Windows Security

By Anna and Seamus

Agenda

- Windows Internals
  - Registry
  - LSA
  - SAM
- Active Directory basics
  - stuff
  - Group Policy
  - Security concerns

The Windows Registry

- A hierarchical key-value store, with 5 root keys
  - HKLM - Computer Specific
  - HKCC - Runtime Information
  - HKCU - Information specific to currently logged in user
  - HKCR - Information for applications
  - HKU - all users
  - HKEY_PERF_DATA
    - Not stored as a standard hive
    - How the performance subsystem is implemented

Local Security Authority (LSA)

- Windows subsystem responsible for managing authentication and local security policy

- Local security policy determines:
  - Which users can access the system and in what way
  - Which users have which permissions on the system
  - What forms of auditing are being performed

Security Accounts Manager (SAM)

- Database that stores users' password hashes
- Two password hashing algorithms have been used
  - Lan Manager (LM) hash
  - NT (NTLM) hash
- On most modern Windows OS versions, the SAM file is encrypted to prevent password cracking

Directory Services

- A Directory Service maps a network resource (applications, services, printers, computers, users) to a network address
- DNS can be considered a directory service
- Many different directory servers out there - IBM, Oracle, Microsoft implemented proprietary ones, as well as open source alternatives

LDAP!

- Open, vendor neutral protocol for accessing directory services
- Originally an alternative to X.500 for the TCP/IP protocol suite
- In Plain English: “Search in the company email directory for all people located in Nashville, whose name contains “Bob”, return their full name, title, email, and description”

Active Directory

- “Active Directory…keeps track of your user accounts and passwords, storing them in one protected location, improving your users security”
- “An LDAP enabled database with LDAP dependent applications and services on top of it such as DNS, kerberos, etc”
- “...a centralized and standardized system that automates network management of user data, security, and distributed resources…”

...but what is it really?

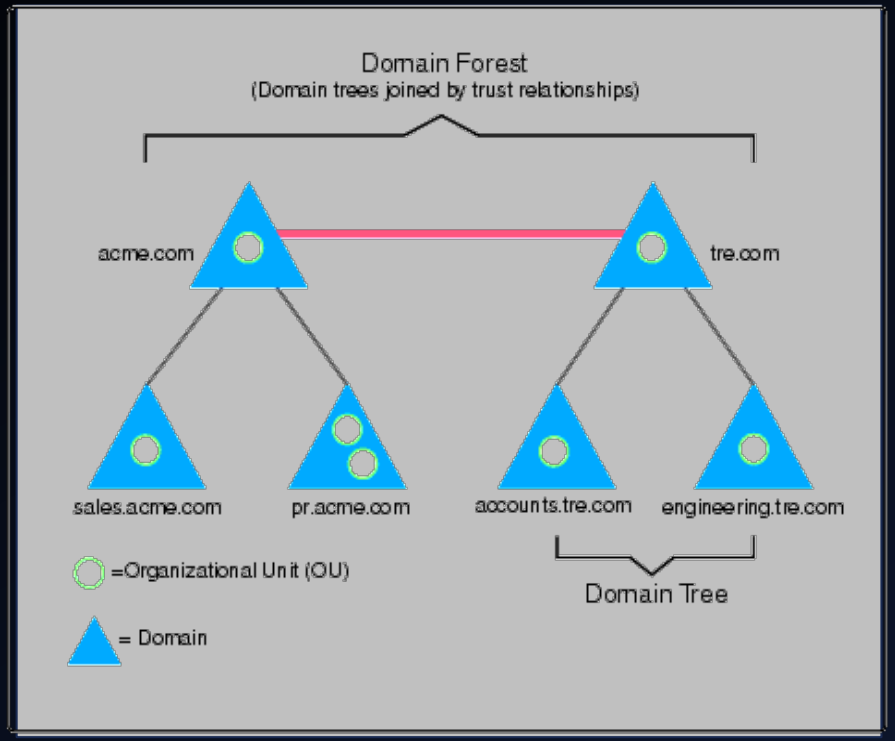
- A distributed, Jet database
- Directory System Agent (DSA)
  - LDAP
  - ADSI
  - SAM
- Jet makes it fast, DSA gives it LDAP

AD on Disk

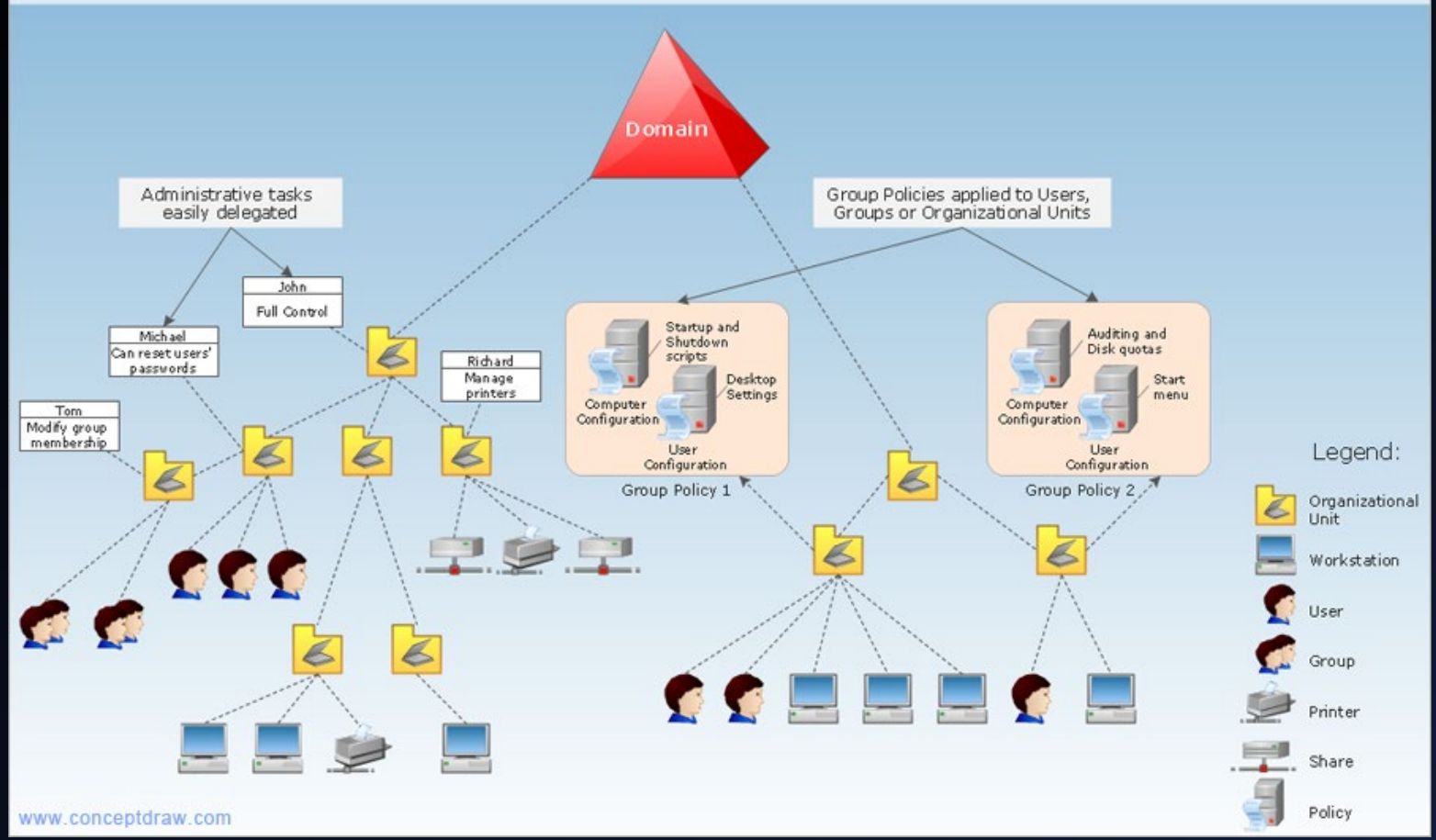
- NTDS.dit
- SYSVOL
  - Group Policies
  - Logon scripts
  - Folders to sync data between DC’s
- NETLOGON
  - Symlink to logon scripts in \SYSVOL

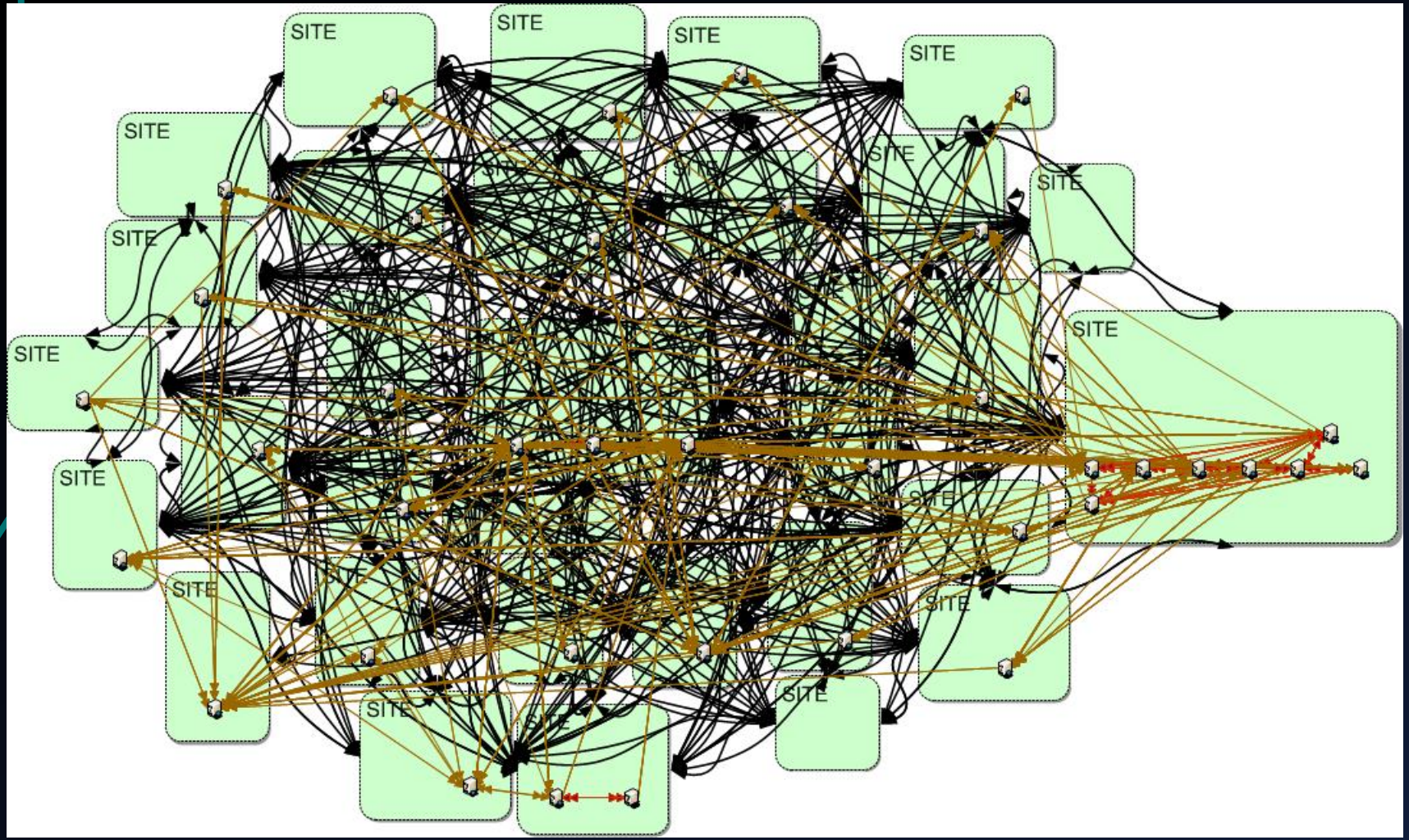
Domain Admin

- Full control of the domain and everything in it
- Admin on the Domain Controllers
- Admin on all workstations
- Admin on all servers
- Everything


Domain Forest
(Domain trees joined by trust relationships)
acme.com
tre.com
sales.acme.com
pr.acme.com
accounts.tre.com
engineering.tre.com
=Organizational Unit (OU)
= Domain
Domain Tree

Active Directory Domain Services Diagram Sample




SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE
SITE

Group Policy

- GP provides centralized management and configuration of the OS and applications' settings
- A set of configurations is grouped into a Group Policy Object (GPO)
- AD can distribute GPOs to computers in the domain
  - Every computer pulls the policy every 90 minutes and checks for updates
- Really powerful for enforcing desired state across multiple computers

Kerberos

- Authentication protocol, uses “tickets” to allow users to authenticate to each other, establish trust about who you are talking to
- MIT developed it, open source
- Used everywhere
  - BSD
  - OS X
  - Solaris
  - HP-UX
  - Windows
  - Linux

Microsoft Kerberos

- KDC - Key Distribution Center - the service which supplies the keys.
- krbtgt - the user account which runs the KDC
- TGT - Ticket Granting Ticket
  - Represents the user after being authenticated
  - Can derive other tickets from this, for services and stuff
  - Stays valid for ~10 hours
  - Encrypted and signed by krbtgt key!!!

Attacking the Domain

- There are two major ways to move around a domain
- Attack NTLM
  - Pass hashes
- Attack Kerberos
  - Golden/silver tickets