DataFlex to New Heights

Security Matters

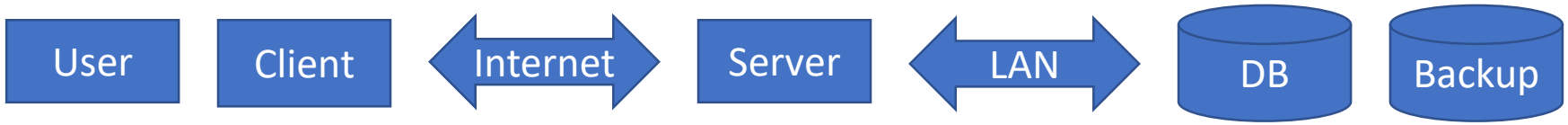
Jeroen Steehouder

Introduction

- General Data Protection Regulation (GDPR)
- Global war in cyberspace
- Information security is about access control

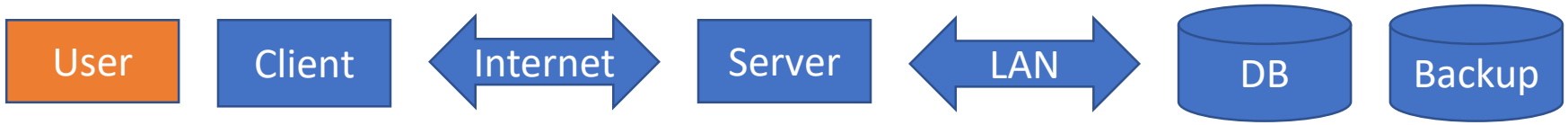
Core requirements

- All data access must be controlled
  - Only via systems enforcing the risk mitigations!
- User access can be trusted
  - Effective identification and authentication



The user

- Identification
- Authentication
  - Prevent users from using weak (leaked) passwords
  - Enforce a sane minimum and maximum passcode length
  - Use a password storage algorithm specifically designed for this purpose
  - Do not enforce periodic passcode renewal or complexity rules
- Account recovery
  - Recovery question / password hint
  - E-mail a recovery link



Intermezzo – DataFlex Security Library

Security Library Contents

- Generic hashes (SHA256)
- Keyed hashes (HMAC-SHA256)
- Symmetric key encryption (AES-CBC)
- Authenticated encryption (AES-GCM)
- Passcode storage methods (PBKDF2, scrypt, Argon2)
- 2FA (TOTP, HOTP, FIDO U2F)

Security Library - Philosophy

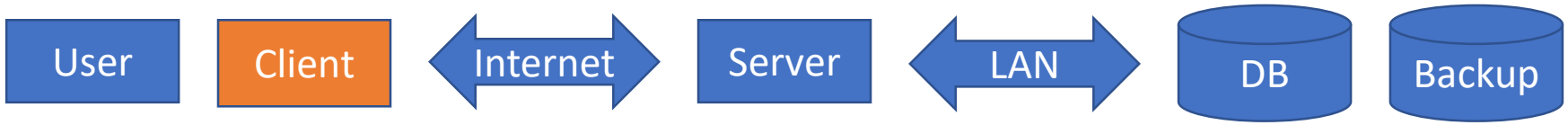
- Flexibility to use multiple engines
  - Microsoft Cryptography API Next Generation (CNG)
  - Libsodium (FOSS dll)
- Simplicity
  - Limited choices to prevent risks
  - Easy to integrate into your products
- Stability
  - Tested, tested again, and retested again and again…


Demonstration


Let’s continue...

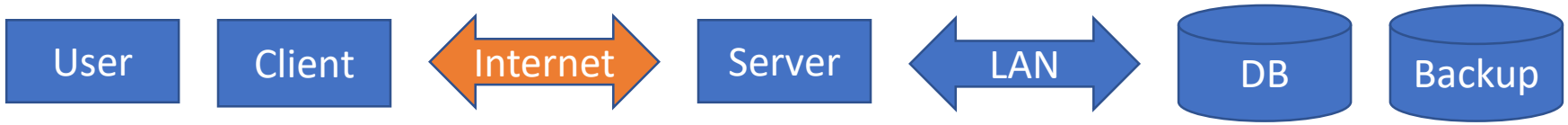
The client

- The device may be compromised
- The user may be milicious
  - Unhide hidden objects
  - Manipulate client-side properties
  - Send fake calls to the server
  - Attempt SQL injections
  - Attempt URL injections
    - Expect users to forward URLs



The internet

- Use HTTPS with HSTS for *all communication*
  - Develop using self-signed certificates and a fake domain name
    - Choose a non-existing TLD
  - Use a trusted CA for public deployments

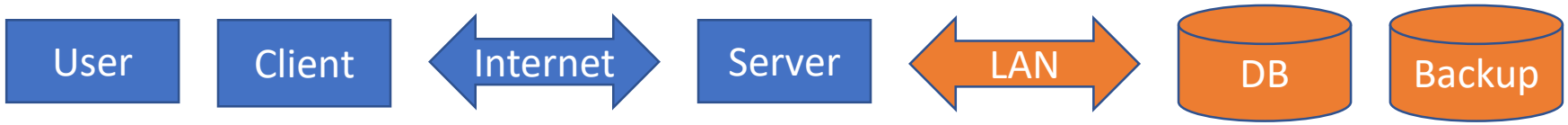


The server

- Use managed SQL connections
  - Disable tools access for network deployments
- Harden your server
  - Unnecessary services
  - Restricted user account
  - Download/upload locations

The local network and database

- Several options:
  - Isolate the network physically
  - Encrypt the database connection
  - Encrypt the data before sending it to the DB
- Assess your risks:
  - System & database administrators
  - Physical security
  - Encrypt your backups: *no exceptions*



The rest

- Check your development process
  - Code signing and verification (PGP)
  - Sign your exe/dll files immediately after build
- Educate your employees, customers, and end-users

Balance

- 100% security = 0% usability
- Find the balance between security and usability for each project


European DataFlex users' conference - Edinburgh, Scotland
EDUC
2018
DataFlex to New Heights
Thank you!
Are there any questions?