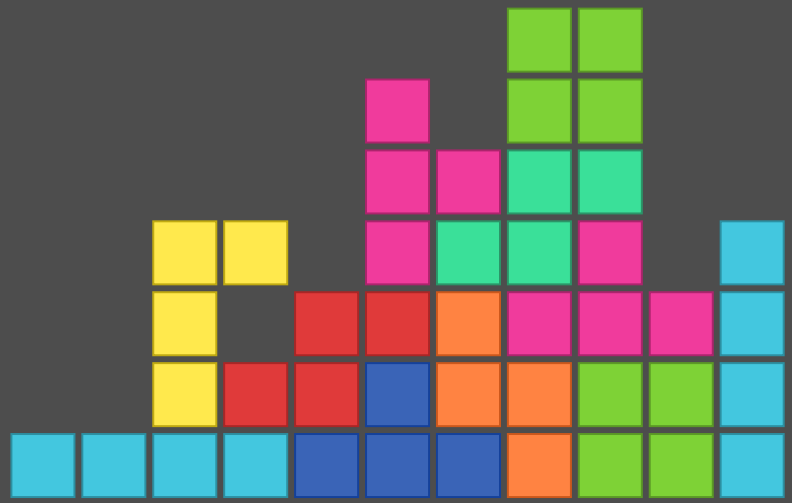
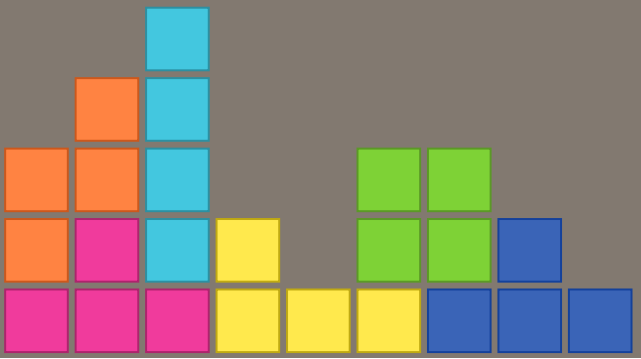
Samba AD / MIT Kerberos: Path out of experimental

SambaXP 2023



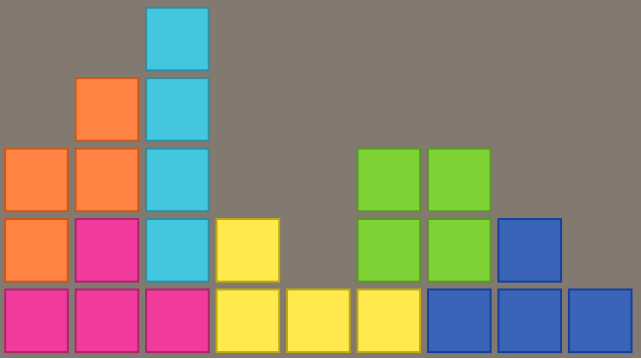
About Alexander

- FreeIPA core developer
- Samba Core Team member since 2003



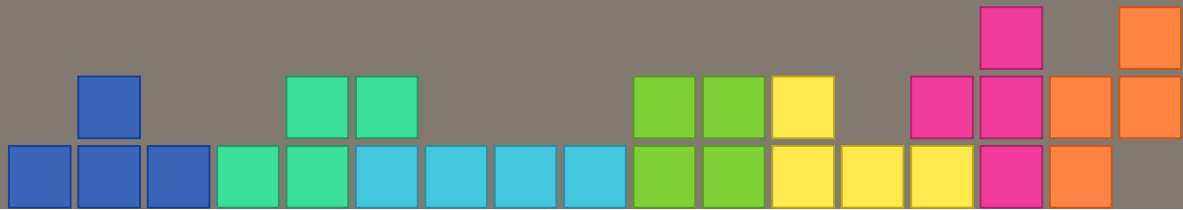
About Andreas

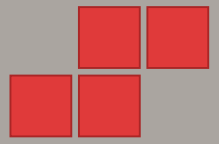
- Samba maintainer at Red Hat
- Samba Core Team member since 2010



1

Who remembers SambaXP 2017





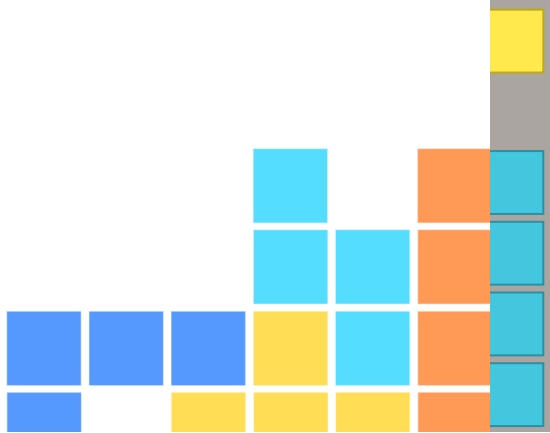
May the force

redhat.

SAMBA AD

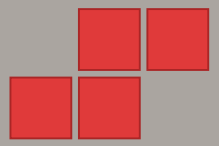
for the Enterprise

May 4th, 2017



Andreas Schneider

Red Hat Inc.



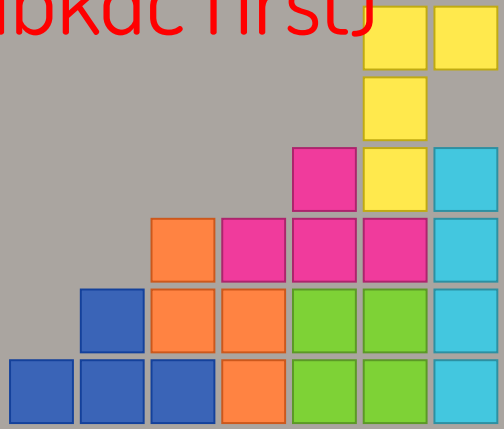
Back to 2017

WHAT IS MISSING?

- → PKINIT support (should work, tests missing)
- → Smartcard support
- → Kerberos impersonation support (S4U2SELF/S4U2PROXY)
- → RODC support (We need a libkdc from MIT Kerberos for that)

What did we do since then?

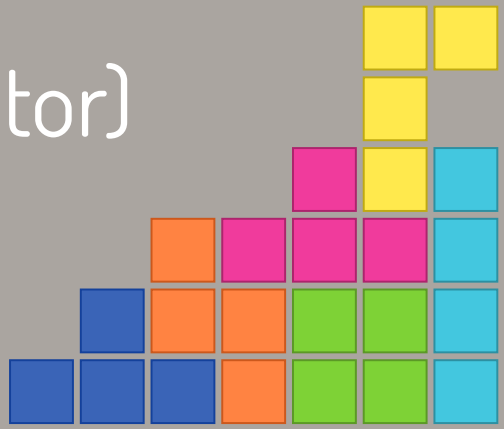
- ✓ PKINIT support
- ✓ Smartcard support
- ✓ Services for you (S4U2Self/S4U2Proxy)
- 😭 RODC support (We need a MIT libkdc first)

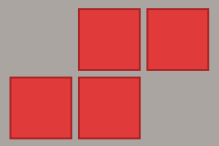


What did we do instead?

We implemented support for

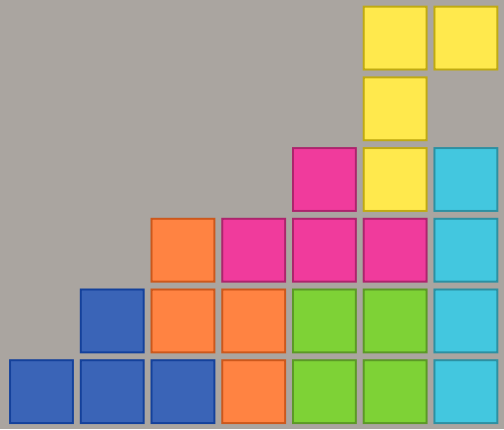
- 🤩 Resource-Based Constrained Delegation (RBCD)
- 😀 Asserted Identity (S4U2Self indicator)





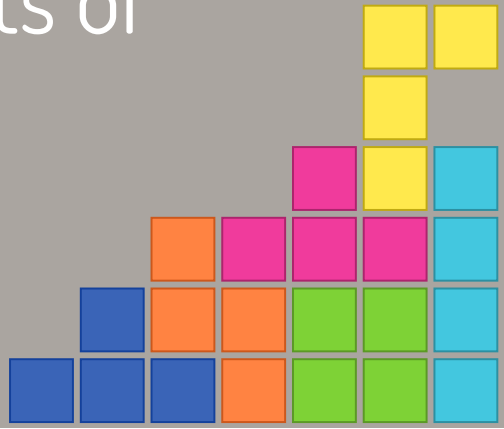
What was driving this work?

- Security bugs in Kerberos protocols and implementations

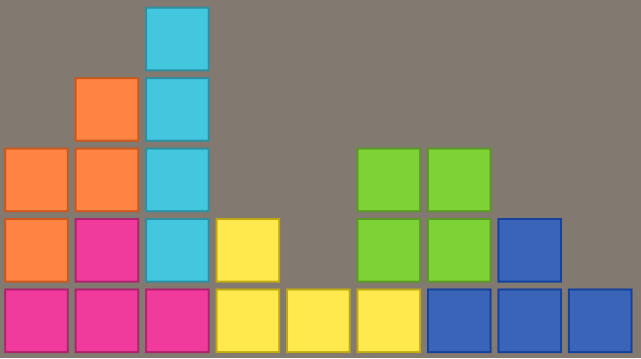


Which security bugs?

- Bronze bit attack (CVE-2020-17049)
- Identity mismatch issues with unprotected parts of Kerberos tickets (CVE-2020-25719, CVE-2020-25718, CVE-2020-25717)
- Yet more issues with unprotected parts of Kerberos tickets (CVE-2022-37967)

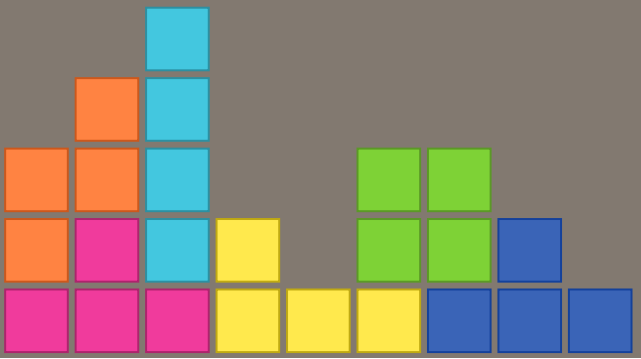


Bronze bit attack (CVE-2020-17049)



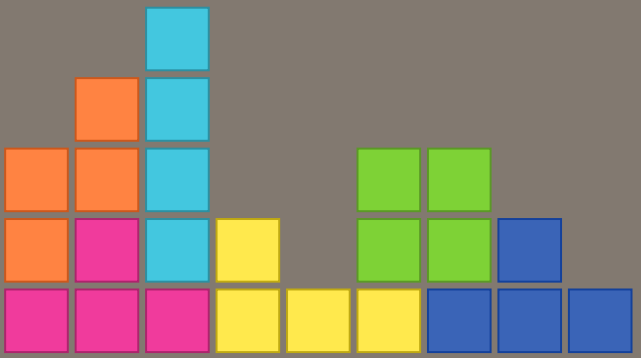
Bronze bit attack

- Bronze Bit attack is another variation of the older Golden Ticket and Silver Ticket attacks against Kerberos authentication



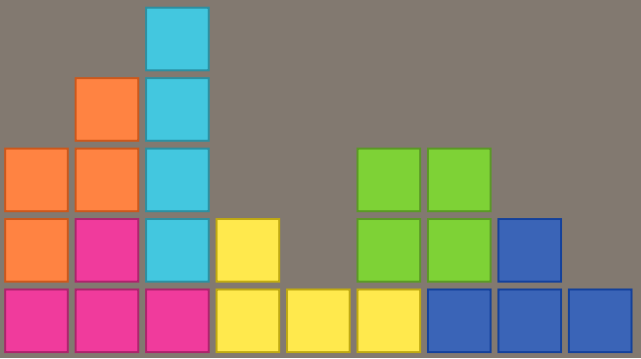
Bronze bit attack

- The difference between Golden Ticket, Silver Ticket, and now the Bronze Bit attacks is in what parts of the Kerberos authentication protocol attackers go after



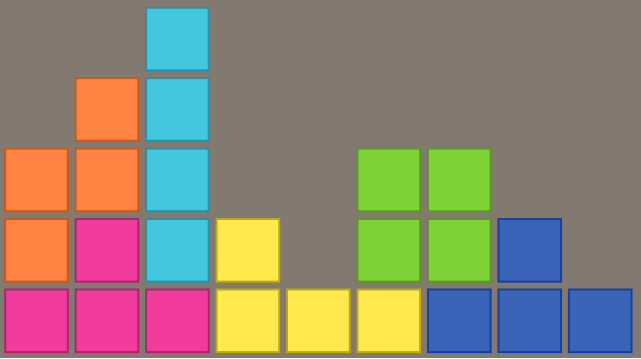
Bronze bit attack

- In the case of Bronze Bit, attackers target the S4U2self and S4U2proxy protocols



Bronze bit mitigation

Pre-requisite work for Resource-Based Constrained Delegation (RBCD) support



Bronze bit work

- RBCD implementation needed in MIT Kerberos
  - Caused API change for the KDB interface how to issue PACs
  - Started by Isaac Boukris and continued by Robbie Harwood, then Andreas and Greg Hudson finished it
  - Isaac also started to implement the client side in Heimdal

Bronze bit work ...

benefited from Kerberos test suite in Samba!

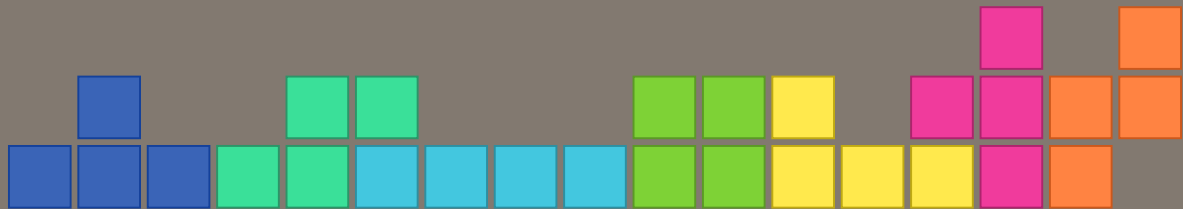
- First time we had comprehensive Kerberos test suite for AD interoperability, thanks to Joseph Sutton and Isaac Boukris!
- MIT KRB5 PR: https://github.com/krb5/krb5/pull/1225
- Samba MR: https://gitlab.com/samba-team/samba/-/merge_requests/2330

RBCD

RBCD is a key for cross-forest communication

- FreeIPA design document collects many use cases here (thanks to Isaac!)
- Delegation of credentials across the forest trust is not possible anymore without RBCD!!
- RBCD is not supported by Heimdal-based Samba AD (yet?)
- `samba-tool delegation --help`

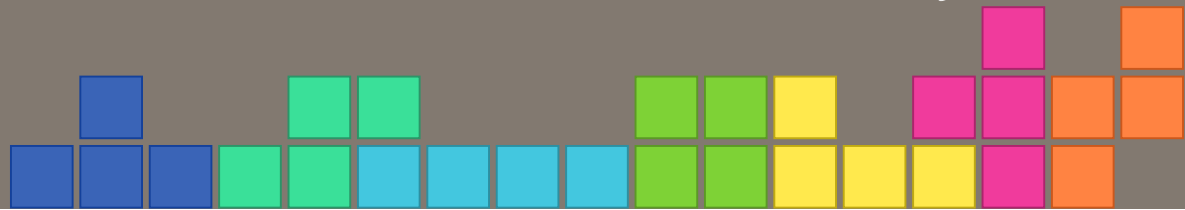
Then it was getting dark in the forest



Security update by MS on Nov 9th 2021

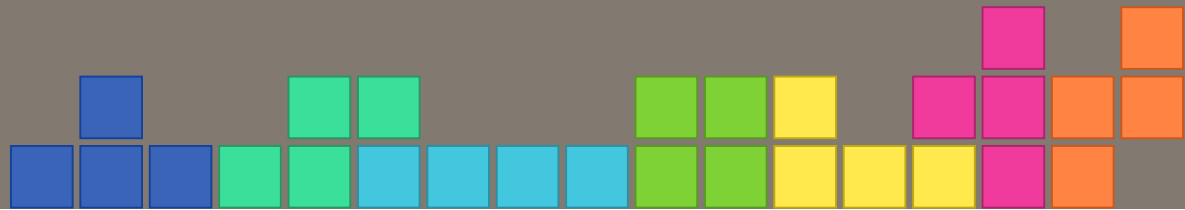
Four issues among the published security fixes were attributed to Samba Team and its members:

- CVE-2021-42291: ADDS EvP Vulnerability
- CVE-2021-42287: ADDS EvP Vulnerability
- CVE-2021-42282: ADDS EvP Vulnerability
- CVE-2021-42278: ADDS EvP Vulnerability



Samba did a coordinated release

- CVE-2020-25717: A user on the domain can become root on domain members
- CVE-2020-25718: Samba AD DC did not correctly sandbox Kerberos tickets issued by an RODC
- CVE-2020-25719: Samba AD DC did not always rely on the SID and PAC in Kerberos tickets



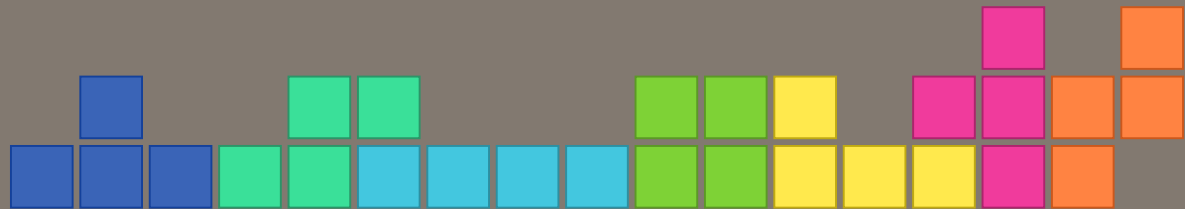
Kerberos identity mismatches

Common problem for MIT Kerberos and Heimdal Kerberos-based Samba AD

- The POSIX identity is not tied to Kerberos principal:
  - If mapping is misused, bad things can happen
  - `root$` machine account could login as root user

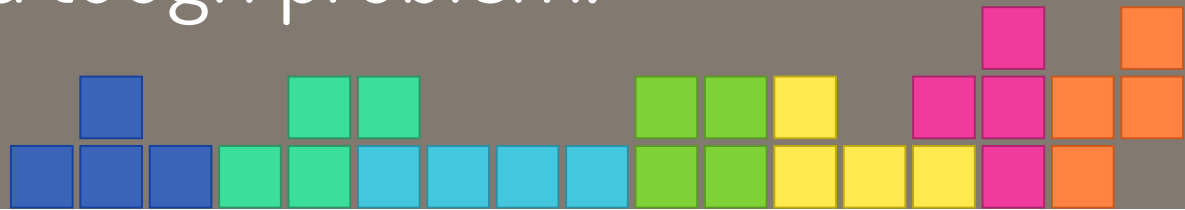
Kerberos identity mismatches

- Name-based authentication has been known to have issues for a long time
- There is a lack of user or group namespaces: a `root` user defined on one Linux machine would not necessarily be the same `root` user as on the other Linux machine



Names/principals in the Kerberos Protocol

- The Kerberos protocol deals with principals user@REALM
- For authorization purposes applications need to map a Kerberos principal to a local operating system user identity.
- Mapping identities between different representations is a tough problem.

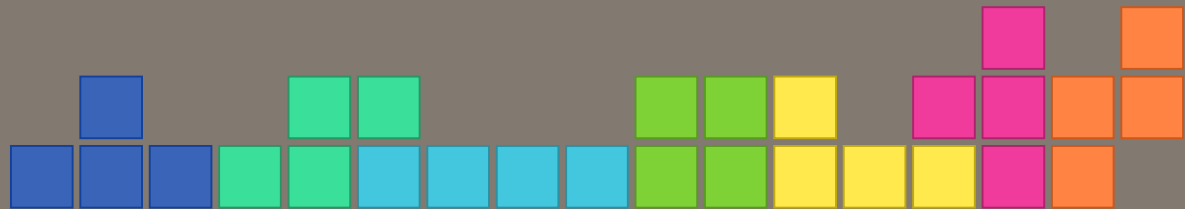


Kerberos and the PAC

- One of extensions to Kerberos protocol introduced in AD is the PAC (Privilege Attribute Certificate)
- If PAC is present the application could use the PAC properties to map the Kerberos principal more precisely -- even on Linux.
- If an attacker is able to request a ticket without PAC, an application would be like a Cyclops: single-eyed and potentially fooled by an attacker.

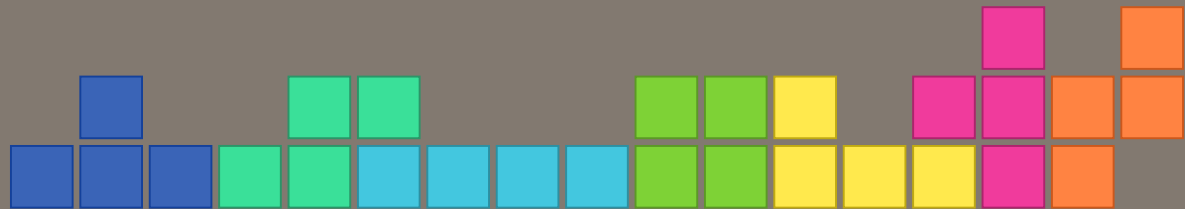
Fixing Kerberos identity mismatches in Samba AD

- Fix required better protection at the database layer in Active Directory
- Also required enforcements of cryptographic signatures in Kerberos tickets
- Enforcement of PACs to convey more information about the environment to apps



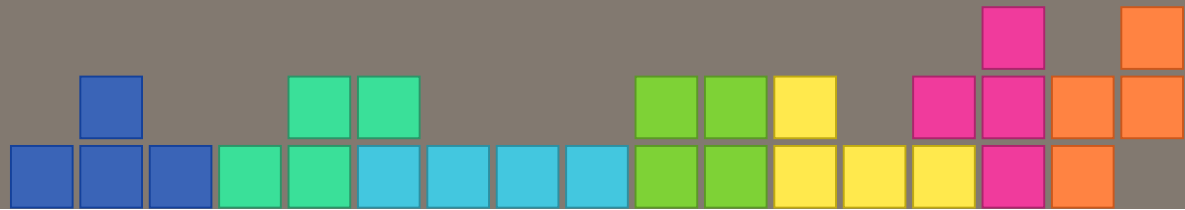
CVE-2020-25719 (Always require PAC)

- We require a PAC to be present now
- New PAC_REQUESTER_SID buffer (in addition)
  - The KDC now validates that the client principal (username) resolves to the same SID that is used in the PAC_REQUESTOR_SID buffer of the PAC



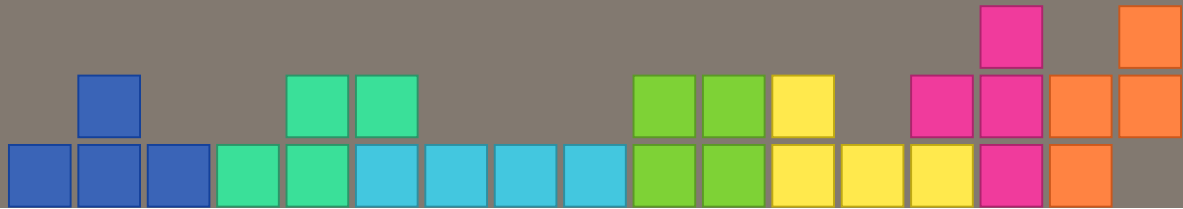
CVE-2020-25718 (RODC)

- Samba support Read-Only Domain Controller (RODC), which is meant to have minimal privileges in a domain.
- Missing RODC checks allowed the RODC to issue Admin tickets (Heimdal only)



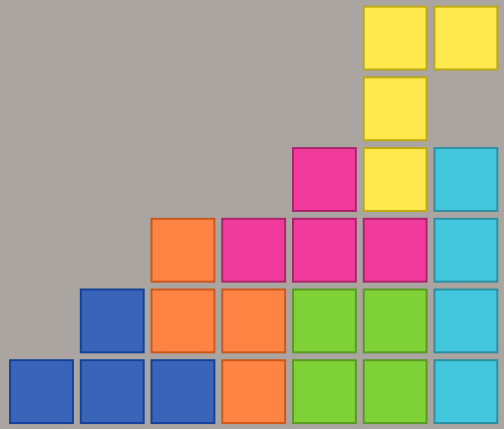
CVE-2020-25718 (User mapping)

- A user in an AD Domain could become root on domain members
- Prevent mapping users lower than a minimum uid (1000 by default)
- `man smb.conf` -> `min domain uid`



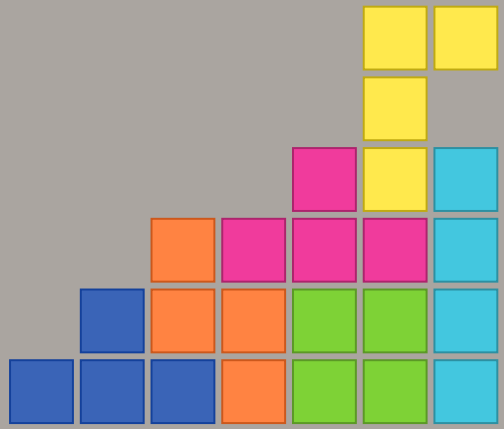
2

Collaboration with MIT Kerberos

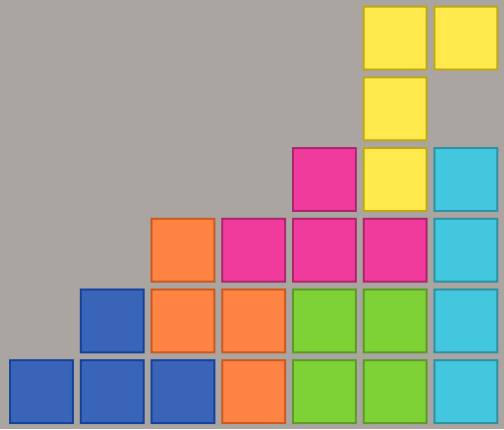


Collaboration with MIT Kerberos

- Responsive community
- People with great knowledge about Kerberos
- Tests cover scenarios we don't cover with Samba

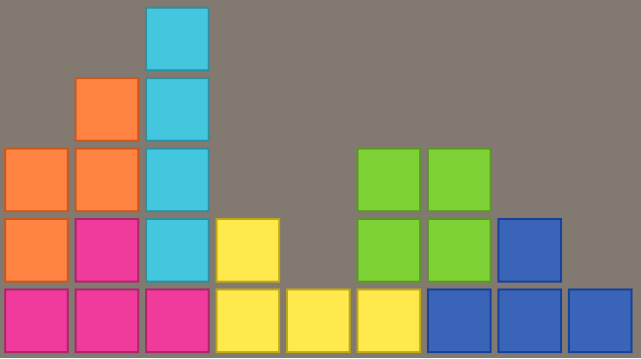


New KDB API for issuing PACs



3

What's still missing



What's still missing

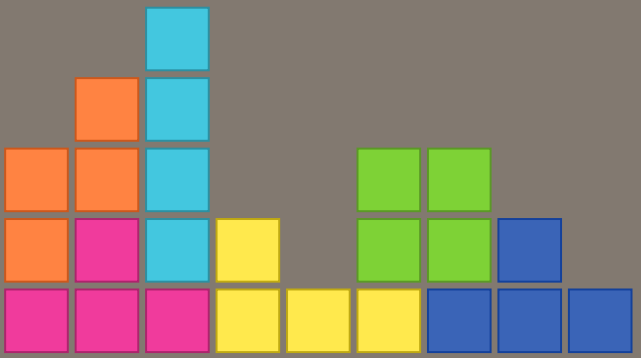
- Authentication audit logging (implemented but tests don't pass) https://git.samba.org/?p=asn/samba.git;a=shortlog;h=refs/heads/asn-mit-kdc-auditlog
- Support for ECC in PKINIT in MIT Kerberos
- Support for compound claims (for AD Federated Services)

Path to productization

- Get Samba tests adjust to accept MIT Kerberos error codes
- Release Samba AD/MIT build as production ready setup in Fedora 39+
- Get Samba selftest running as part of RPM process
- Work with Fedora QA to test Samba AD at compose level

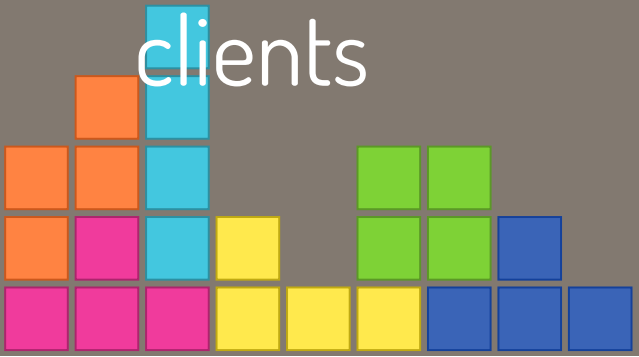
Running Samba selftest

- Run Samba selftest as part of Fedora gating
- Gating runs tests after building packages and before they go into the distro
- Allows to detect issues early

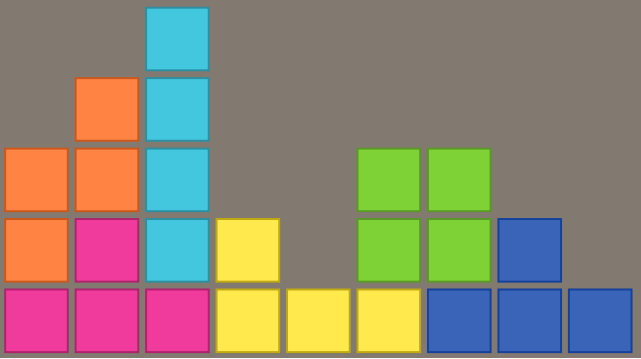


Fedora QA integration

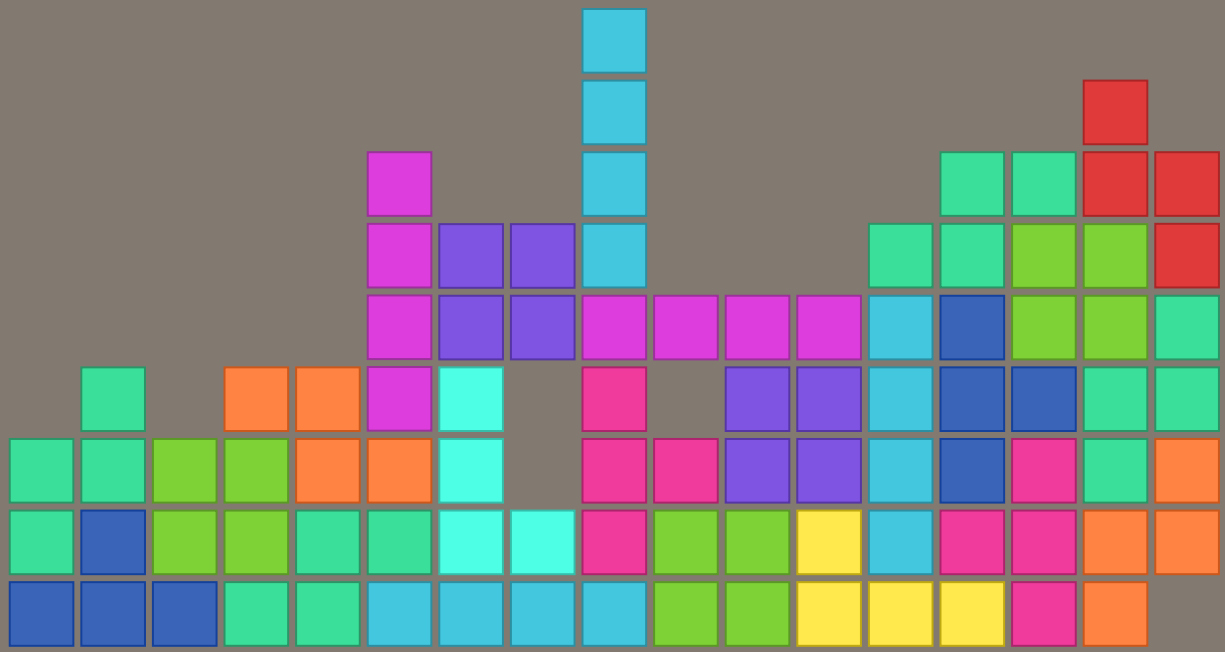
- Fedora QA runs OpenQA instance
- Allows to test full cycle: boot VM, network, graphics, etc.
- Already runs FreeIPA domain controllers and clients

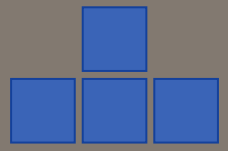


Fedora QA integration



GAME OVER





Questions?

Mastodon: @cryptomilk:mastodon.social

Blog: blog.cryptomilk.org