Migrating from Windows NT 4.0 to Windows 2000 in the real world:

The good, the bad, and the dirty little secrets

Marc DeBonis
Operating Systems Analyst – IS&C
Virginia Tech (VPI&SU)
Marc.DeBonis@vt.edu

Overview

- **Before**: why convert, politics, test lab, MS tools, in-house tools, giving notice, rules of engagement, training staff
- During
- After

Overview

- Before
- **During**: crack, backup 4.0, build accounts, save 4.0 info, bring up w2k standalone, bring down 4.0, add accounts, backup w2k, edit wins, recreate trusts, move accounts to OUs, rebuild global groups, edit web page tool, install backup sw, monitor logs
- After

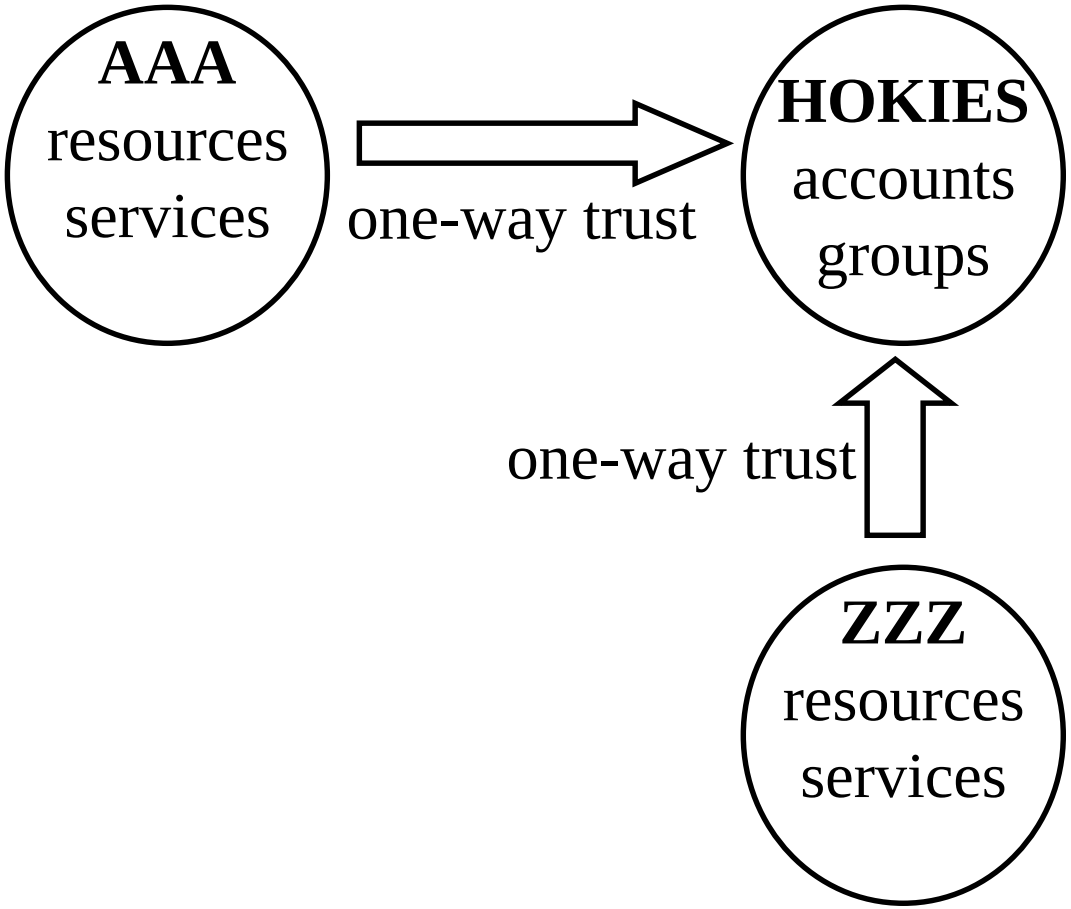
Overview

- Before
- During
- **After**: cleanup, building new OUs, security pitfalls, lessons learned, in conclusion

Why convert?

- Get ahead of the curve. Didn't get idea of NT 4.0 master accounts domain (HOKIES) out to masses fast enough
- Avoid "castles in the sky" syndrome
- Domain administrators clamoring for sub-administrative authority for accounts
- New features/functionality of w2k

Fig 1 - Current NT 4.0 domain topology



~800 Win domains/ workgroups in WINS

~400 third tier dns zones at Tech.

Politics

- Domains administrators with trust relationships to the current NT 4.0 domain HOKIES (~30)
- Communications and Network Services (CNS)
  - Controls all network infrastructure for Tech.
  - Runs Unix/BIND DNS servers.
- Call center, front line computer help desk
- Information Resource Management (IRM), manages user/resource accounts for current NT 4.0 domain
- Accounts (user and resource), ~2200 in current domain

Test lab

- Equipment
  - 20 Dell Optiplex GX1 workstations, part-time.
  - Two Dell 6300 servers, full-time.
- Tested interaction with CNS's BIND v8.9.2 implementation
  - AD – BIND interaction failed.
  - Ran w2k DDNS
  - Built w2k-pilot.vt.edu zone
- Loaded all faculty/staff ideas into "flat" AD (~8200)
- Allowed other test w2k domains to join pilot

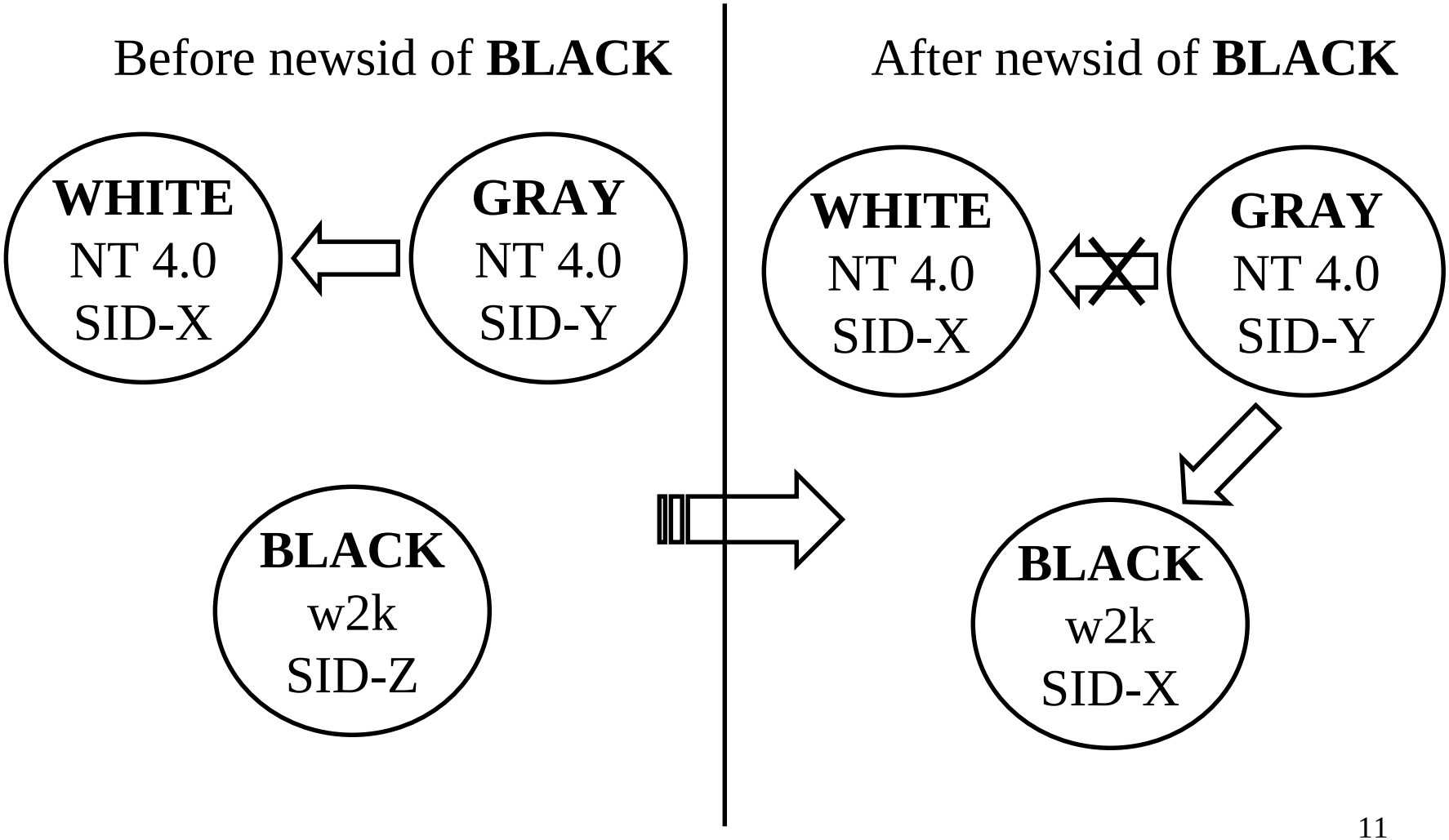
MS tools

- Copied production NT 4.0 domain to isolated subnet with Norton Ghost
- Created a trusting domain that utilized these copied accounts for authentication
- Created new w2k domain in same subnet.
- Migrated accounts and groups into w2k domain with ADMT
- Encountered “account unknown” problem in trusting domain

In-house tools

- Used WinBatch (www.windowware.com) to create 20 custom tools
- Used newsid (www.sysinternals.com) to synched system SID from NT 4.0 domain to standalone w2k server
- Promoted w2k server to DC
- Made domain names of w2k and NT 4.0 domains identical (wasn’t necessary)
- Moved trust from NT 4.0 domain to w2k Domain
- Did not encounter “unknown user” problem

Fig 2 - Re-SID'ing the w2k standalone



SID Example: S-1-5-21-515967899-920026266-1801674531

Giving notice

- Began process months in advance
- Built w2k website for FAQs, email addresses, etc.
- Created email listserv, signed up all known NT 4.0 admins with HOKIES domain trusts
- Scheduled classes to educate Call Center and IRM staff on changes between user manager and MMC
- Sent email to all “global” lists explaining changes and affects on services
- Told purchasing department not to distribute w2k cds until the root AD was ready, and then with a special label

Rules of engagement

- Developed rules for w2k administrators bringing a child domain into the AD tree
- Very strict because testing showed much greater interdependency between domains in w2k than 4.0
- See bunbun.ais.vt.edu/work/w2k/rules.html

Training

- Classes for all NT 4.0 trusting domain admins
  - Cheat sheet with FAQ (www.w2k.vt.edu).
  - Explained how they would have admin authority over those in their OU (if specified)
- Classes for Call Center and IRM
  - Familiarize staff with MMC
  - Call Center given ability to reset passwords

Crack

- In-house migration tools and ADMT would not migrate account passwords
- **Process**
  - Extracted production NT 4.0 PDC SAM to a flat file
  - Ran L0pht crack for ~ one month
  - Used most complex crack algorithm, 25,000 word dictionary
  - Dual Xenon 550 with 1GB RAM
- Results

Crack

- In-house migration tools and ADMT would not migrate account passwords
- Process
- **Results**
  - 80% of ~2200 accounts.
  - Queried LDAP for SSN/DOB pairing for those we couldn’t get or had changed from start of crack (15%)
  - Remaining 5% reset to random password as a pseudo forced expired

Backup 4.0

- Used Norton Ghost to do a partition level backup of BDC and PDC
- Disabled the ability for users to change password or user information as migration began

Build accounts

- Built .csv file of user account with all NT 4.0 account specific info (name, description, password, etc.)
- Used password/ssn-dob from crack or random/expired password for each account (user and resource)
- Sorted .csv file by SID to recreate them in order in new domain
- Could not use NT 4.0 resource kit adduser program or the like to add to w2k - would fubar account information (expiration, etc)

Fig 3 - Example of export account .csv file

```
#_of_entries
1001,U, account_name,full_name,description,password
1002,G, global_group_name,full_sid,,
1004,U, account_name,full_name,description,password
.
.
.
last_entry,U, account_name,full_name,description,password
```

- 1st # is significant account part of the SID (starts at 1001)
- U or G depending if entry is a user/resource account or group
- Skipped SIDs recreated as account_name = DEL_SID#

Save 4.0 info

- Saved all account, local group and global group information to flat files in the case we need to recover from a catastrophic failure
- Used Dumpsec (www.systemtools.com/somarsoft) to dump account and group info
- Built account correlation between NT 4.0 SAM attributes and w2k AD LDAP
  - 25 in NT 4.0
  - 207 in base w2k AD

Bring up w2k standalone

- Brought up w2k PDC standalone
  - Isolated from network
  - Did not allow it to register with WINS
- Put on network to run newsid and synched SIDs between w2k standalone and NT 4.0 PDC
- Removed from network

Bring down NT 4.0

- Brought down BDC
- Brought down PDC
- Deactivated automated monitor tools watching these machines
- Ignored any calls that started coming in

Add accounts

- Added local accounts to w2k standalone, using
  - In-house tools (WinBatch)
  - Created accounts .csv file in previous step
- Added accounts in order of their sid (sequentially)
- For accounts that had been previously deleted, made placeholder accounts to use those SIDs
- Global groups
  - Create placeholder accounts since they can't be recreated.
  - Named account "DEL_groupname" to indicate anything acl'ed by them in trusting domains

Backup w2k

- Brought standalone w2k server into AD
  - Installed DDNS
    - Zone authority for all xxx.w2k.vt.edu
  - Used same netbios domain name as NT 4.0 domain
- Brought up as root of AD
- Backed up w2k with Norton Ghost and scheduled MS backup

Edit WINS

- Windows Internet Naming Service (WINS) running because CNS does not bridge netbios broadcasts across subnets
- Altered static WINS entries so netbios lookups for the HOKIES domain points to new system
- Netbios name lookups can be cached on Windows machines (see nbtstat) might force some users to manually clear cache or reboot

Recreate trusts

- Began testing between a trusting domain (Exchange server domain) and the new HOKIES domain
- Forced to break and re-establish trusts. Unable to migrate trusts because
  - Originally established with a one-time password
  - Automatically updated
- Contacted ~30 trusting domain admins and re-establish one-way trusts - slow process

Move accounts to OUs

- Asked each NT trusting domain admin for a .csv file with HOKIES accounts from their department
- Created OUs based on DNS zones of departments
  - Avoided much political fighting
  - Eliminated multiple domains in same department
  - Example: PDC with dns entry *foo*.*bar*.vt.edu, OU = *bar*
- Moved requested users into created OUs
- Gave admins partial “account operator” privileges over accounts in corresponding OU

Rebuild global groups

- Could not recreate global groups directly
  - Had created accounts before installing AD, so "global" accounts did not exist
- Created global groups in their appropriate OUs and added users from saved flat files
- Had to re-acl security in each domain
  - Due to new global group SIDs
  - Only ~5 -- phew!

Edit web page tool

- Custom web page to change HOKIES account password for
  - Apple Macintosh users
  - Outlook users
  - Users without access to a Windows client
- Uses WinBatch and Imatix's Xitami httpd (www.imatix.com)
- Altered code to point to new PDC IP address

Install backup sw

- Current backup client did not understand AD system files and state
- Developed a three phase backup program
  - Used Norton ghost to backup OS and NTDS partitions to file, burned these to cd
  - Scheduled full nightly MS backups to backup system to a flat file (including system state)
  - Use Legato NSR client for nightly backups of the flat file to tape, stored off-site

Monitor logs

- Turned on logging for the following logs:
  - Account logon events [fail]
  - Account management [fail,success]
  - Directory service access [fail]
  - Logon events [fail]
  - Policy change [fail,success]
  - Privilege use [fail]
- Filled up security event log VERY quickly.
  - Primarily due to Outlook clients left logged in, and their password having been changed.
  - DoS via Outlook! 5-15% cpu overhead due to this alone!

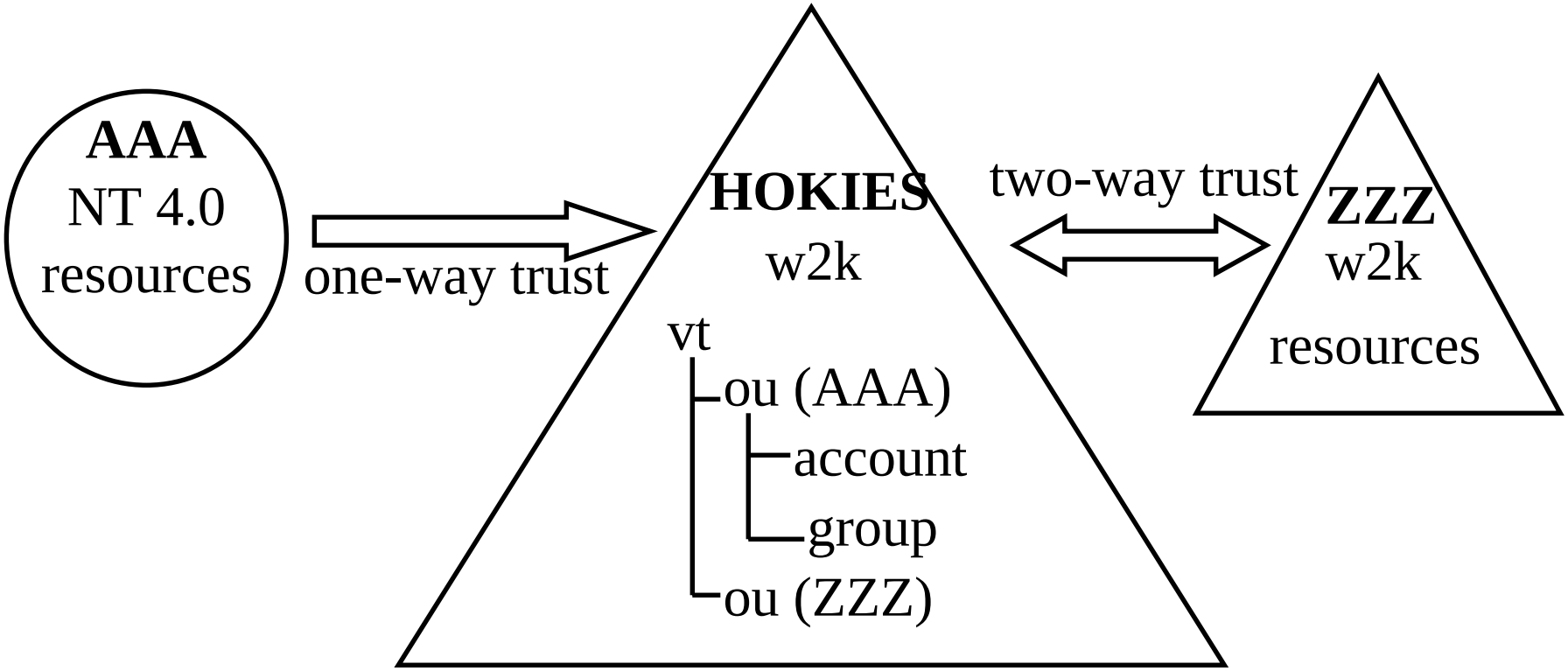
Cleanup

- Disabled accounts that had been disabled in NT 4.0 domain
- Put accounts that had no defined OU into the “not-ou” OU
- Wrote a simple web page to discover via DNS what OU a person belonged to for IRM
- Wrote a program to move resource accounts into OUs of responsible person
- Did not to move from Mixed to Native mode

Building new OUs

- Process for IRM to add new users to AD
  - OUs not already existing are created on the fly
  - Based on DNS on user's desktop machine
- Automated OU creation and user moving
  - Wrote a program to locate user accounts in "not-ou" and match to WINS entry
  - Dangerous!

Fig 4 – Current W2K domain topology



Security pitfalls

- Anonymous users can not enumerate accounts
  - Unlike NT 4.0
  - Decided this when installing AD
  - Added the Everyone account to “Pre-Windows 2000 Compatible Access” group
  - Guest is still disabled
- Authenticated users can add workstations to the domain (w2k default) – whoops!
- Enterprise admins must authorize use of w2k DHCP in AD (can be delegated)

Calendar of events

- January
  - 12, W2K released, stopped cd distribution
  - 28, Added informational label, started cd distribution
- February
  - 1, Created w2k steering committee
  - 21, Started part-time test lab, brought up w2k-pilot
- March
  - 10, began to allow in child domains to w2k-pilot
  - 20, loaded all faculty/staff accounts into pilot (~8200)
- April
  - 3, move pilot to native mode, tested new management
  - 17, developed rules of engagement for production

Calendar of events

- May
  - 1, began to allow in child domains to w2k-pilot (again)
  - 4, tested backup/recovery of w2k AD
- June
  - 5, developed migration path
  - 30, trained Domain admins, IRM, Call Center
- July
  - 1, Began advertising AD Day
  - 10, AD day, performed migration to production w2k.vt.edu
  - 28, joint review of AD migration

Lessons learned

- Give people plenty of notice so they can't complain later they weren't in the loop.
- Stick to a schedule, don't allow feature creep
- Get acknowledgement of tasks from all involved well in advance (key dependency meetings, project charts, calendar notices, etc)
- Test in an environment approximating production conditions
- Identify hidden dependencies
- Get the metrics before, during and after the migration - Management loves numbers!

Conclusions

- Migration possible with few resources and without fancy (i.e. expensive) software
- Identifying common errors in the pilot avoids the upset stomach **when** they occur in production
- Politics is a major piece of the AD puzzle

Thanks to…

- **Michael Johnson –** My lone staff member. Without his help the migration wouldn't have been successful.
- **Randy Marchany –** Security expert and frequent SANS speaker. Thanks for helping me get this gig.
- **Nancy Brauer –** My S.O. who humored my late hours and bought chocolate covered espresso beans to keep us going for all of AD day.
- **WindowWare –** For WinBatch, Marty, and ADSI extender. Which allowed us to make the in-house tools.
- **SysInternals –** For NewSid, the critical component.