

iOS Vulnerabilities and Fixes

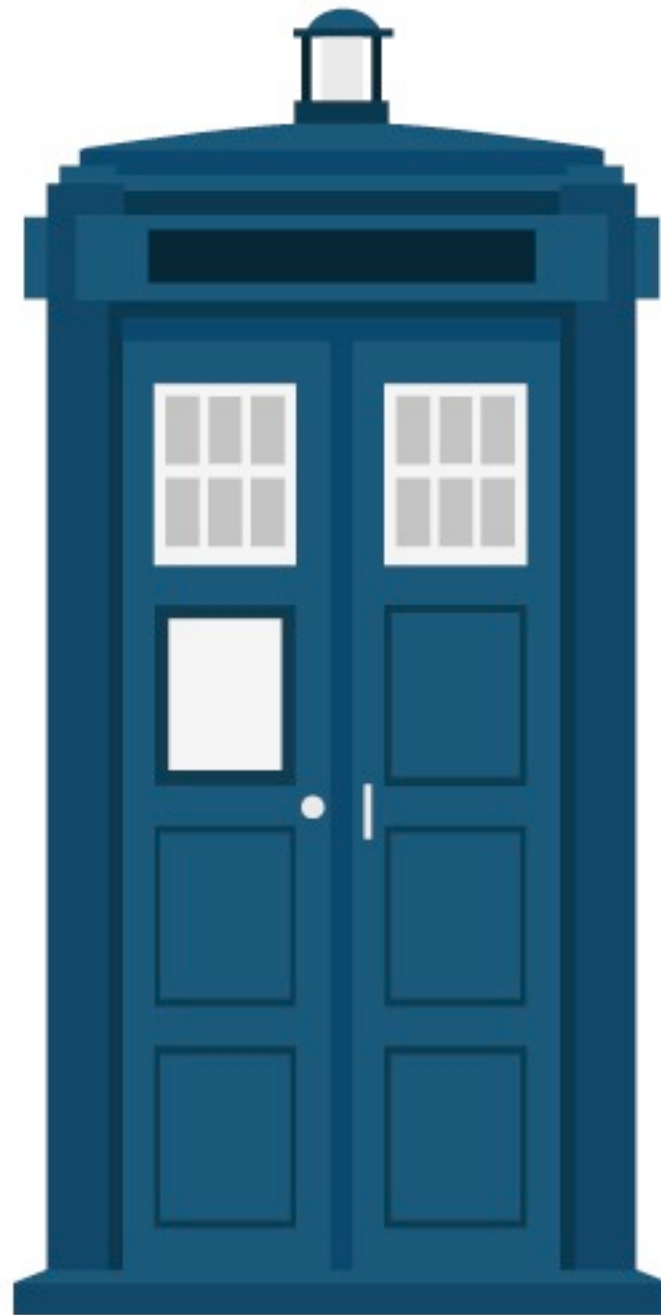
Graham Lee / @secboffin
Smartphone Security Boffin, The Lab @O2

INTERNATIONAL
SOFTWARE DEVELOPMENT
CONFERENCE

gotocon.com

iPhone Code Session

iPhone Code Session



State of the Union



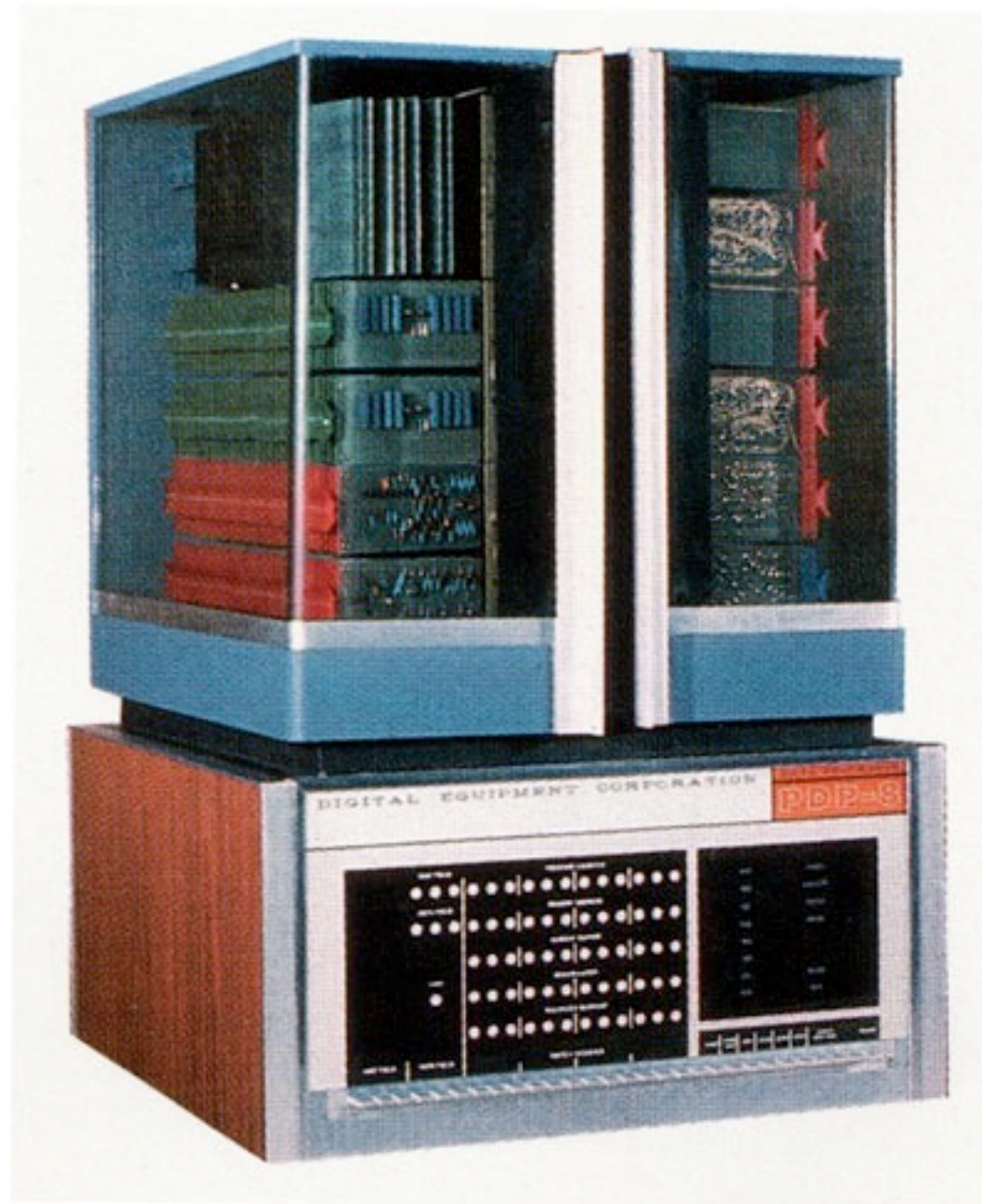
State of the Union

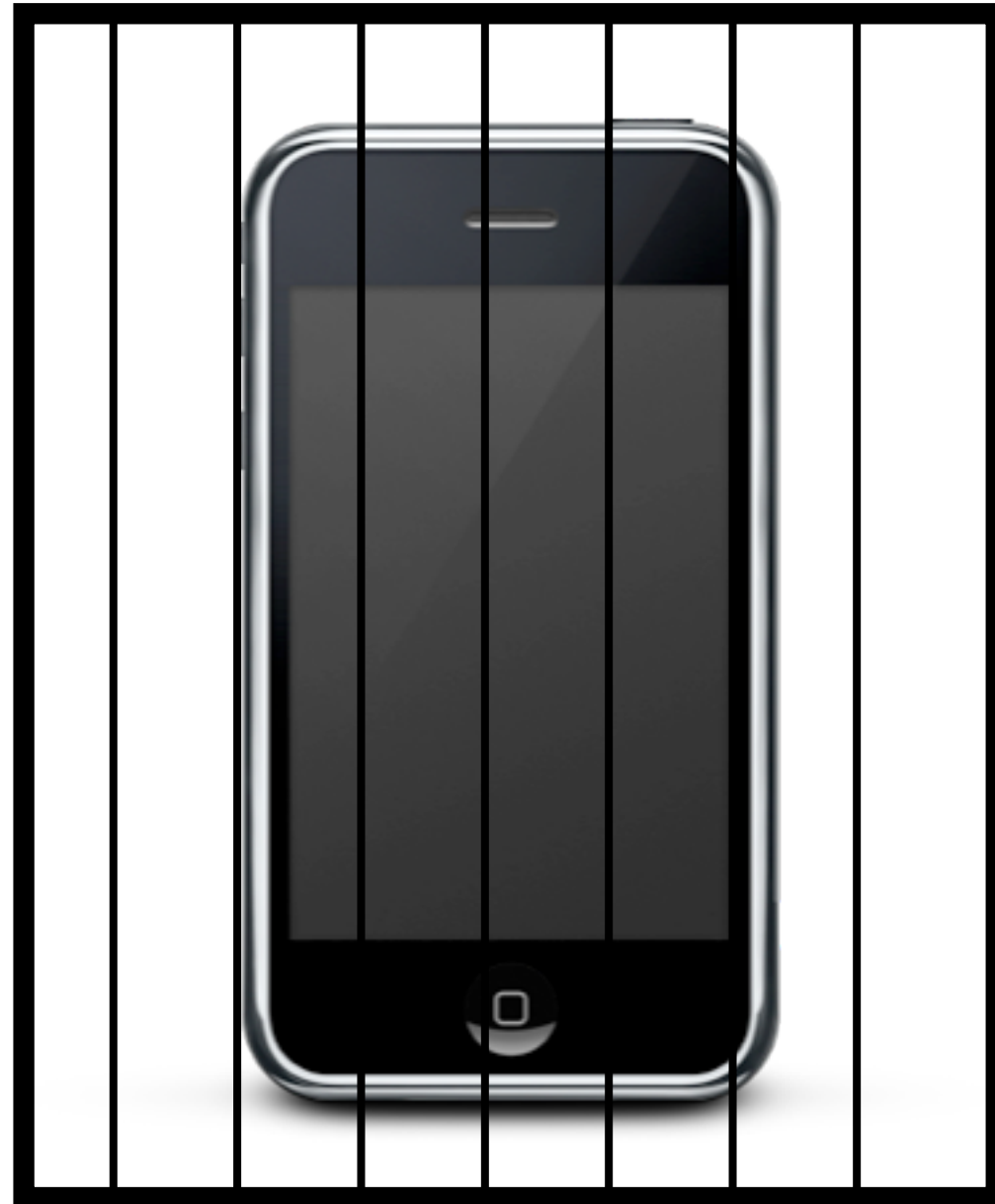


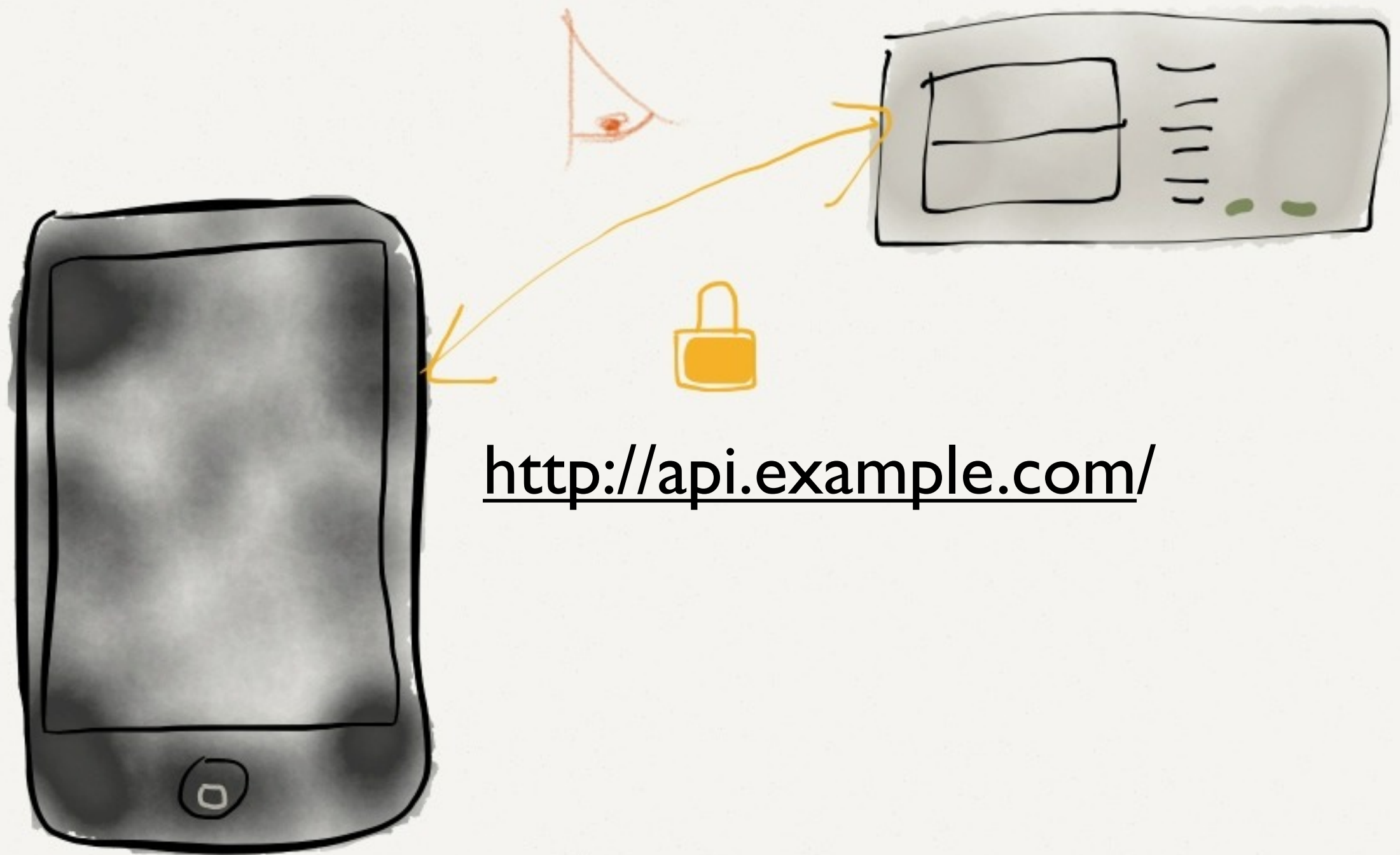
State of the Union

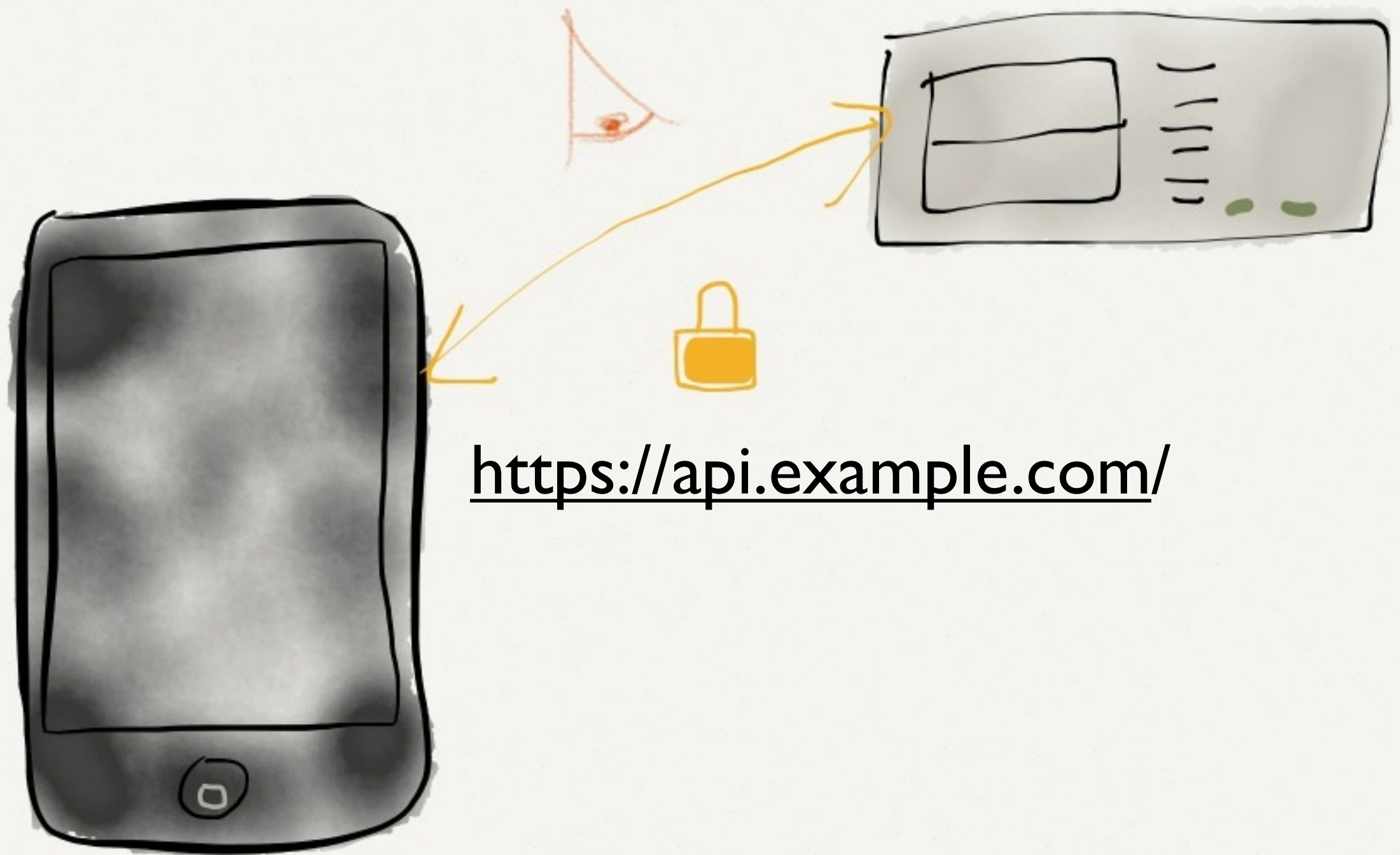


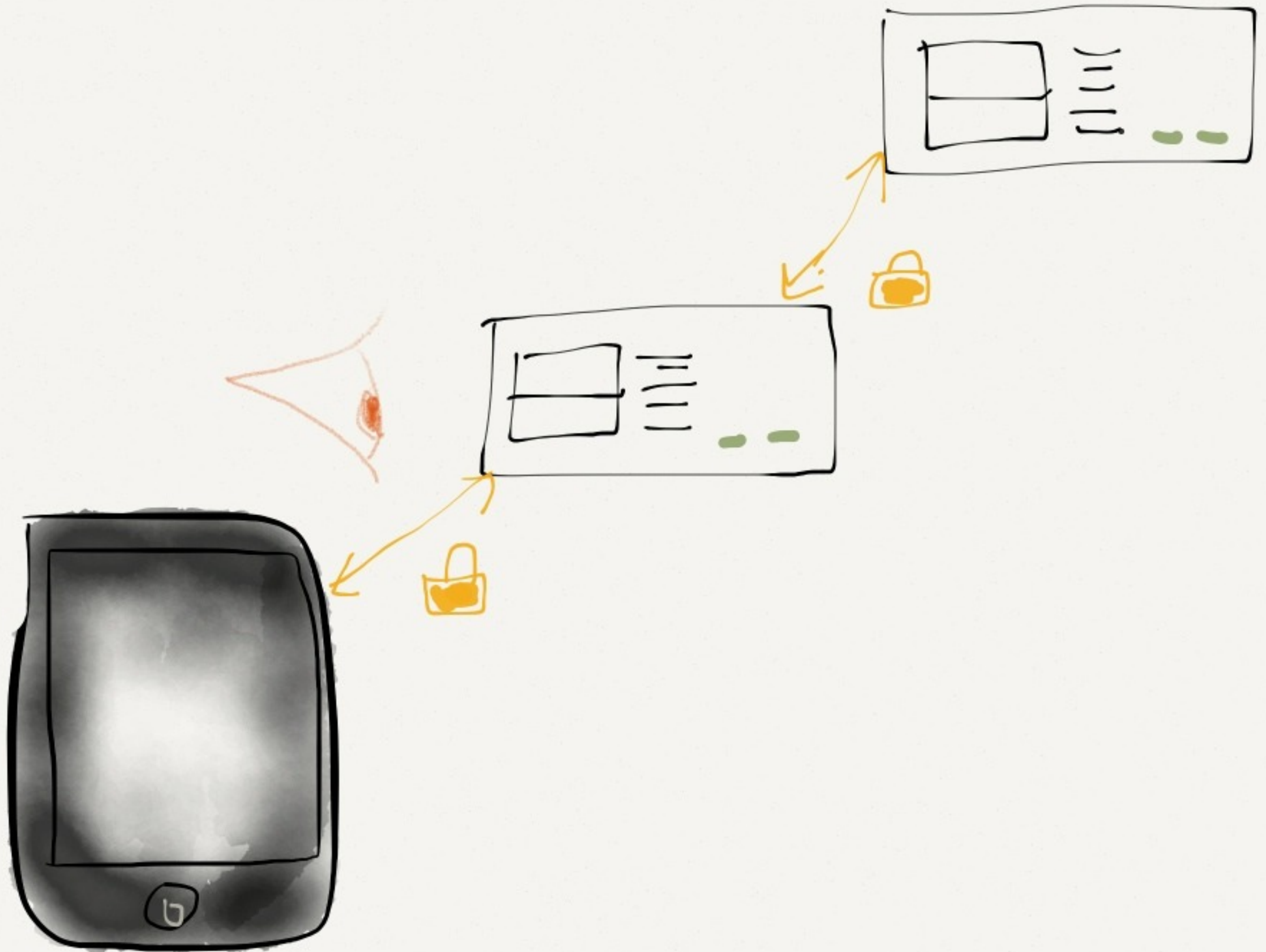
State of the Union



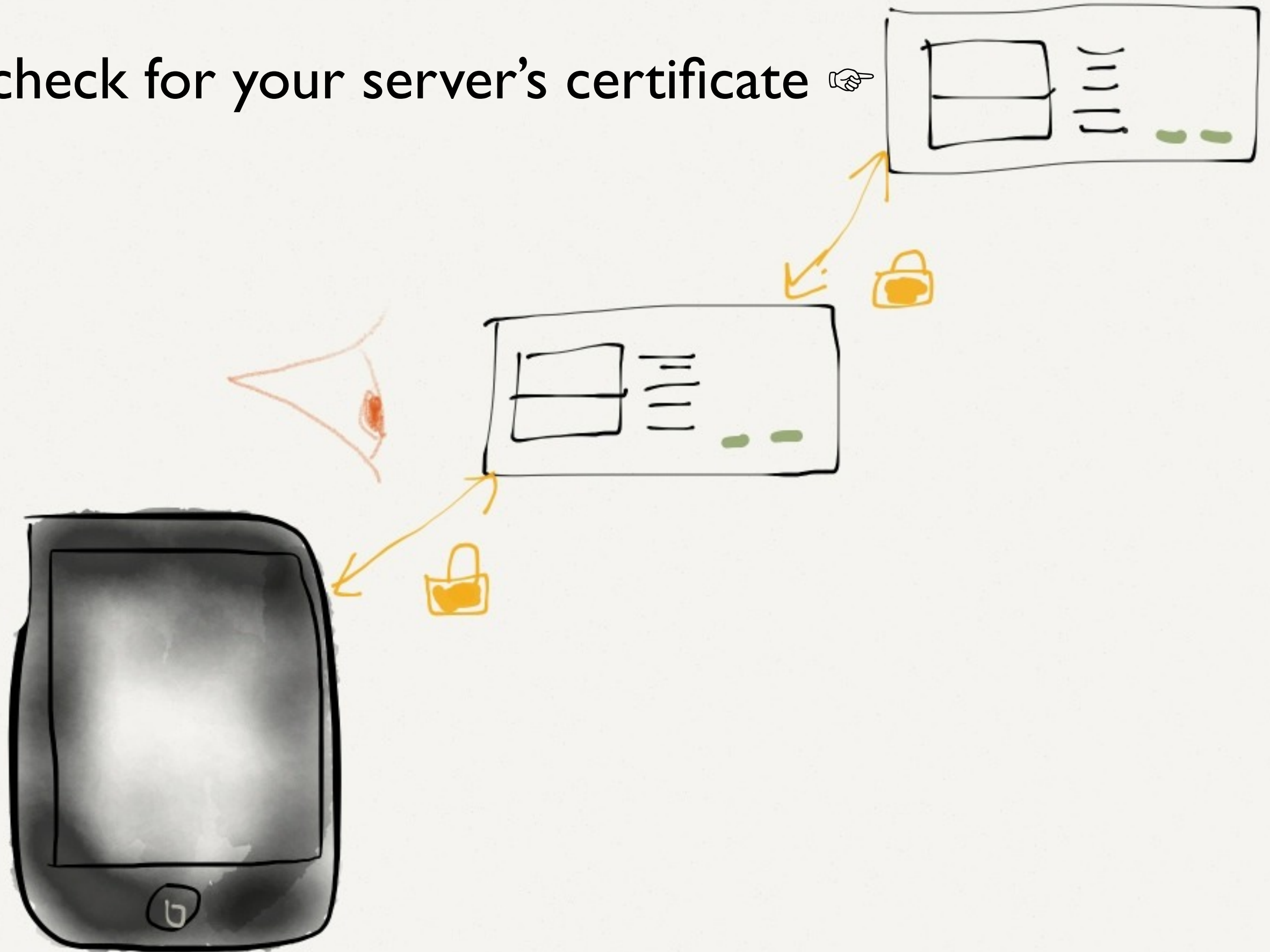




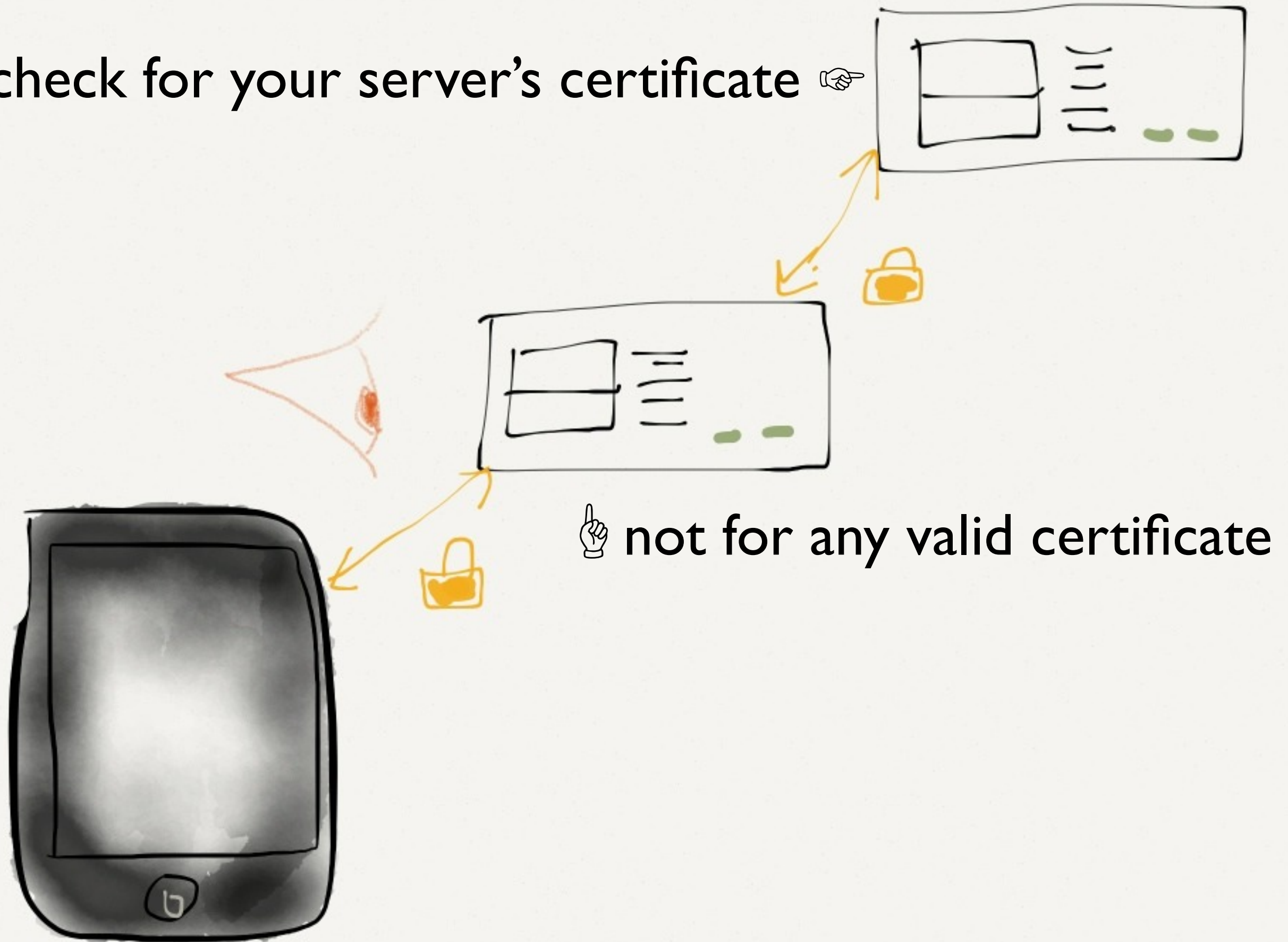




check for your server's certificate 



check for your server's certificate 📖



📖 not for any valid certificate


```
– (BOOL)connection:(NSURLConnection *)connection  
canAuthenticateAgainstProtectionSpace:  
(NSURLProtectionSpace *)protectionSpace {  
    return ([protectionSpace.authenticationMethod  
isEqualToString:  
NSURLAuthenticationMethodServerTrust]);  
}
```



```
- (void)connection:(NSURLConnection *)connection
didReceiveAuthenticationChallenge:
(NSURLAuthenticationChallenge *)challenge {
    if ([[challenge protectionSpace]
authenticationMethod] isEqualToString:
NSURLAuthenticationMethodServerTrust) {
        SecTrustRef serverTrust = [[challenge
protectionSpace] serverTrust];
        (void) SecTrustEvaluate(serverTrust, NULL);
        NSData *localCertificateData = [NSData
dataWithContentsOfFile: [[NSBundle mainBundle]
pathForResource: serverName
 ofType: @"cer"]];
```

```

    SecCertificateRef
remoteVersionOfServerCertificate =
SecTrustGetCertificateAtIndex(serverTrust, 0);
    CFDataRef remoteCertificateData =
SecCertificateCopyData(remoteVersionOfServerCertif
icate);
    BOOL certificatesAreTheSame =
[localCertificateData isEqualToData: (__bridge
NSData *)remoteCertificateData];
    CFRelease(remoteCertificateData);
    if (certificatesAreTheSame) {
        [[challenge sender] useCredential:
[NSURLCredential credentialForTrust: serverTrust]
forAuthenticationChallenge: challenge];
    }
    else {
        [[challenge sender]
cancelAuthenticationChallenge: challenge];
    }
}

```

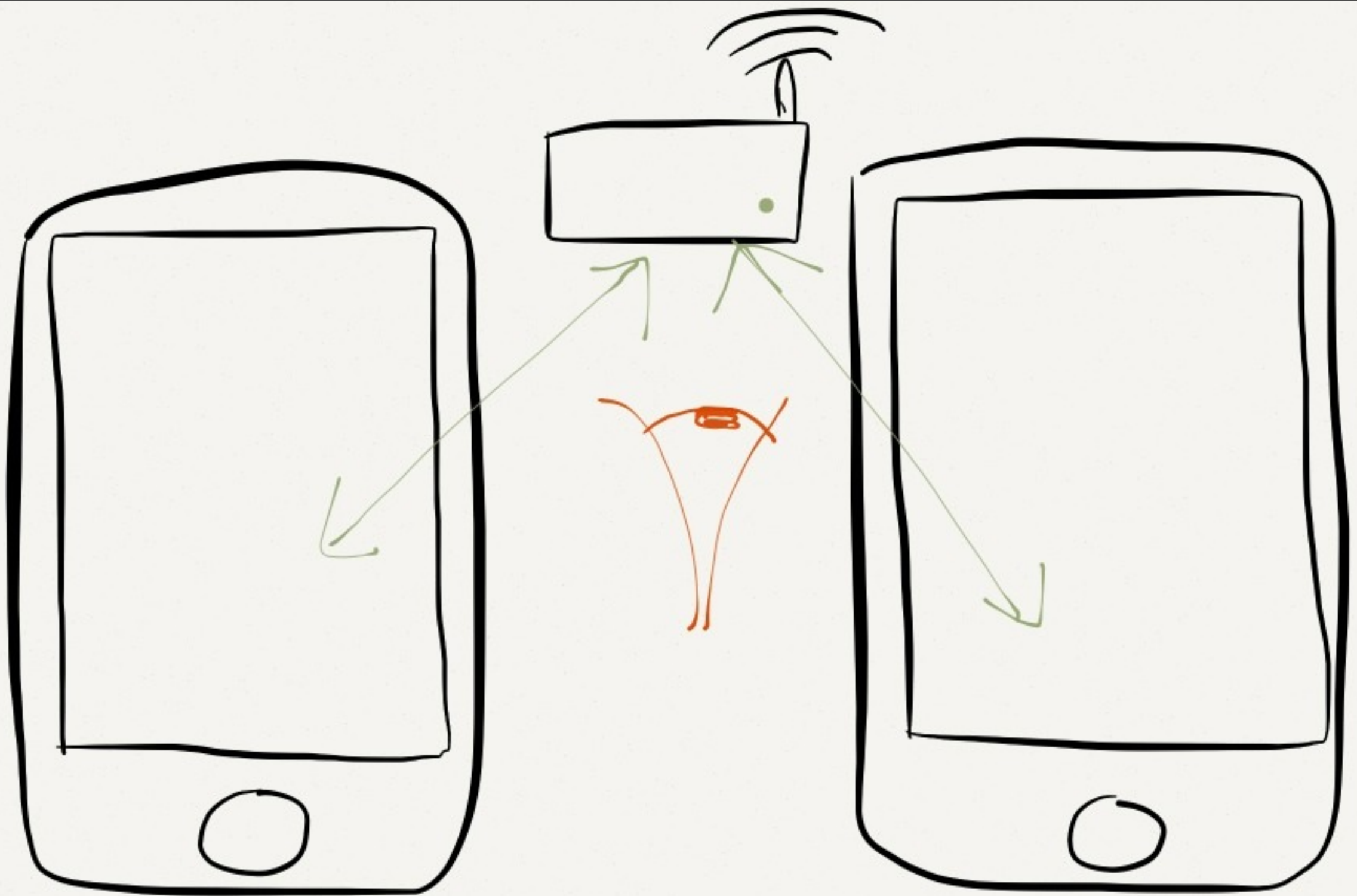
```
#import <Security/SecureTransport.h>

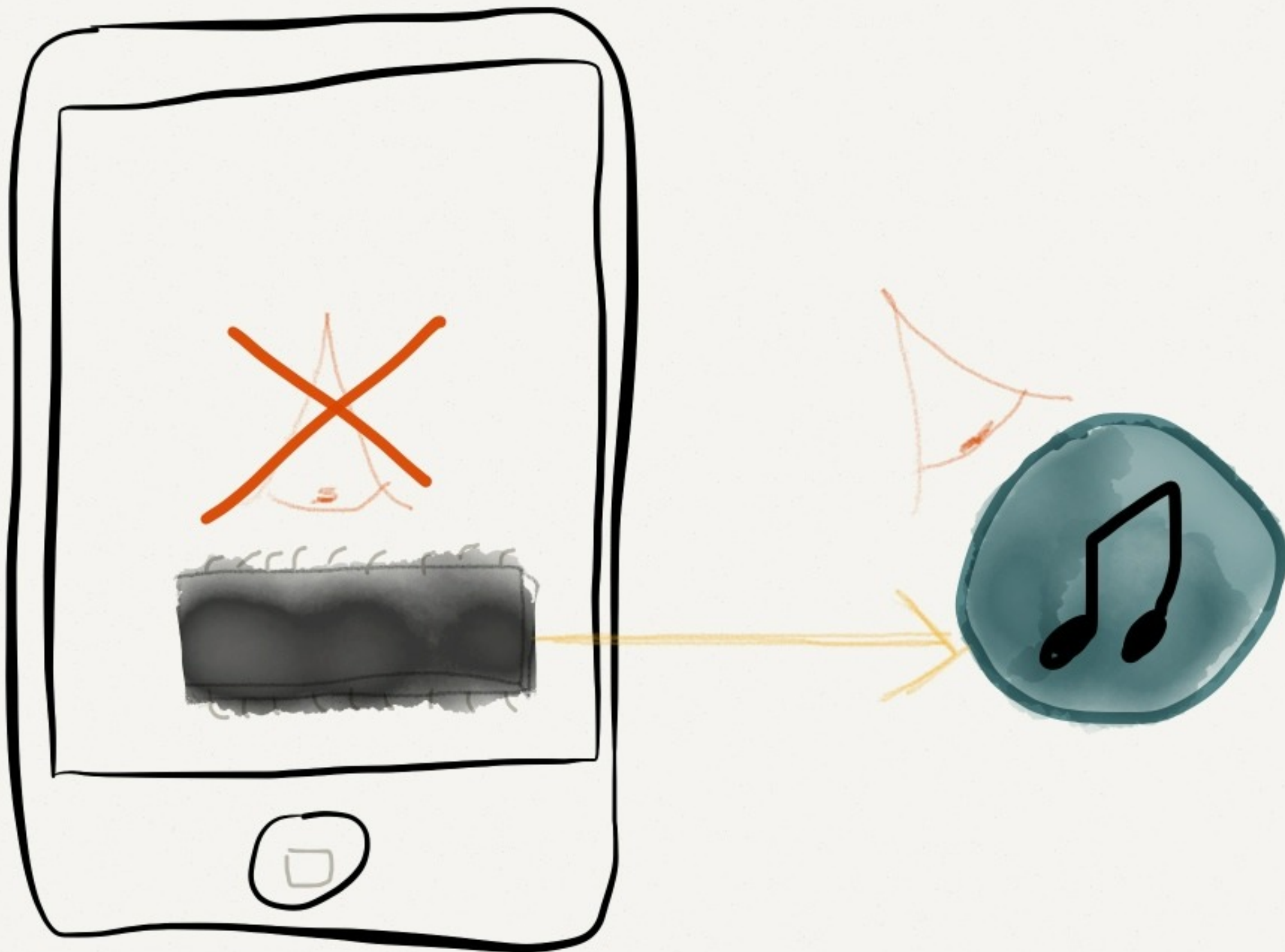
SSLNewContext(isServer, &context);

SSLSetSessionOption(context, option, value);
...
SSLSetIOFuncs(/*callbacks*/);

SSLSetCertificate(context, cert);

SSLHandshake(context);
```





NSFileProtection...
NSDataWritingFileProtection...
kSecAttrAccessible...

NSFileProtection...
NSDataWritingFileProtection...
kSecAttrAccessible...



NSFileProtection...
NSDataWritingFileProtection...
kSecAttrAccessible...

- ☒ Easy
- ☒ Reliable

NSFileProtection...
NSDataWritingFileProtection...
kSecAttrAccessible...

- ☒ Easy
- ☒ Reliable
- ☒ Auto-migrate

NSFileProtection...
NSDataWritingFileProtection...
kSecAttrAccessible...

- ☒ Easy
- ☒ Reliable
- ☒ Auto-migrate
- ☒ Burden-free

NSFileProtection...

NSDataWritingFileProtection...

kSecAttrAccessible...

- ☒ Easy
- ☒ Reliable
- ☒ Auto-migrate
- ☒ Burden-free
- ☐ Always on

NSFileProtection...

NSDataWritingFileProtection...

kSecAttrAccessible...

- ☒ Easy
- ☒ Reliable
- ☒ Auto-migrate
- ☒ Burden-free
- ☐ Always on
- ☐ Can see if used

NSFileProtection...

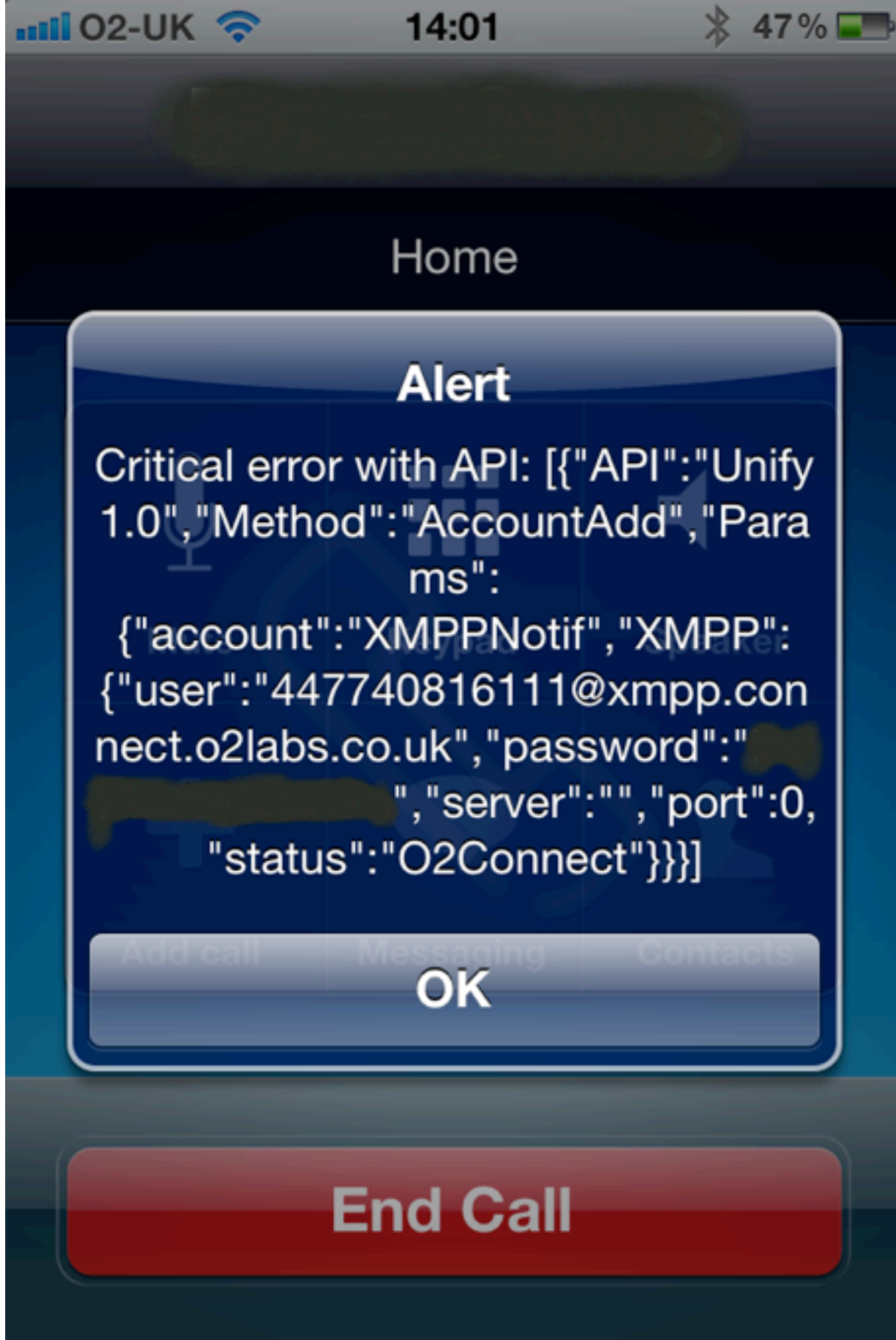
NSDataWritingFileProtection...

kSecAttrAccessible...

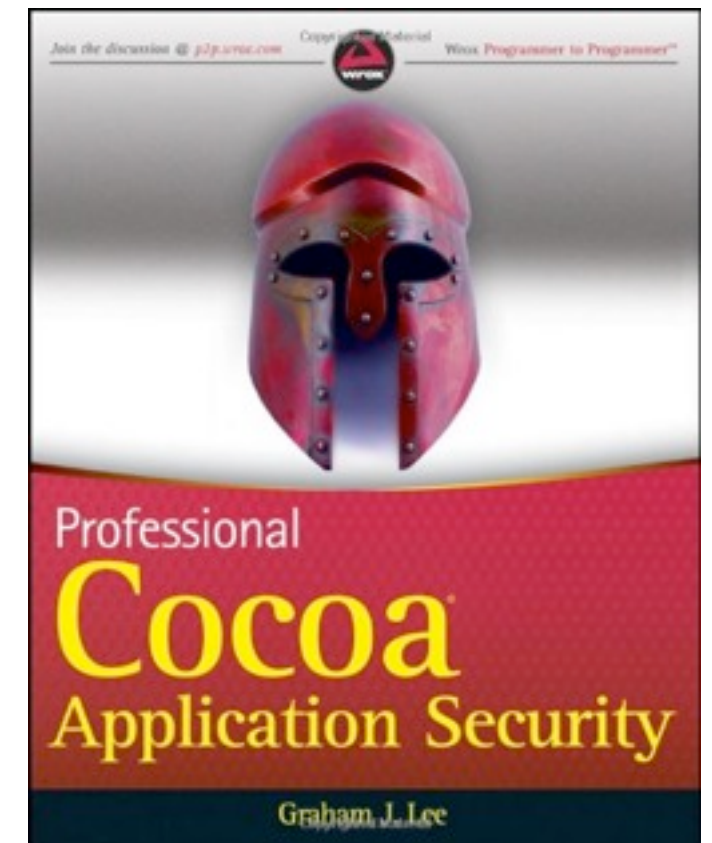
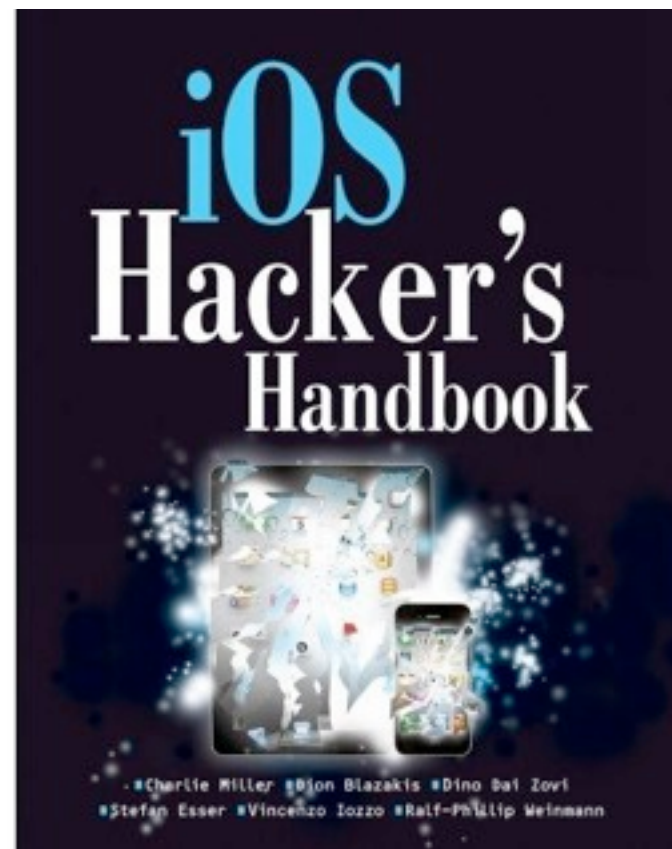
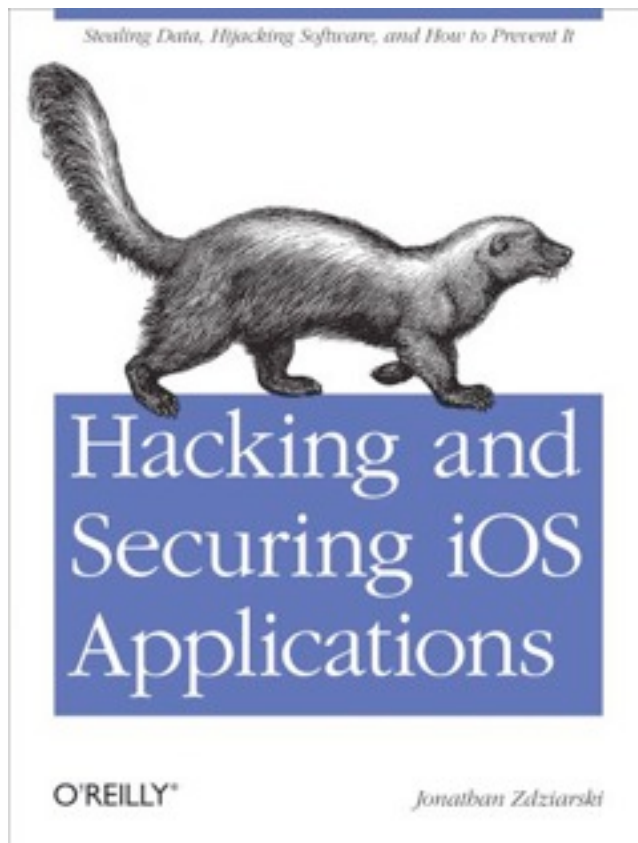
- ☒ Easy
- ☒ Reliable
- ☒ Auto-migrate
- ☒ Burden-free
- ☐ Always on
- ☐ Can see if used
- ☐ Can control when used

NSFileProtection...
NSDataWritingFileProtection...
kSecAttrAccessible...

- ☒ Easy
- ☒ Reliable
- ☒ Auto-migrate
- ☒ Burden-free
- ☐ Always on
- ☐ Can see if used
- ☐ Can control when used
- ☐ Uses your boss's favourite algorithm



Further Reading



Graham Lee / @secboffin

Smartphone Security Boffin, The Lab @O2