Securing PostgreSQL From External Attack

BRUCE MOMJIAN,
ENTERPRISEDB

September, 2009

Abstract

Database systems are rich with attack vectors to exploit. This presentation explores the many potential PostgreSQL external vulnerabilities and shows how they can be secured.

 http://momjian.us/presentations

Attack Vectors

External Attack Vectors

- 'Trust' security
- Passwords / authentication theft
- Network snooping
- Network pass-through spoofing
- Server / backup theft
- Administrator access

Internal Attack Vectors (Not Covered)

- Database object permissions
- Application vulnerability
- Operating system compromise

Authentication Security

http://www.my-time-machines.net/mosler_34.htm

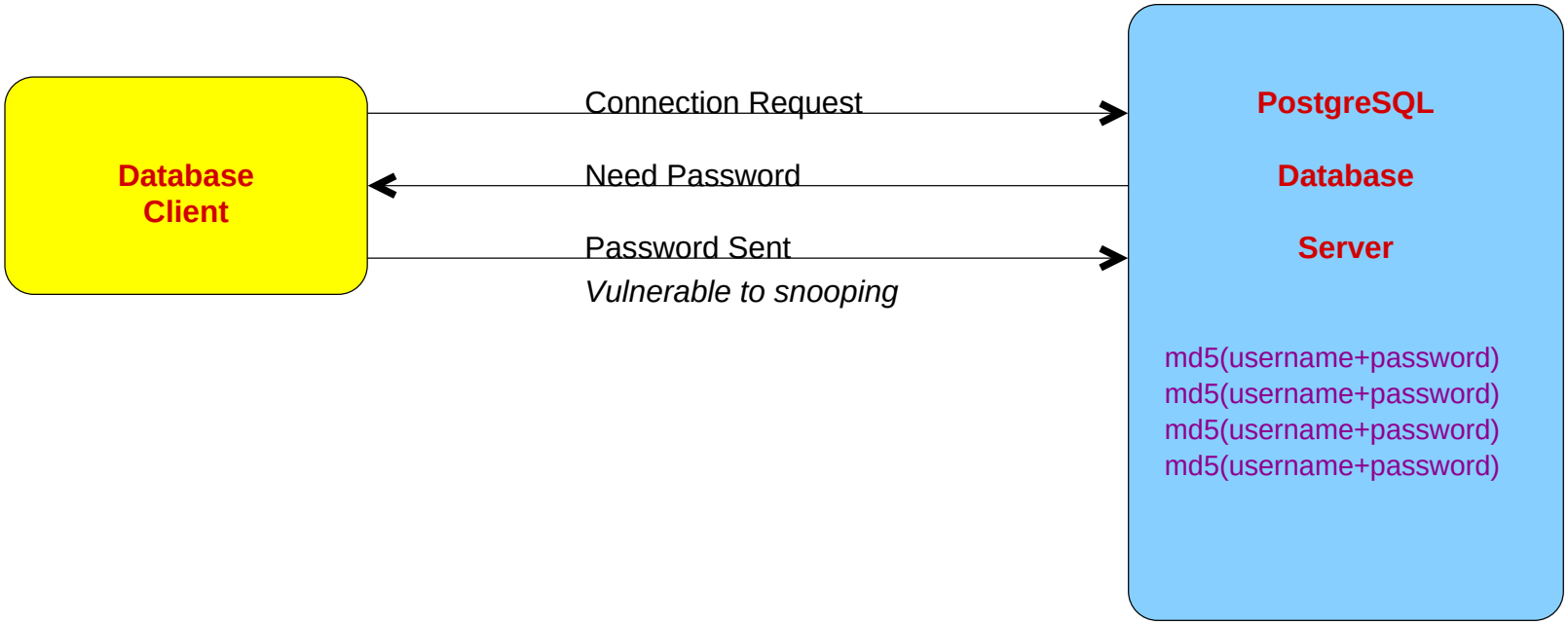
Avoid 'Trust' Security

```
# TYPE  DATABASE    USER        CIDR-ADDRESS          METHOD
# "local" is for Unix domain socket connections only
local   all         all                               trust
# IPv4 local connections:
host    all         all         127.0.0.1/32          trust
# IPv6 local connections:
host    all         all         ::1/128               trust
```

Solution: Use the initdb *-A* flag, i.e., you don't want to see this:

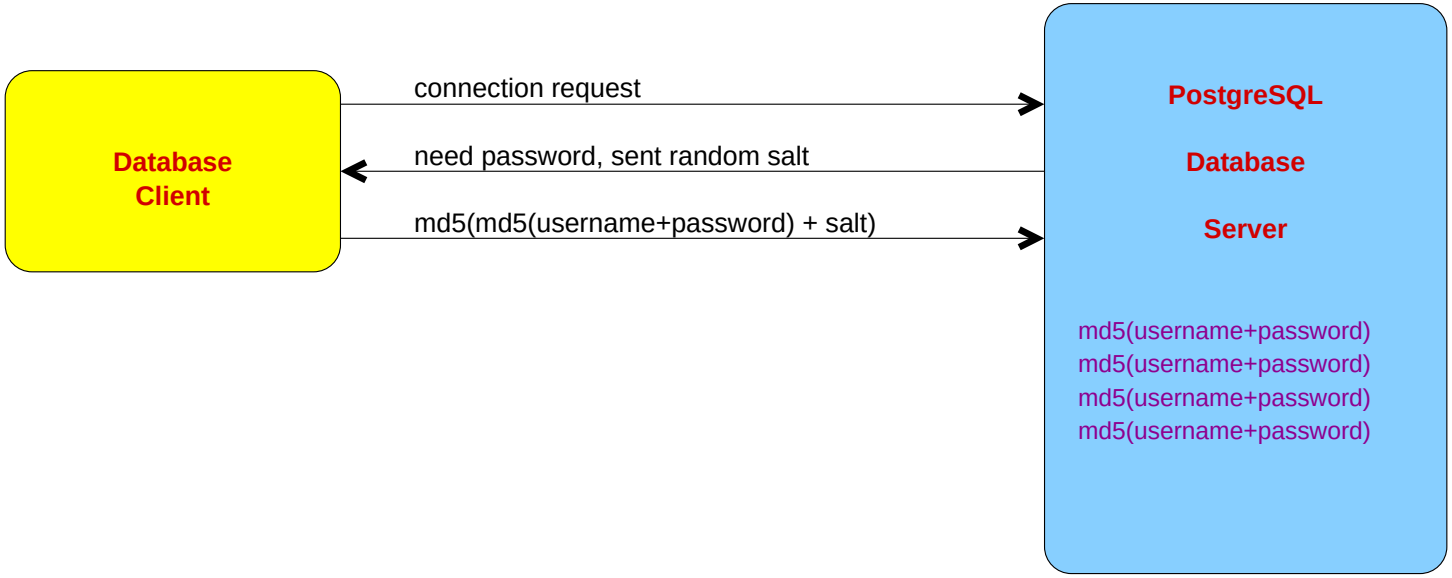
> WARNING: enabling "trust" authentication for local connections
> You can change this by editing pg_hba.conf or using the -A option the next time you run initdb.

Password Snooping

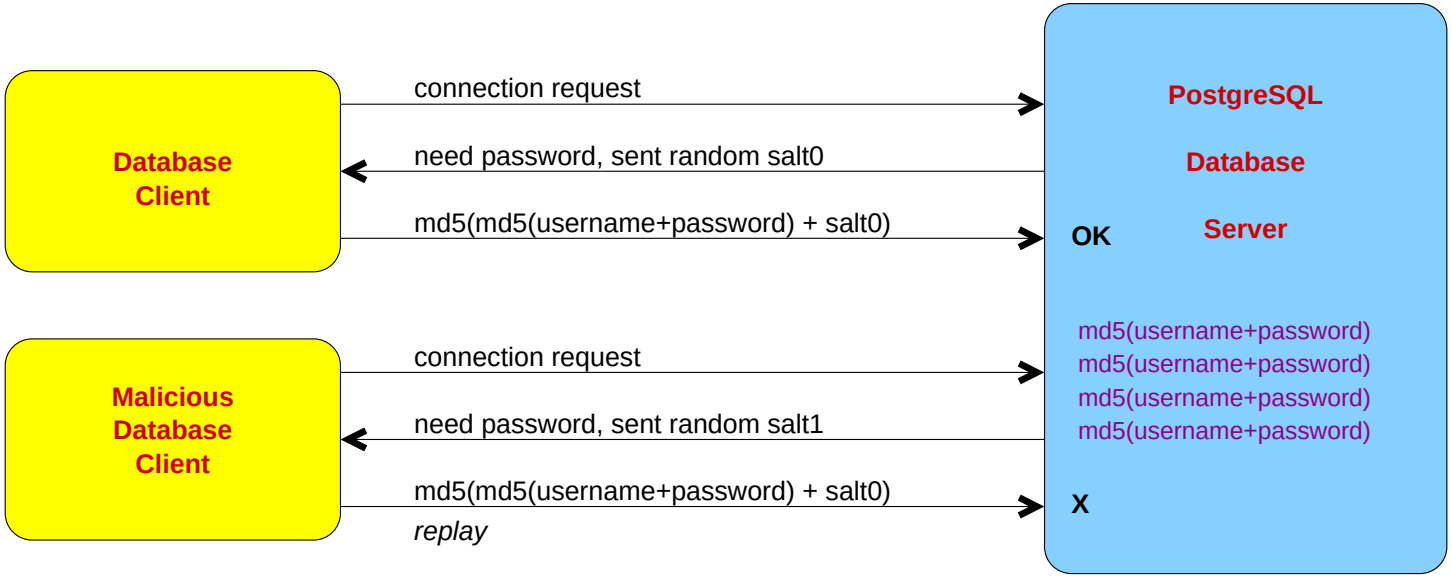


Using 'username' in the MD5 string prevents the same password used by different users from appearing the same. It also adds some randomness to the md5 checksums.

MD5 Authentication Prevents Password Snooping



MD5 Authentication Prevents Password Replay



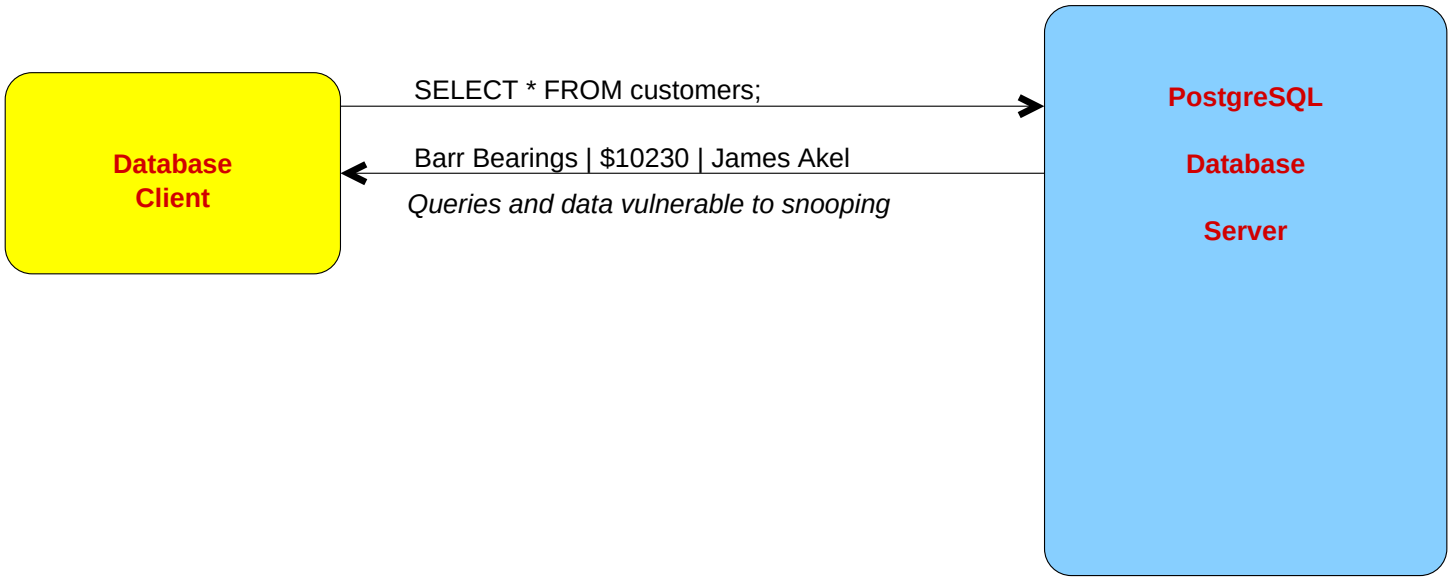
salt is a random four-byte integer so millions of connection attempts might allow the reuse of an old authentication reply.

Password Attacks

- Weak passwords
- Reuse of old passwords
- Brute-Force password attacks

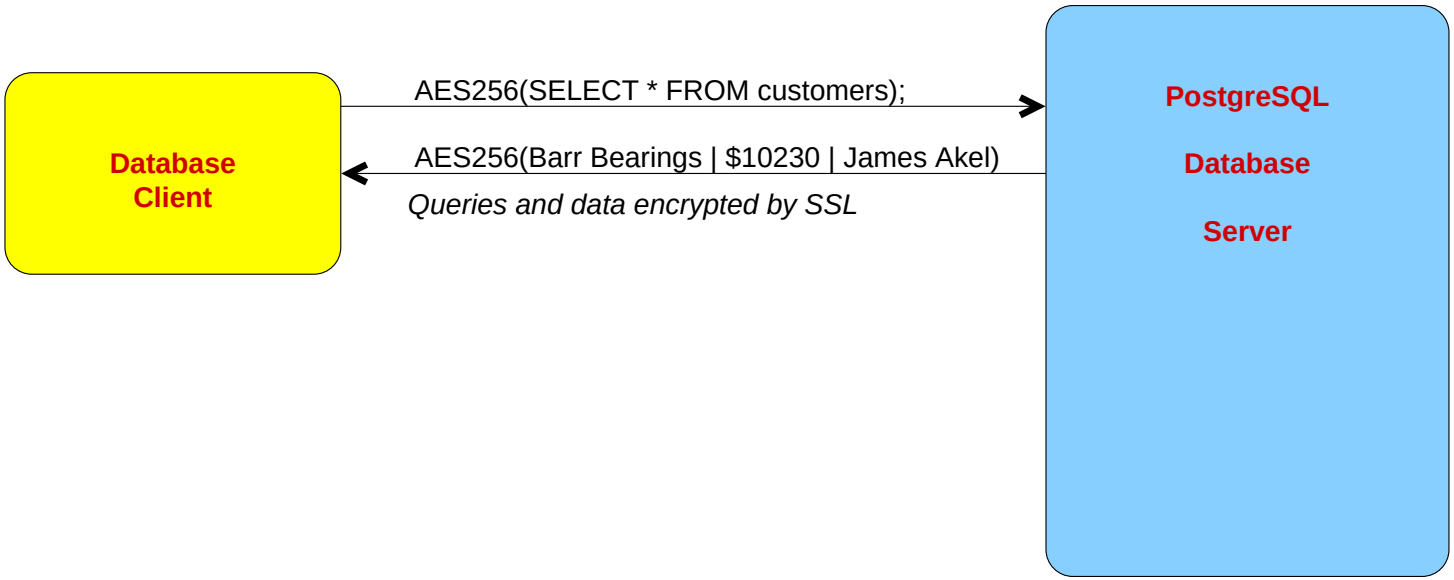
None of these vulnerabilities is prevented by Postgres directly, but external authentication methods, like LDAP, PAM, and SSPI, can prevent them.

Queries and Data Still Vulnerable to Network Snooping



Password changes are also vulnerable to snooping.

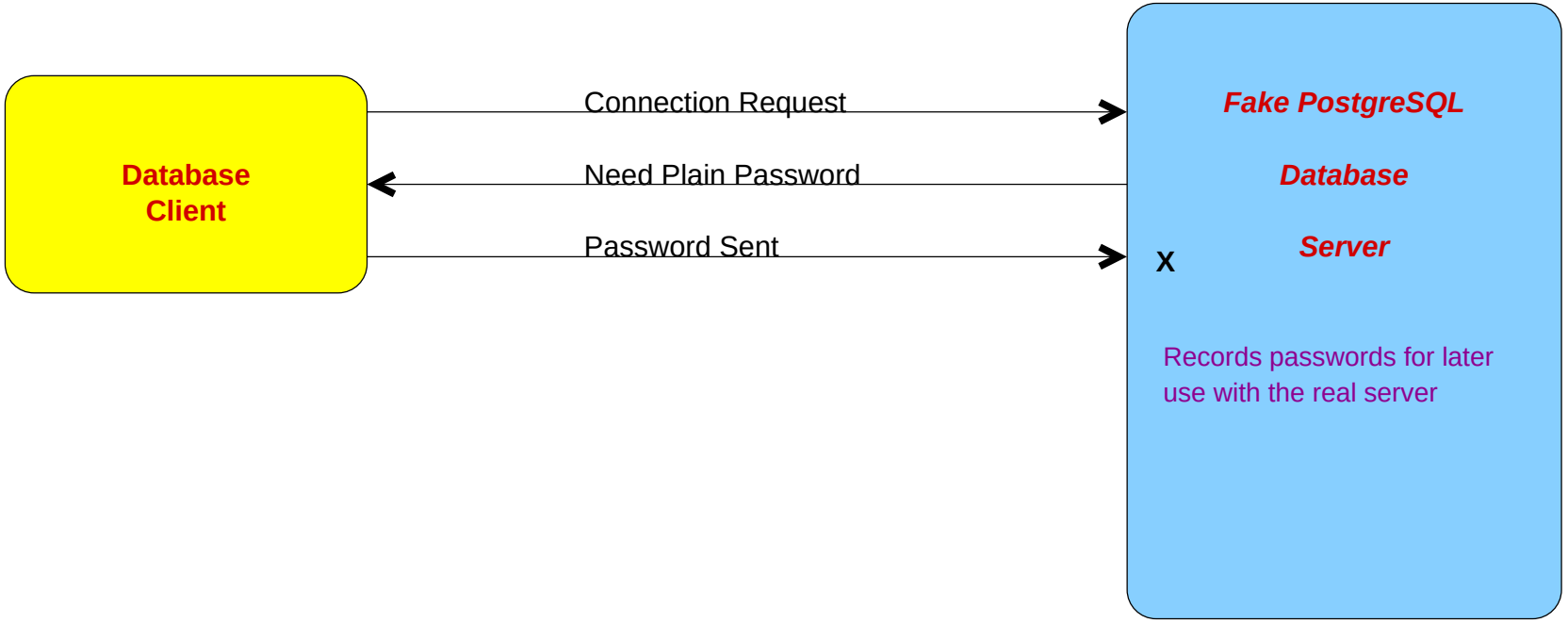
SSL Prevents Snooping By Encrypting Queries and Data



Preventing Spoofing

http://redwing.hutman.net/~mreed/warriorshtm/impostor.htm

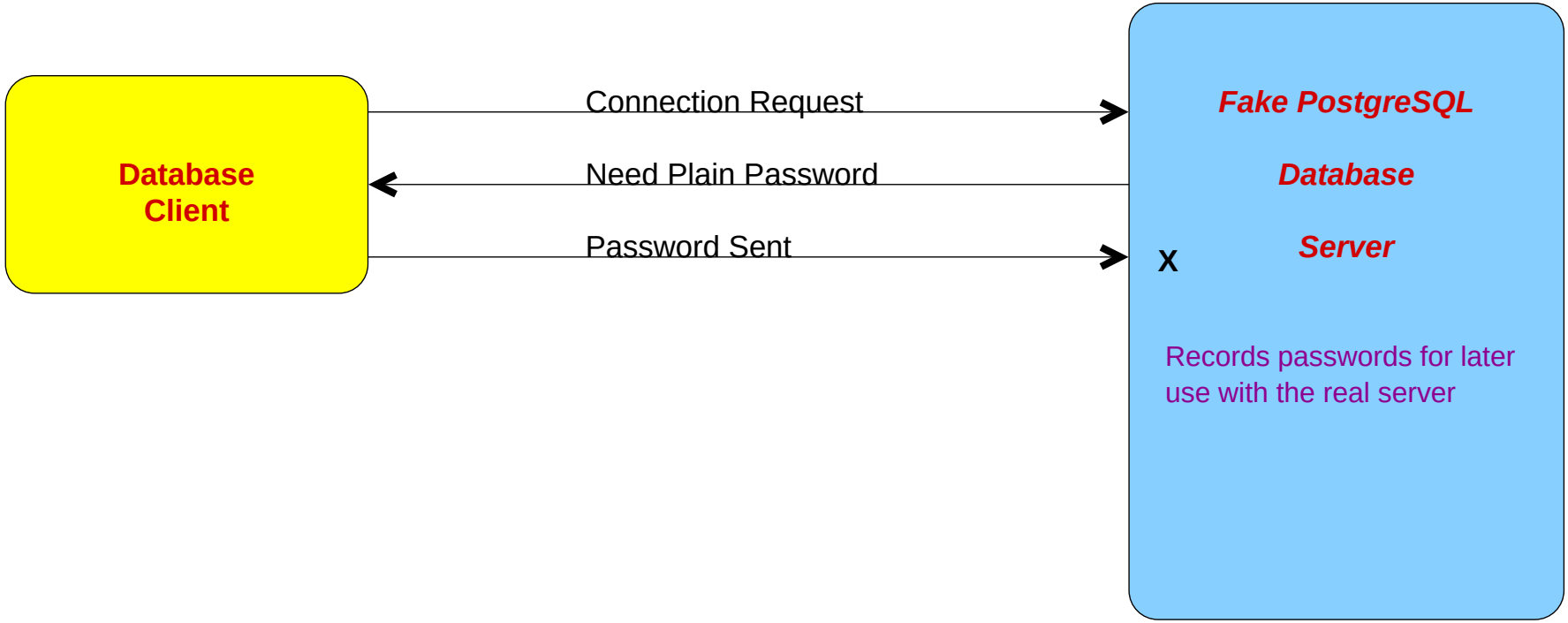
Localhost Spoofing
While the Database Server Is Down



Uses a fake socket or binds to port 5432 while the real server is down. (/tmp is world-writable and 5432 is not a root-only port.)

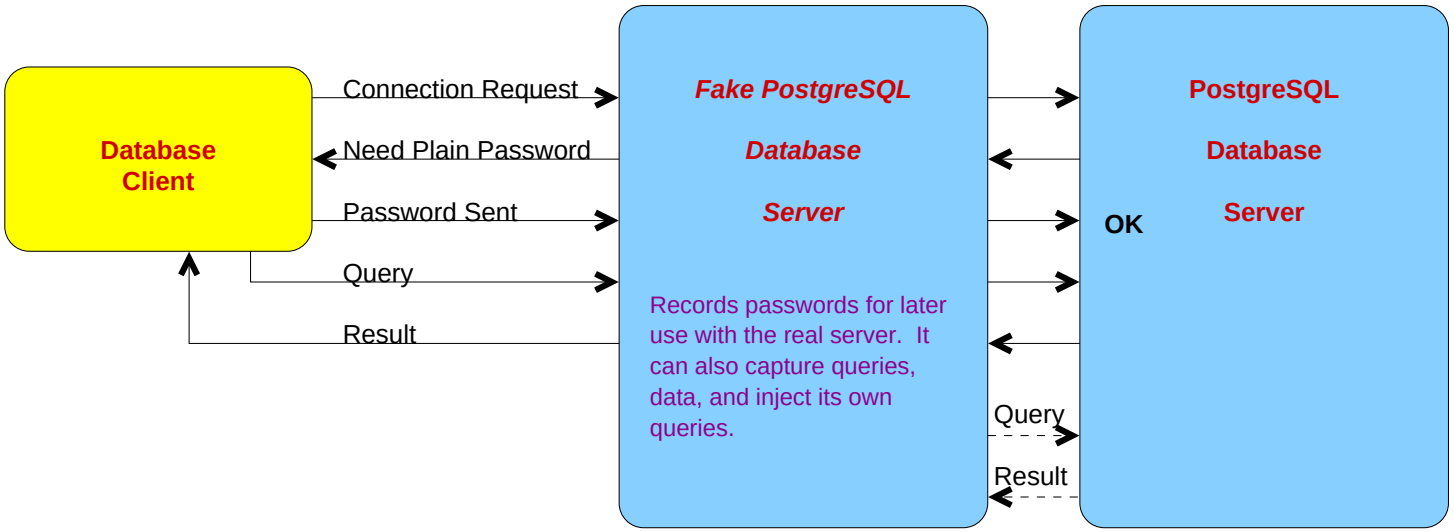
The server controls the choice of 'password' instead of 'md5'.

Network Spoofing



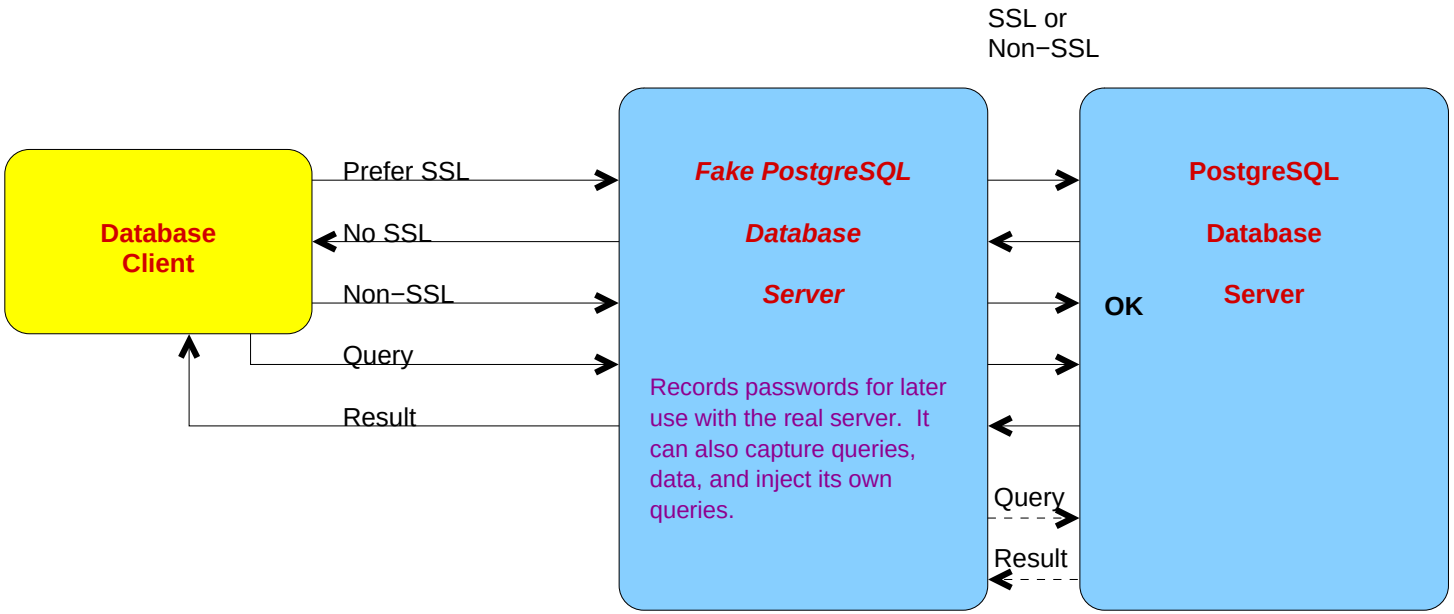
Without SSL 'root' certificates there is no way to know if the server you are connecting to is a legitimate server.

Network Spoofing Pass-Through



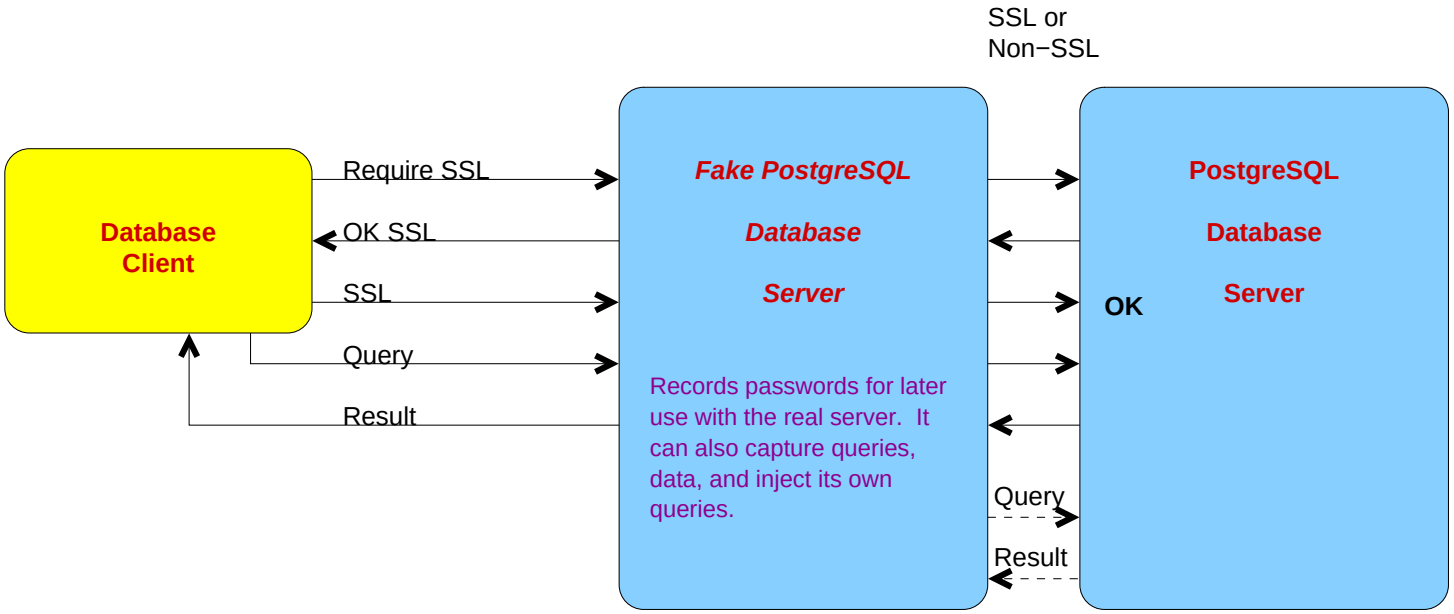
Without SSL 'root' certificates there is no way to know if the server you are connecting to is a legitimate server.

SSL 'Prefer' Is Not Secure



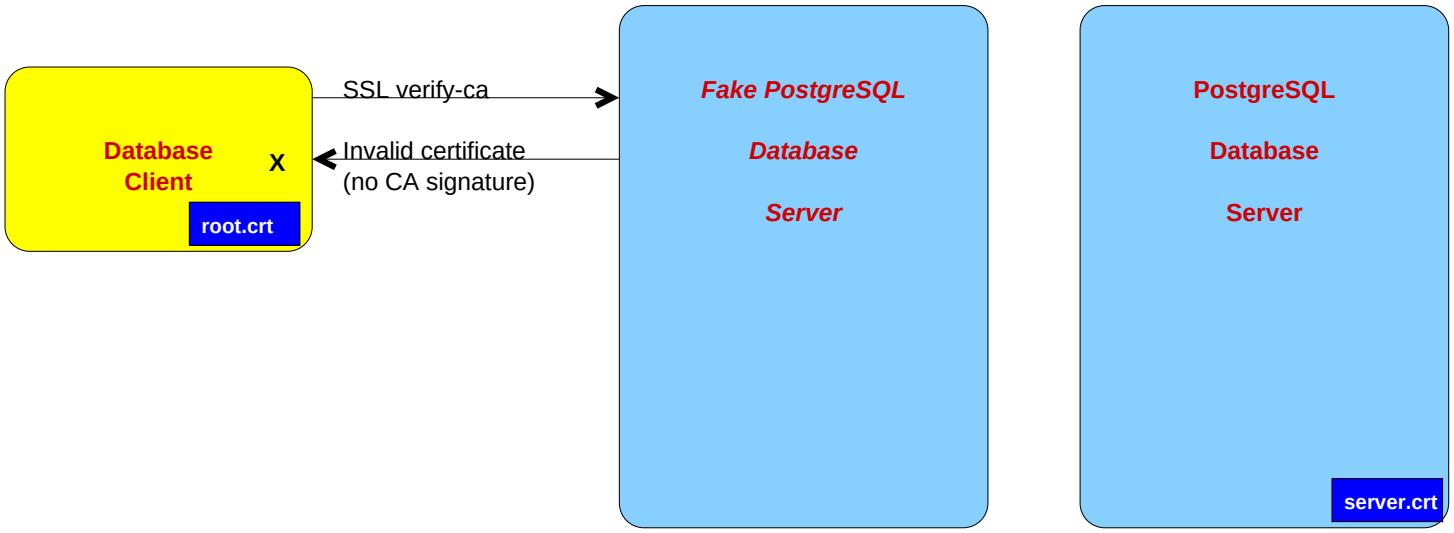
Without SSL 'root' certificates there is no way to know if the server you are connecting to is a legitimate server.

SSL 'Require' Is Not Secure From Spoofing

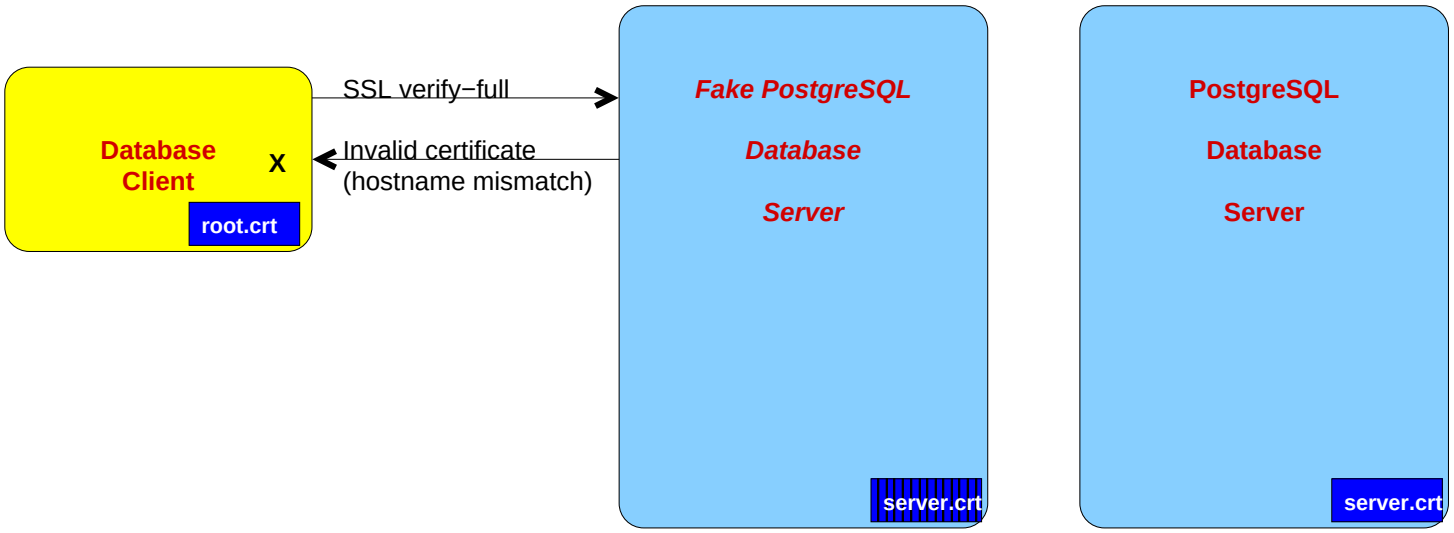


Without SSL 'root' certificates there is no way to know if the server you are connecting to is a legitimate server.

SSL 'Verify-CA' Is Secure From Spoofing



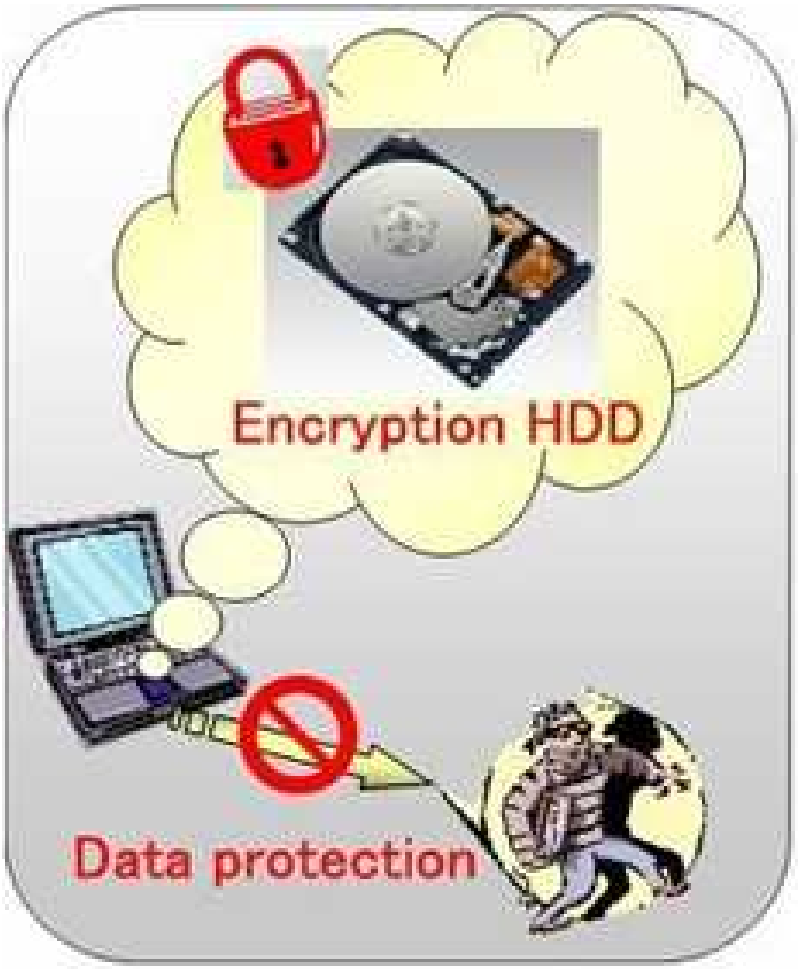
SSL 'Verify-full' Is Secure Even From Some Certificate Thefts



Data Encryption
To Avoid Data Theft

http://jproc.ca/crypto/enigma.html

Disk Volume Encryption



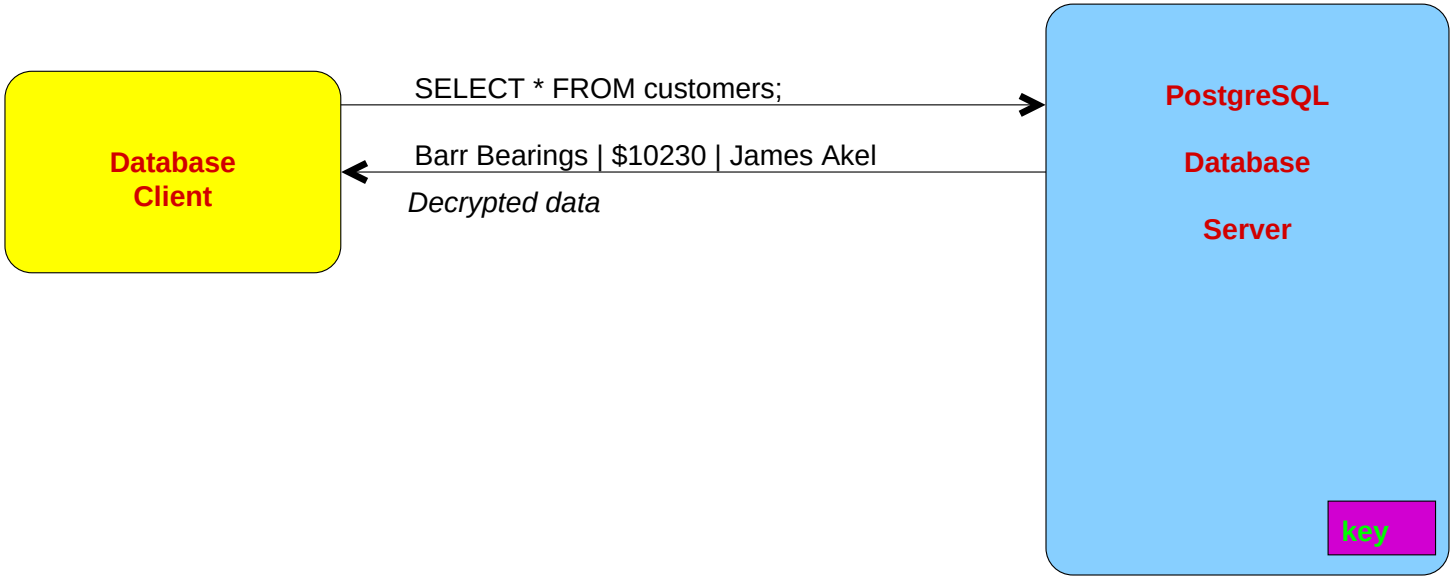
http://www.pclaunches.com/

Column Encryption

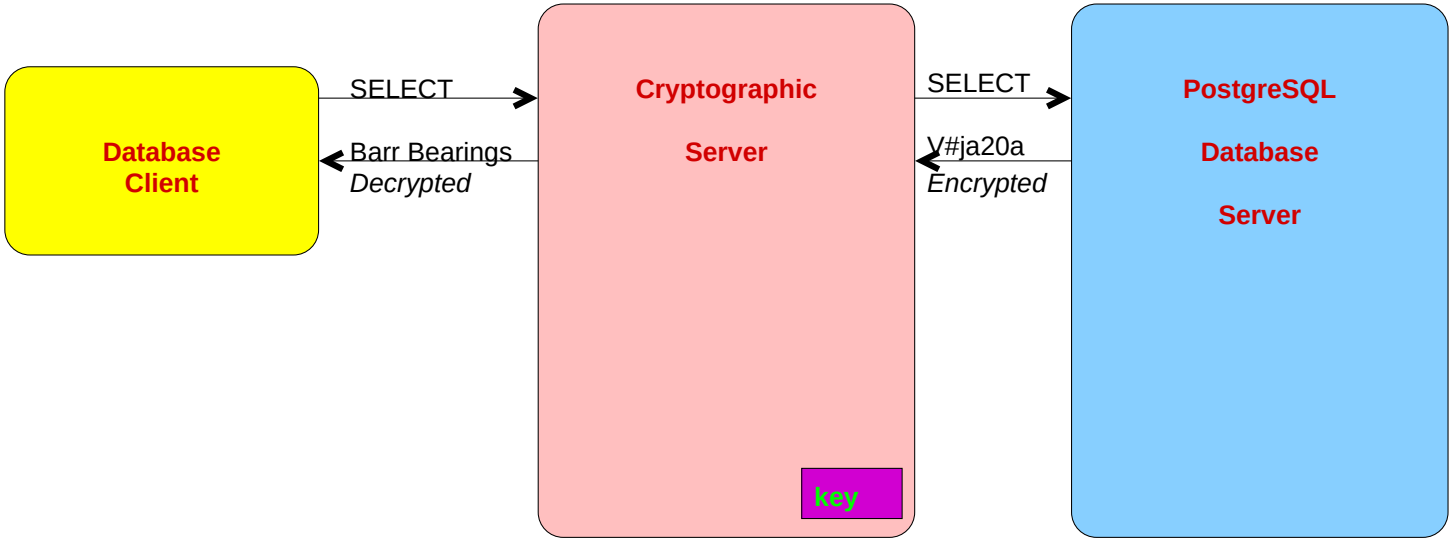
```
   id    |         name         |          credit_card_number
---------+----------------------+------------------------------
 428914 | Piller Plaster Co. | \xc30d04070302254dc045353f28
                               ; 456cd241013e2d421e198f3320e8
                               ; 41a7e4f751ebd9e2938cb6932390
                               ; 5c339c02b5a8580663d6249eb24f
                               ; 192e226c1647dc02536eb6a79a65
                               ; 3f3ed455ffc5726ca2b67430d5
```

Encryption methods are decryptable (e.g. AES), while hashes are one-way (e.g. MD5). A one-way hash is best for data like passwords that only need to be checked for a match, rather than decrypted.

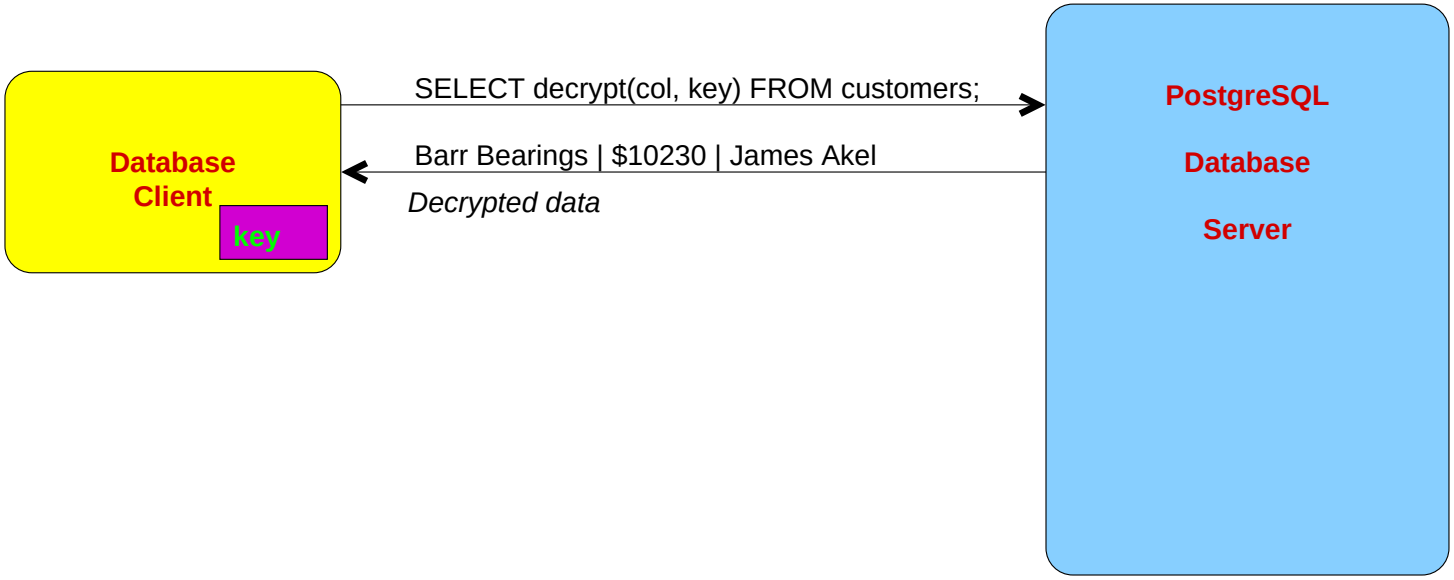
Where to Store the Key?
On the Server



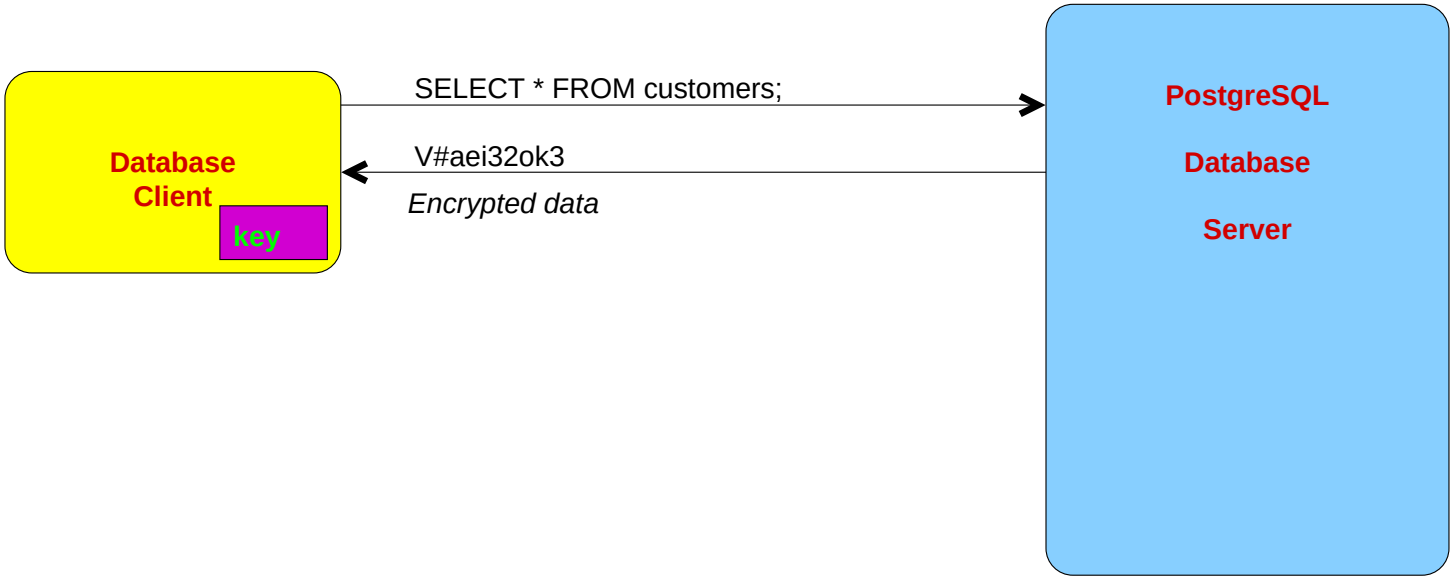
Store the Decryption Key On an Intermediate Server



Pass the Decryption Key Via SQL From the Client

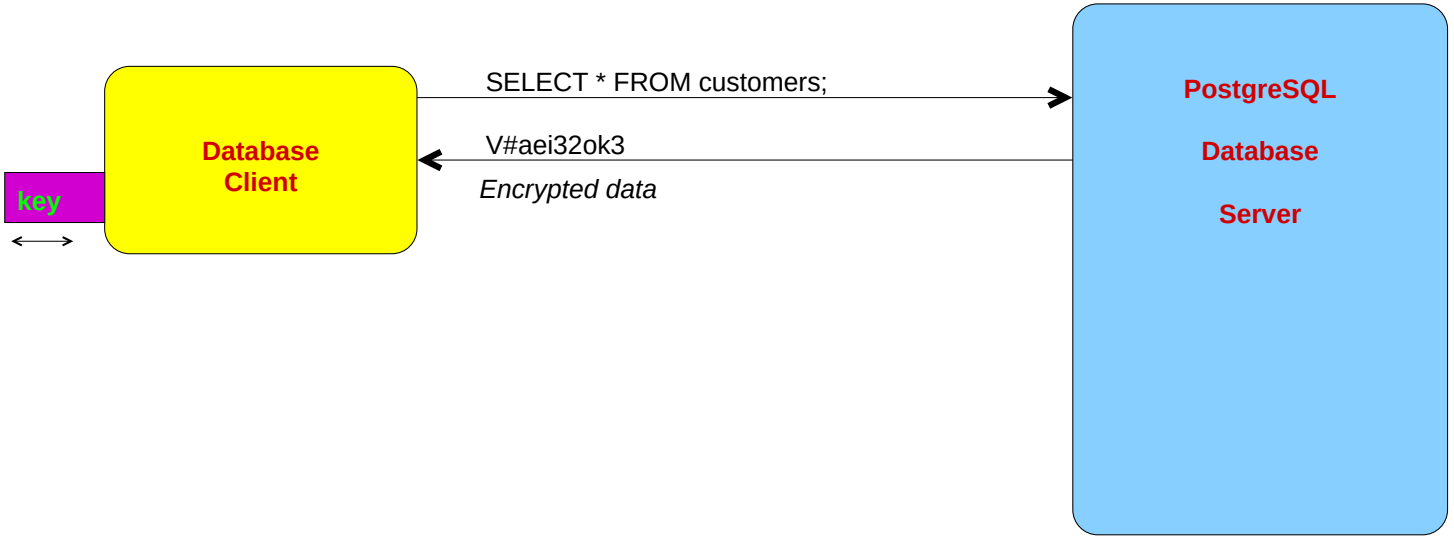


Decrypt On the Client



This prevents server administrators from viewing sensitive data.

Store the Decryption Key On a Client Hardware Token



This prevents problems caused by client hardware theft.

Conclusion

Todd Ehlers, Flickr