

Re: Active Directory – security boundaries

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-09/msg00012

- *From:* "Joe Richards [MVP]" <humorexpress@xxxxxxxxxxxx>
 - *Date:* Thu, 31 Aug 2006 19:29:23 -0400
-

There was discussion a few weeks back on AD ORG from the RODC folks that mentioned the ability to exclude attributes from being replicated to RODCs. Their purpose is to make it so secrets aren't replicated, however I see benefit in setting most of the non-NOS attributes the same way since the primary need for DCs in branch sites is auth/authZ. If you are just replicating NOS info around, it doesn't have the churn the other data does and there isn't much to it so it would considerably lighten the replication load. It isn't in there yet, but it is something they are looking at.

—
Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

David Chadwick wrote:

Hi Joe,

Thanks very much for taking the time to reply. I really appreciate the effort you have put into this thread!

Just one thing – what is different in the Longhorn AD model that will help with replication?

Thanks again!

Cheers,
David

"Joe Richards [MVP]" <humorexpress@xxxxxxxxxxxx> wrote in message
news:uIYatqHzGHA.1304@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

It sounds to me like the domain was initially meant to be a
"security
boundary"

Re: Active Directory – security boundaries

The domain in NT4 was designed to be a security boundary. When Microsoft moved to the forest model, the domain became a so so policy boundary (some policies span domains) and so so replication boundary (DCs don't just replicate domain info). In all honesty, mostly what it is is a SAM name realm.

If these exploits didn't exist,
it would be a different story – is that right?

Yes but it would require a different implementation of AD. It isn't that AD is broken and the issues are outside of the design, they are key components of the design.

If any DA in any domain can escalate themselves to EA,
then domains relegate themselves to being useful for what?
Controlling replication? Differing password policies?
Containers for objects? Not much else? :)

Correct, there aren't a lot of good reasons for having multiple domains in a forest and lots of good reasons for having a single domain. Once MSFT fixes the issues with password policies you should see the case where lots of folks can collapse into single domains. Replication is still a problematic thing and probably always will though I have mentioned in other forums how that could be sort of alleviated as well within the model that Longhorn is supposedly going to run with. The branch based replication model of Novell is nowhere near happening with AD, the environments are just too different to pull it off with the current design as much as I would like to see branch level replication control.

It doesn't actually make sense that the forest is the ONLY security boundary unless you do understand that this is the case due to exploits

Microsoft is very clear now on the forest being THE security boundary. They don't lay out the details just like I don't lay out the details. And don't put your eggs in the basket labeled exploit and think everything is fine. Again, these are key design pieces not buffer overflows, etc.

MS doesn't say in their documentation "due to well known exploits, all of this is useless". :)

Nope they don't, but they do say that the forest is THE security boundary. Admins who set up forests need to actually understand what that means. An admin who today sets up a multidomain forest and configured different domains with different DAs is not heeding the documentation which clearly

Re: Active Directory – security boundaries

states that the Domain is NOT the security boundary.

I'm assuming that these exploits exist at the core of AD and it's not actually a "bug", but rather a design flaw that can be compromised?

It isn't even honestly design flaws. It is a fact of how things HAVE to work for the intended capability. If you go all the way back to the initial guidelines from Microsoft it was all about collapsing to a single domain. Do everything in a single domain. They messed up by not allowing multiple domain password policies per domain. That certainly would have helped more folks go to that initial design idea. A better replication model to handle slow bandwidth sites would have been nice as well but quite honestly, the bandwidth use doesn't get bad until you start throwing things in like Exchange and other applications. The goal never should have been to put everything into one single directory like it was then. Now the idea is to have multiple directories but strong sync capabilities. It was nice to see MSFT turn the ship on that concept because some of us working in very large orgs just started laughing in 2000 when we saw the power points MSFT put out saying they were going to be the one and only directory in companies. They were in many small ones but in larger orgs it breaks down pretty fast.

Finally if they had been very up front right off the bat that the forest was the security boundary and not the domain that would have helped considerably. The key developers and folks who understood AD knew this but they aren't the people writing the documentation. If that were the case we would have better documentation but no forward progress.

joe

—

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

—O'Reilly Active Directory Third Edition now available—

<http://www.joeware.net/win/ad3e.htm>

David Chadwick wrote:

Hi Joe,

Re: Active Directory – security boundaries

Many thanks for your detailed reply.

Keep in mind that my post was about trying to understand concepts, not really about existing or real projects or places. I'm merely trying to learn more by sorting it out in my head. On face value when reading documentation about domains what I was saying I think is true. It is correct at a theoretical level. Of course if you add into the mix "there are well known exploits which mean any DA in any domain can escalate to be an EA and or a DA of any other domain" then it blows it all out of the water.

It sounds to me like the domain was initially meant to be a "security boundary" of sorts (although not the ultimate one, obviously) – would that be fair to say? It's only because of these escalation exploits that the domain is useless as a security boundary. If these exploits didn't exist, it would be a different story – is that right? Obviously you'd still be able to access resources in other domains in the forest (if you have rights), but if the exploits weren't there then the domain would be a security boundary of some sort.

If any DA in any domain can escalate themselves to EA, then domains relegate themselves to being useful for what? Controlling replication? Differing password policies? Containers for objects? Not much else? :)

It is just difficult to work out these concepts based on Microsoft documentation. It doesn't actually make sense that the forest is the ONLY security boundary unless you do understand that this is the case due to exploits. If you took the MS documentation about domains at face value, the things I was saying are more or less correct. It's only due to these exploits that everything completely changes. MS doesn't say in their documentation "due to well known exploits, all of this is useless". :)

I'm assuming that these exploits exist at the core of AD and it's not actually a "bug", but rather a design flaw that can be compromised? That would make sense as to why it hasn't been fixed (and possibly can't be fixed).

Thanks very much for your help! It's very interesting stuff.

Cheers,
David

"Joe Richards [MVP]" <humorexpress@xxxxxxxxxxxx>
wrote in message
news:%23YOW3nxyGHA.1936@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Re: Active Directory – security boundaries

You won't get from me, and hopefully from no one else the theory behind why the forest is the security boundary and what the holes are inside of a forest. Giving that info out tells people how to take advantage of it and hack it. If they could be blocked that would be one thing, but they can't so spreading the information to folks who don't figure it out on their own is irresponsible; on par, well actually worse than publishing OS Bug exploits that allow escalations and untrusted code to operate. Worse because it can't be stopped with a simple patch like you can do for say blocking an RPC exploit. Someone who is very familiar with AD will quickly come to see where the issues come in because they are very logical points "that follow" due to the design.

In my experience "security experts" always recommend scenario 1

You can change that to security experts and AD experts. Often though, AD experts ARE security experts since AD is the security core of Windows networks. It is tough to be an expert on the core of the Windows Network without being a fairly decent overall security expert or a reasonable facsimile of one.

I'm happy that all administrators in the internal domain (which is the forest root) will automatically be able to administer the external domain.

This is not necessarily explicitly true. It is enterprise admins that get those rights. However, anyone who has any level of admin rights or actually even less in any domain (or any individual domain controller) in the forest have the ability to escalate themselves to enterprise admins. They may not have the knowledge necessary

Re: Active Directory – security boundaries

but they certainly have the ability available. Obviously escalating a DA or Administrator or server operator in the root domain to EA is child's play, but the others are nearly as trivial.

The reverse should not be true though, as the external domain is not the tree root – right?

On the surface, they don't have rights. As I indicated above though, they can escalate themselves to have the rights and again, no I won't share those details.

With the other scenario (separate forests plus 1-way trust), isn't the same the case?

Nope, there is no immediate mechanism for escalation except to directly attack the DCs of the other forest.

They have effectively been isolated in their own "security boundary", haven't they?

Maybe. But probably not. :)

say you can guarantee that no administrator will ever make a mistake in scenario 2

This actually made me laugh.

Re: Active Directory – security boundaries

In the real world, they need
to be part of our
Exchange 2003 organisation
and none of that works
across forests.

I am guessing you never heard of the
Exchange resource forest model...

<http://www.microsoft.com/technet/prodtechnol/exchange/guides/PlanE2k3MsgSys/4d>

This is actually a very good way to
implement Exchange and I heartily
recommend it many circumstances and my
"real life" job is all about Exchange and AD
in one of the largest managed services
companies in the world. We literally run
Exchange for millions of users across many
many companies and when we do it I far
prefer using a single domain Resource
Forest than running Exchange out of the
customers internal AD.

Placeholder forest root
domain, only a single
trusted
administrator has access (me
:))
Tree root domain for
standard company stuff (the
normal IT
admins live here)
Tree root domain for
finance department (with
their own admins)

This is bad from a several angles.

1. You shouldn't be the only one in the root, if some admin decides he is sick of you and puts a bullet in your head, your company then has to hack the forest. Thankfully it is relatively easy but just the same, most admins don't know how so it will cost them money.

2. The finance department whenever they felt they wanted to could take over the root domain and boot you right out and I am

Re: Active Directory – security boundaries

quite confident you couldn't do the same to them.

3. Exchange sucks in a multi-Exchange enabled domain forest, there are all sorts of little gotchas that can and often do bite you that you end up trying to jump through hoops trying to avoid. Thankfully, they are slowly fixing the holes because people like me have been beating on the Exchange team for like 4–5 years to fix them. Unfortunately, they can't fix all of them unless they make some radical design changes in both Exchange and Outlook or convince the AD guys to make some radical changes in AD which I expect not to happen.

When you build a forest, there should be one set of domain/enterprise admins, approx 3–5 and they should be the ONLY DAs in any of the domains. I know this is completely possible as I did it with 3 DAs and a Manager with DA account he wasn't allowed to use for a Fortune 5 company. If you poke around you can easily find enough info on me to figure out exactly which company it is.

This effectively achieves a security boundary between us, doesn't it?

Ummm I thought you said you understood technically the forest is the security boundary..... The answer to this question is NO. The domain is not a security boundary, the forest is the security boundary. Never since the domain was based on AD was the domain a security boundary, even though MSFT and Lucent documented it as such. When those papers started coming out back in like 2001 or so, those of us who figured out the holes started beating on them so Lucent recalled their paper and Microsoft made it a point to tell everyone the forest is the security boundary.

Re: Active Directory – security boundaries

but the point is that
administrators in each
domain
wouldn't be able to grant
themselves access to
resources in the other
domain. That's correct, isn't
it?

Nope. The forest is the security boundary.

The only way to stop this
happening is to make a
placeholder tree
root

The empty root does nothing to increase
security for this.

then am I correct in thinking
that all the other
administrators of the
standard domain can't grant
themselves access to
resources in the finance
domain?

Nope. The forest is the security boundary.

Sorry about the long post.
I'm grateful for any insights!

No problem, the main thing you need to
understand is that the forest is the security
boundary, not the domain. Forest, not
domain. Forest, not domain. This is not
likely to change any time soon. The forest is
STILL the security boundary in Longhorn
AD.

The next thing you need to understand is a
core security concept. You can not prove
something secure, you can only prove
something insecure. If you think something
is secure, it is simply unknown for its

Re: Active Directory – security boundaries

security state or BELIEVED to be secure due to faulty logic (e.g. I can't think of a way to hack it, hence it can't be hacked...). Someone else may very well know how to compromise what you consider secure.

This design you have is an excellent example of that core security concept. You believe it to be secure because you aren't aware of or understand the possible holes and I know that if I were a finance domain DA I could escalate myself to Enterprise Admin and boot you out likely in the first 30 minutes I sat down to do it. If I have physical access to a root DC it would take even less. If I were a standard domain administrator I could also escalate myself to EA but it would probably be more fun just to escalate myself to have rights in the Finance domain to make you look bad because if you say absolutely no one could possibly infiltrate the Finance domain except you and the Finance domain gets infiltrated, you have just admitted to doing it. :)

joe

--

Joe Richards Microsoft MVP Windows
Server Directory Services
Author of O'Reilly Active Directory Third
Edition
www.joeware.net

---O'Reilly Active Directory Third Edition
now available---

<http://www.joeware.net/win/ad3e.htm>

David Chadwick wrote:

Hi,

I hear time and time again
that a domain is not a
security boundary in AD
and that only the forest is a

Re: Active Directory – security boundaries

true security boundary.
Obviously this is technically true.

My question is not because I don't understand AD structure, but because I'm trying to understand what the risks are in using multiple domains in a forest rather than separate forests. I understand the technical side of AD, but not necessarily the theory and the "why".

Let's say we have a typical scenario – an internal domain for normal company users and an external domain in the perimeter for customers. I'm trying to understand the fundamental security differences (I understand the schema side of things) between having these domains in separate forests or in the same forest.

Scenario 1 – separate forests with a 1-way trust where the external domain trusts the internal domain. Both domains are forest roots.

Scenario 2 – external domain is in the same forest either as a child domain or the root of a new tree.

Internal domain is the forest root.

In my experience "security experts" always recommend scenario 1 and it makes sense that it would be more secure. However, no one has been able to articulate to me exactly WHY it is more secure at a technical level. Why is a separate domain in the same forest not an

Re: Active Directory – security boundaries

"acceptable security boundary"?

My understanding is as follows:

Domains are in the same forest. Internal domain is the tree root. Internal and external domain will trust each other for authentication (due to automatic trusts between domains within a forest). I'm happy that all administrators in the internal domain (which is the forest root) will automatically be able to administer the external domain. The reverse should not be true though, as the external domain is not the tree root – right?

Users in the external domain can only access resources that they have group membership of. If they aren't members of groups that have access to any resources in the internal domain, then what is the problem? They have effectively been isolated in their own "security boundary", haven't they?

With the other scenario (separate forests plus 1-way trust), isn't the same the case? They still won't be able to access resources in the internal domain as they can't be in resource groups from this domain. The difference is that it's not even POSSIBLE for them to be in these groups, as the internal forest does not trust the external forest (it's only the other way around).

Re: Active Directory – security boundaries

Is that the only difference?
The fact that scenario 1 is more secure because it makes it impossible to "accidentally" give them access to internal resources (because the trusts don't allow it)? That's a fair enough reason that it is more secure, I realise this.

However, let's say you can guarantee that no administrator will ever make a mistake in scenario 2 and the external users will never be placed in groups that have access to internal resources. I realise that in the real-world you can't guarantee this, and that's why you'd make the decision to use scenario 1 in the first place, but I am trying to understand the technicalities here rather than the realities.

If we can assume that these users will never be placed in groups that give them access to internal resources, then this would be secure too, wouldn't it? Again, keep in mind that I am trying to work out the technicalities rather than real-world. I want to understand the validity of saying "given the assumption that users in the external domain will never be placed in groups that give them access to internal resources, then they are effectively in a security boundary". Of course in reality the fact that an administrator COULD put them in one of these groups (accidentally or on purpose)

Re: Active Directory – security boundaries

makes it less secure by definition.

Here is another scenario I have been asked to implement:

The finance department does not want to be on our domain as they don't trust the administrators of the company domain with access to their files. In a 100% secure world we'd say "the only true security boundary is a forest, create your own forest". In the real world, they need to be part of our Exchange 2003 organisation and none of that works across forests.

So instead of separate forests, we implement the following:

Placeholder forest root domain, only a single trusted administrator has access (me :))

Tree root domain for standard company stuff (the normal IT admins live here)

Tree root domain for finance department (with their own admins)

This effectively achieves a security boundary between us, doesn't it? The administrators in the standard company domain will not be able to grant themselves access to resources in the finance domain (and vice versa). We would be able to grant THEM access to our resources (and they could grant us access to theirs), but the point is that

Re: Active Directory – security boundaries

administrators in each domain wouldn't be able to grant themselves access to resources in the other domain. That's correct, isn't it? The only person who could grant themselves access to resources in both domains would be me, as I control the forest root and can therefore be an Enterprise Admin etc.

In this scenario, you HAVE to use 3 domains to achieve what we need, is that right? If either the standard internal domain or the finance domain is the forest root, then all those administrators can escalate themselves to be Enterprise Administrators and therefore grant themselves access to the other domain. The only way to stop this happening is to make a placeholder tree root and make only super-trusted users administrators in the root. Obviously from a "political" point of view this requires the owners of both the standard internal domain and the finance domain to agree that it is ok for a third-party (me) to be the "overall administrator".

The only TRUE way for the finance people to know that only they have access to their stuff is to be in their own forest – but assuming they are happy with knowing just 1 person (or a subset) or administrators have access to the forest root, then am I correct in thinking that all the other administrators of the

Re: Active Directory – security boundaries

standard domain can't grant themselves access to resources in the finance domain? Am I also correct in thinking that the only way to achieve this is with 3 domains (because I can't allow either of the other domains to be the forest root)?

Sorry about the long post.
I'm grateful for any insights!

Cheers,
David