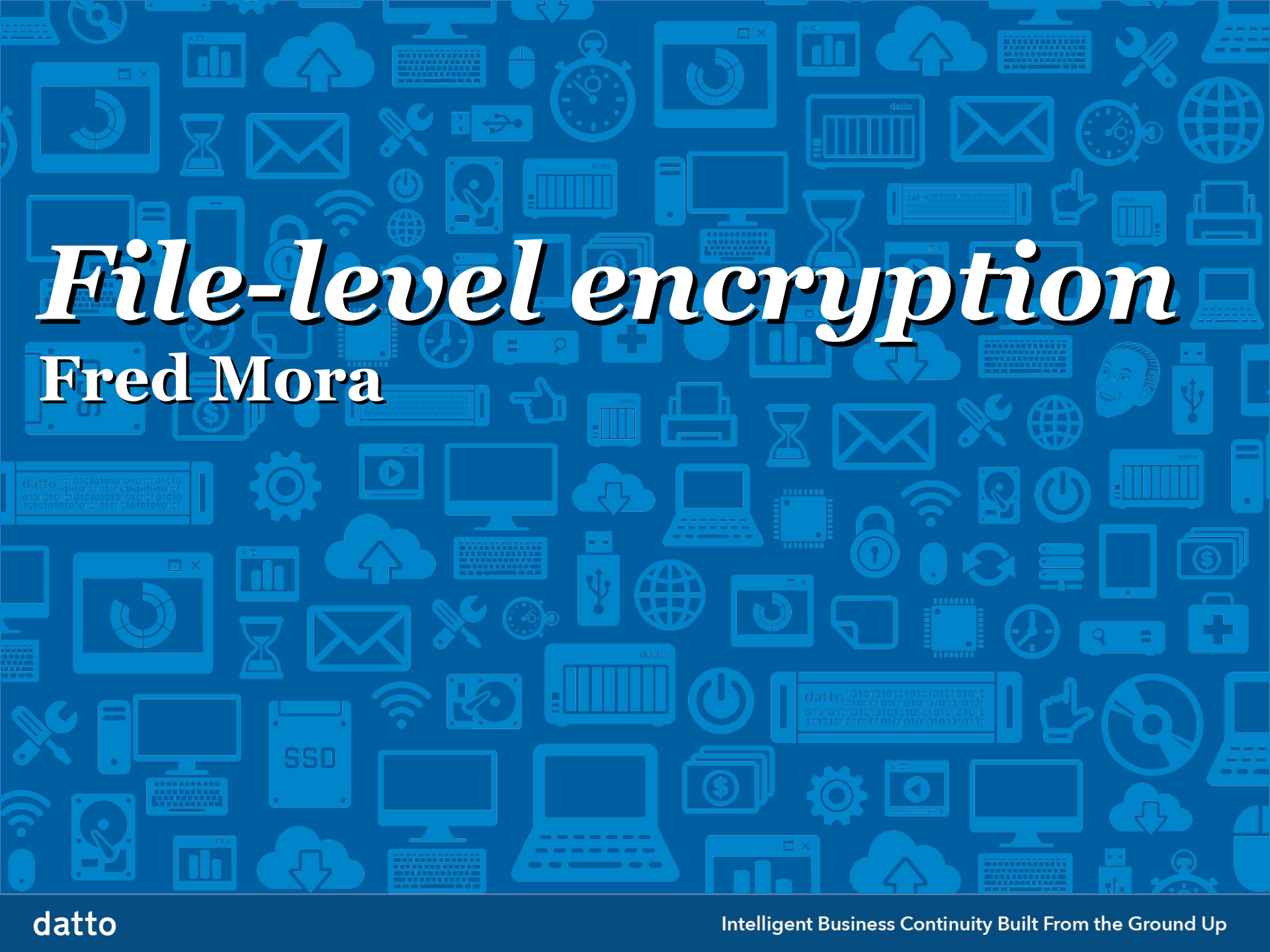

File-level encryption
Fred Mora
datto
Intelligent Business Continuity Built From the Ground Up

Why file-level?

- Linux supports encrypted drives
- Why not simply use that?
- Because…
  - Encrypted disk solves the lost laptop problem
  - But does not solve the data leak problem
  - Application bugs can be exploited to leak data
  - Backups of encrypted disks are not encrypted…
- So we still need a solution for files we really want to protect.

eCryptfs

- eCryptfs is a kernel module
- Part of kernel since 2006
- Offers filesystem encryption
- User interacts with userspace tools
- User package is ecryptfs-utils.
- POSIX compliance
- Basis of Ubuntu encrypted home dir

Usage scenarios

- You have really confidential files in a directory:
  - Medical history
  - Legal documents
  - IRS
- You want this dir to be available (decrypted) only when you need to access these files
- The rest of the time, keep data encrypted.

Implementing the scenario

- Create and encrypt a directory in place

  You will be prompted for a passphrase. Memorize it.

```
$ PERSDIR=$HOME/personal
$ mkdir $PERSDIR
$ chmod u=rwx,go=- $PERSDIR
$ sudo mount -t ecryptfs $PERSDIR $PERSDIR
Passphrase:
Select cipher:
 1) aes: blocksize = 16; min keysize = 16;
max keysize = 32 (not loaded)
 2) blowfish: blocksize = 16; min keysize =
16; max keysize = 56 (not loaded)
 3) des3_ede: blocksize = 8; min keysize =
24; max keysize = 24 (not loaded)
 4) twofish: blocksize = 16; min keysize =
16; max keysize = 32 (not loaded)
 5) cast6: blocksize = 16; min keysize = 16;
max keysize = 32 (not loaded)
 6) cast5: blocksize = 8; min keysize = 5;
max keysize = 16 (not loaded)
Selection [aes]: 1
Select key bytes:
 1) 16
 2) 32
 3) 24
Selection [16]: 16
Enable plaintext passthrough
(y/n) [n]: n
Enable filename encryption (y/n)
[n]: n
Attempting to mount with the
following options:
  ecryptfs_unlink_sigs
  ecryptfs_key_bytes=16
  ecryptfs_cipher=aes
  ecryptfs_sig=e5e8e368a0475ff9

Mounted eCryptfs
```

Implementing (cont'd)

- Now you can put these options in fstab (all on one line):

```
/home/fmora/personal  /home/fmora/personal
 ecryptfs  rw,
ecryptfs_sig=e5e8e368a0475ff9,
user,noauto,key=passphrase,
ecryptfs_passthrough=n,
ecryptfs_cipher=aes,
ecryptfs_key_bytes=16       0   0
```

Mounting script

- You want to mount the dir only when necessary
- Create a small helper script, `mount-pers.sh`:

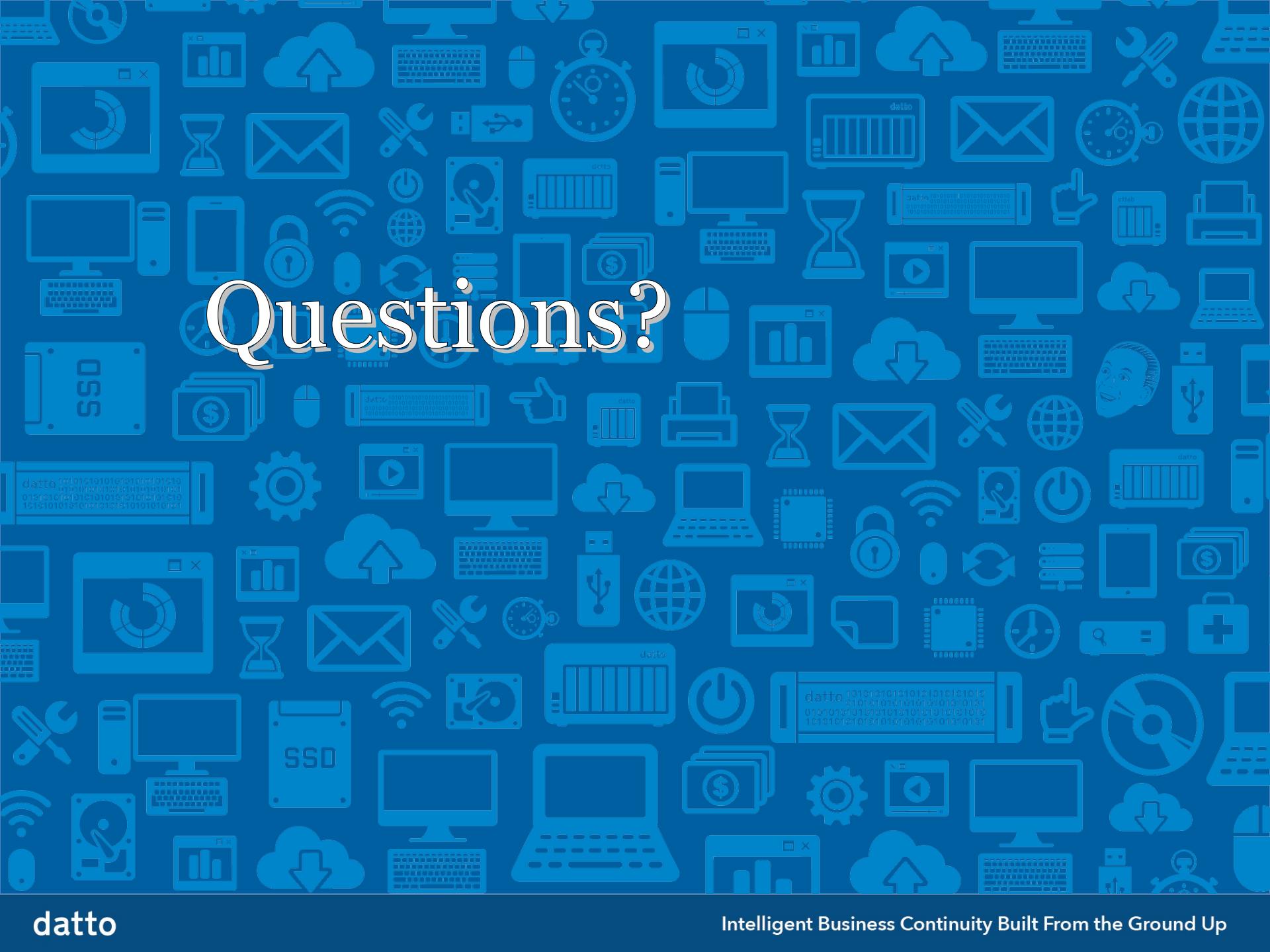
```
PERSDIR=$HOME/personal
# Check to see if already mounted

c=$(mount | grep -c "$PERSDIR")
if [ $c == 1 ]
then
  echo "$PERSDIR already mounted"
  exit 1
fi

# Prompt for key, put key in keyring
ecryptfs-manager

# Call with -i to avoid prompting for
# password again
mount -i $PERSDIR
```

To access your files:
`./mount-pers.sh`
When done:
`umount ~/personal`


Questions?