FNAL CD Meeting

WMS-related security activities

Pilot security issues

- Pilots enter the site as a user and run jobs of another user
- Pilot jobs introducing new security problems
  - users sharing UID with pilots
  - site policy not used
  - no final user accounting/accountability
- Two vectors for solving the problem
  - providing tools (gLExec)
  - getting pilots to use them
    - glideinWMS
    - collaboration with other pilot groups (PANDA)

Middleware security issues

- A compromise of a job handling service compromises all the users using it
  - Resource brokers (PUSH model)
  - Pilot WMSes (PULL model)
  - Portals, adapters, converters
- All of the above is not under site's control
  - Sites only aware of pilots
- An end-to-end solution seems the best approach
  - FNAL-driven collaboration with Madison on Epensys

Priorities (1)

1) gLExec deployment on OSG highest priority (1 FTE month)
   - gLExec in VDT and being tested in ITB
   - will need to convince sites to deploy it
2) Help all pilot groups use it (1 FTE month)
   - glideinWMS has it
   - Get CDF to use glideinWMS
   - Get PANDA use the gLExec-compliant part of glideinWMS

Priorities (2)

3) End-to-end security (3 FTE months)

- Understand the problem
- Get the basic tools and implement a prototype
- Integrate with basic Grid tools (Condor-G and gLExec)
- Integrate with other Grid tools (TBD)
- Deploy OSG wide

Extension of the VO Services Tactical Plan?

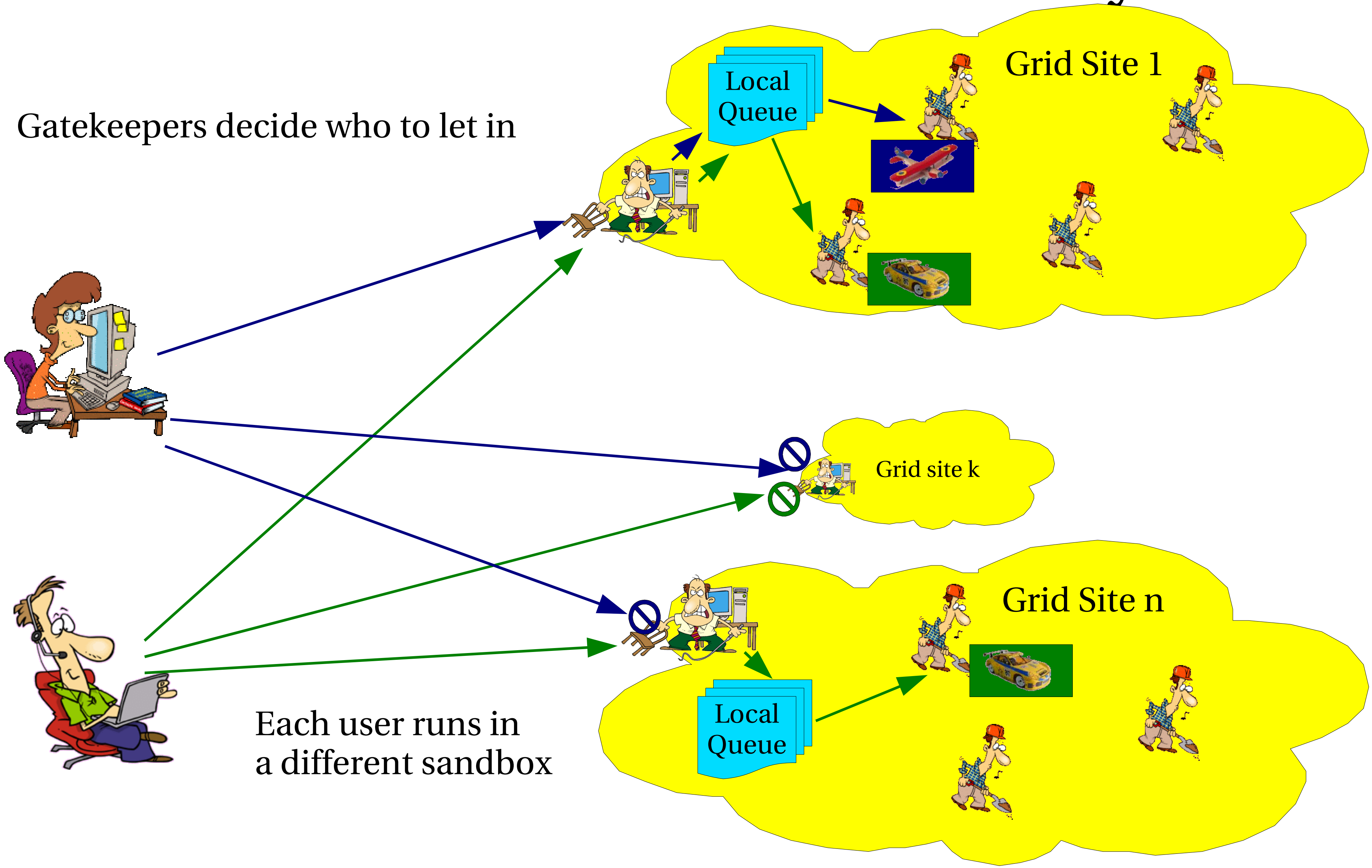
Backup slides

Parallel activities (1 FTE month)

- Standardize AuthZ callouts
  - Possibly discontinue PRIMA code
  - Two vectors
    - Standardize over-the-wire protocol with GUMS and SAZ
    - Standardize C-callout (extend current Globus one)
- Participation in policy discussions (OSE, OSG, JSPG)

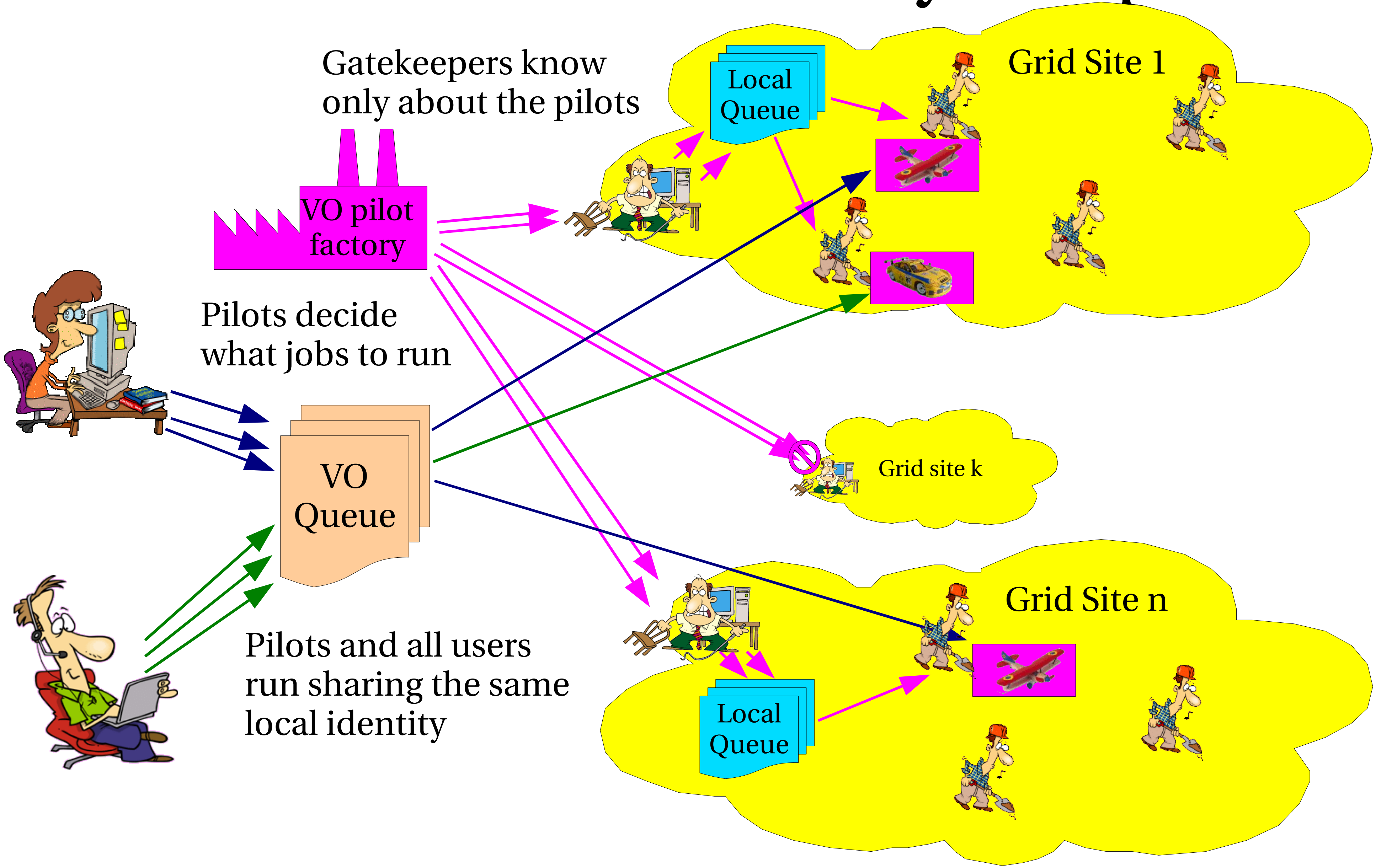
Traditional Grid security

Gatekeepers decide who to let in



Each user runs in a different sandbox

Problems introduced by the pilots



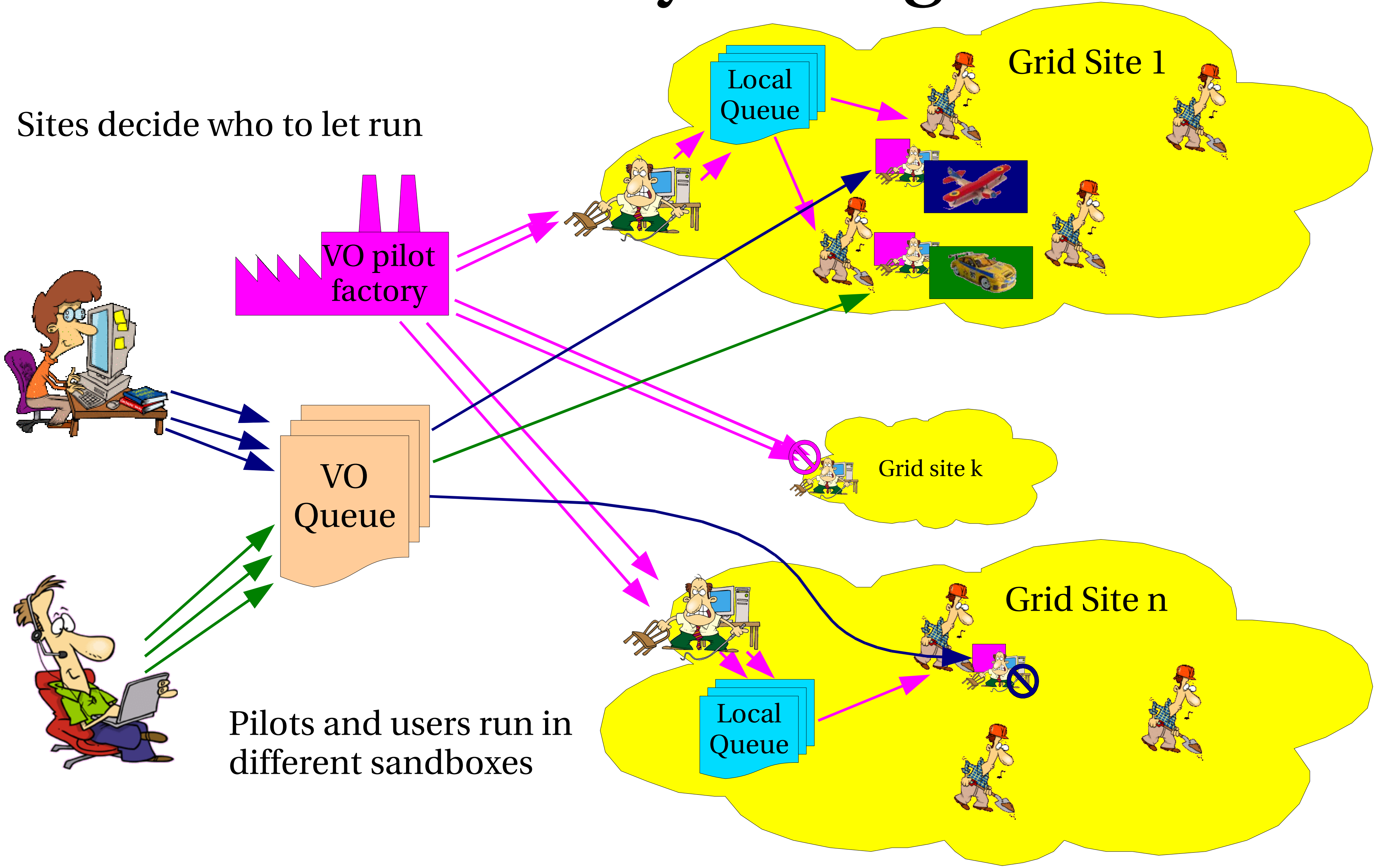
Gatekeepers know only about the pilots

Pilots decide what jobs to run

Pilots and all users run sharing the same local identity

Pilot security with gLExec

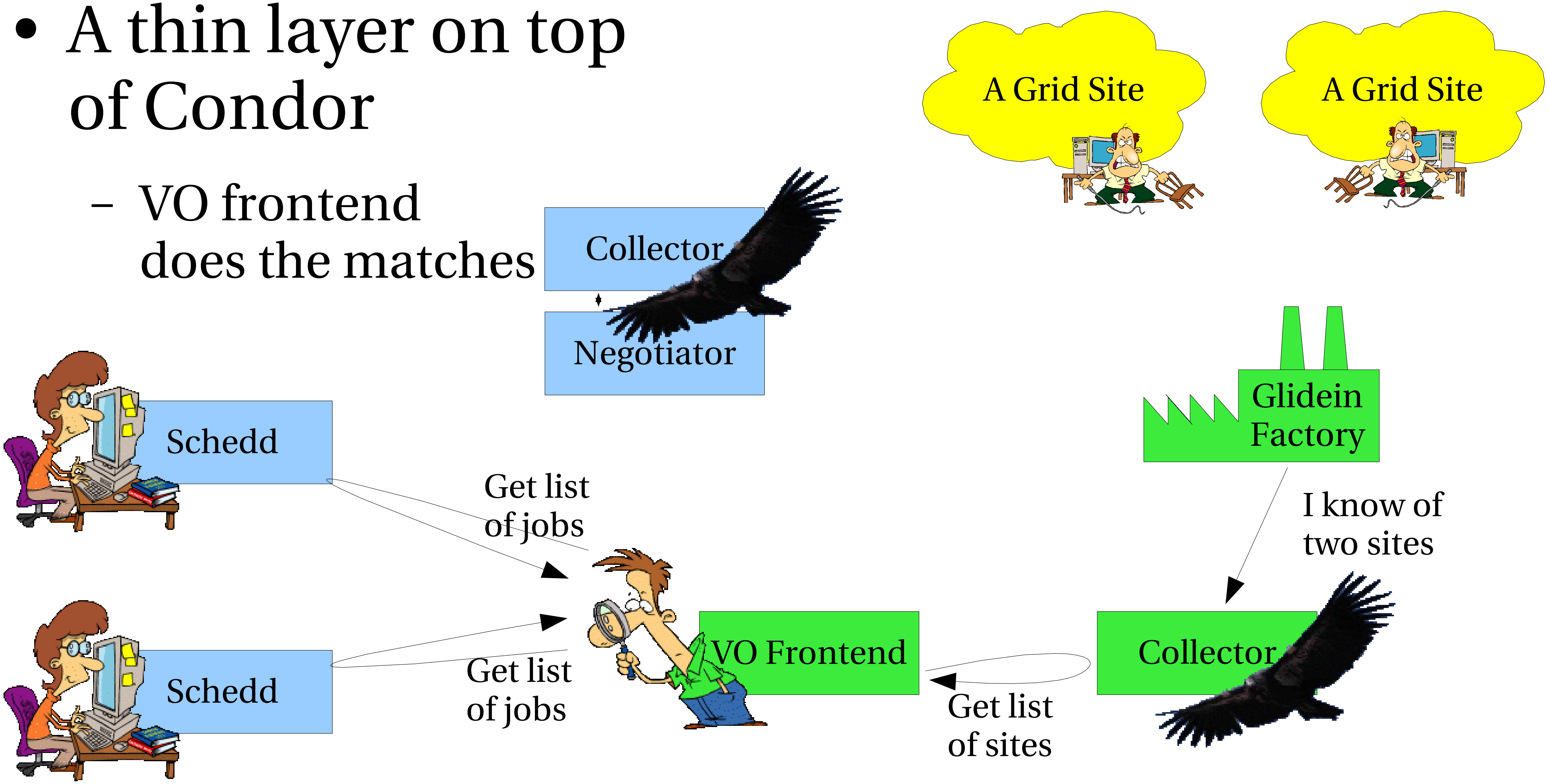
Sites decide who to let run



Pilots and users run in different sandboxes

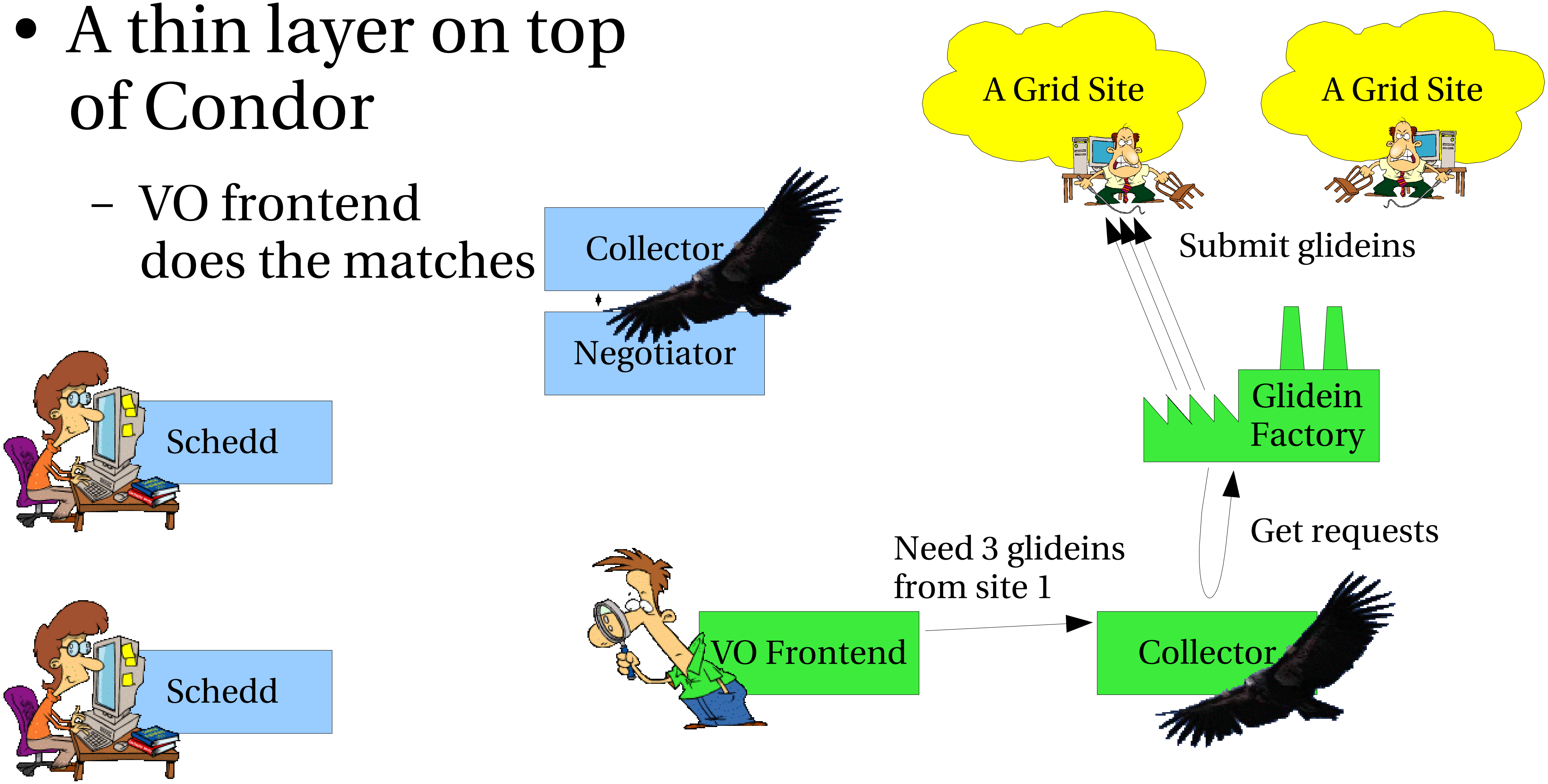
glideinWMS (1)

- A thin layer on top of Condor
  - VO frontend does the matches



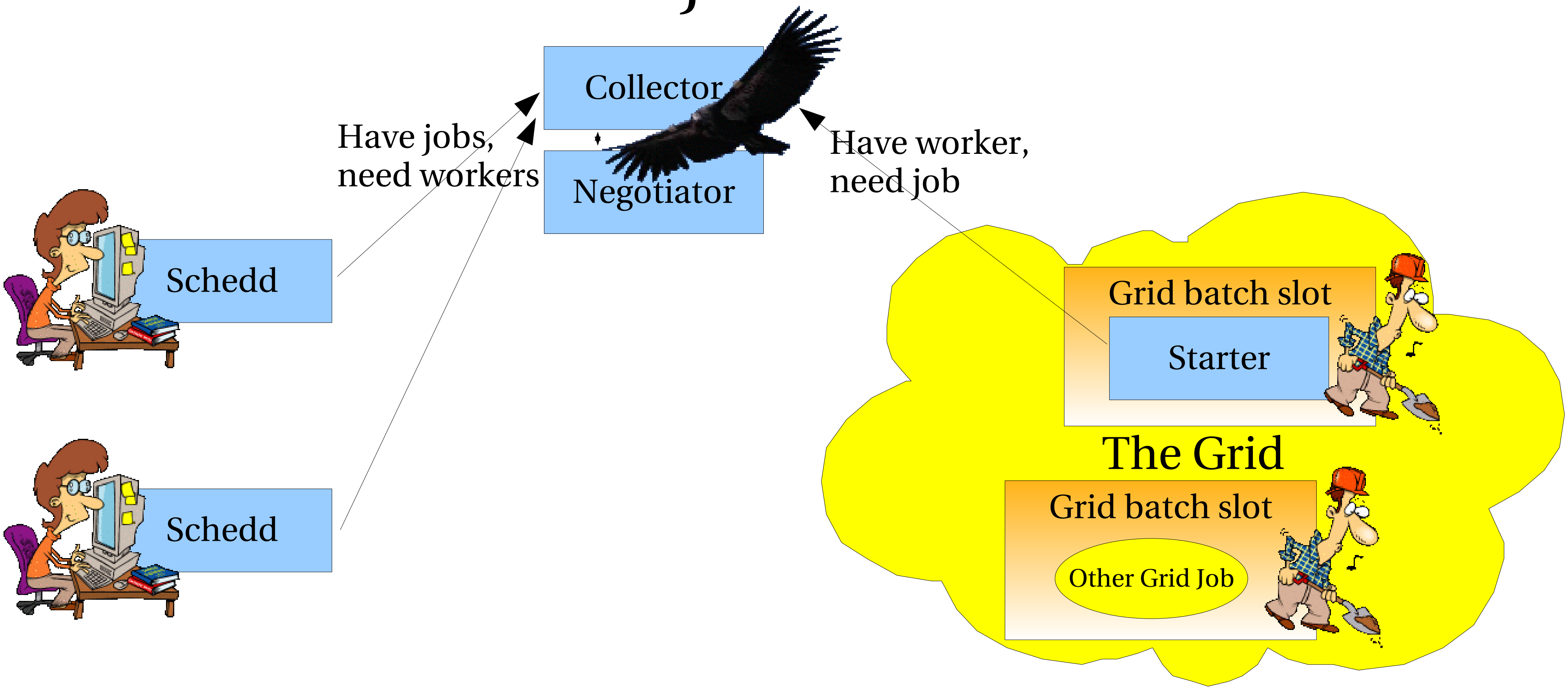
glideinWMS (2)

- A thin layer on top of Condor
  - VO frontend does the matches



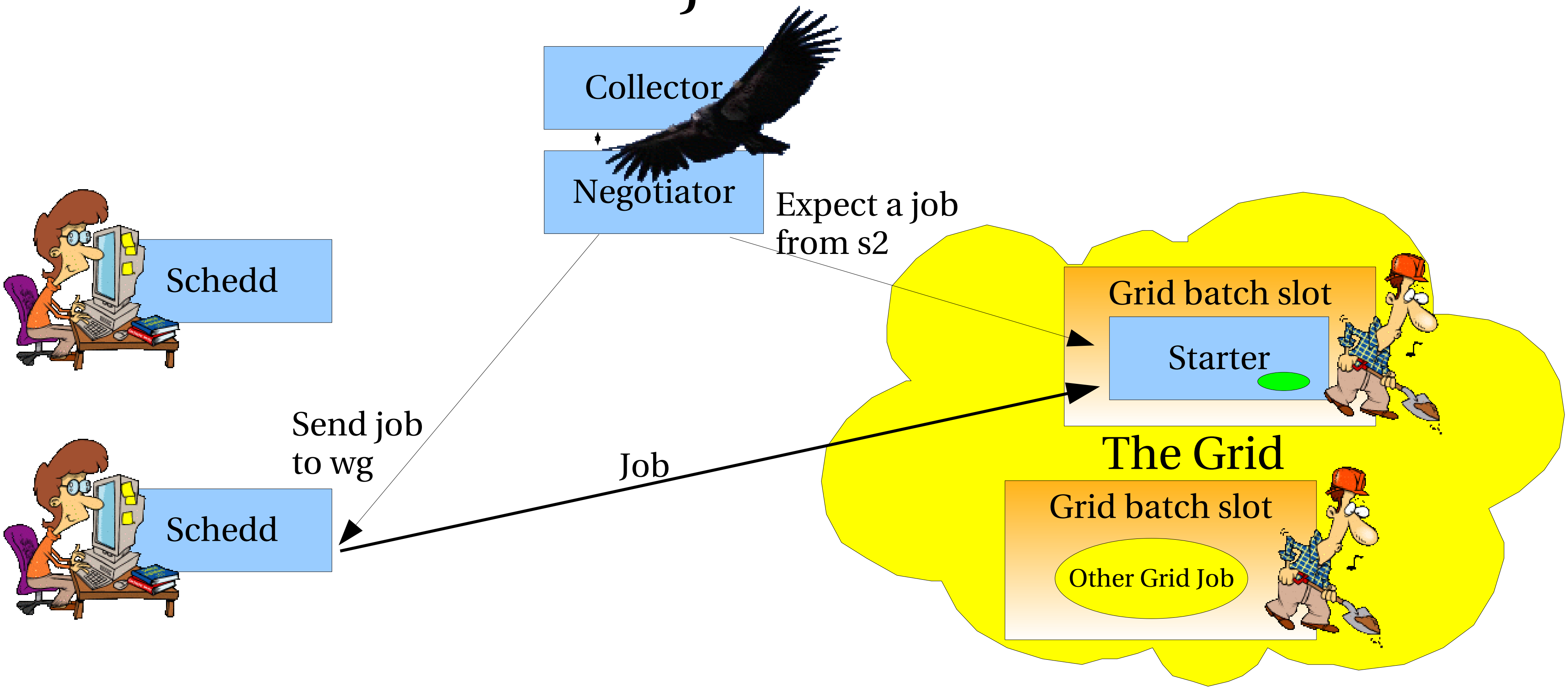
Glideins (1)

- Just regular starters
- Submitted as a Grid job

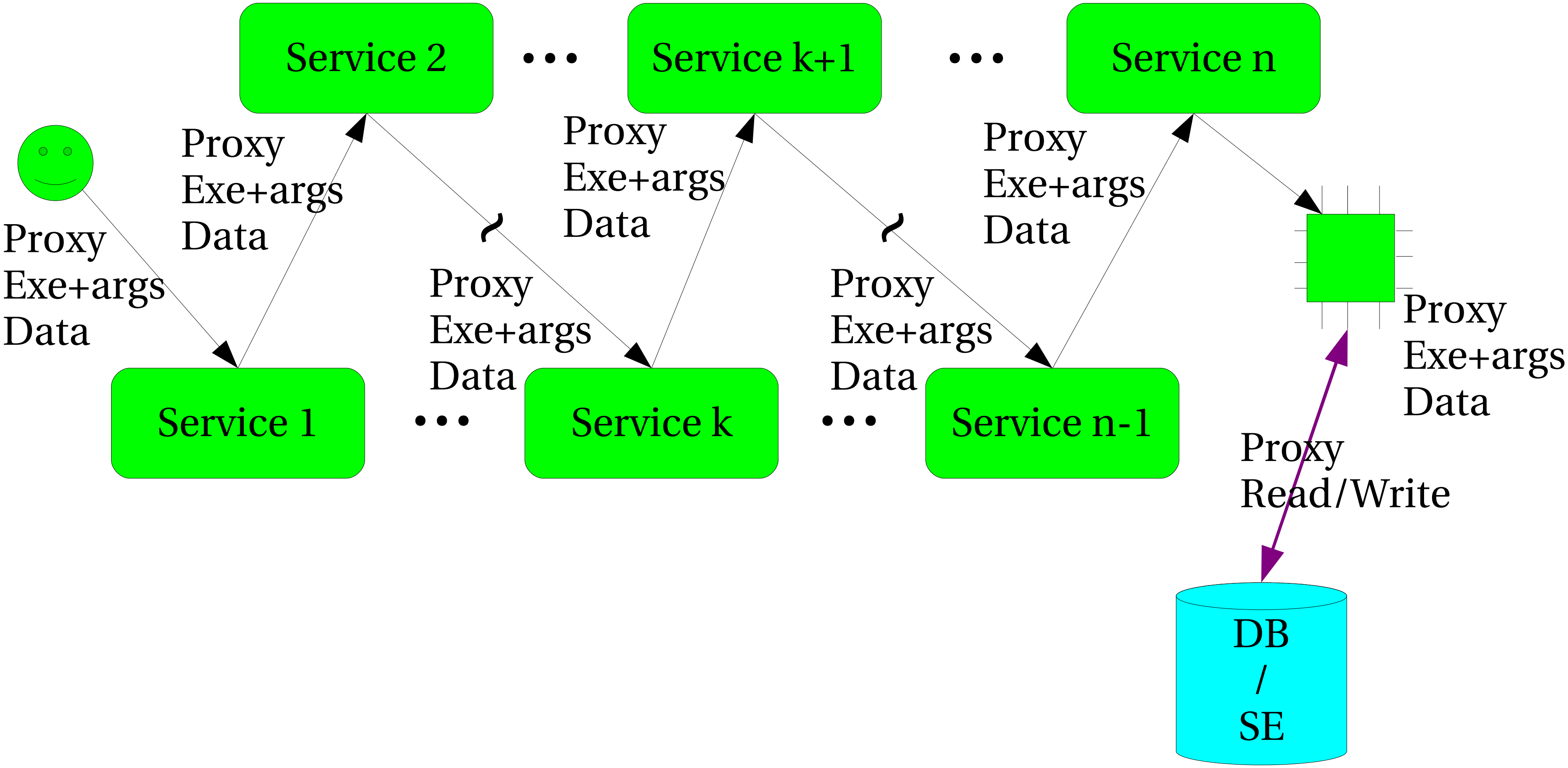


Glideins (2)

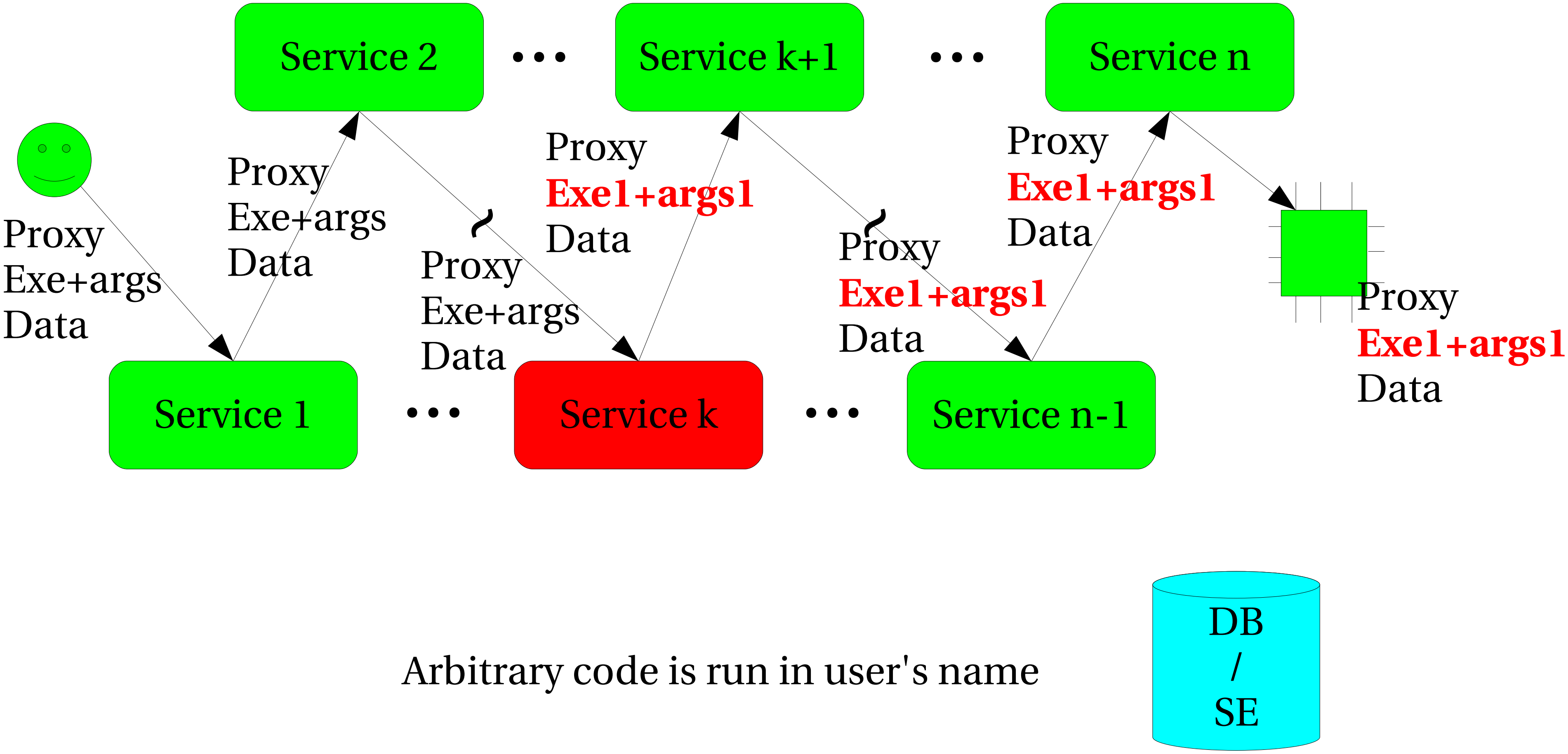
- Just regular starters
- Submitted as a Grid job



Today, we need to trust all the services

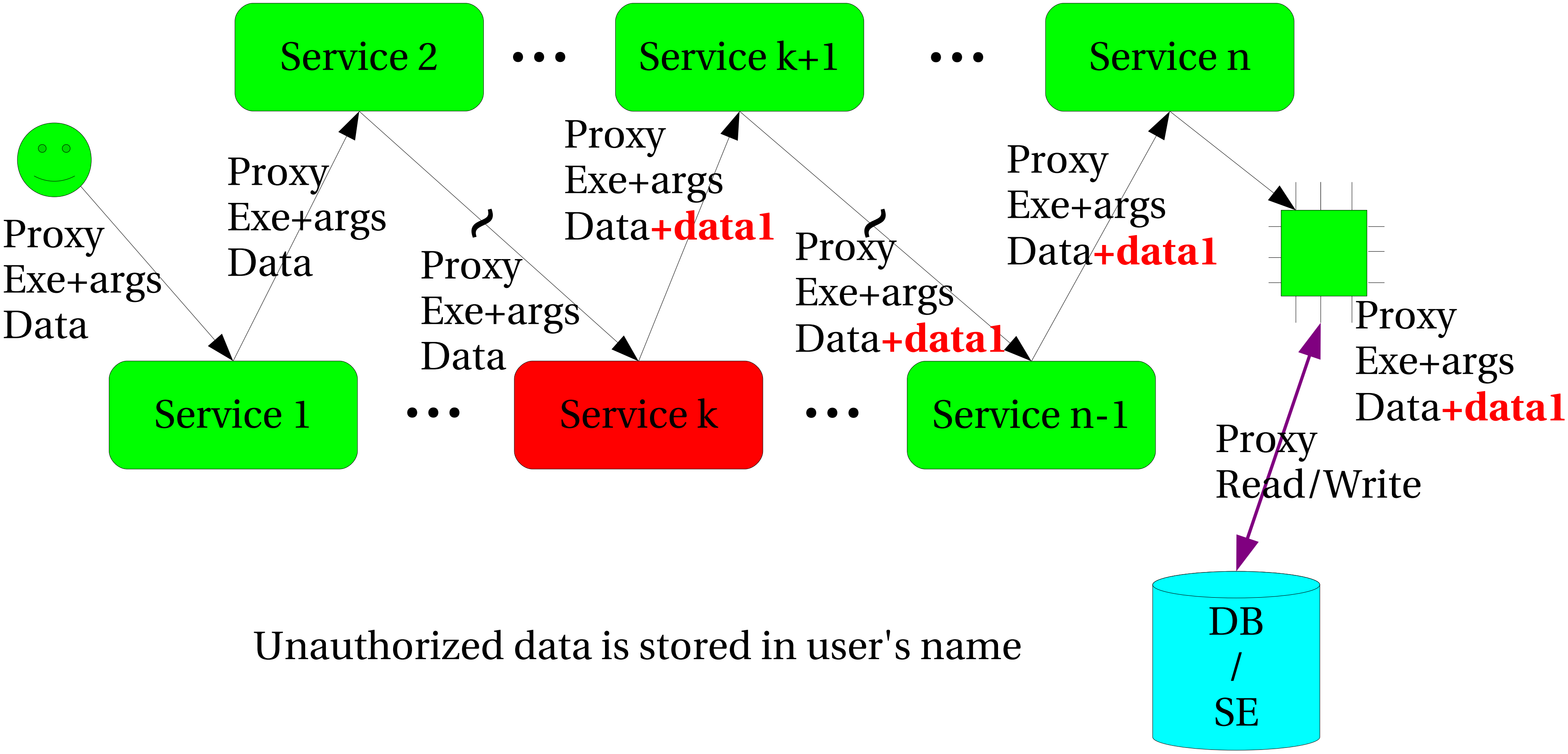


Three results of compromise - 1



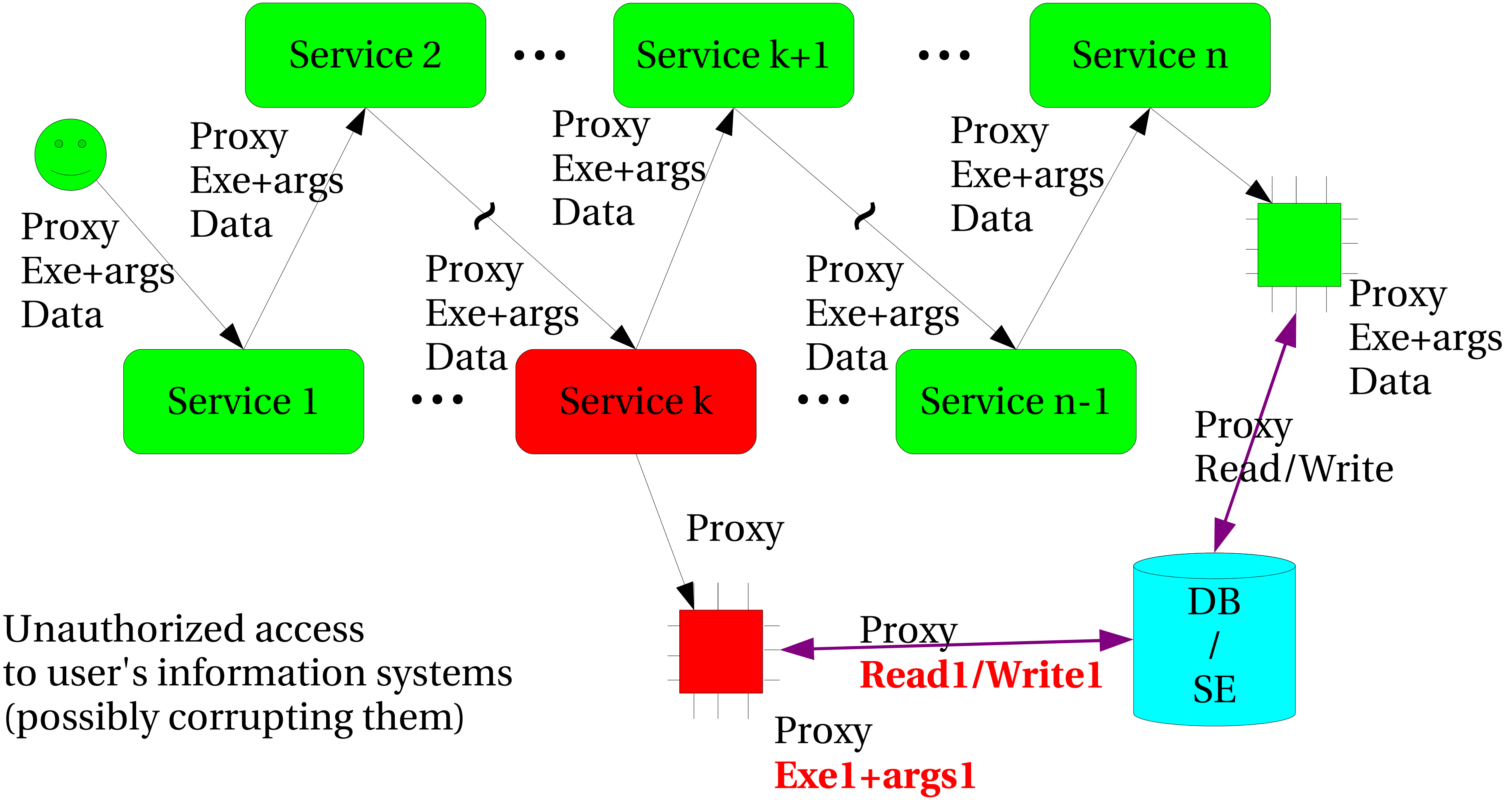
Arbitrary code is run in user's name

Three results of compromise - 2



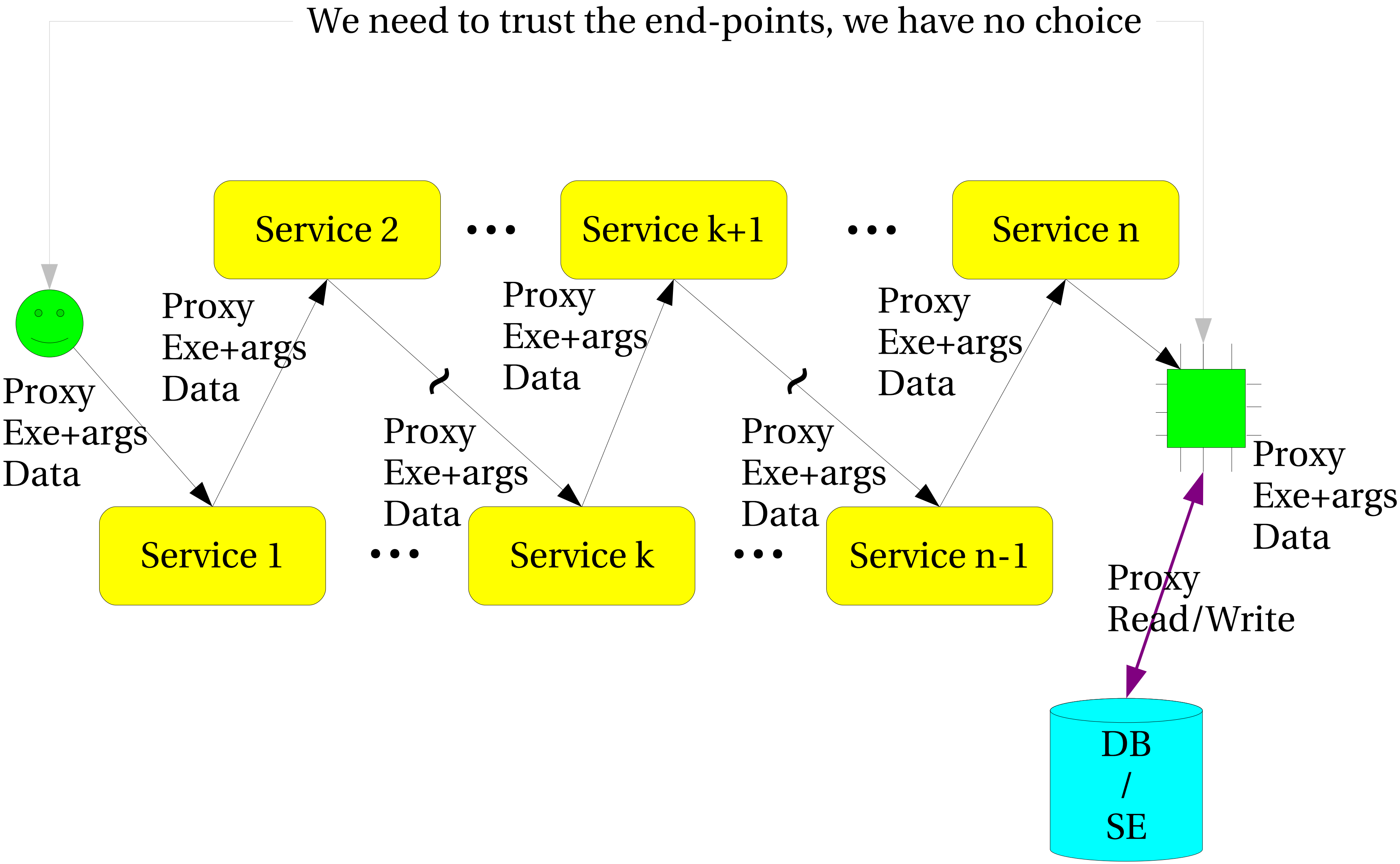
Unauthorized data is stored in user's name

Three results of compromise - 3



Unauthorized access
to user's information systems
(possibly corrupting them)

Can we live with untrusted services?



We need to trust the end-points, we have no choice