Mandos

http://www.recompile.se/mandos

Disk encryption is essential for physical computer security, but seldom used due to the trouble of remembering and typing a password at every restart. We describe Mandos, a program which solves this problem, its security model, and the underlying concepts of its design.

Any security system must have a clear view of its intended threat model – i.e. what threats it is actually intended to protect against; the specific choices and tradeoffs made for Mandos will be explained. Another danger of security system design is the risk of its non-use; i.e. that the system will not be used for some real or perceived drawbacks, such as complexity. The deliberate design choices of Mandos, involving low-interaction, “invisible” and automatic features, will be covered.

Mandos

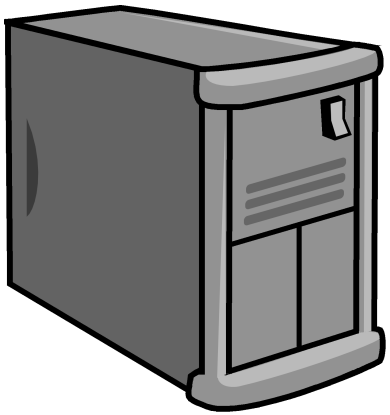
http://www.recompile.se/mandos

TL;DL

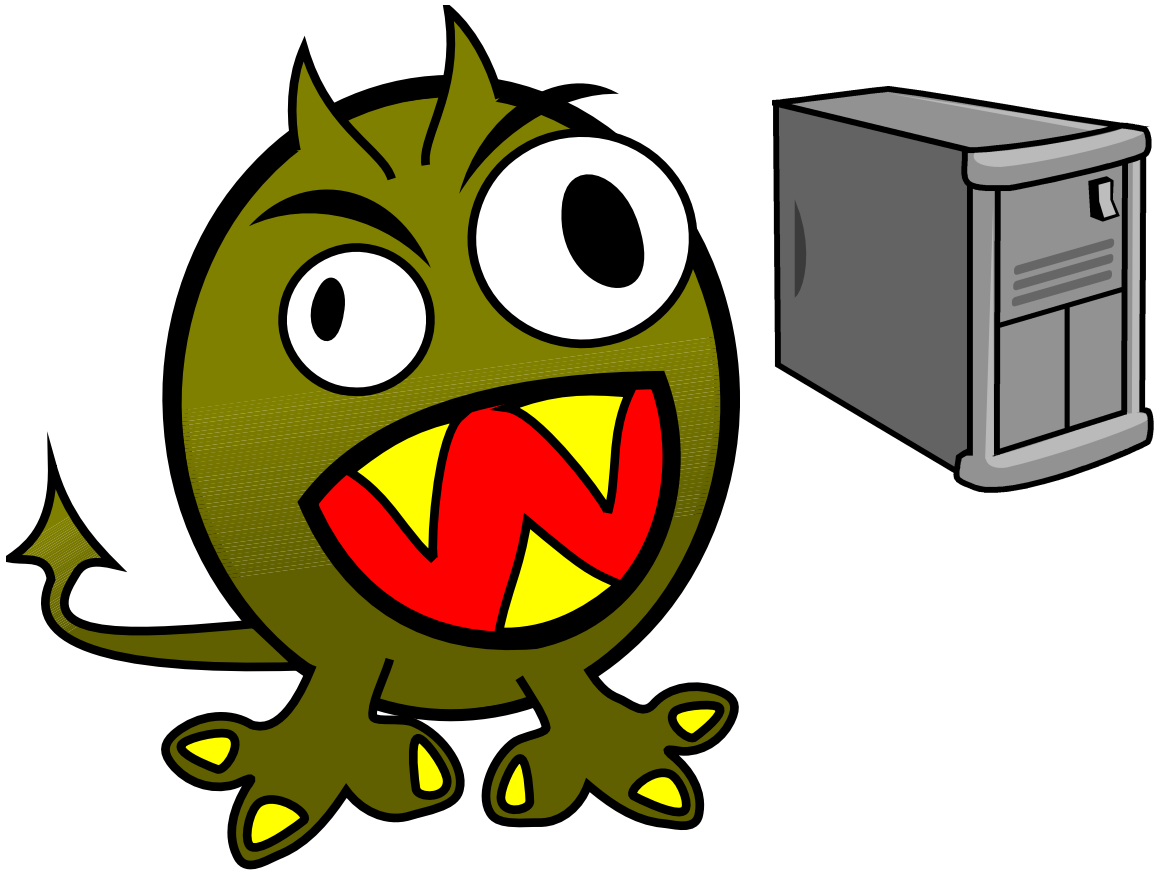
```
aptitude install mandos
aptitude install mandos-client
```

Threat Model

Threat Model

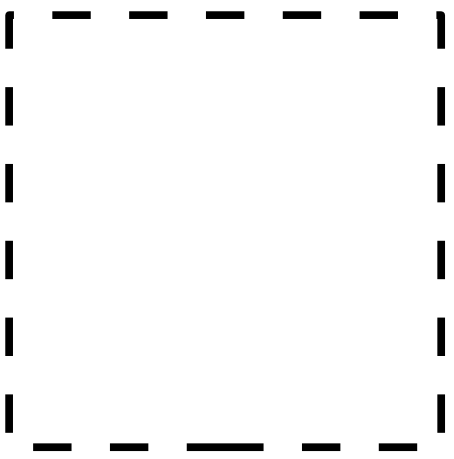


Threat Model

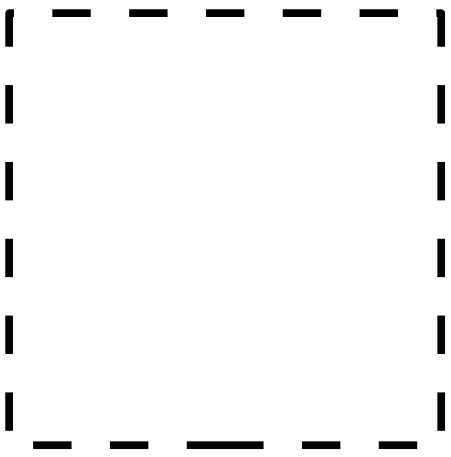


Threat Model

Threat Model

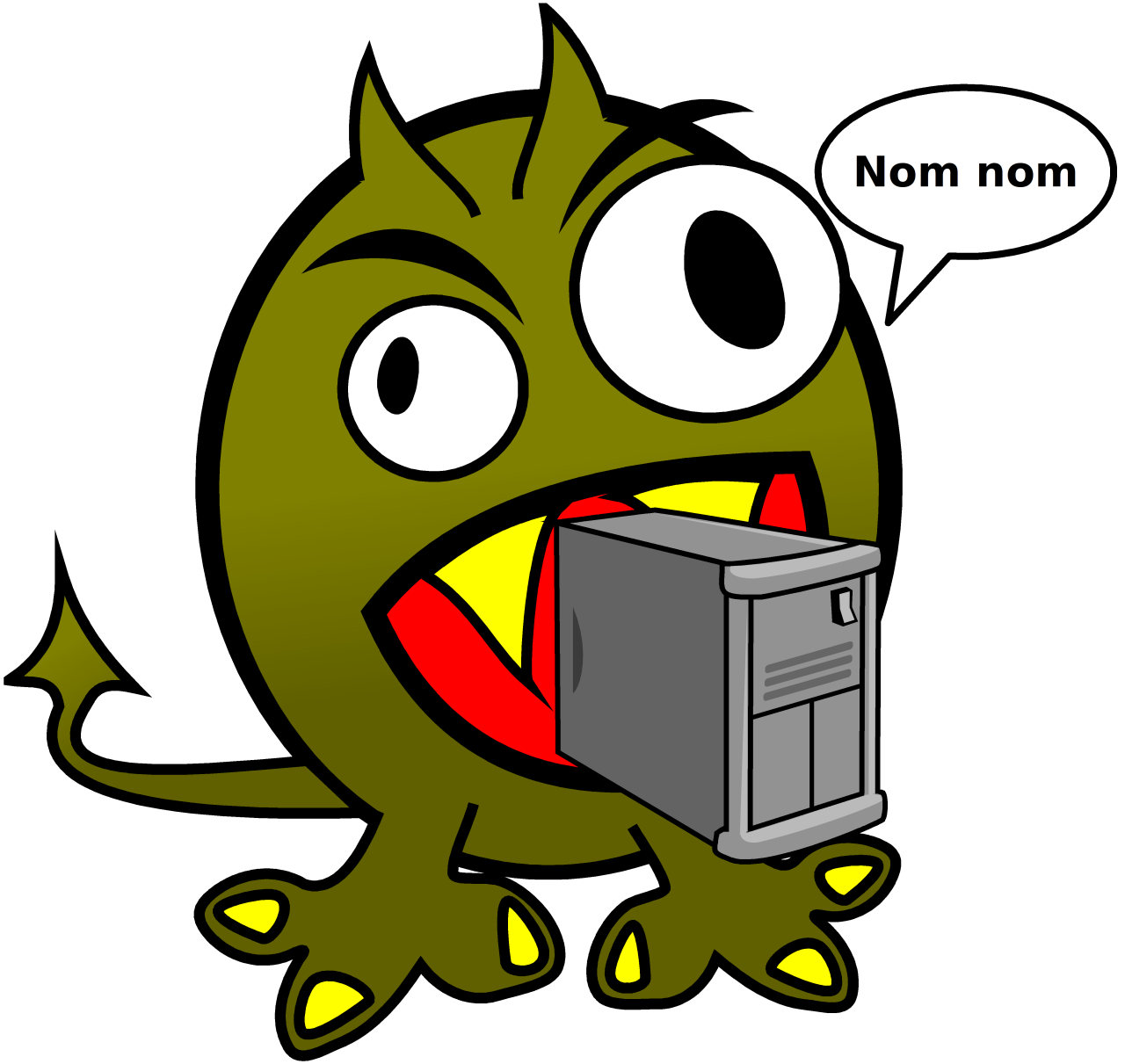


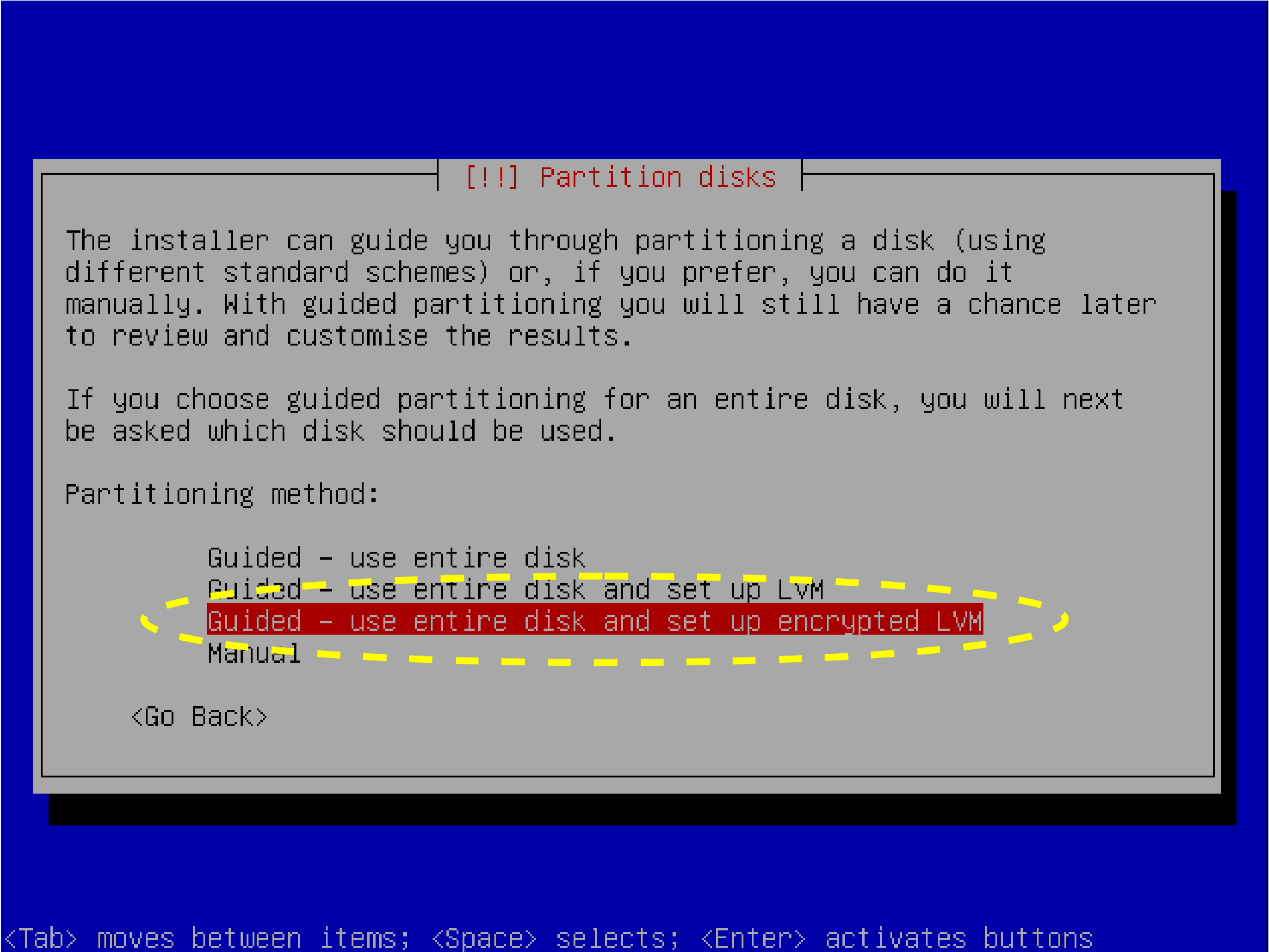
Threat Model

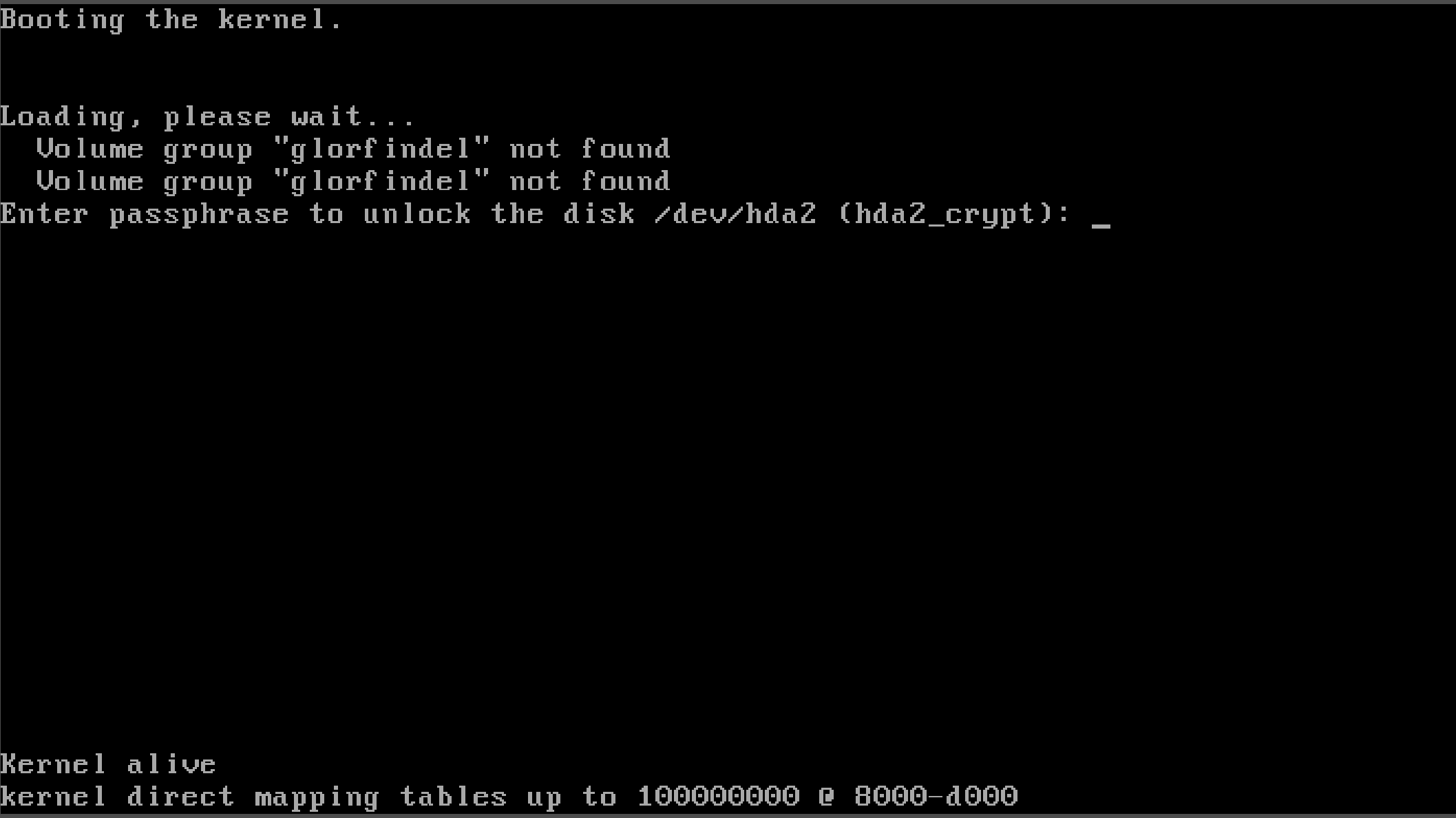


No Server

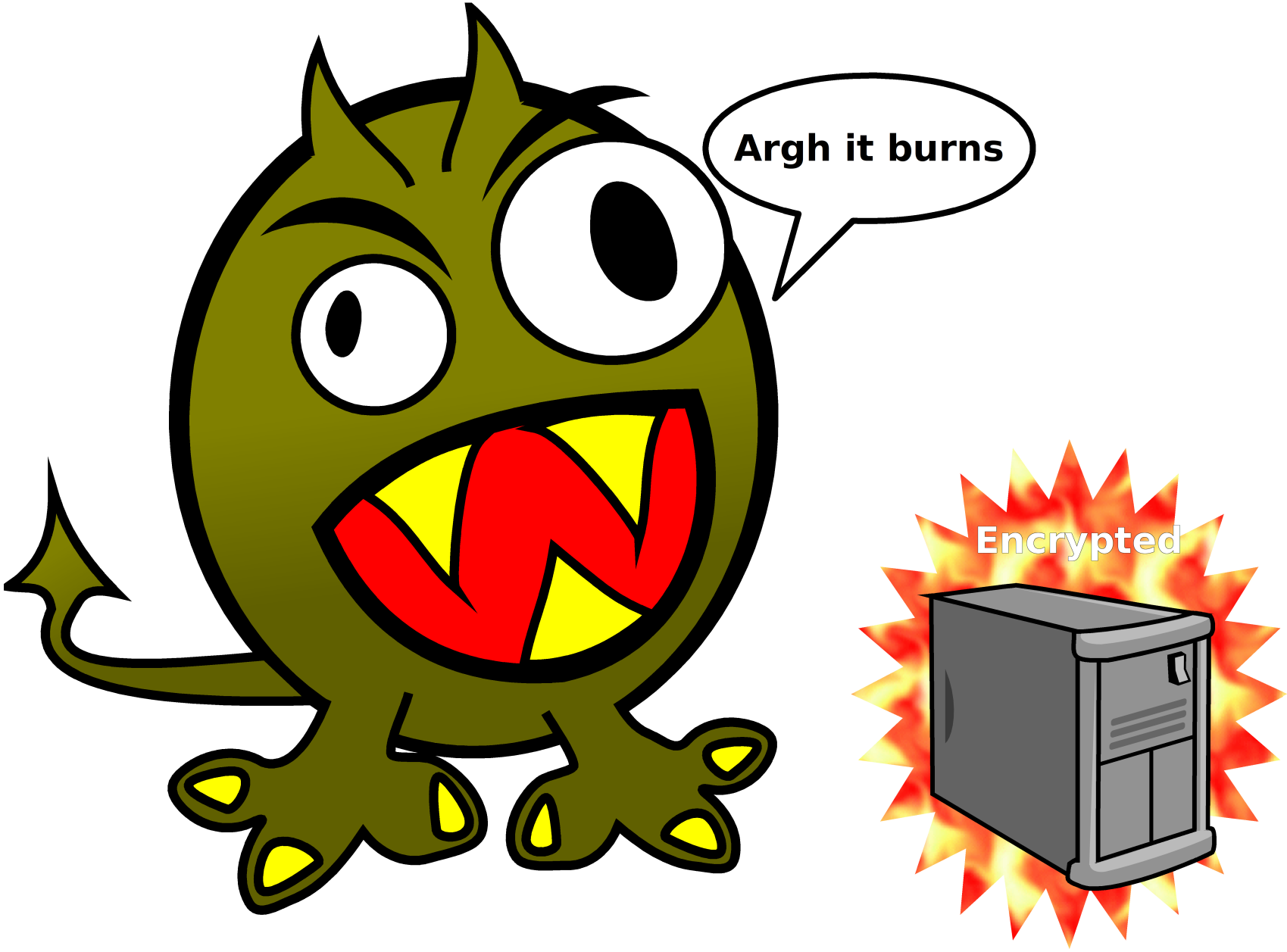
Threat Model




[!!] Partition disks
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.
Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
<Go Back>
<Tab> moves between items; <Space> selects; <Enter> activates buttons


Booting the kernel.
Loading, please wait...
Volume group "glorfindel" not found
Volume group "glorfindel" not found
Enter passphrase to unlock the disk /dev/hda2 (hda2_crypt): _
Kernel alive
kernel direct mapping tables up to 100000000 @ 8000-d000

Threat Model



New threat: non-use

Inconvenient
Burdensome
“I’ll do it some day”

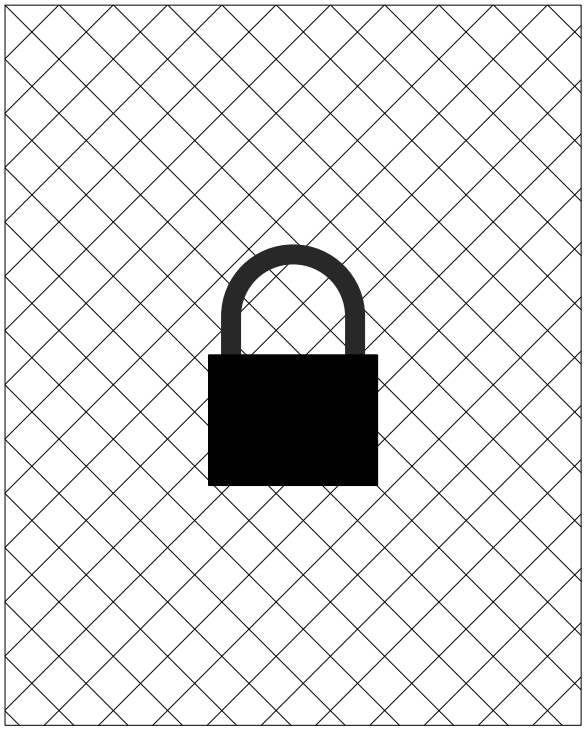
New threat:

Security needs to be *transparent*

Full Disk Encryption

/boot

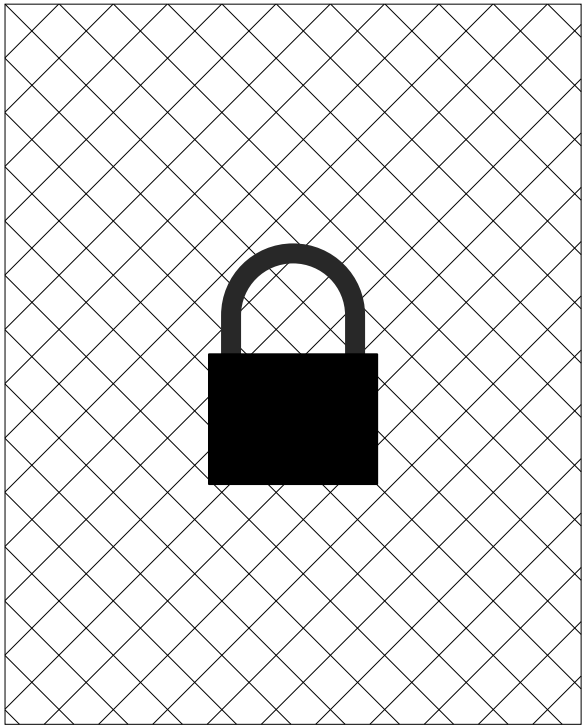
(rest of disk)



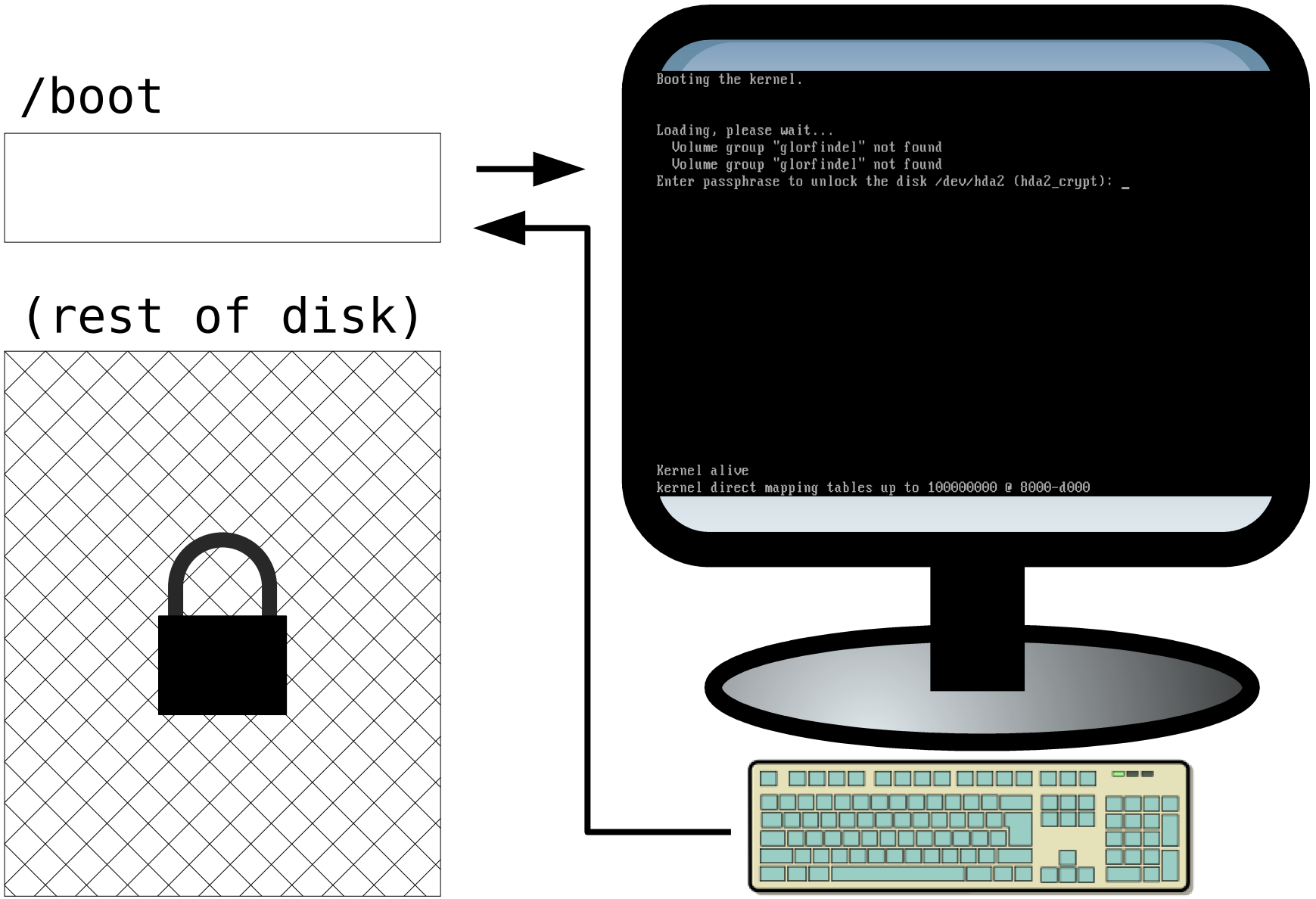
Full Disk Encryption

/boot

(rest of disk)



Full Disk Encryption



Full Disk Encryption

/boot

(rest of disk)

Mandos

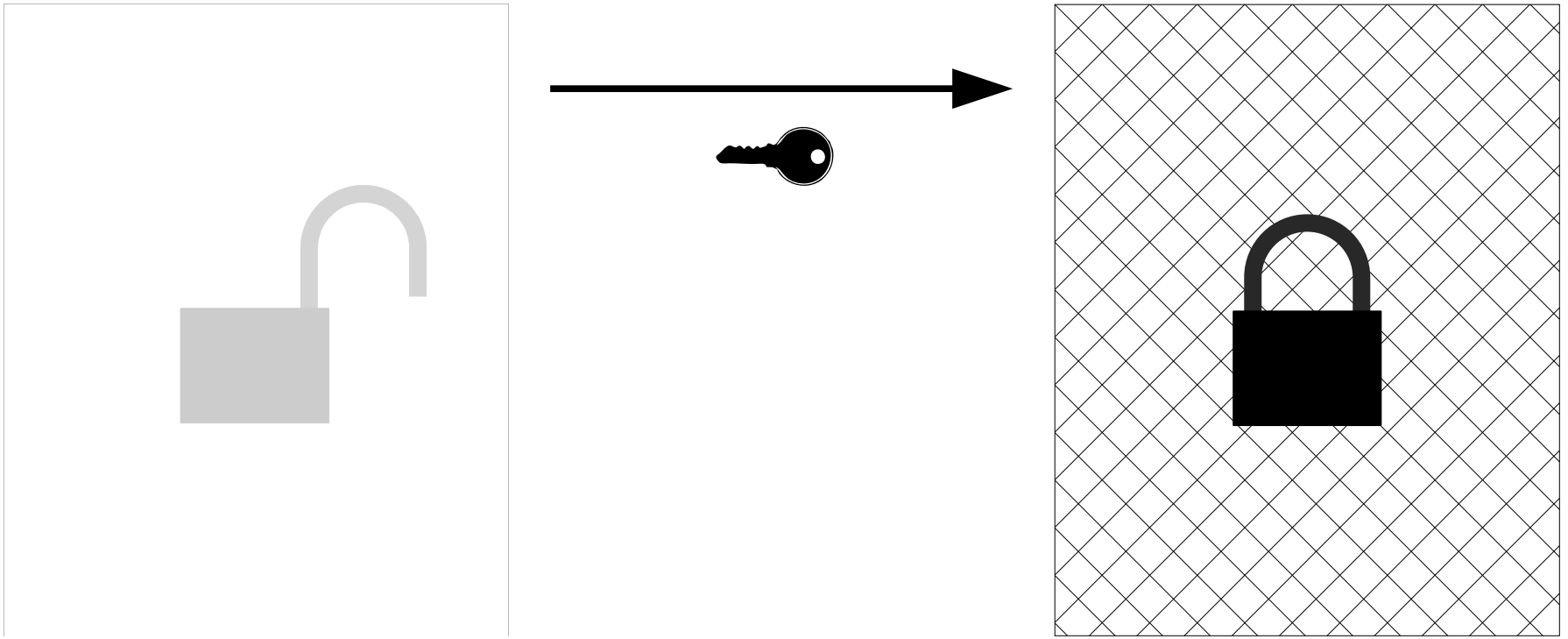
http://www.recompile.se/mandos

Servers provide passwords to *each other*

Mandos

http://www.recompile.se/mandos

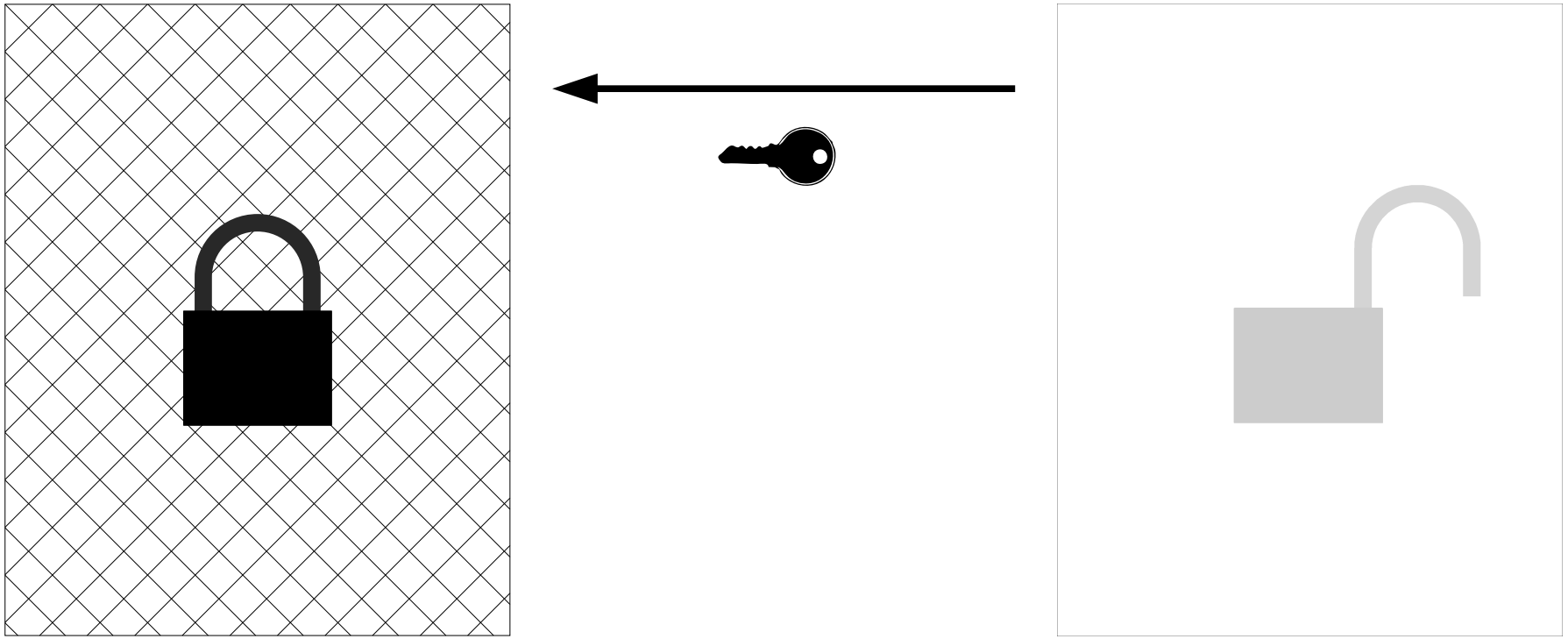
Normal operation



Mandos

http://www.recompile.se/mandos

Normal operation

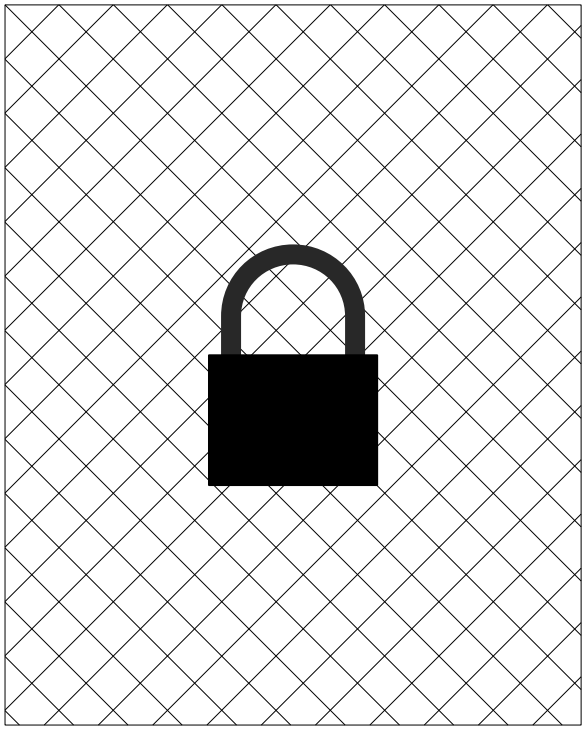


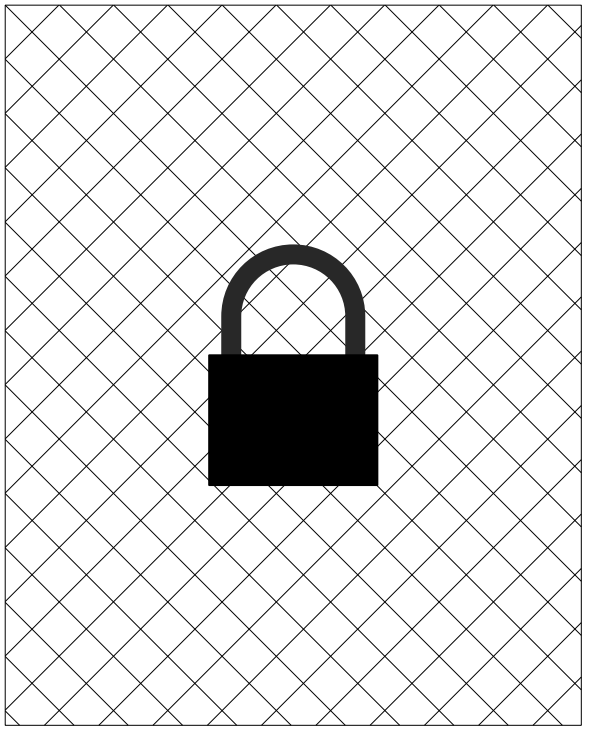
Mandos

http://www.recompile.se/mandos

Lockdown state

Administrator attention required



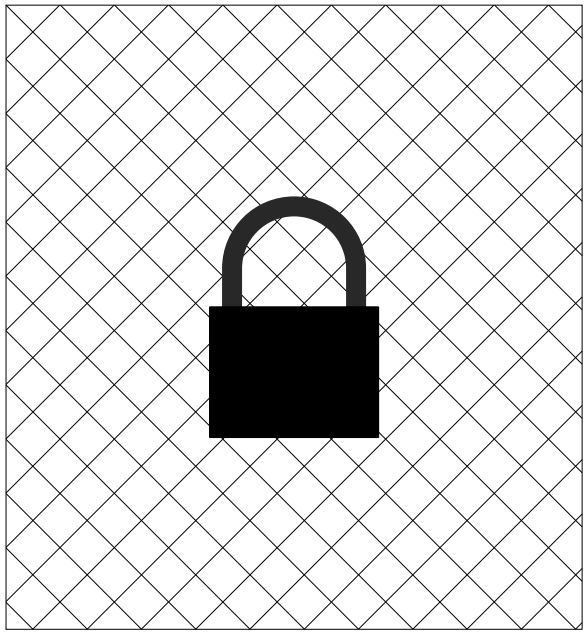


Mandos

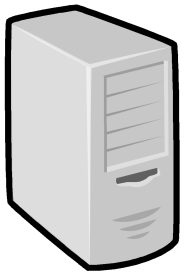
http://www.recompile.se/mandos

/boot

(rest of disk)



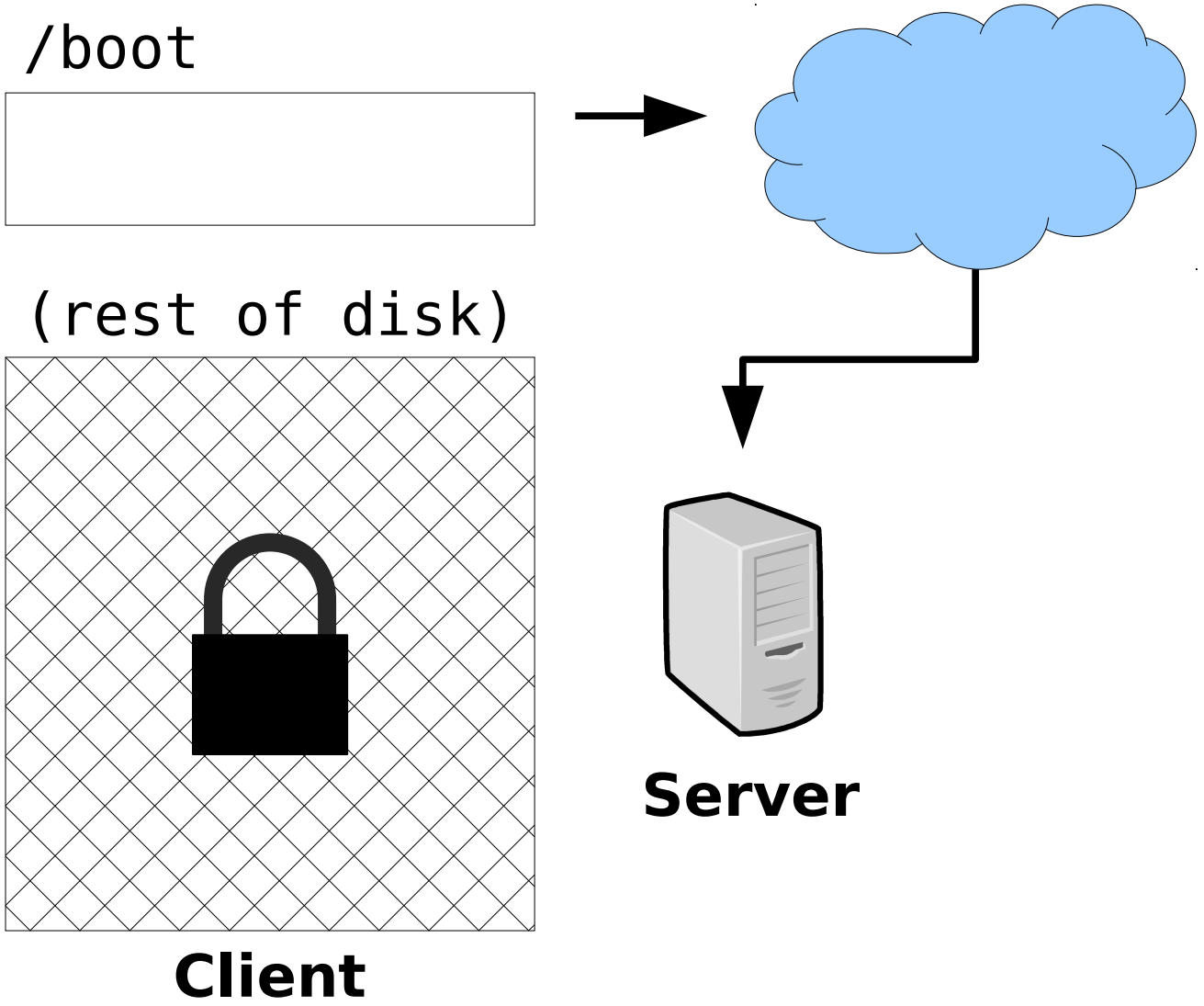
Client



Server

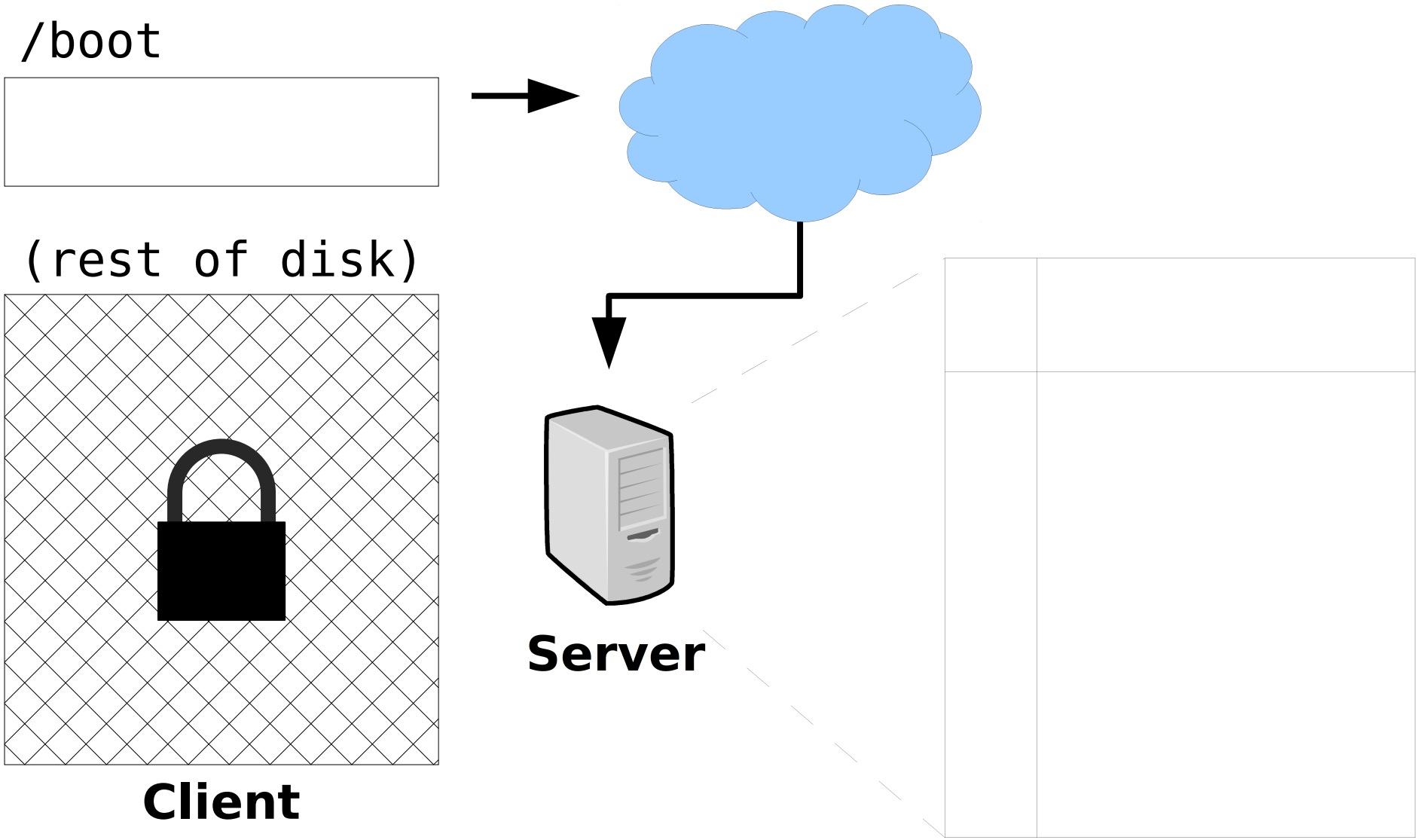
Mandos

http://www.recompile.se/mandos



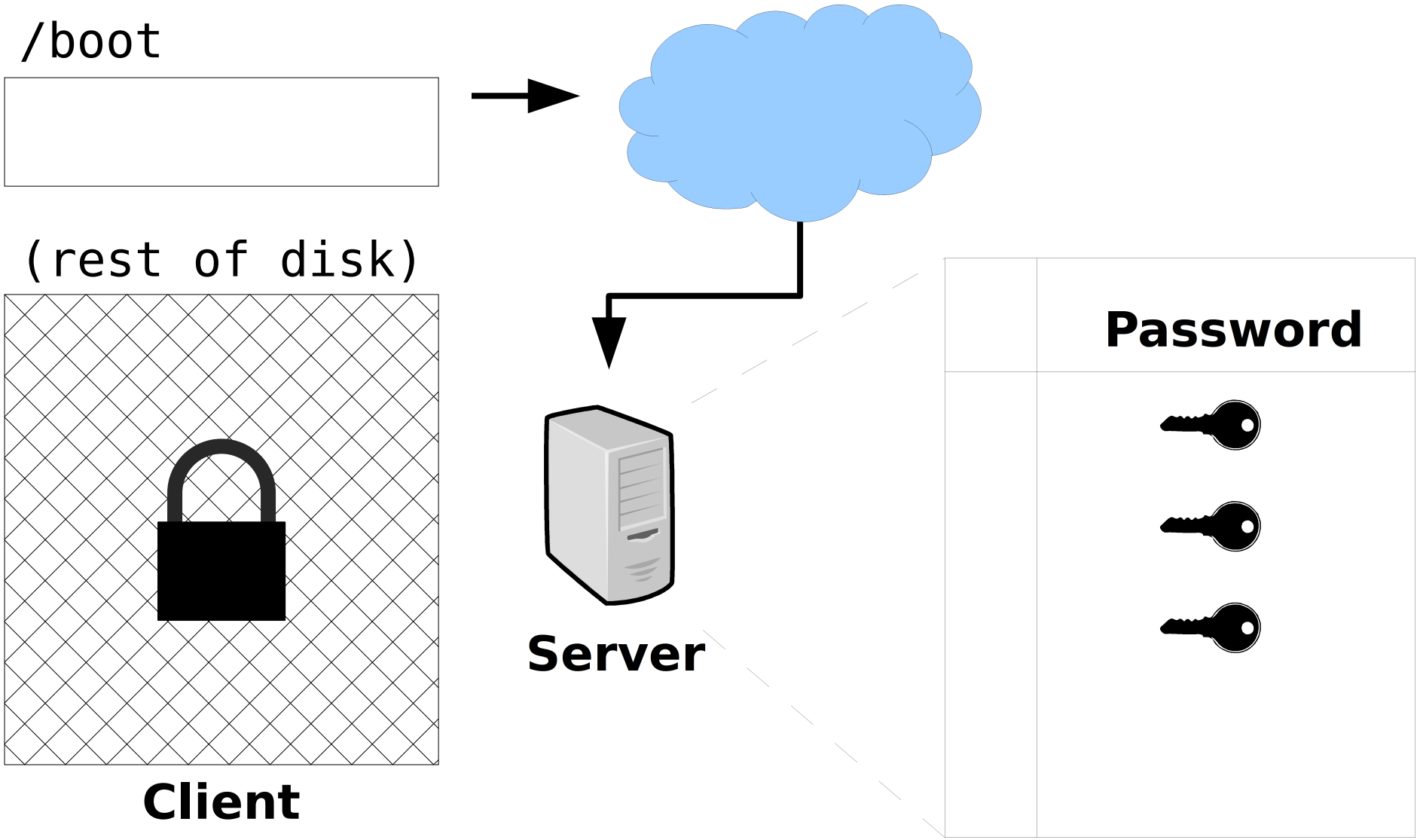
Mandos

http://www.recompile.se/mandos



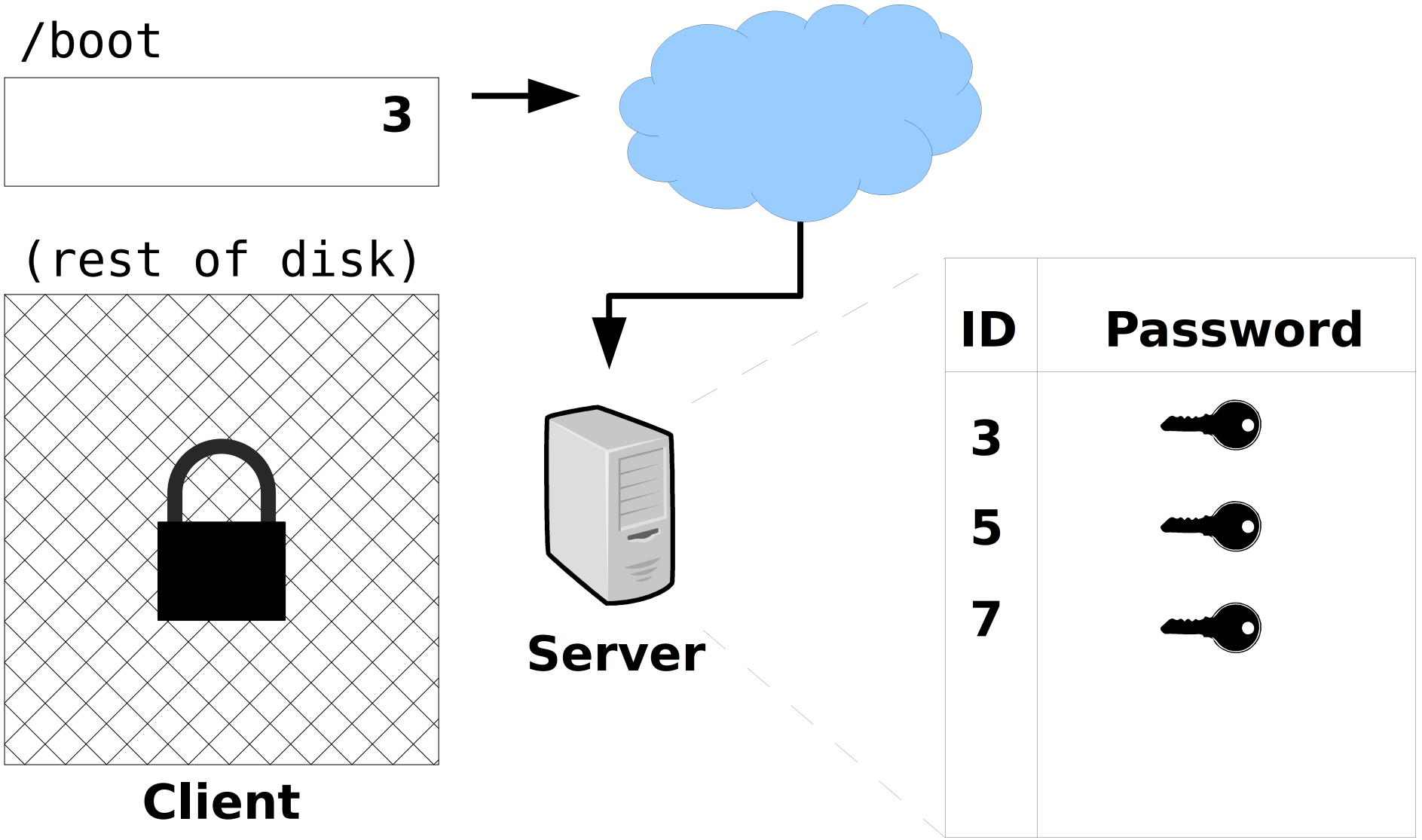
Mandos

http://www.recompile.se/mandos



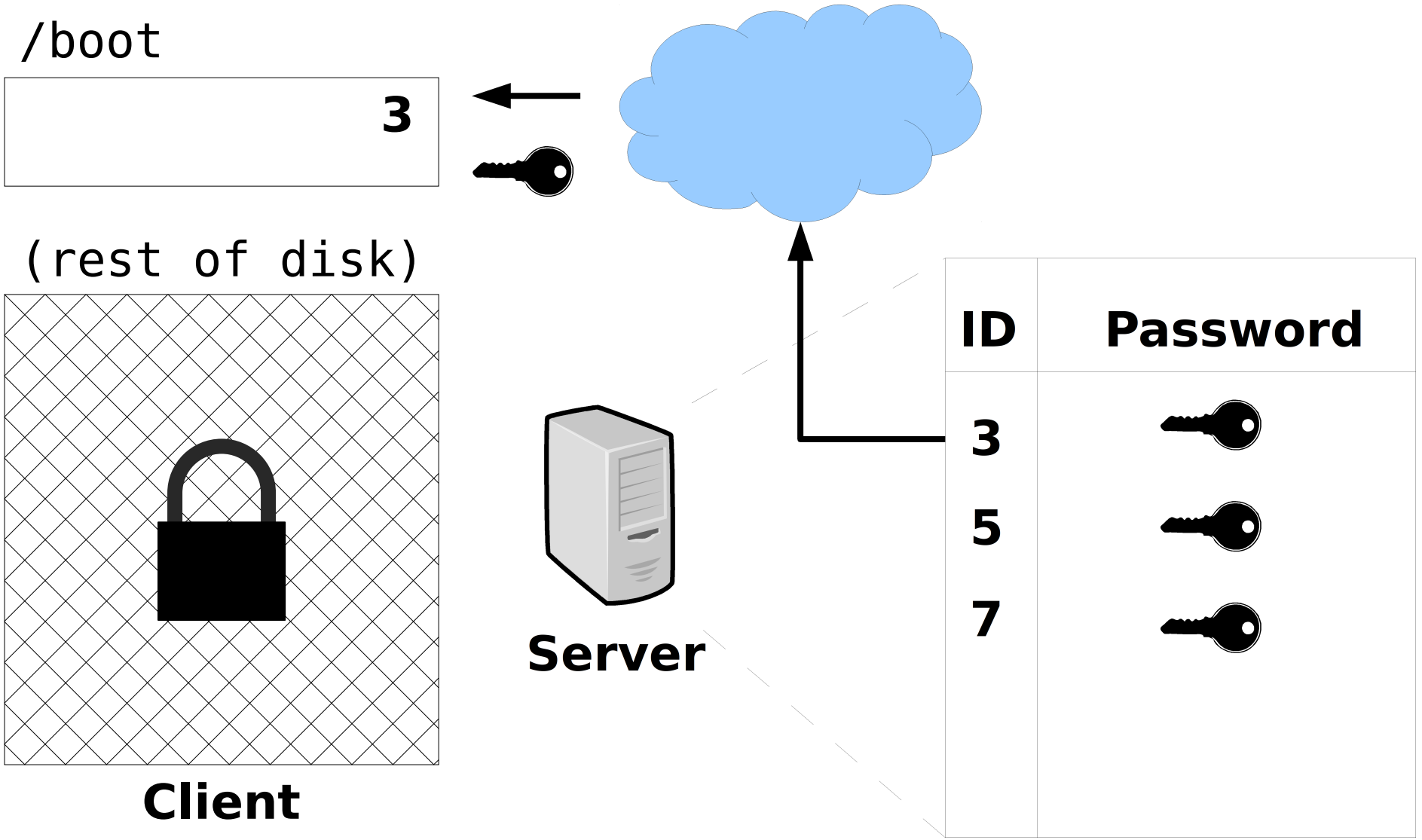
Mandos

http://www.recompile.se/mandos



Mandos

http://www.recompile.se/mandos



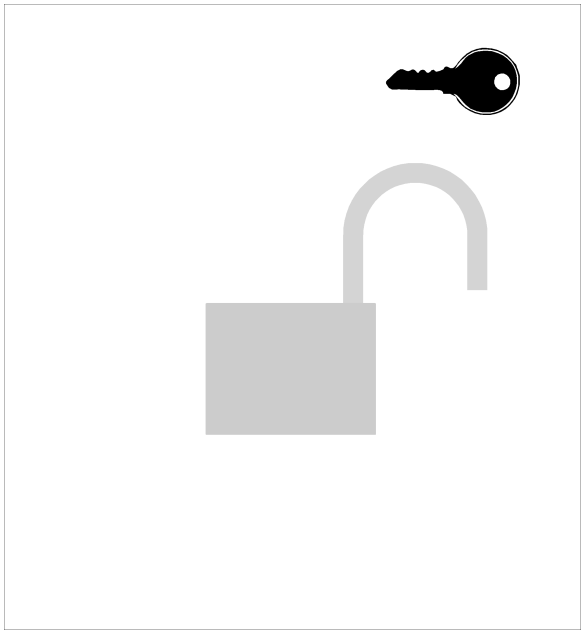
Mandos

http://www.recompile.se/mandos

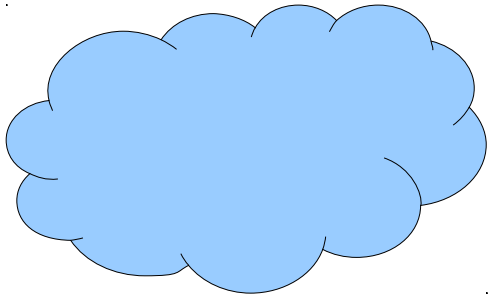
/boot

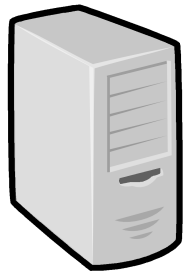
3

(rest of disk)



Client



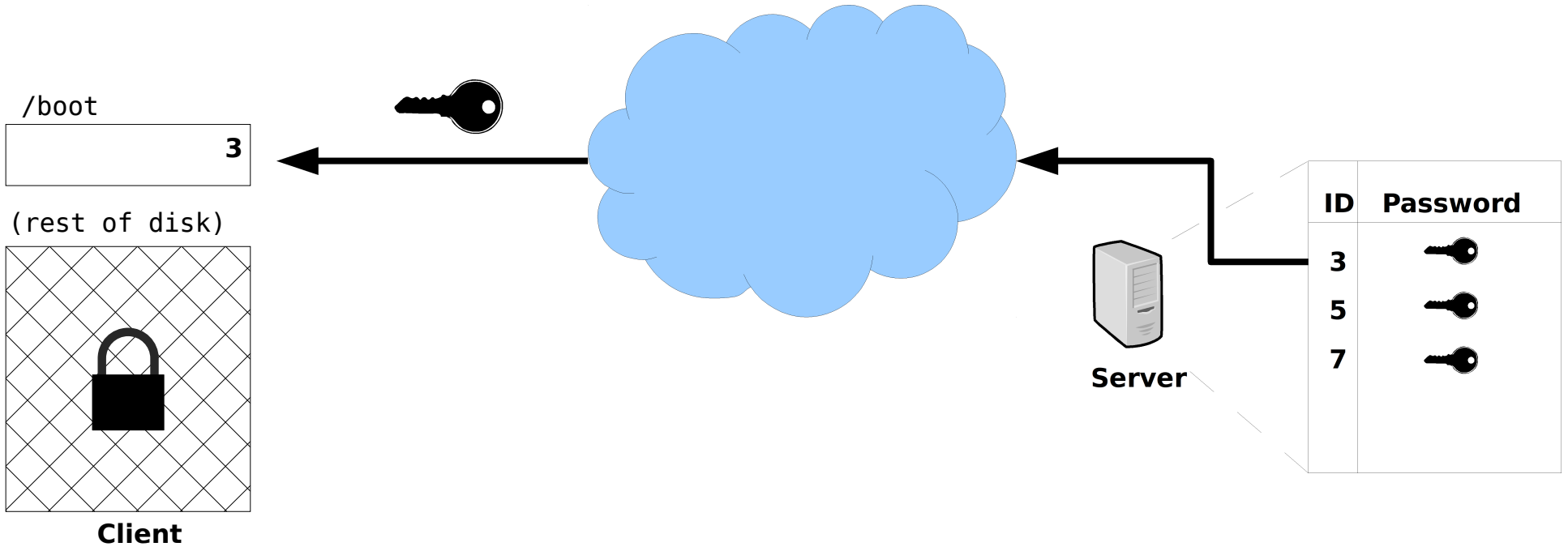


Server

ID	Key
3	
5	
7	

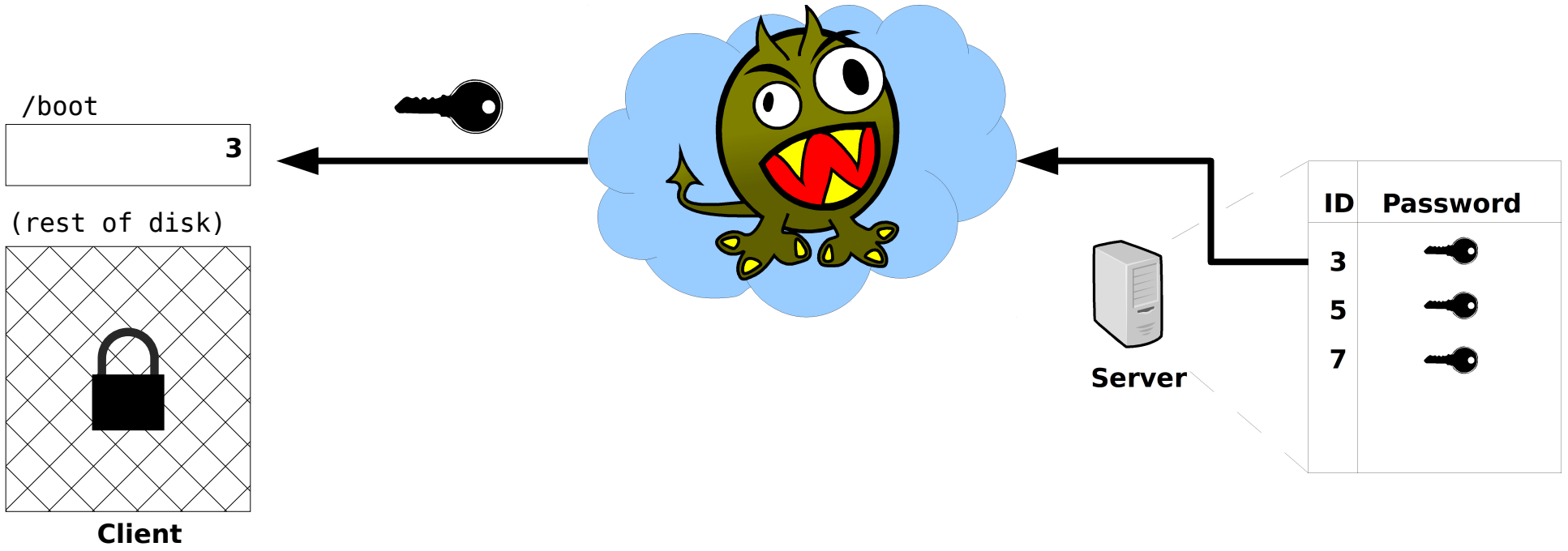
Mandos

http://www.recompile.se/mandos



Mandos

http://www.recompile.se/mandos



“GPG for data at rest. TLS for data in motion.”

If You're Typing The Letters A-E-S Into Your Code, You're Doing It Wrong
http://www.cs.berkeley.edu/~daw/teaching/cs261-f12/misc/if.html

TLS has a “server” side and a “client” side, and the “server” side *needs* a key.

The TLS key can be a X.509 certificate

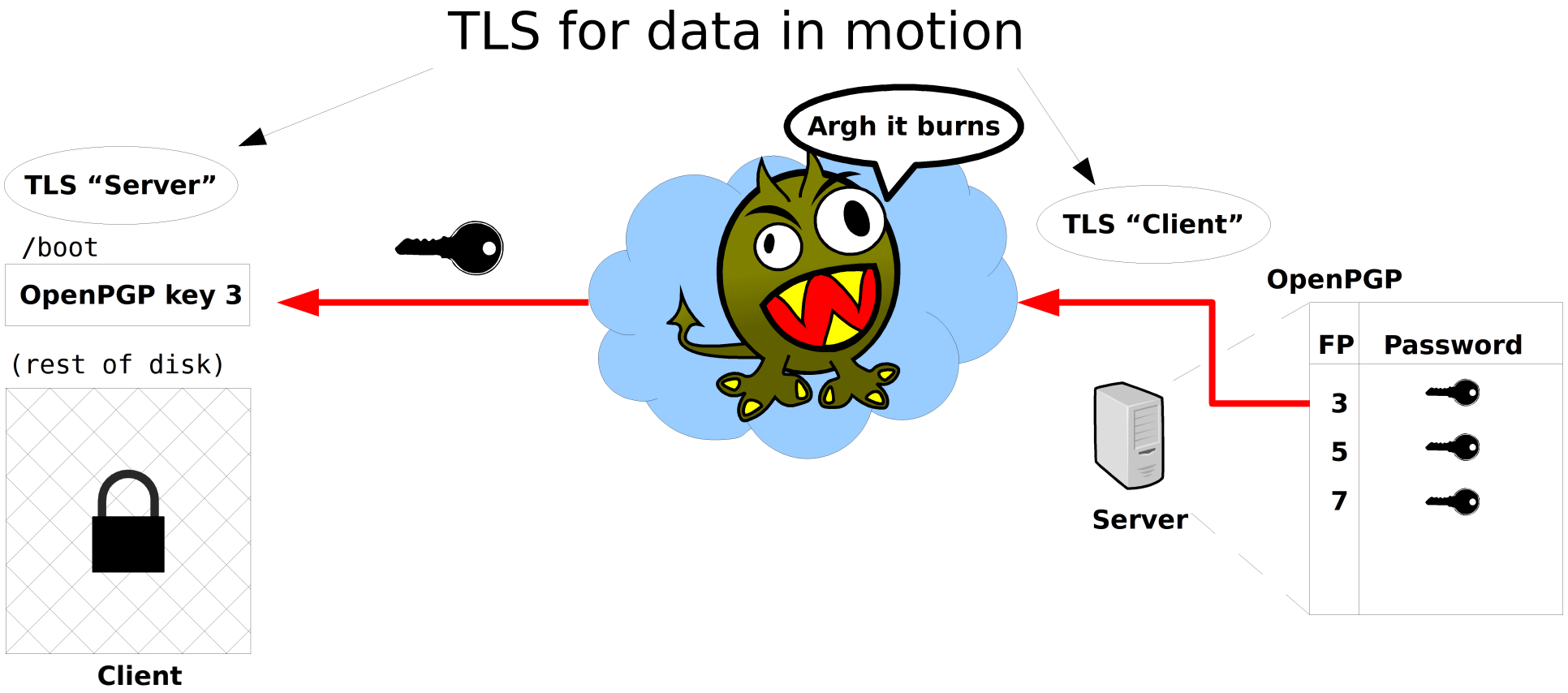
X.509:

“Someone tried to explain public-key-based authentication to aliens. Their universal translators were broken and they had to gesture a lot.”
— Peter Gutmann
Everything you Never Wanted to Know about PKI but were Forced to Find Out

Alternatively, the TLS key can be an OpenPGP key

Mandos

http://www.recompile.se/mandos

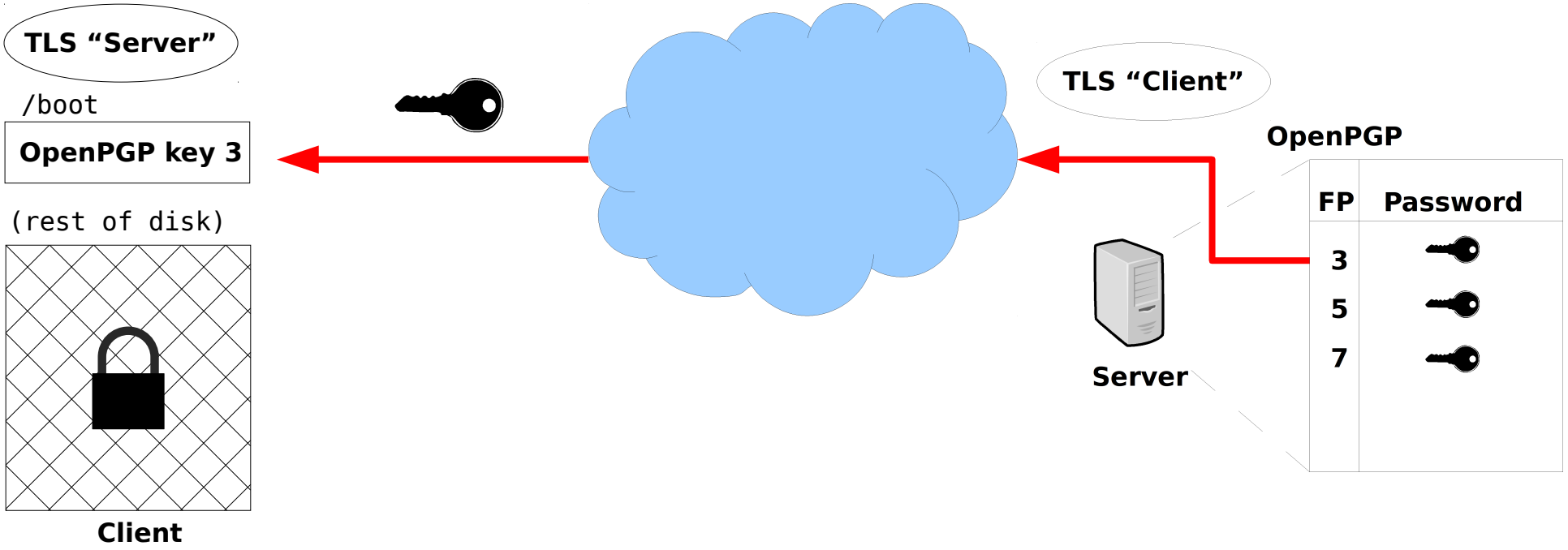


“GPG for data at rest”?

Mandos

http://www.recompile.se/mandos

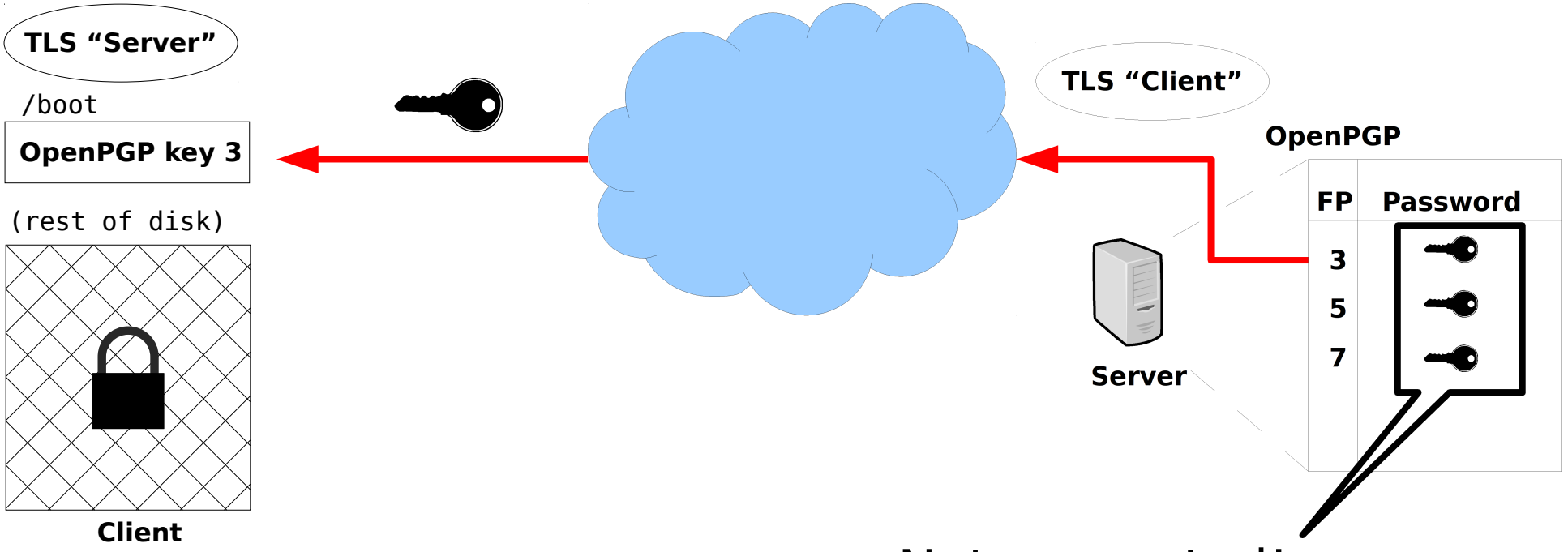
TLS for data in motion



Mandos

http://www.recompile.se/mandos

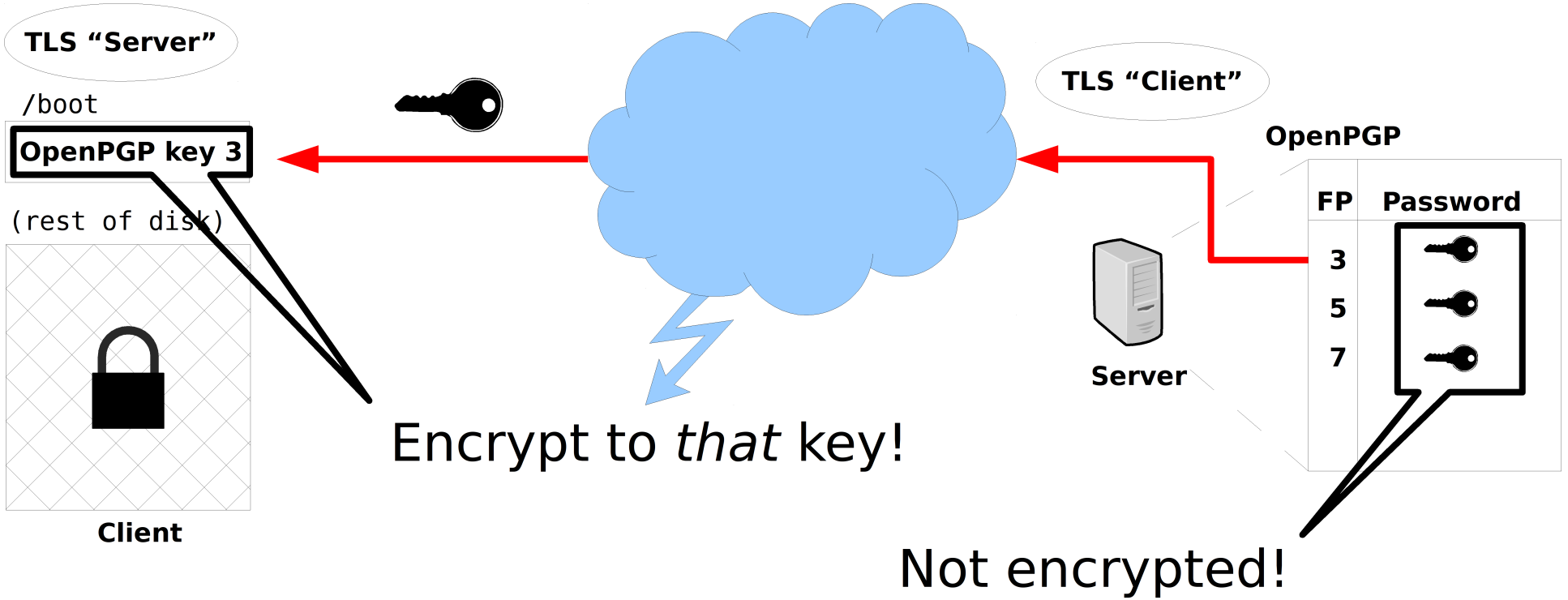
TLS for data in motion



Mandos

http://www.recompile.se/mandos

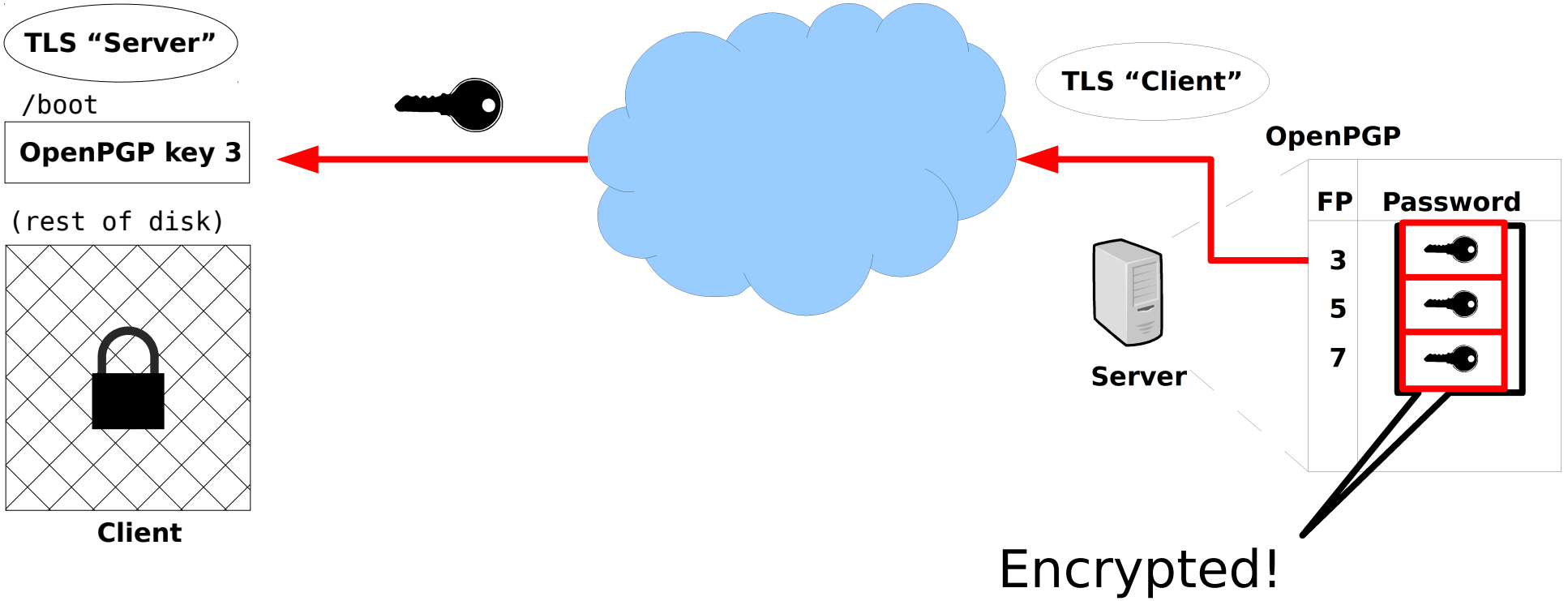
TLS for data in motion



Mandos

http://www.recompile.se/mandos

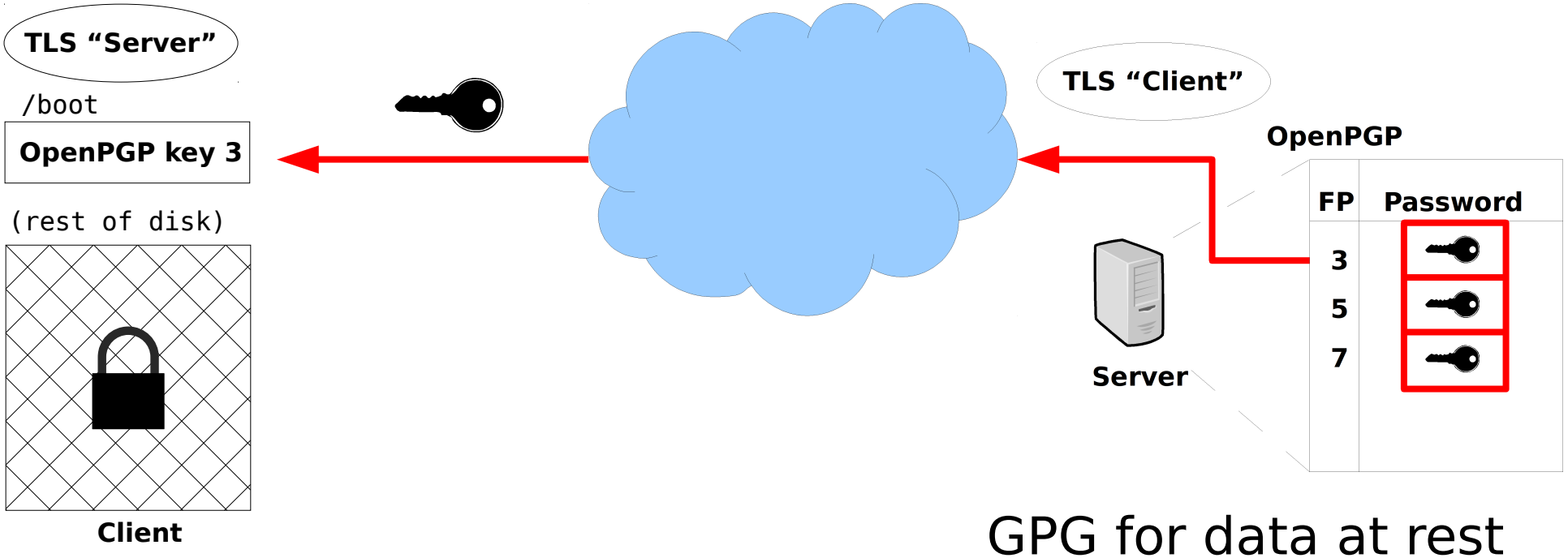
TLS for data in motion



Mandos

http://www.recompile.se/mandos

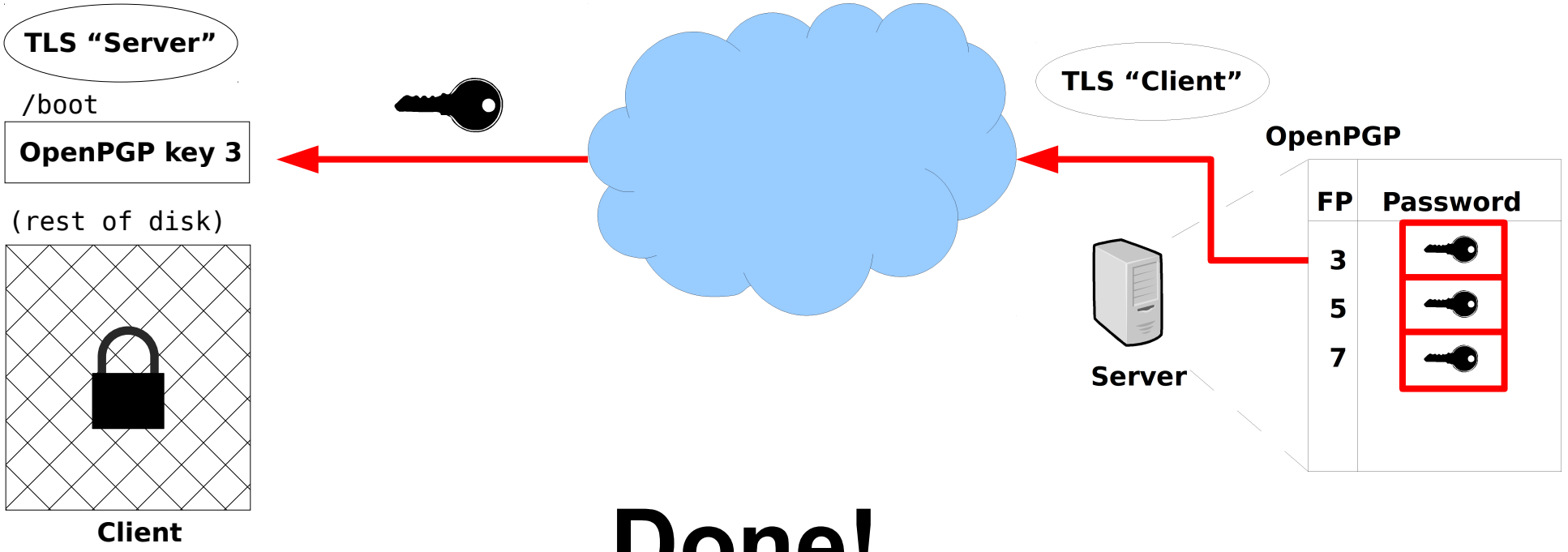
TLS for data in motion



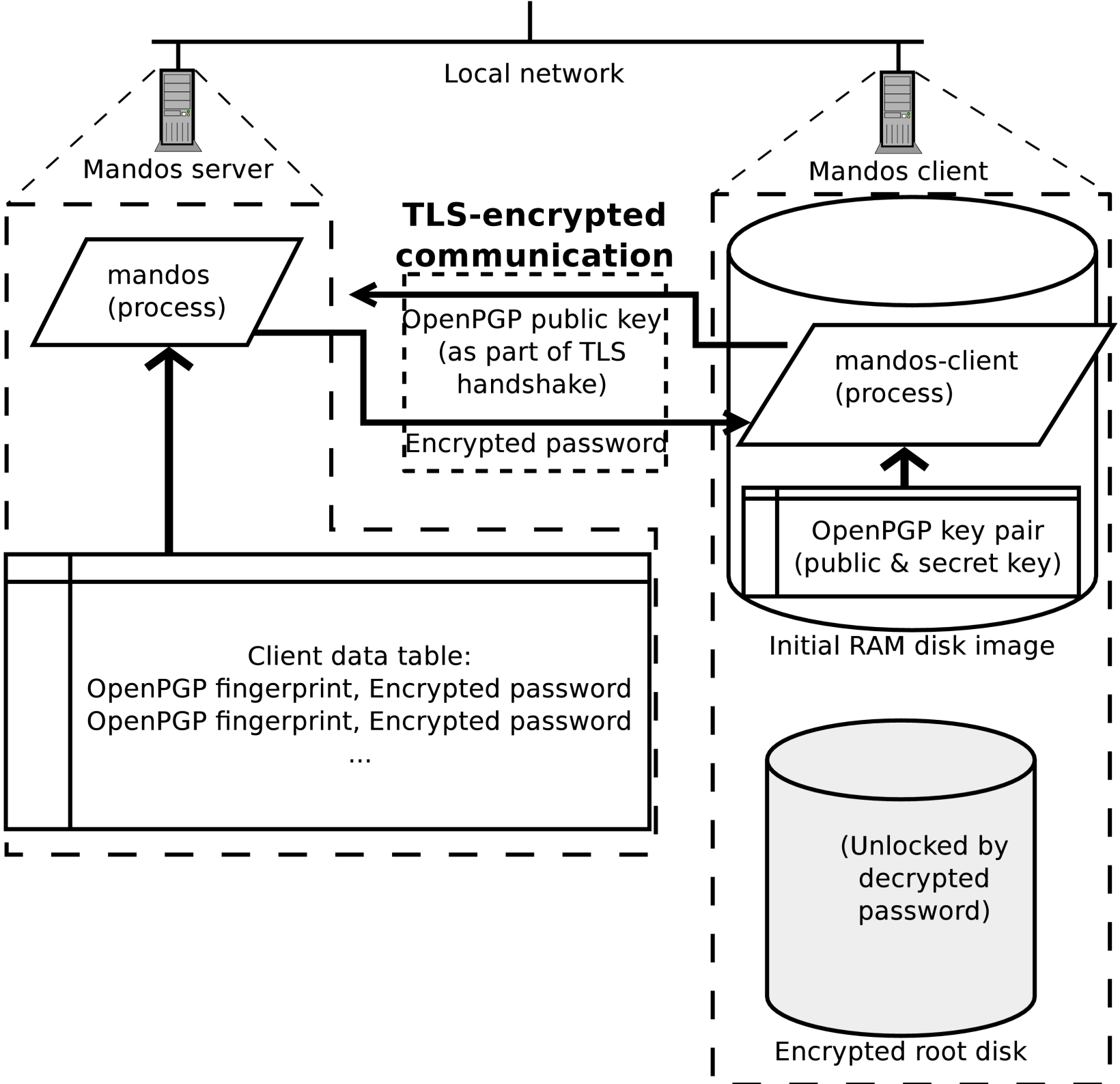
GPG for data at rest

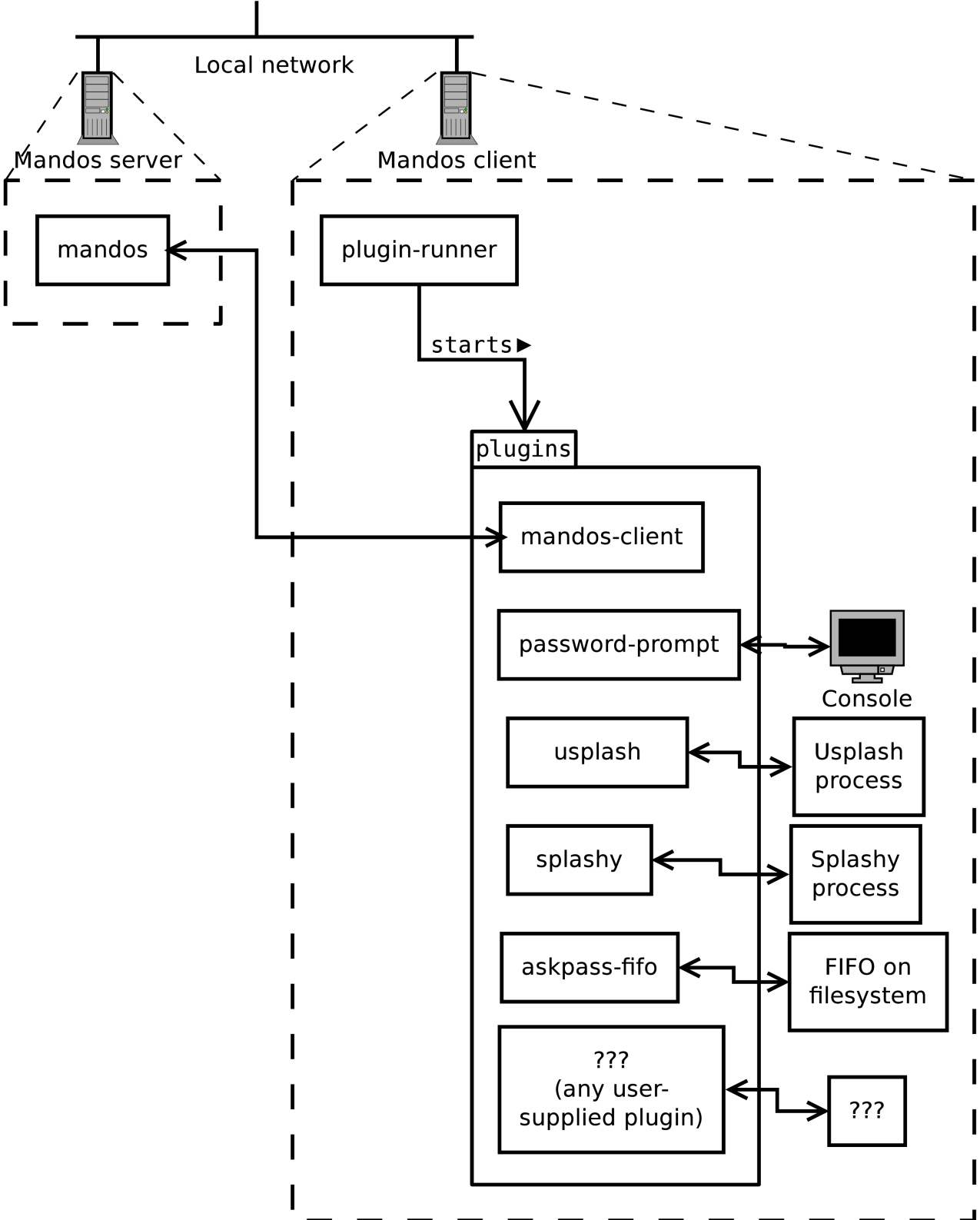
Mandos

http://www.recompile.se/mandos



Done!


Local network
Mandos server
Mandos client
TLS-encrypted communication
mandos (process)
OpenPGP public key (as part of TLS handshake)
Encrypted password
mandos-client (process)
OpenPGP key pair (public & secret key)
Initial RAM disk image
Client data table:
OpenPGP fingerprint, Encrypted password
OpenPGP fingerprint, Encrypted password
...
(Unlocked by decrypted password)
Encrypted root disk


Local network
Mandos server
Mandos client
mandos
plugin-runner
starts
plugins
mandos-client
password-prompt
Console
usplash
Usplash process
splashy
Splashy process
askpass-fifo
FIFO on filesystem
??? (any user-supplied plugin)
???

FAQ

Grabbing the Mandos client key from the `/boot` partition's `initramfs` image really quickly?

Mandos

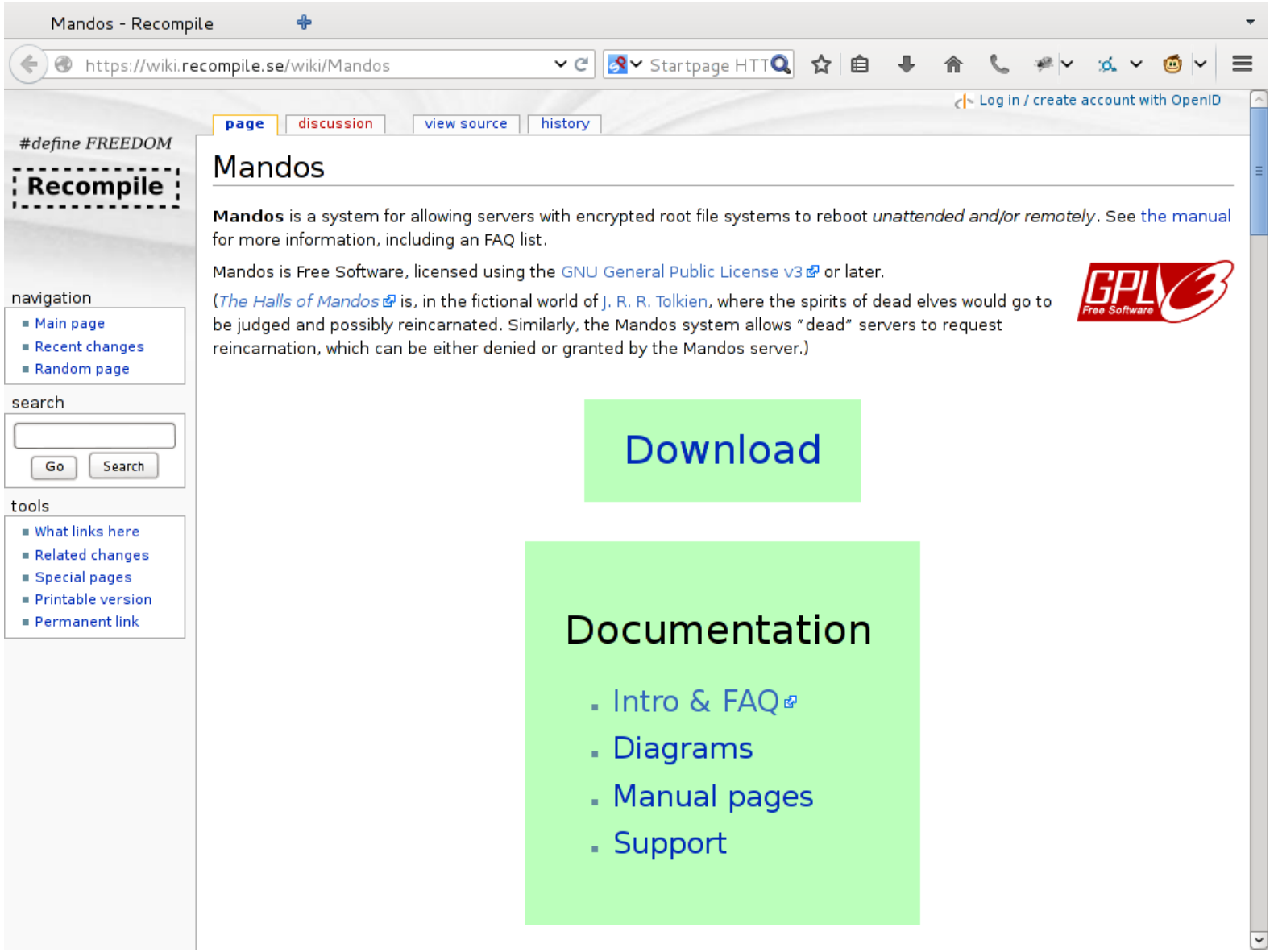
http://www.recompile.se/mandos

- **In Ubuntu “universe” since 2009**
- **In Debian since 2011**

```
aptitude install mandos
aptitude install mandos-client
```

Mandos

http://www.recompile.se/mandos



Mandos

http://www.recompile.se/mandos

http://ftp.recompile.se/pub/mandos/misc

Mandos

http://www.recompile.se/mandos

Disk encryption is essential for physical computer security, but seldom used due to the trouble of remembering and typing a password at every restart. We describe Mandos, a program which solves this problem, its security model, and the underlying concepts of its design.

Any security system must have a clear view of its intended threat model – i.e. what threats it is actually intended to protect against; the specific choices and tradeoffs made for Mandos will be explained. Another danger of security system design is the risk of its non-use; i.e. that the system will not be used for some real or perceived drawbacks, such as complexity. The deliberate design choices of Mandos, involving low-interaction, “invisible” and automatic features, will be covered.

Mandos

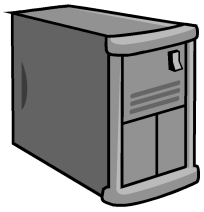
http://www.recompile.se/mandos

TL;DL

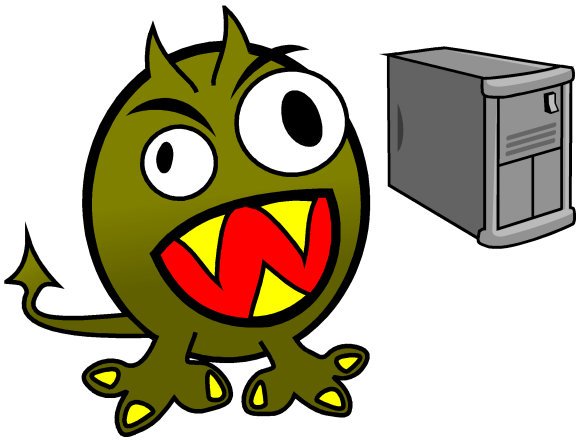
```
aptitude install mandos
aptitude install mandos-client
```

Threat Model

Threat Model

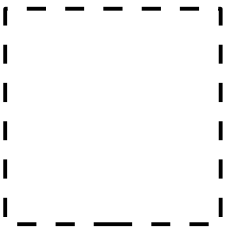


Threat Model

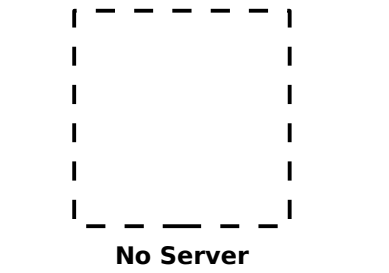


Threat Model

Threat Model

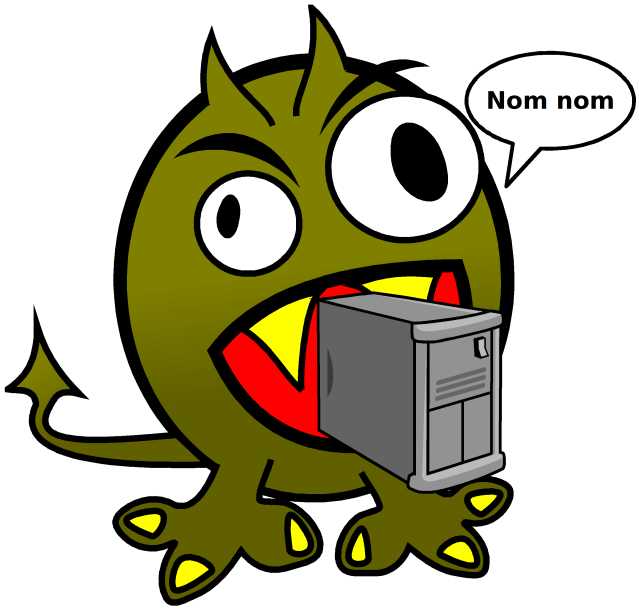


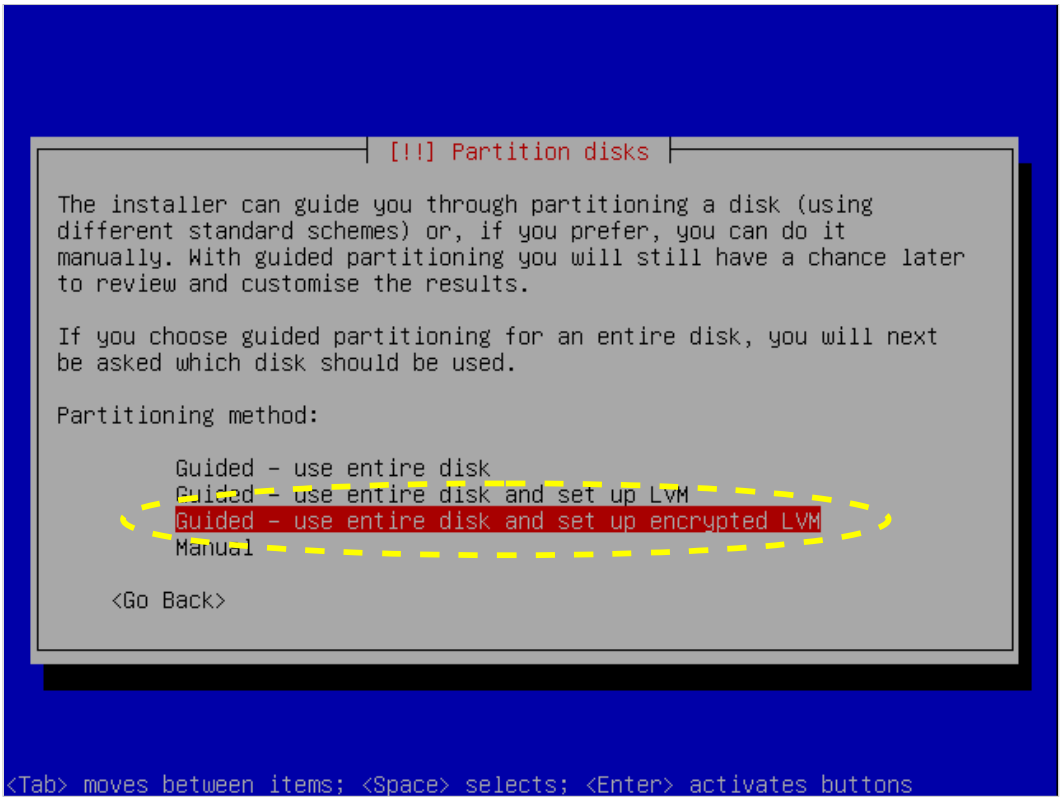
Threat Model

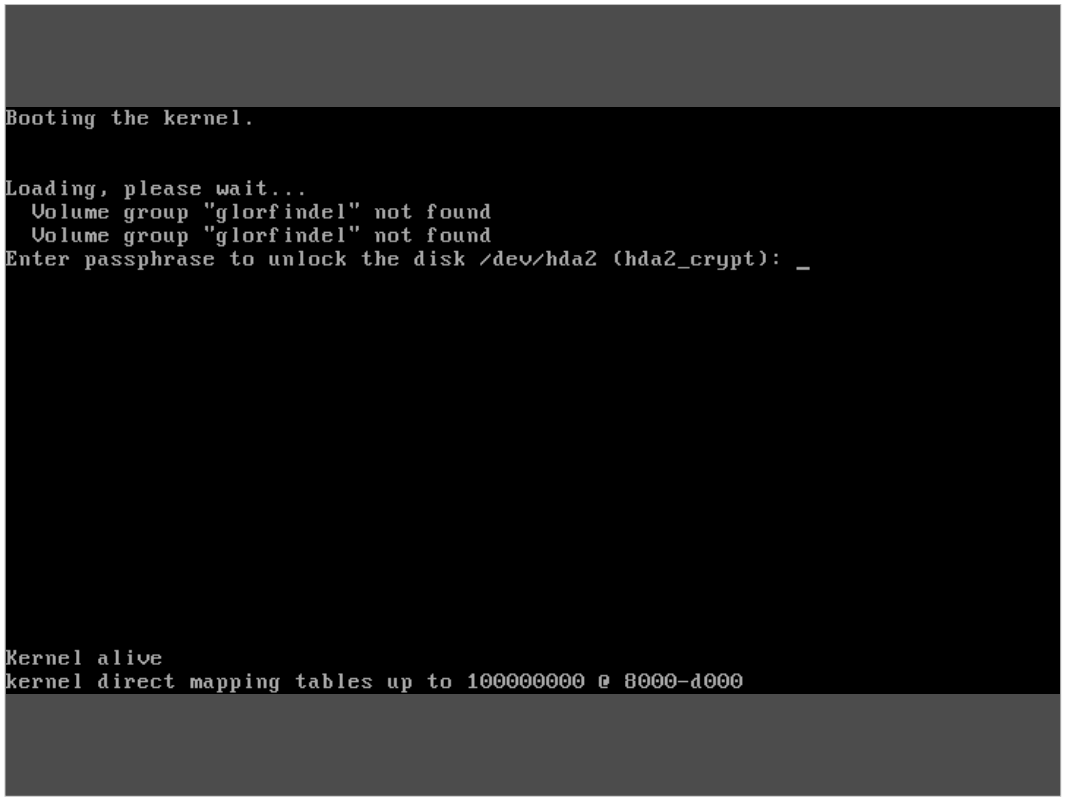


Sad users

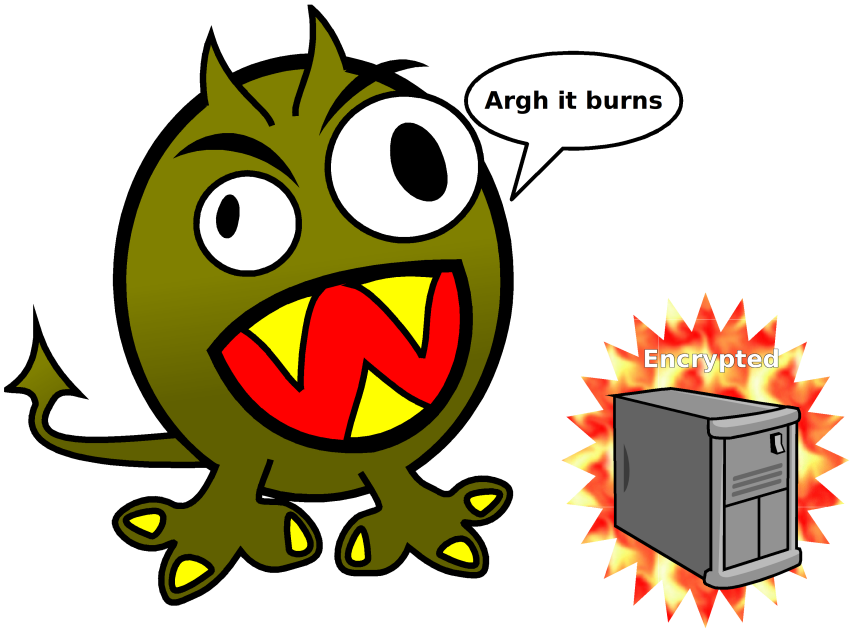
Threat Model




[!!] Partition disks
The installer can guide you through partitioning a disk (using
different standard schemes) or, if you prefer, you can do it
manually. With guided partitioning you will still have a chance later
to review and customise the results.
If you choose guided partitioning for an entire disk, you will next
be asked which disk should be used.
Partitioning method:
Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual
<Go Back>
<Tab> moves between items; <Space> selects; <Enter> activates buttons


Booting the kernel.
Loading, please wait...
Volume group "glorfindel" not found
Volume group "glorfindel" not found
Enter passphrase to unlock the disk /dev/hda2 (hda2_crypt): _
Kernel alive
kernel direct mapping tables up to 100000000 @ 8000-d000

Threat Model



New threat: non-use

Inconvenient
Burdensome
“I’ll do it some day”

Mail servers especially common to not be encrypted. Co-location make passwords inconvenient.

New threat:

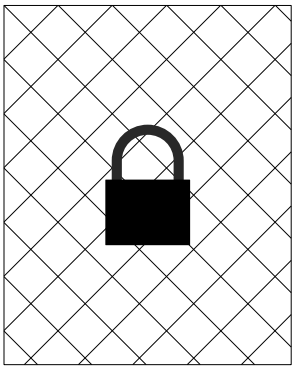
Security needs to be *transparent*

Model after IPsec.
User behavior can stay unchanged.

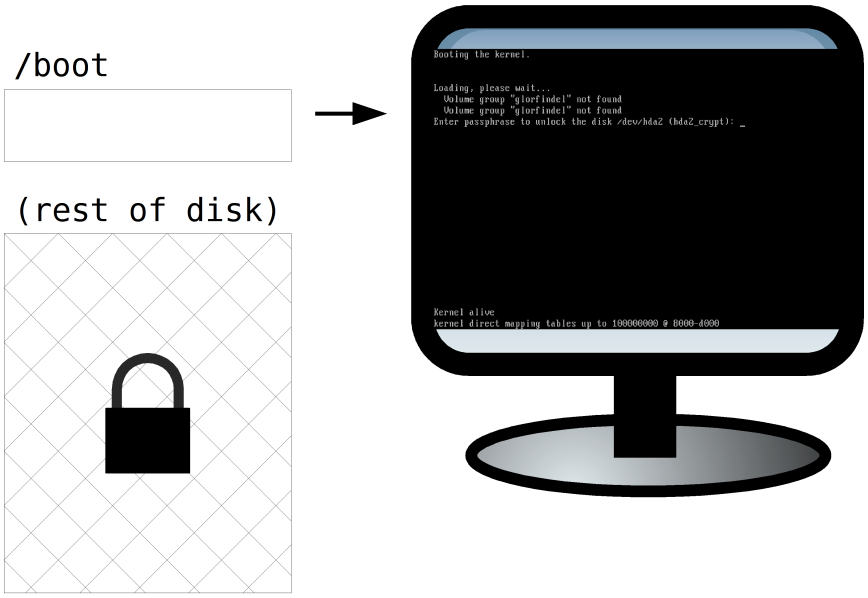
Full Disk Encryption

/boot

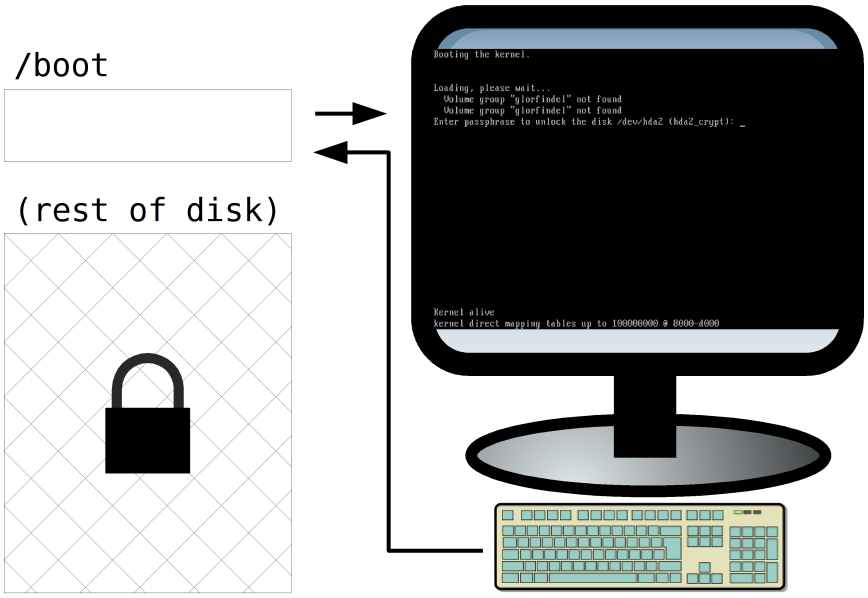
(rest of disk)



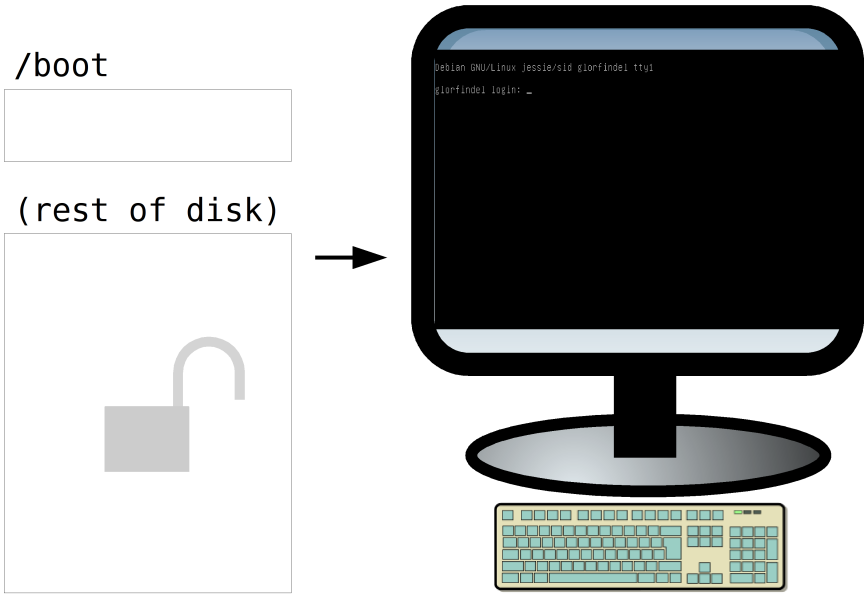
Full Disk Encryption



Full Disk Encryption



Full Disk Encryption



Mandos

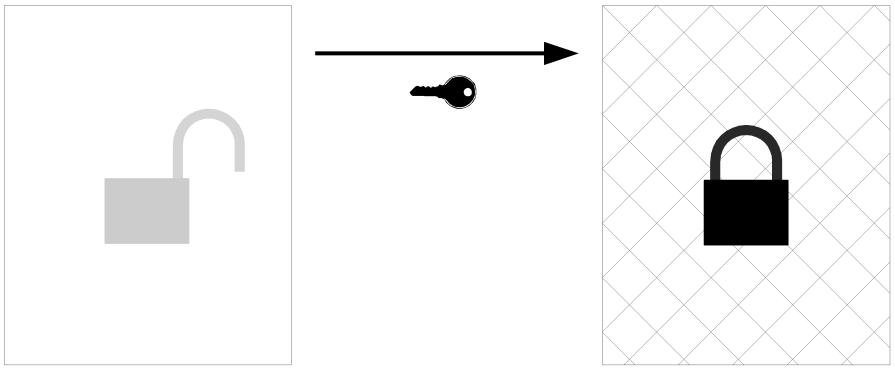
http://www.recompile.se/mandos

Servers provide passwords to *each other*

Mandos

http://www.recompile.se/mandos

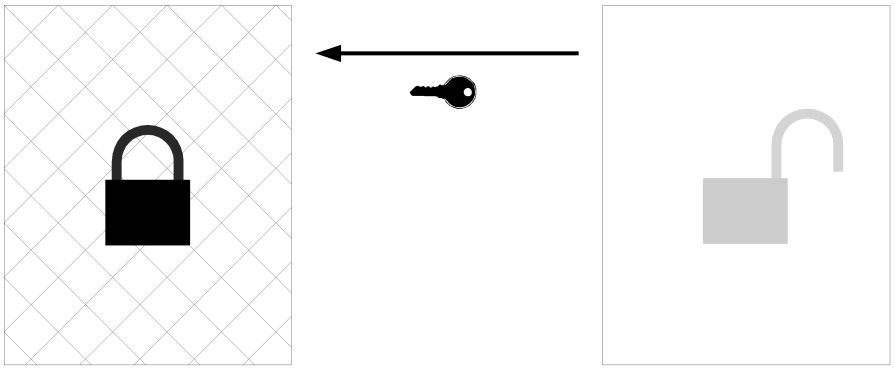
Normal operation



Mandos

http://www.recompile.se/mandos

Normal operation

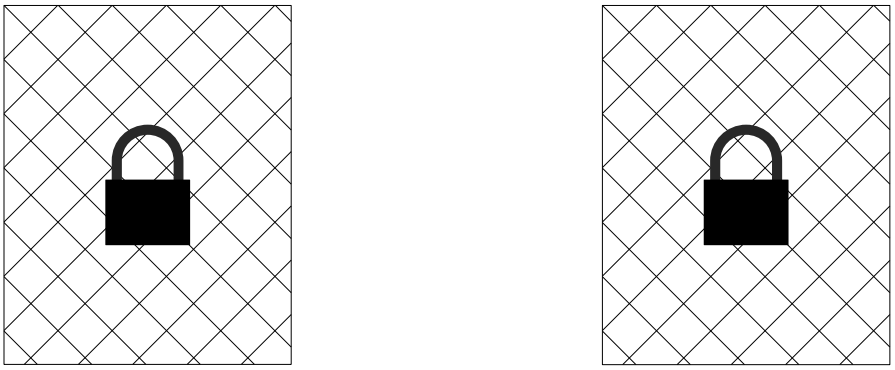


Mandos

http://www.recompile.se/mandos

Lockdown state

Administrator attention required



Deadlock / bootstrap problem as security feature!

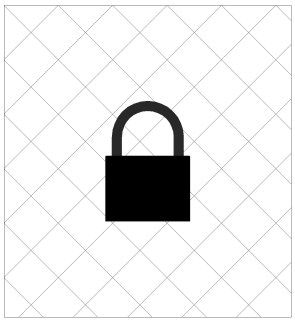
This is the usual state when you really need encryption.

Mandos

http://www.recompile.se/mandos

/boot

(rest of disk)

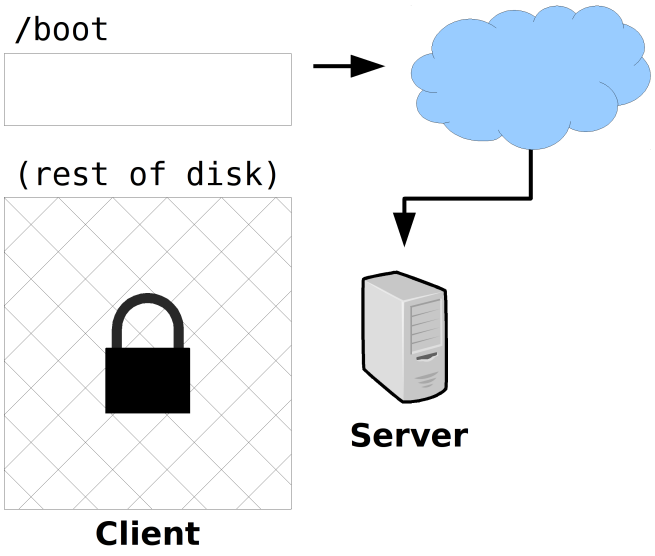


Client

Server

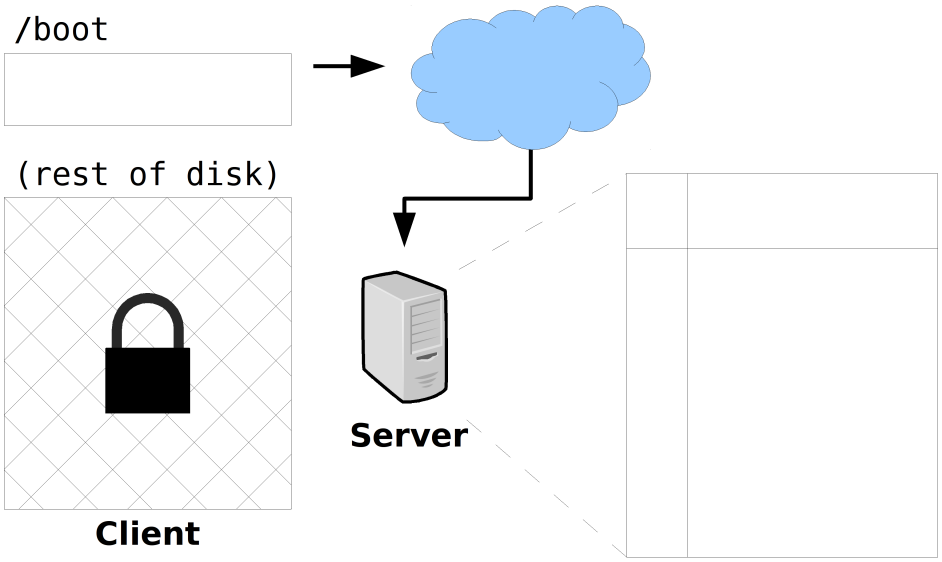
Mandos

http://www.recompile.se/mandos



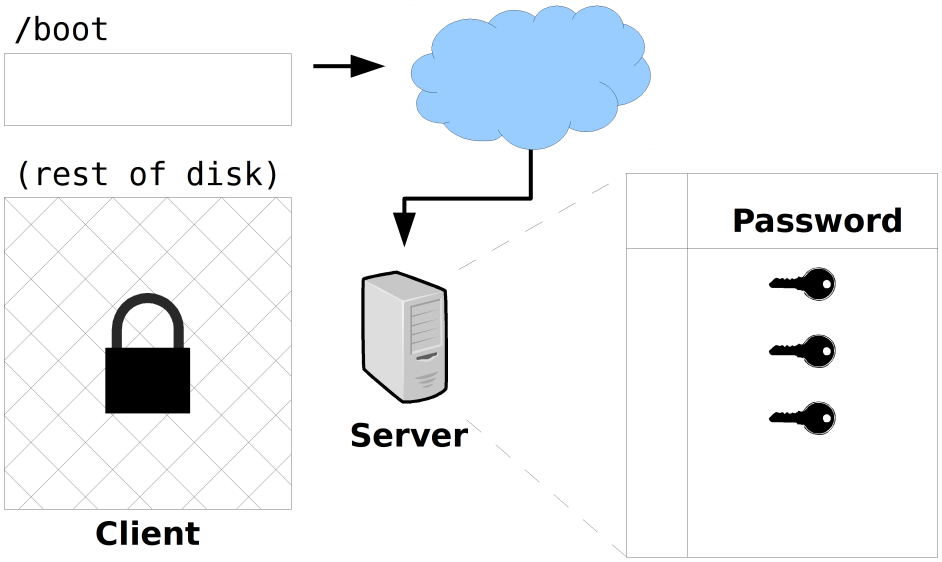
Mandos

http://www.recompile.se/mandos



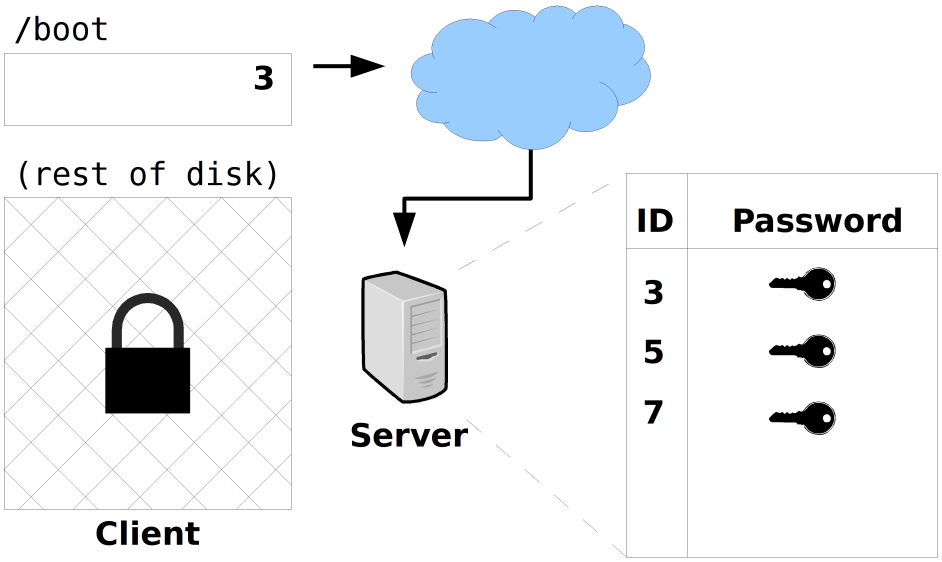
Mandos

http://www.recompile.se/mandos



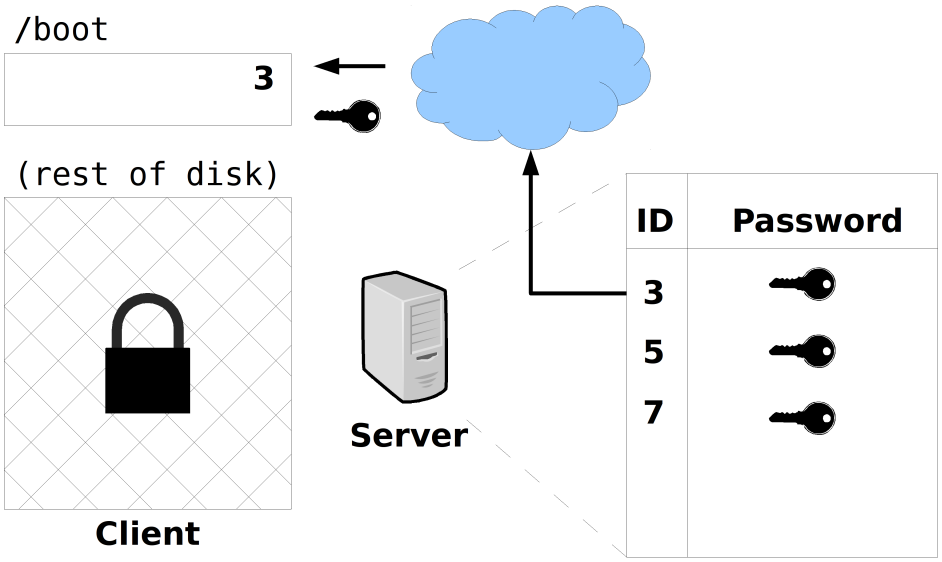
Mandos

http://www.recompile.se/mandos



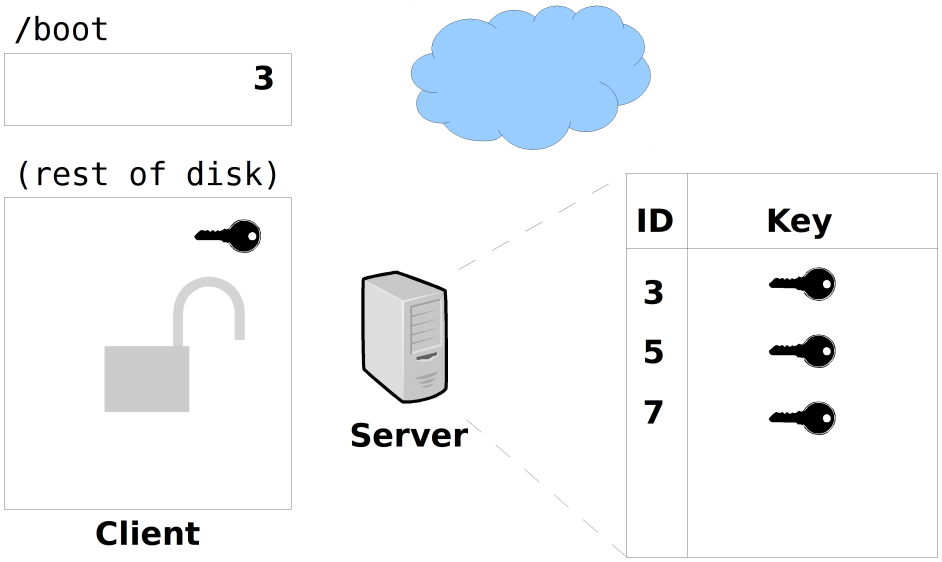
Mandos

http://www.recompile.se/mandos



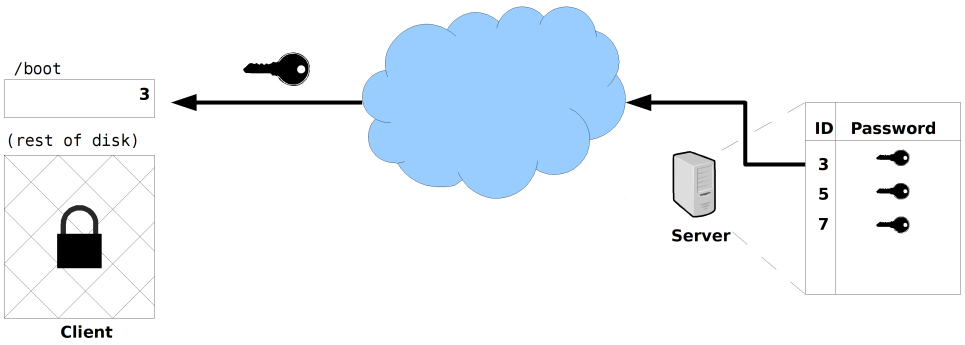
Mandos

http://www.recompile.se/mandos



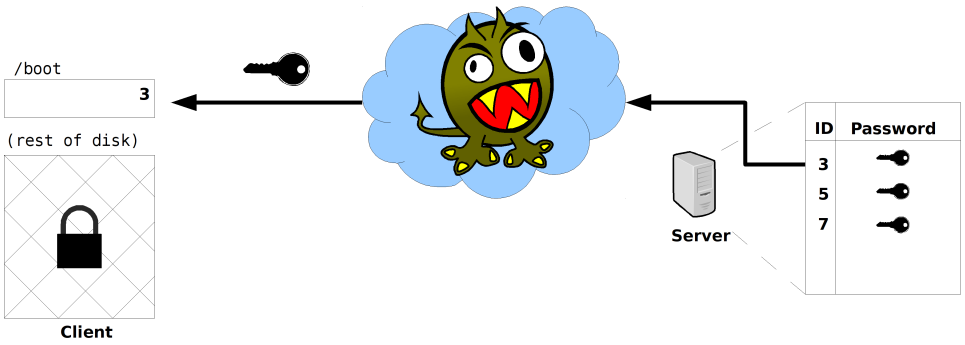
Mandos

http://www.recompile.se/mandos



Mandos

http://www.recompile.se/mandos



“GPG for data at rest. TLS for data in motion.”

If You're Typing The Letters A-E-S Into Your Code, You're Doing It Wrong
http://www.cs.berkeley.edu/~daw/teaching/cs261-f12/misc/if.html

TLS has a “server” side and a “client” side, and the “server” side *needs* a key.

The TLS key can be a X.509 certificate

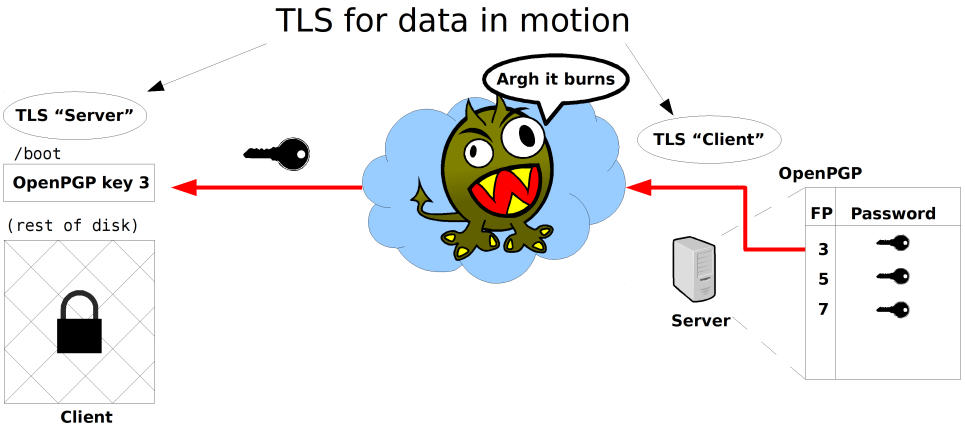
X.509:

“Someone tried to explain public-key-based authentication to aliens. Their universal translators were broken and they had to gesture a lot.”
— Peter Gutmann
Everything you Never Wanted to Know about PKI but were Forced to Find Out

Alternatively, the TLS key can be an OpenPGP key

Mandos

http://www.recompile.se/mandos



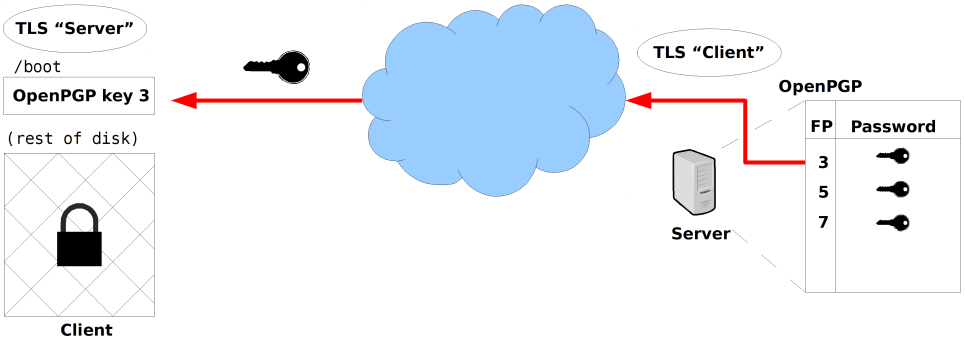
“FP” means fingerprint

“GPG for data at rest”?

Mandos

http://www.recompile.se/mandos

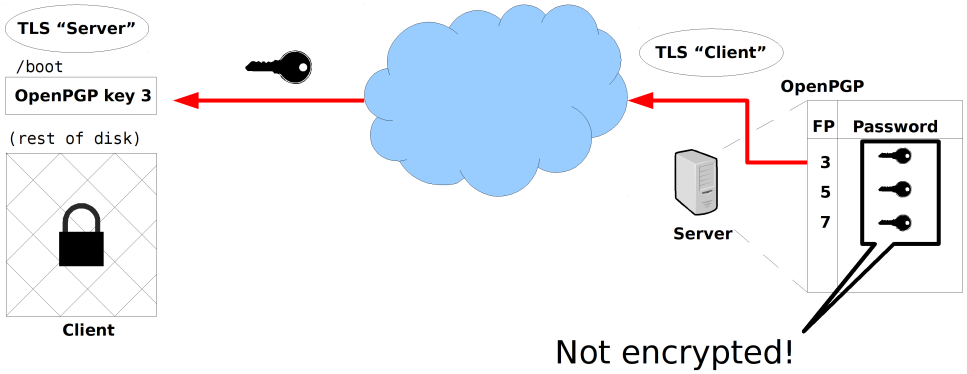
TLS for data in motion



Mandos

http://www.recompile.se/mandos

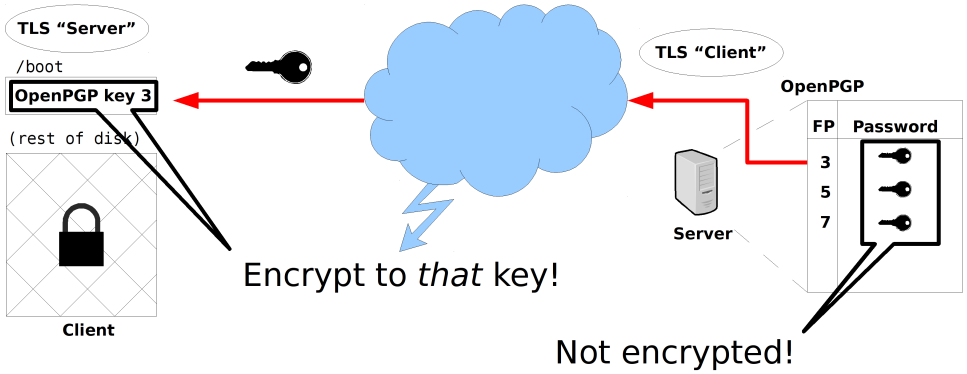
TLS for data in motion



Mandos

http://www.recompile.se/mandos

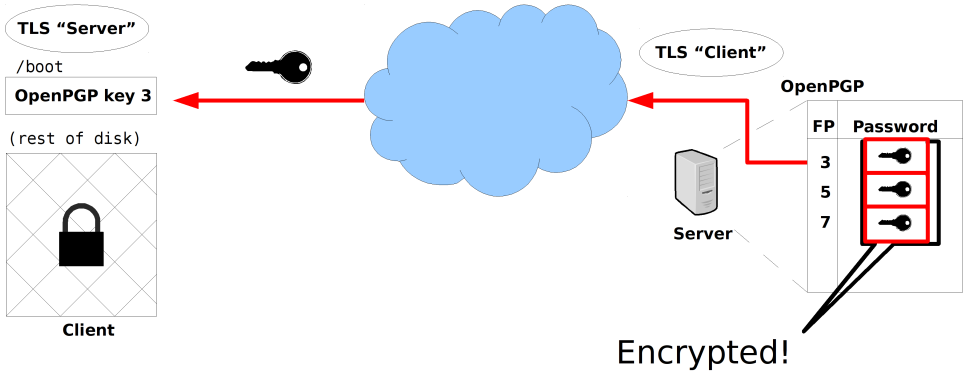
TLS for data in motion



Mandos

http://www.recompile.se/mandos

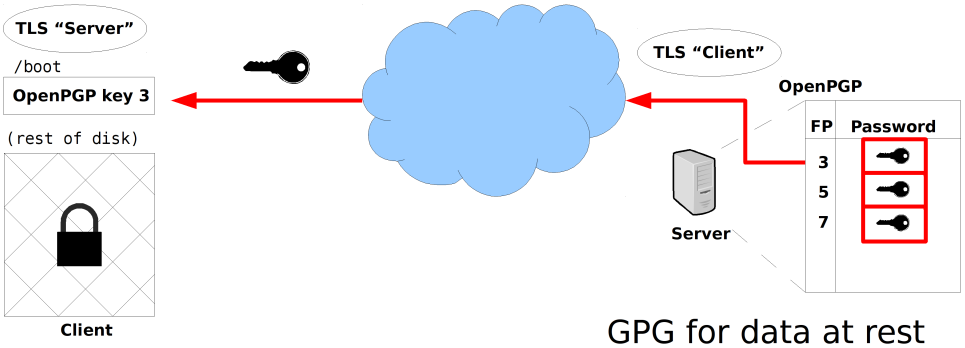
TLS for data in motion



Mandos

http://www.recompile.se/mandos

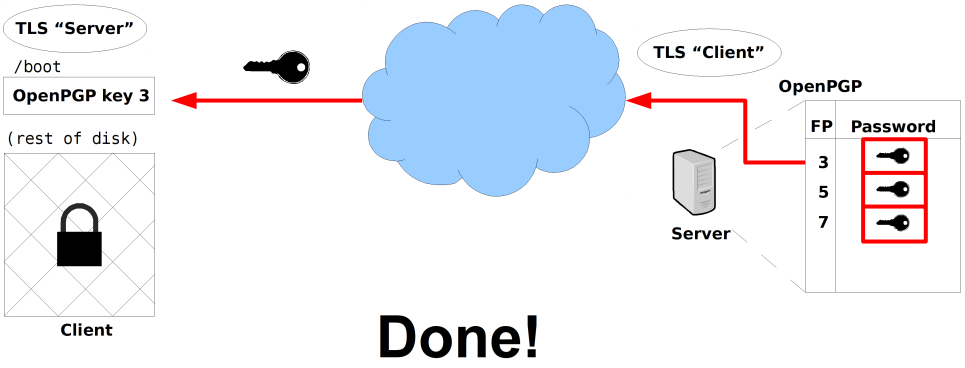
TLS for data in motion



GPG for data at rest

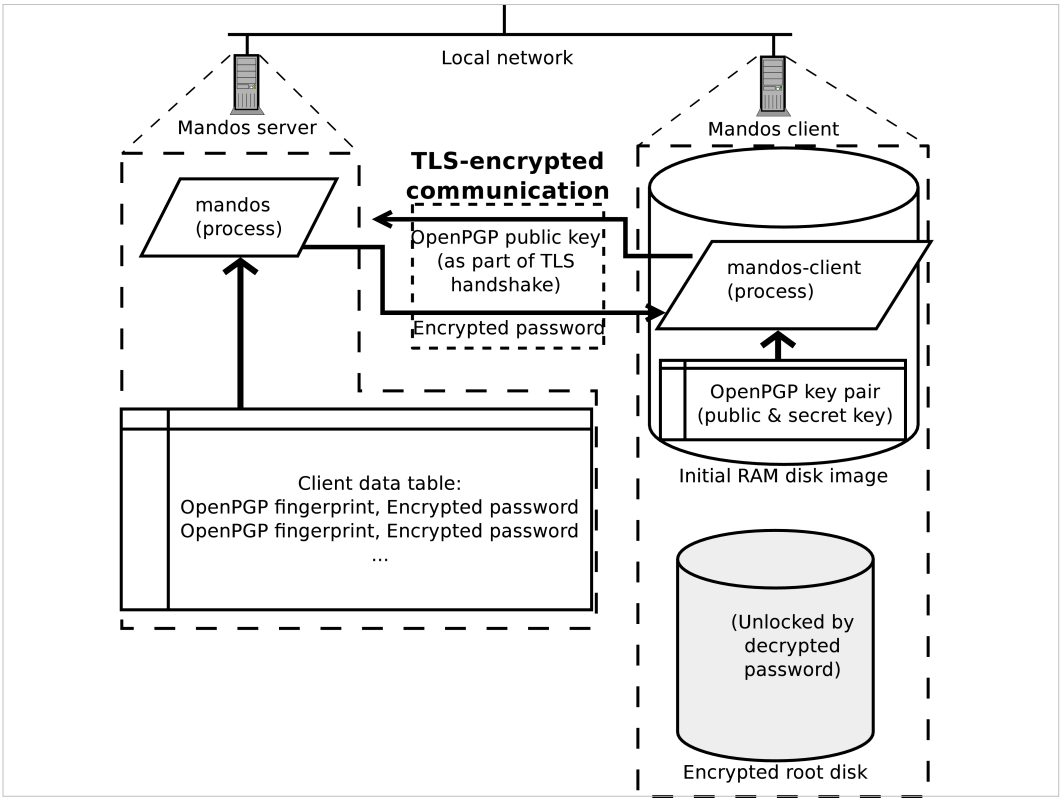
Mandos

http://www.recompile.se/mandos

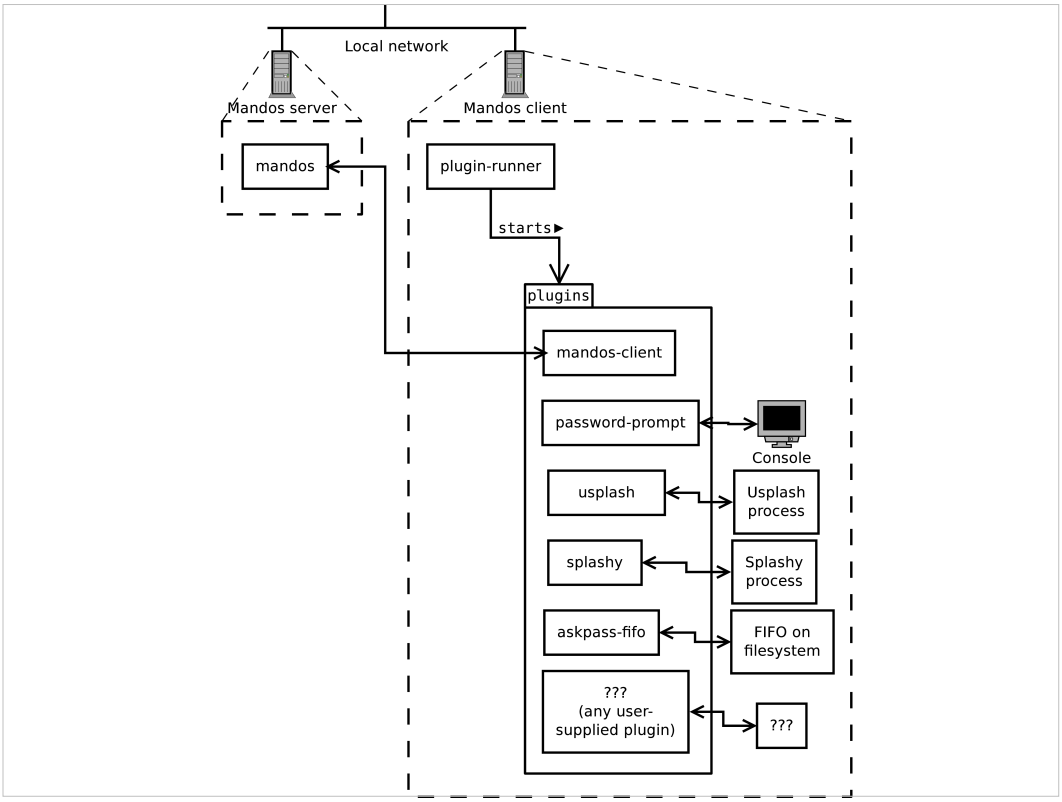


Done!

Finished



Older diagram attempting to show the same thing



Client-side process model with plugins for various input methods, etc.

FAQ

Grabbing the Mandos client key from the `/boot` partition's `initramfs` image really quickly?

Threat model: people grabbing servers fast. Sophisticated attackers can and will do cold-boot.

Mandos shrinks the window of opportunity to default 5 minutes, customizable

Mandos

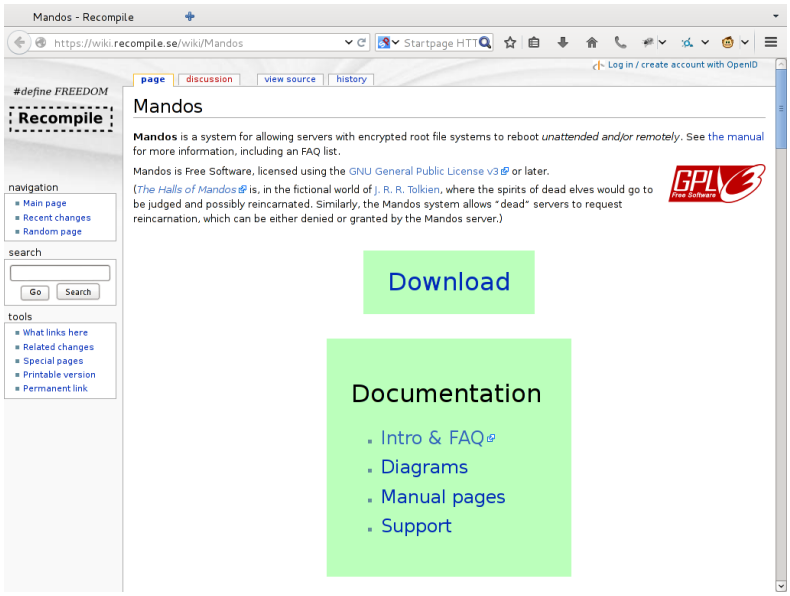
http://www.recompile.se/mandos

- **In Ubuntu “universe” since 2009**
- **In Debian since 2011**

```
aptitude install mandos
aptitude install mandos-client
```

Mandos

http://www.recompile.se/mandos



Mandos

http://www.recompile.se/mandos

http://ftp.recompile.se/pub/mandos/misc

These slides and more