

THE SECURITY PLAN

SAFEGUARDING THE FILEMAKER CASTLE

vienna calling

bitwork

CRISTINA ÁLVAREZ DÁVILA

- ▶ Málaga, Cádiz, Madrid...
- ▶ Filemaker since... don't remember
- ▶ Bitwok... a lot of years
- ▶ Dog & Cooking lover
- ▶ Speaker and Problem solver



calvarez@bitwok.es



WHAT WILL WE TALK ABOUT TODAY?

SAFEGUARDING THE FILEMAKER CASTLE

- Protecting your data, project and happiness



WHY PROTECT THE CASTLE?

- ▶ Growing risks
- ▶ Legal rules
- ▶ Client trust
- ▶ Data safety
- ▶ Easy



LOCKING THE CASTLE'S PHYSICAL GATES

- ▶ Server in a secure Data Center
- ▶ Closed rack
- ▶ Data in encrypted DB
- ▶ Limited access to the backups
- ▶ Everything is better in the cloud.



CONTROLLING LOGICAL ACCESS TO THE CASTLE

- ▶ Public service: create DMZ
- ▶ Access restricted only by VPN
- ▶ Minimal privileges
- ▶ Control of access to the files
authentication (always two-factor)
- ▶ SSL Certificate



Principle of least privilege: give users only what they need to do their job

Choose privileges and save them as a "Privilege Set," which can be used by one or more accounts. If you edit a set, all accounts that use it will be affected.

Privilege Set Name

Description

PrivilegeAll

No thinking, no driving

Data Access and Design

Records: Create, edit, and delete in all tables

Layouts: All modifiable

Value Lists: All modifiable

Scripts: All modifiable

Extended Privileges

☒ Access via FileMaker WebDirect (fmwebdirect)

☒ Access via ODBC/JDBC (fmjdbc)

☒ Access via FileMaker Network (fmapp)

☒ Require re-authentication after the specified minutes in sleep/background. (fmreauthenticate10)

☒ Access via XML Web Publishing - FMS only (fmxml)

☒ Access via PHP Web Publishing - FMS only (fmphp)

☒ Allow Apple events and ActiveX to perform FileMaker operations (fmextscriptaccess)

☒ Allow URLs to run FileMaker scripts (fmurlscript)

☒ Access via FileMaker Data API (fmrest)

☒ Access via OData (fmodata)

☒ Validate cross-file plug-in access (fmplugin)

Other Privileges

☒ Allow printing

☒ Allow exporting

☒ Manage extended privileges

☒ Manage accounts that don't have Full Access

☒ Allow user to override data validation warnings

☒ Disconnect user from server when idle

☒ Allow user to modify their own password

☐ Must be changed every

30

days

☐ Minimum password length:

5

characters

Available menu commands: All

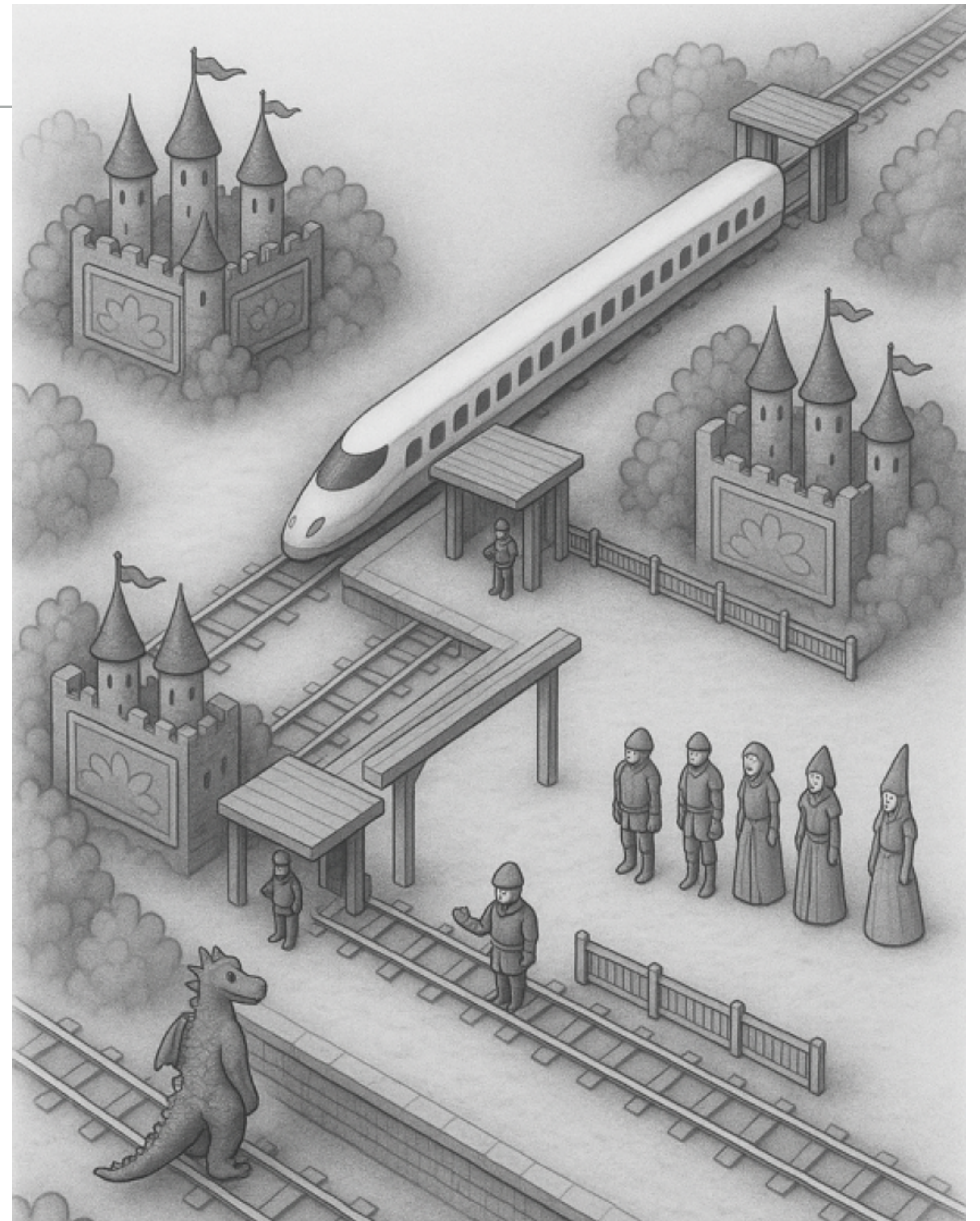
CONTROLLING LOGICAL ACCESS TO THE CASTLE

- ▶ Public service: create DMZ
- ▶ Access restricted only by VPN
- ▶ Minimal privileges
- ▶ Control of access to the files
authentication (2FA better)
- ▶ SSL Certificate



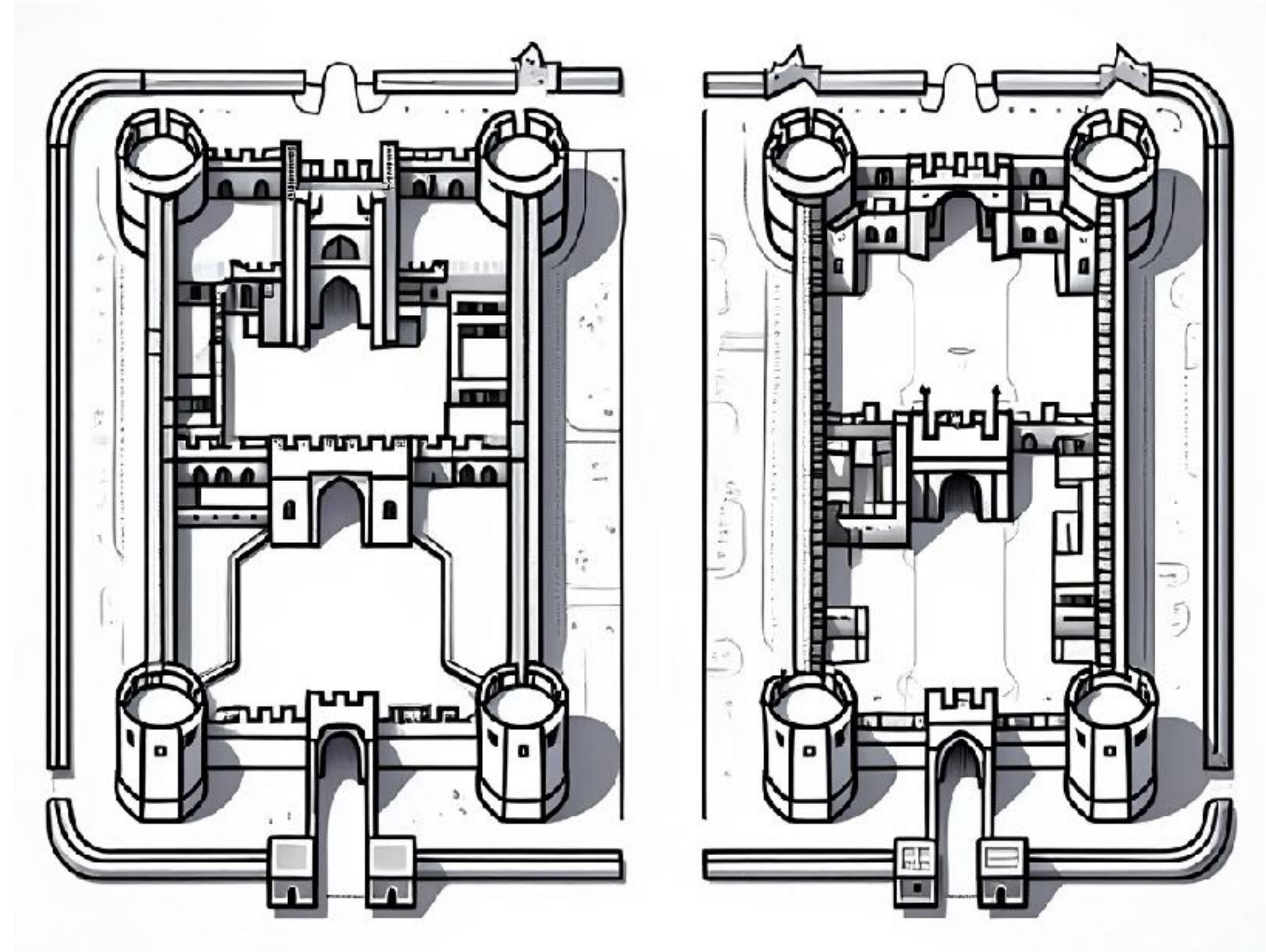
PREVENTING DIRECT ACCESS TO CASTLE FILES

- ▶ Hide all files
- ▶ Create an access control file
- ▶ Use Filemaker Server



ACCESSING FILES BY CASTLE MODULES

- ▶ Create a security module files (front & back)
- ▶ Control access permissions
- ▶ Create file with access menu
- ▶ A data separation model is essential



KEEPING THE CASTLE WELCOMING

- ▶ The security should not harm the user
- ▶ Should be implemented layer by layer
(layer cake)
- ▶ Permissions should be organised in a
separate environment



CLASSIC LAYERS IN SECURITY

LAYER 01 – CRITICAL ASSETS

Highly sensitive data!!

LAYER 02 – DATA SECURITY

Module, separation, layers!

LAYER 03 – APPLICATION SECURITY

Limit access to file fmp.12 - Hide!

LAYER 04 – ENDPOINT SECURITY

Control FMS, updates, passwords, logout

LAYER 05 – NETWORK SECURITY

VPN, DMZ...

LAYER 06 – PERIMETER SECURITY

Limit physical access (racks, cloud...)

LAYER 07 – HUMAN LAYER

The weakest one!

BUT THE BEST SECURITY IS BASED ON:

- ▶ Common sense
- ▶ Training to avoid social engineering
- ▶ Education
- ▶ Common sense again

BUT THE BEST SECURITY IS BASED ON:



"THERE IS NO PATCH FOR STUPIDITY."

Kevin Mitnick
Condor / Wire Ghost