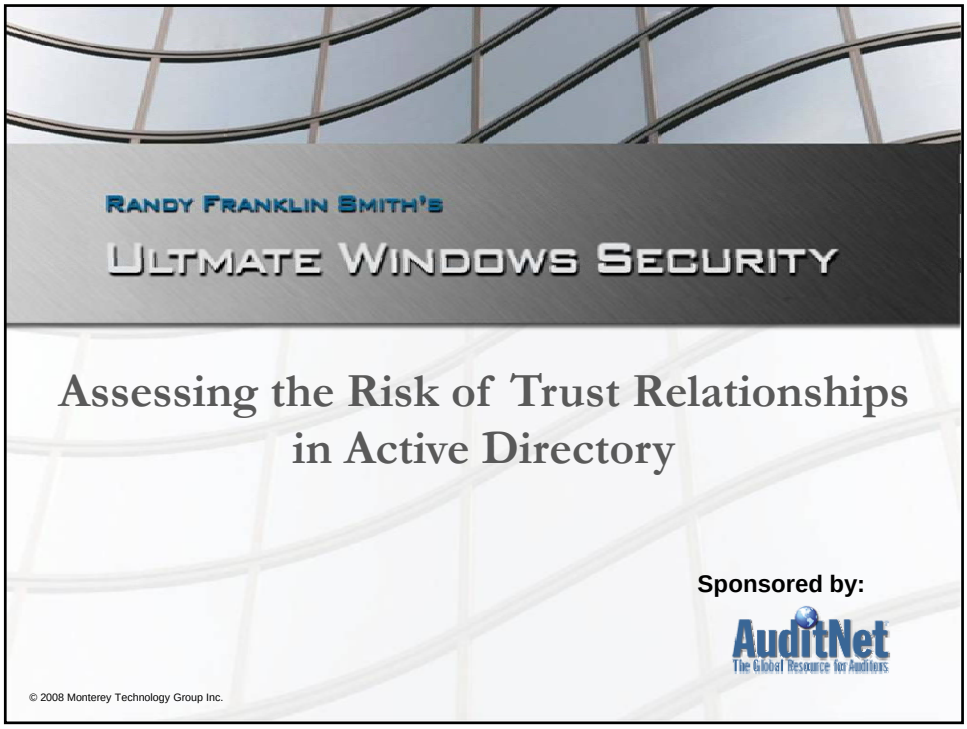


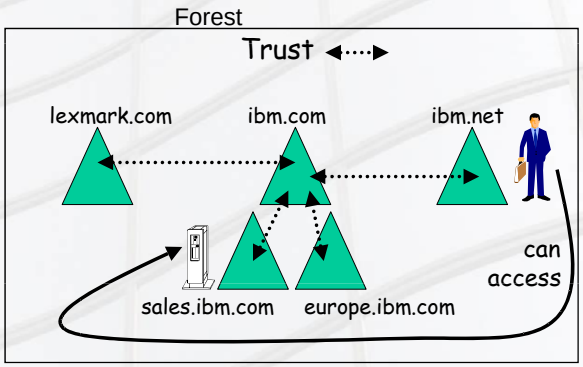
Preview of Key Points

- Domains and Forests
- Trust Relationships
  - Transitivity
  - Direction of trust
  - Risks of trust
  - External trusts
- Auditing trust relationships

3

Domains and Forests

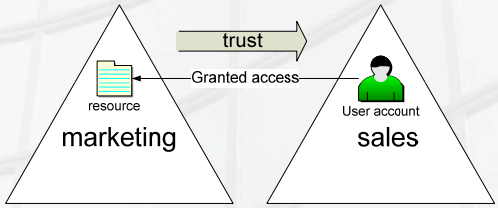
- The forest is the outer most, largest object in Active Directory
- A forest is essentially a set of domains that all trust each other.



4

Trust

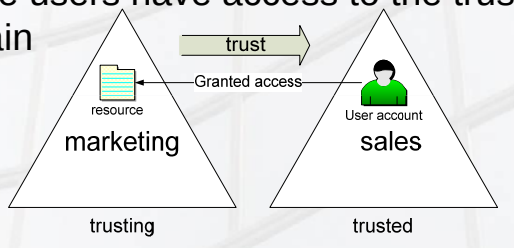
- A trust relationship is a logical link between two domains facilitating transfer of authentication and authorization
- Users from the trusted domain can connect to servers in the trusting domain without reauthenticating or requiring a 2nd user account in the trusting domain



5

Trust

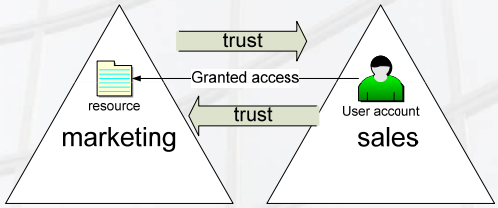
- Key trust terminology:
  - Trusting domain: Domain that allows access to users from another domain
  - Trusted domain: Domain that is trusted and whose users have access to the trusting domain



6

Trust

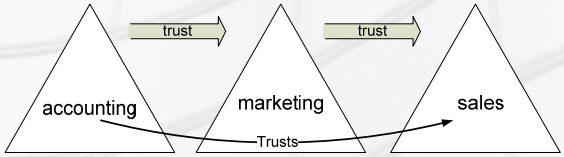
- Key trust terminology:
  - One-way trust: One domain allows access to users on another domain, but the other domain does not allow access to users on the first domain
  - Two-way trust: Two domains allow access to users on each other's domain



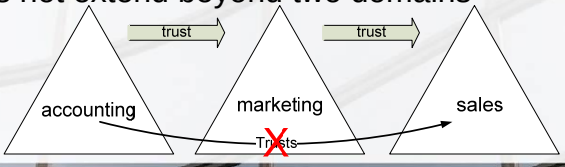
7

Trust

- Key trust terminology:
  - Transitive trust: Trust that can extend beyond two domains to other trusted domains in the tree



  - Non-transitive (intransitive) trust: One way trust that does not extend beyond two domains



8

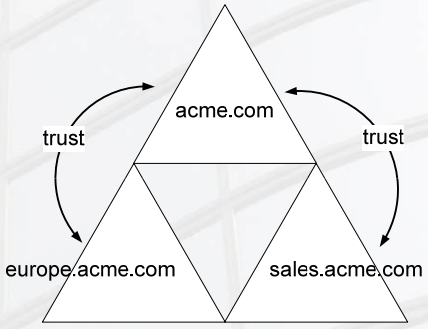
Trust Types

- Parent/Child
- Tree Root
- External
- Kerberos Realm
- Forest Trusts

9

Trust Types

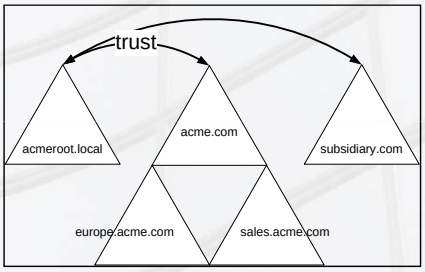
- Parent/Child
  - Trust between two AD domains that share a contiguous DNS namespace and belong to the same forest.



10

Trust Types

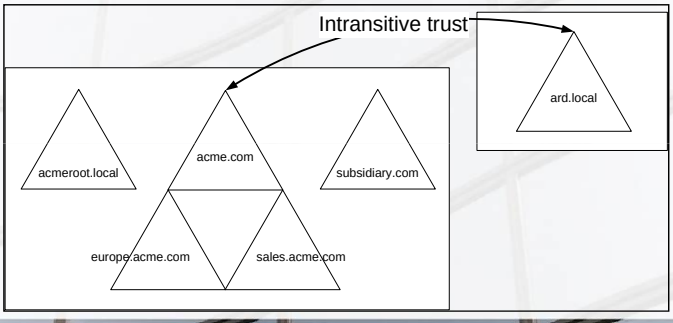
- Tree Root
  - Trust between root domains in the same forest that do not share a common DNS namespace.



11

Trust Types

- External
  - Trust used to connect to other domains outside of your forest; can also create a trust between an AD domain and NT4 domain or Samba domain

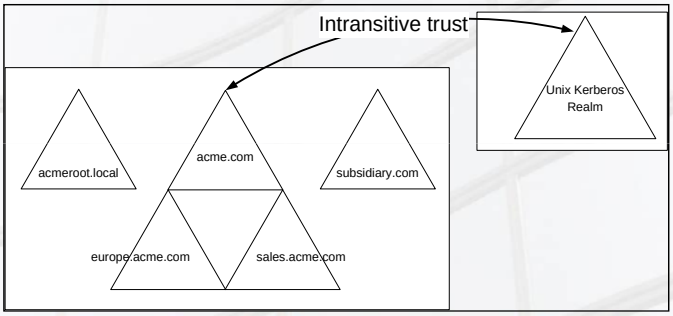


12

AuditNet & Randy Franklin Smith's UltimateWindowsSecurity.com

Trust Types

- Kerberos Realm
  - Trust between an AD domain and an MIT v5 Kerberos realm

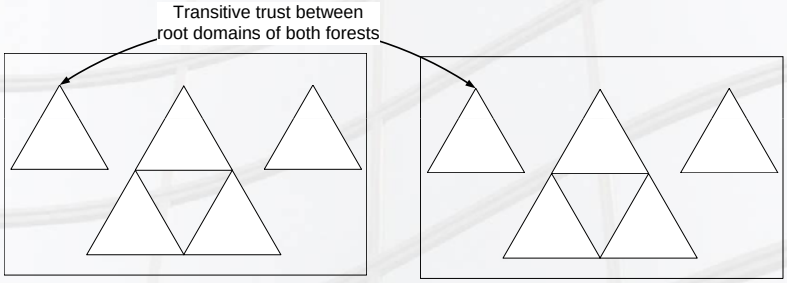


13

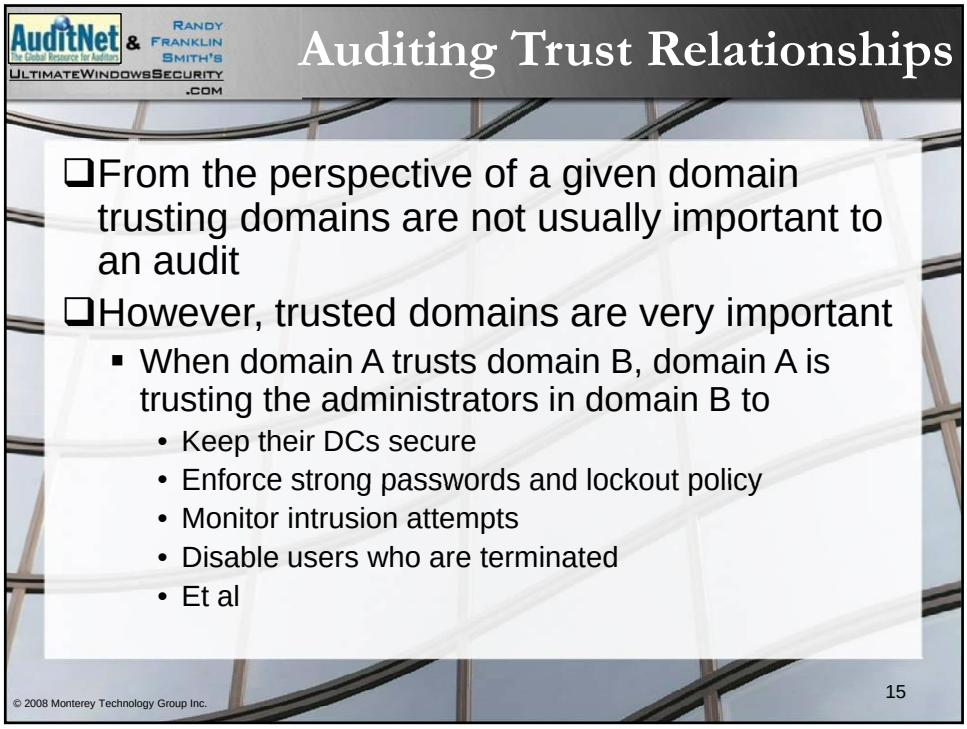
AuditNet & Randy Franklin Smith's UltimateWindowsSecurity.com

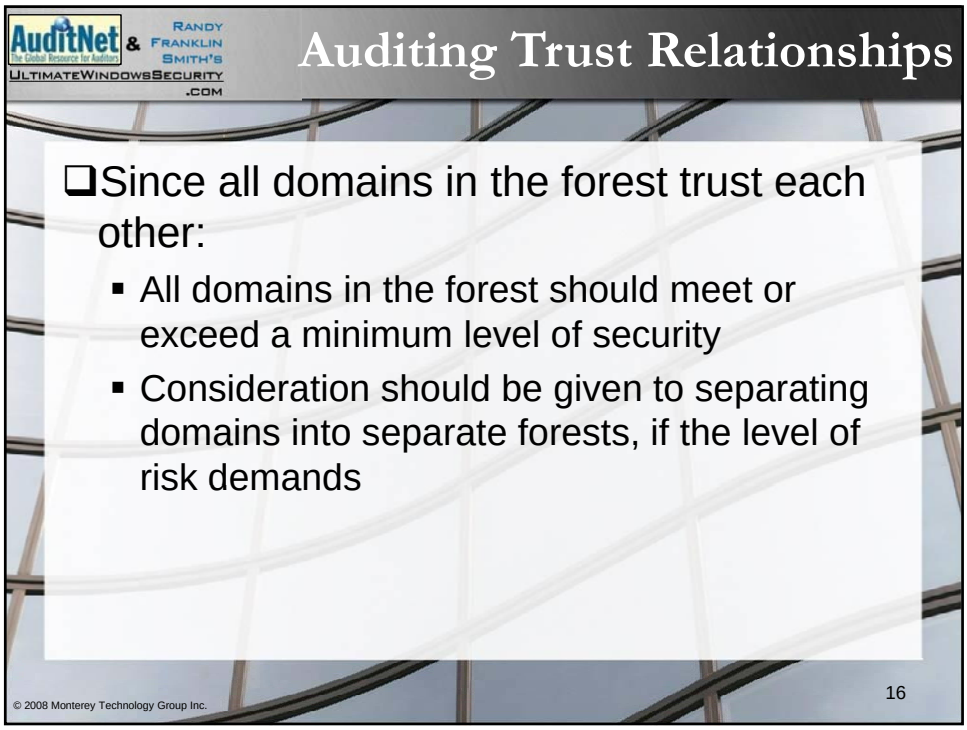
Trust Types

- Forest Trusts
  - Trust between two AD forests
  - Both forests must be running in Windows 2003 functionality level or higher



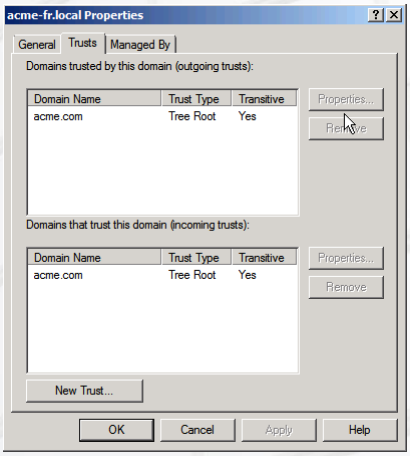
14





Auditing Trust Relationships

- Trust relationships can be viewed with Administrative Tools\Domains and Trusts
- Open properties for a given domain and examine its trusts

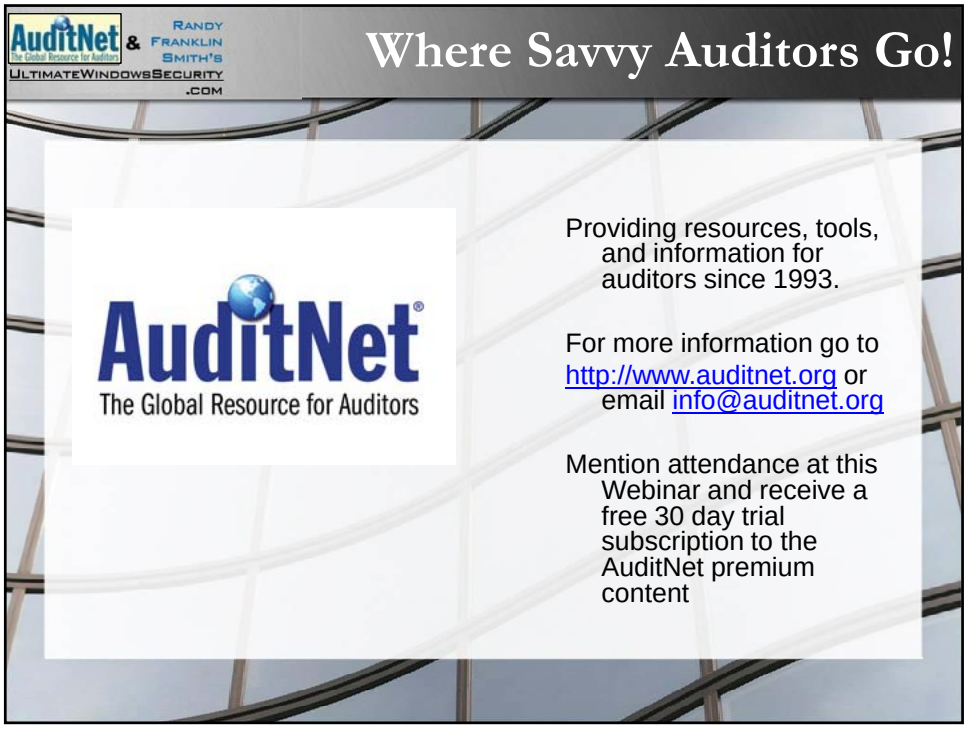


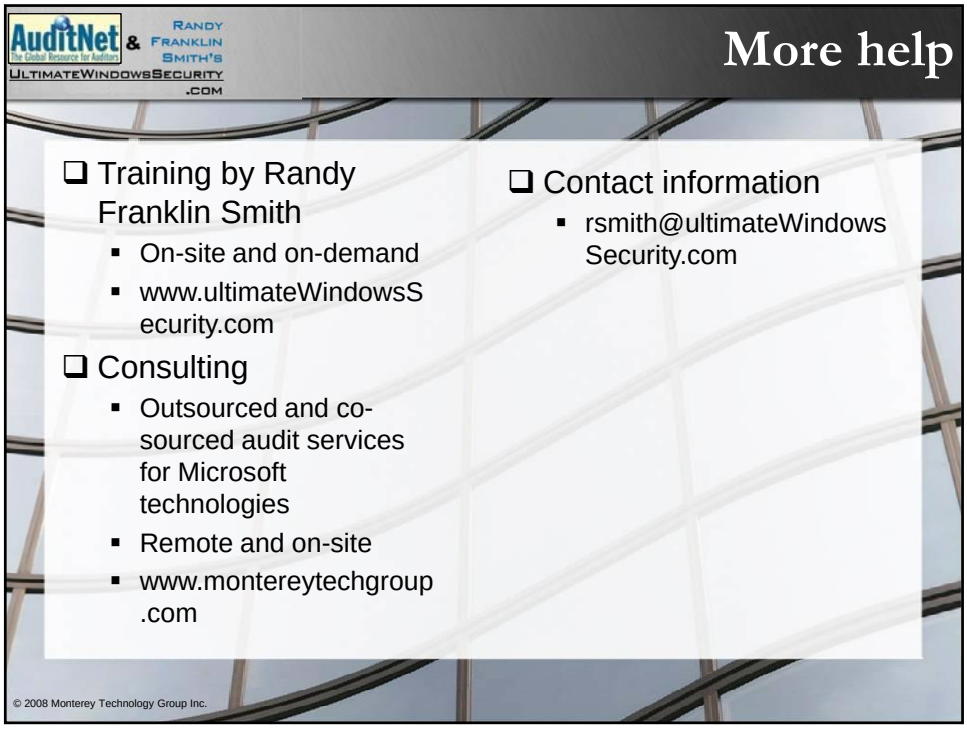
17

Review Points

- All domains within the forest trust each other
  - No real separation between admins inside forest
- When assessing trusts ignore
  - Parent
  - Child
  - Tree root
- The only external trust that is transitive is a cross-forest trust
- External trusts that should assessed
  - Realm
  - Forest
  - External
- Risk of a trust depends on
  - Difference in security quality between the 2 domains
  - Value of resources made available to trusted domain

18




AuditNet
The Global Resource for Auditors
&
Randy Franklin Smith's
UltimateWindowsSecurity.com
.com
More help
Training by Randy Franklin Smith
On-site and on-demand
www.ultimateWindowsSecurity.com
Consulting
Outsourced and co-sourced audit services for Microsoft technologies
Remote and on-site
www.montereytechgroup.com
Contact information
rsmith@ultimateWindowsSecurity.com
© 2008 Monterey Technology Group Inc.