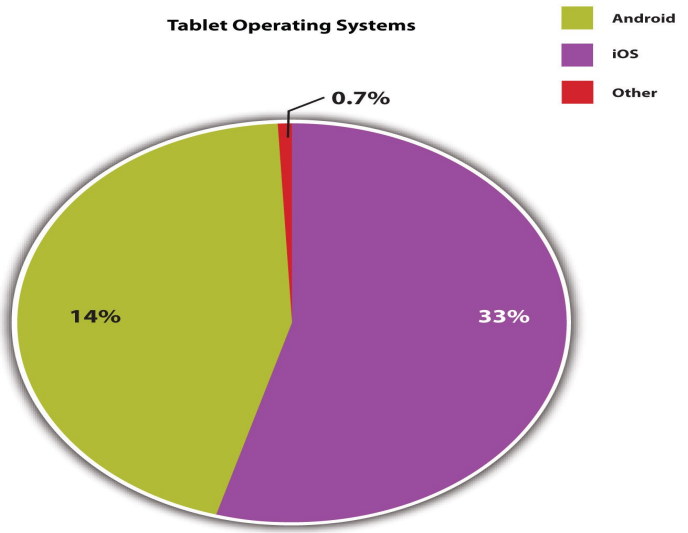
A myth in the real world!











Source: HitsLink (desktop, May 2012), IDC (server, Q1 2012), Gartner (mobile, May 2012), and IDC (March 2012).

Enterprise LAN

Windows is often there

Open Source Interop

Defining Some Basics

NIS/NIS+

- NIS – Centralized authentication based on RPC. Security isn't the best.
- Trusted host security model
- NIS+ - Sun's (Oracle) “evolutionary” step from NIS
- Never really took off

Kerberos

- Network authentication via symmetric key cryptography
- NOT a directory service
- Widely available and supported on Linux
- Key element in AD (bastardized a bit)

LDAP

- Central store of information
- Protocol for accessing directory information over a network
- Central store for many other types of info
- Devices, Name, Address, Computer Account Info, Office number, Phone Number, etc,

Active Directory

- Centralized database of everything – replicated to other domain controllers
- Centrally administer a windows network at a very granular basis via Group Policy
- Manages users, computer, printers, other devices
- Manage users, security, authentication, resources

AD

- Around since W2K – Windows 2000
- LDAP
- Authentication – Kerberos (encrypts usernames/passwords on wire)
- AD relies on DNS
- Tied into DNS (DDNS)
- Slightly Microsoftized versions of Kerberos, DNS, LDAP

Some Want to Leverage AD

- Simplification
- Consolidation
- Cost Savings

Name Resolution

DNS

- Thankfully replace NIS and WINS
- Maps IP to machine and vice versa
- Bind, Samba DNS, etc.
- Alternatives to BIND and PowerDNS

Windows DNS

- Integral to AD
- Most use it for AD and integrated resources
- But you can use 3rd party DNS in a number of ways

BIND

- Widely deployed DNS Server
- Can integrate into Windows AD DNS as primary (requires more work and gets little benefit) or delegated subdomain or even split brain configuration
- Supports DNSSEC for AD integrated zone – adds sec to dynamic client updates

Assumptions For Sake Of Scope

evolutionaryIT™
BEST PRACTICE IT

No Dead Tech

There are supernumerary ways to integrate...

No one “right” way for everyone

Samba 3.x

- Suite of daemons
- Since 1992
- Name originates from SMB (Server Message Block) – protocol used by MS Windows network file system
- Implementation of SMB/CIFS protocols
- File and print services

Samba 3.x

- Daemons
- smbd (file/print)
- nmbd (netBIOS name resolution)
- Windbind authentication to AD accounts (connects DC with Linux native authentication system PAM) – no AD changes required
- SWAT (Web based GUI Administration)

Samba 3.x

- Integration into Windows Domain
- Not Active Directory!
- PDC (Primary Domain Controller)
- BDC to Samba PDC
- AD domain controller

Samba 4

Samba 4.x

- Version 4.x (12/11/12) brings AD compatible Domain Controller or join to existing DC
- Samba Active Directory Domain
- LDAP Server, Heimdal Kerberos Authentication, Dynamic DNS
- Group policy, Roaming profiles
- SMB2.1/3

Administering SAMBA

Administering Samba

- CLI
- Webmin (Samba Module)
- Gadmin Samba
- SWAT/SWAT2
- System-config-samba

SWAT

- Samba Web Administration Tool for 3.x
- Official Part of Samba Suite
- Will remove any parameters (no longer supported) or comments are lost
- Supports SSL/TLS
- SWAT Website

SWAT 2

- Specifically written for Samba 4.x
- SWAT 2
- Python
- SWAT 2 Website

Windows RAT & GPMC

- Remote Administration Tools and Group Policy Management Console
- Window Vista RAT
- Windows 7 RAT
- Windows 8 RAT
- Windows GPMC

Baking Samba Solutions - Variables

Variables

- **Authentication** – NIS, LDAP, Winbind, Kerberos, etc.
- **Directory Services** – Many LDAP solutions, Windows AD, etc.
- **NTP (Time)** – Ntp daemon, Windows, etc.
- **Name Resolution (DNS)** – Bind, Windows DNS, etc.
- **File/Print** – SAMBA, Windows SFU, Commercial variations of SAMBA

Samba Integration Choices

- NIS with SFU
- Winbind (authenticating directly via AD)
- LDAP for Linux client Samba auth for Windows
- LDAP sync to AD or meta directory
- pGina integrated with NIS, OpenLDAP, Kerberos
- Samba 4.x alone
- Commercial 3rd Party Applications – Centrify, Beyond Trust, etc.

Few Examples

Windbind

- Windbind – ties together DC with Linux authentication mechanism of Pluggable Authenication Modules (PAM) and NSS Name Service Switch
- ID Tracking & Name Resolution via NSS
- Mapping of ID's via idmap
- Effectively plugging into AD

389 Directory + Samba

- 389 Directory for authentication & directory services
- Two way sync to AD
- Samba for File/Print

Centrify

- Centrify Suite and
- Centrify-Enabled Samba

Pure Samba 4

- No licensing headaches
- No closed
- No headaches

SAMBA Support

- Community
- IT Consulting Organizations
- Commercial Linux Vendors

LDAP Options

OpenLDAP

- Full featured open LDAP server
- Libraries implementing LDAP protocol, utils, tools, client
- Support for SSL/TLS and Kerberos
- SASL – middle man for applications and authentication systems
- Strong cross platform support

OpenLDAP GUI's

- PhpLDAP Admin
- Webmin
- LDAP Admin (Windows)
- LDAP Administrator (commercial)

389 Directory Server

- 389 Directory Server (formerly Fedora Directory Server)
- Redhat community sponsored project
- Multi-master replication
- AD sync (user/group)
- Graphical interface

Red Hat Directory Server

- Red Hat's supported version of 389 Directory Server
- Runs on HP, Sun as well as RHEL
- AD Sync

Sun Java System Directory Server

- AKA Sun ONE Directory Server, iPlanet Directory Server, Netscape Directory Server
- Supports Two way AD Sync
- Part of Oracle Directory Server Enterprise Edition

Microsoft SFU
Services For Unix
&
Subsystem for UNIX-based Applications (SUA)

Microsoft SFU

- Services for Unix
- Unix subsystem and network services to Windows
- Uses Interix (POSIX-conformant UNIX subsystem for Windows
- Migration toolkit
- 3.5 EOL (End of Life)

Microsoft SFU

- Includes ~400 Unix utlities such as vi, ksh, csh, cat, awk, etc
- GCC,CDB
- X11 tools and libraries
- ≤W2K3 Only (Not W2K3 R2 or >)

Microsoft SFU

- Base Utilities for Interix (BaseUtils; including X11R6 and X11R5 utilities)
- UNIX Perl for Interix (UNIXPerl)
- Interix SDK (InterixSDK; including headers and libraries for development and a wrapper for Visual Studio compiler)
- GNU Utilities for Interix (GNUUtils, again about 9 utilities)
- GNU SDK for Interix (GNUSDK; including gcc and g++)
- NFS Client for Windows (NFSClient)
- NFS Gateway for Windows (NFSGateway)
- NFS Server for Windows (NFSServer)
- NIS Server for Windows (NIS)
- Password synchronization (PasswdSync)
- Windows Remote Shell Service (RshSvc)
- Telnet Server for Windows (TelnetServer)
- NFS User Name Mapping (Mapsvc)
- NFS Authentication Server (NFSServerAuth)
- PCNFS server (Pcnfsd)
- ActiveState Perl (Perl)

Subsystem for UNIX-based Applications (SUA)

- Most of SFU components
- NFS, SUA/Interix, Identity Management for Unix
- Removed NFS, Username Mapping, NIS Server, Passwd Sync)
- ≥ W2K3 R2 - W2012, Client side Vista/Win7/Win8

Identity Management for Unix

- Integrates Windows into Unix/Linux Authentication via
- NIS Server
- Password synchronization
- ≥W2K3 R2 – W2012
- >RFC 2307 - Extends LDAP to contain other info like UID/GID

Formerly Likewise
Focus on Privilege and Identity Management
&
Vulnerability Management

Likewise Open
Now
Beyond Trust – PowerBroker Open

PowerBroker Open

- Allows Linux, Unix, Mac systems to join AD, password policies, cached credentials
- PBIS Agent
- No AD schema or attribute changes required
  (schema=set of rules that control the types of information or objects that the server can hold)
- GUI Domain Join Tool
- PAM, NSS, Kerberos, NTLM, etc.
- Integrates with Samba

Beyond Trust – PowerBroker Identity Services for Active Directory Bridging

Beyond Trust – PBIS for AD Bridging

- PowerBroker Identity Services for Active
- Brings Linux, Unix into AD
- Directory Bridging & Group Policy
- Maps UIDs and GIDs to AD
- No change to AD Schema (schema=set of rules that control the types of information or objects that the server can hold)
- Integrates with Samba

Beyond Trust PBIS for AD Bridging

- SSO with Kerberos, LDAP for Samba, SSH, Jboss, MySQL Oracle, etc.
- Graphical web based management console
- Reporting features for managing and viewing privileges
- Helps w/ compliance w PCI, DSS, SOX, HIPPA

evolutionaryIT
BEST PRACTICE IT

Centralized Management & User Administration
SSO, Auditing, etc.

Centrify

- SSO
- AD Integration and extension of group policies
- Brings AD services to Linux/Unix (OSX)
- Cloud Aware

Centrify Express Suite

- Core component of AD integration suite
- Base level product – other commercial versions have more features/integration options
- Direct Control Express, Direct Manage Express, some Open Source Tools
- “Free” as in price with some FOSS components

Centrify Open Source Tools

- Aid in integration into Centrify Suite and AD
- Centrify-Enabled Samba
- Centrify-Enabled OpenSSH
- Centrify-Enabled PuTTY
- Centrify-Enabled Kerberos Tools

Centrify Suite Editions

Centrify Suite Editions

Show More Detail

Product	Features	Editions: Express	Standard	Enterprise	Platinum	Options
DirectManage	Centralized Management and User Administration	◒	●	●	●	
DirectControl	Centralized Authentication and Access Control	◒	●	●	●	
DirectAuthorize	Role-Based Authorization and Privilege Management		●	●	●	
DirectAudit	Detailed Auditing of User Activity			●	●	
DirectSecure	Server Isolation and Protection of Data-in-Motion				●	
Applications *	Single Sign-On for Applications					●

* Optional modules that are compatible with all Centrify Suite editions

Other Awesome Inter-op Related Misc

Cygwin

- Complete set of Unix tools on Windows
- Linux-like environment for Windows
- Red Hat sponsored

Running Local Windows Apps

- Wine
- Codeweavers Crossover
- Wine 3rd Party Apps

Virtualization

- KVM
- Xen
- Virtual Box
- VMWare
- Hyper-V

Thank You!

Let's Connect

- Joseph Guarino
- http://social.evolutionaryit.com
- http://www.evolutionaryit.com

- BNUG is on Meetup
- Meetup.com/B-N-U-G
- Sign up!!