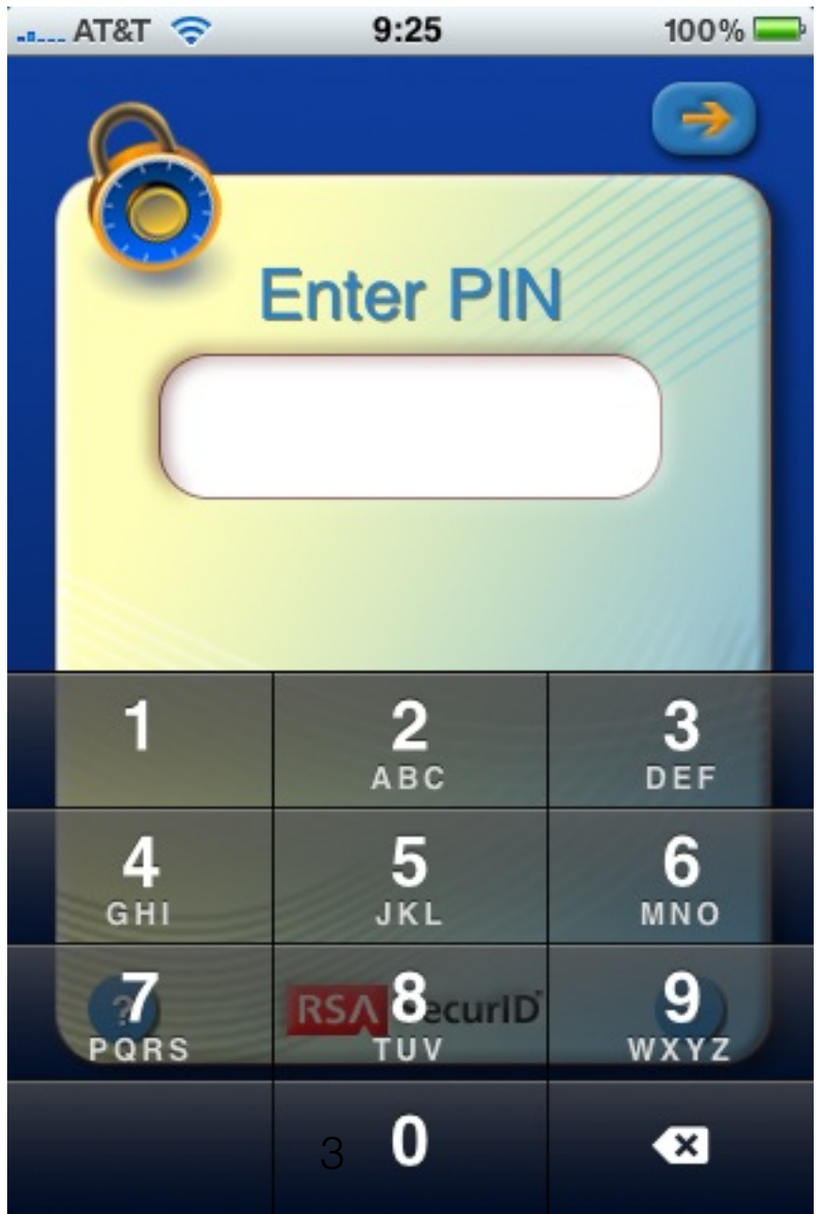
Smartphone security: a study

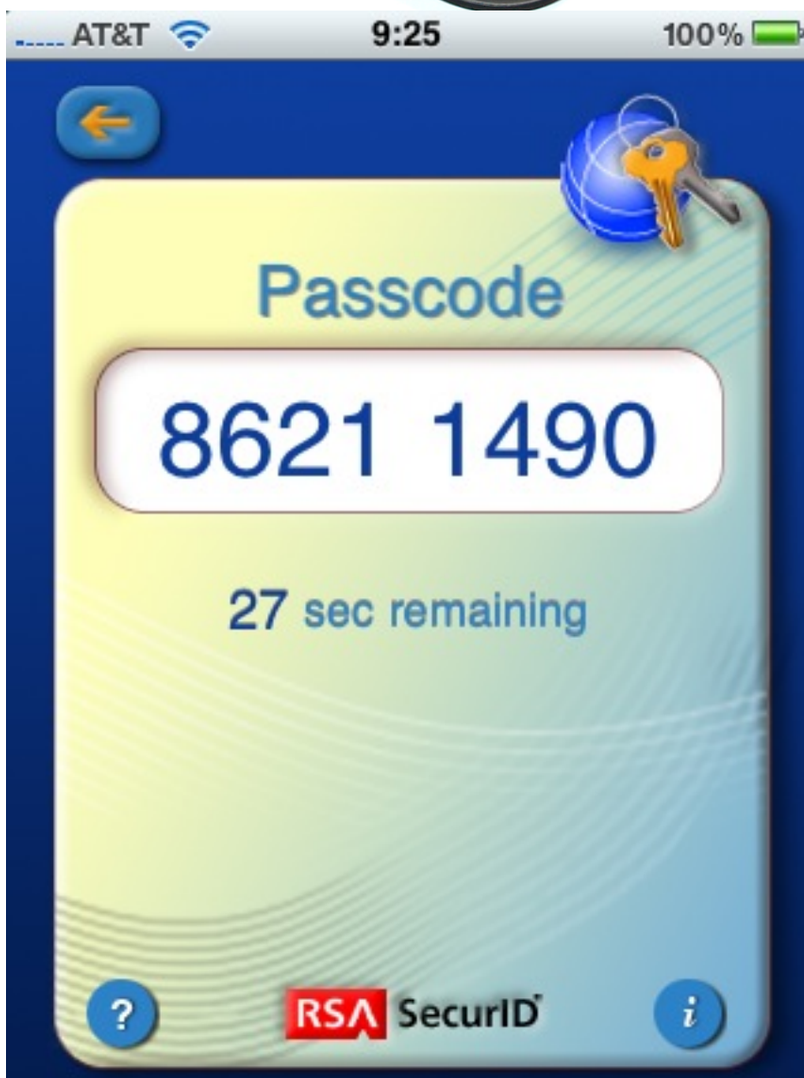
Bill Cheswick
ches@cheswick.com
Visiting Scholar, U Penn.


SecureNet Key
DIGITAL PATHWAYS
7
8
9
4
5
6
1
2
3
0
ON
ENT


832849
RSA SecurID®


982334
RSA SecurID®


AT&T
9:25
100%
Enter PIN
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
RSA SecurID

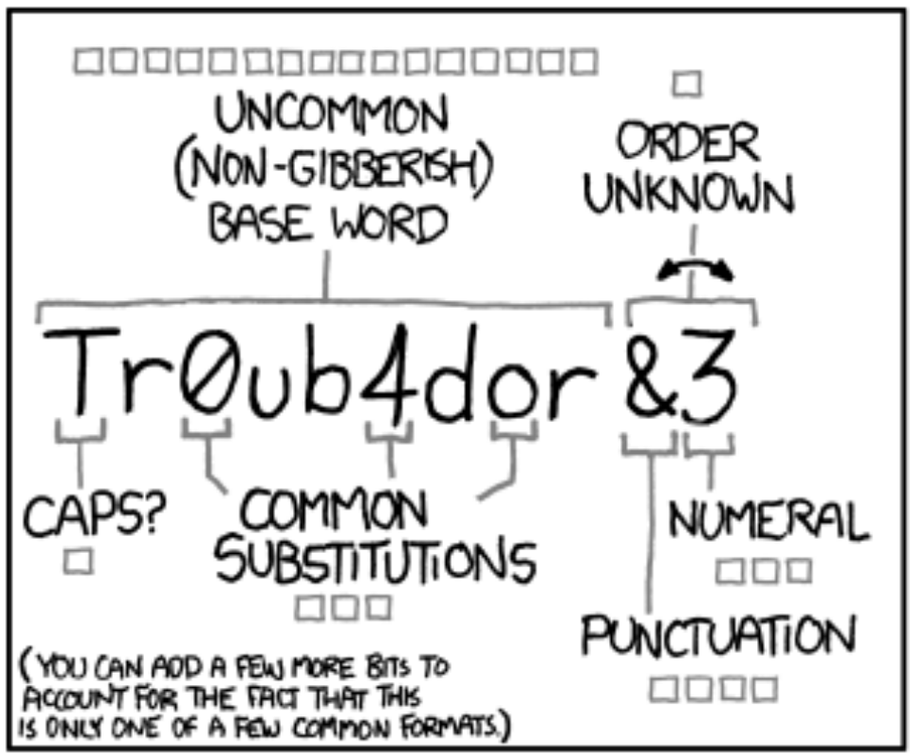

AT&T
9:25
100%
Passcode
8621 1490
27 sec remaining
RSA SecurID

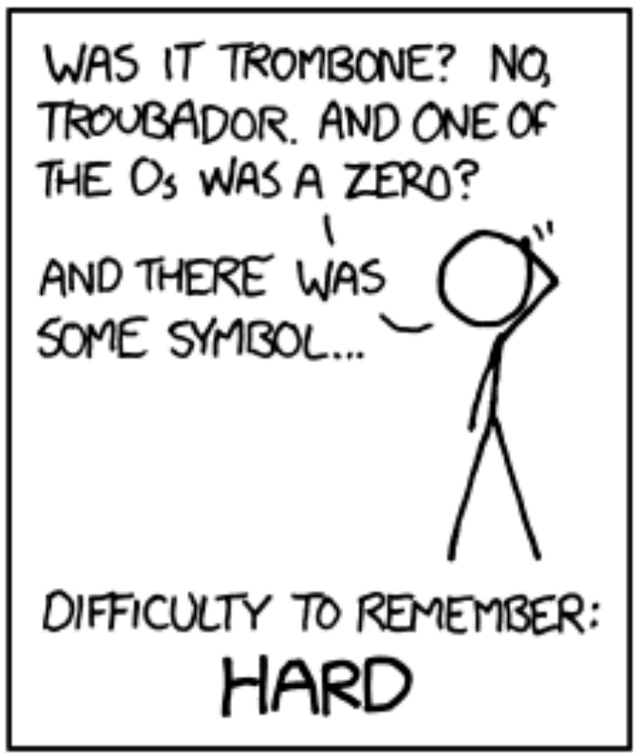
Amlogic S905 SoC: bypassing the (not so) Secure Boot to dump the BootROM

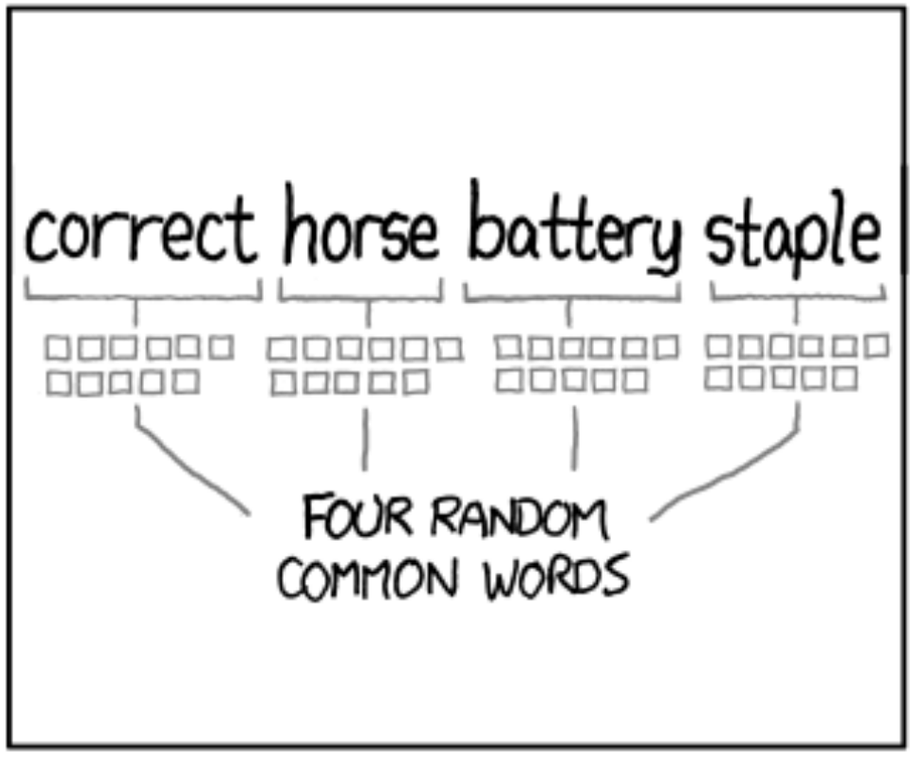
- http://www.fredericb.info/2016/10/amlogic-s905-soc-bypassing-not-so.html

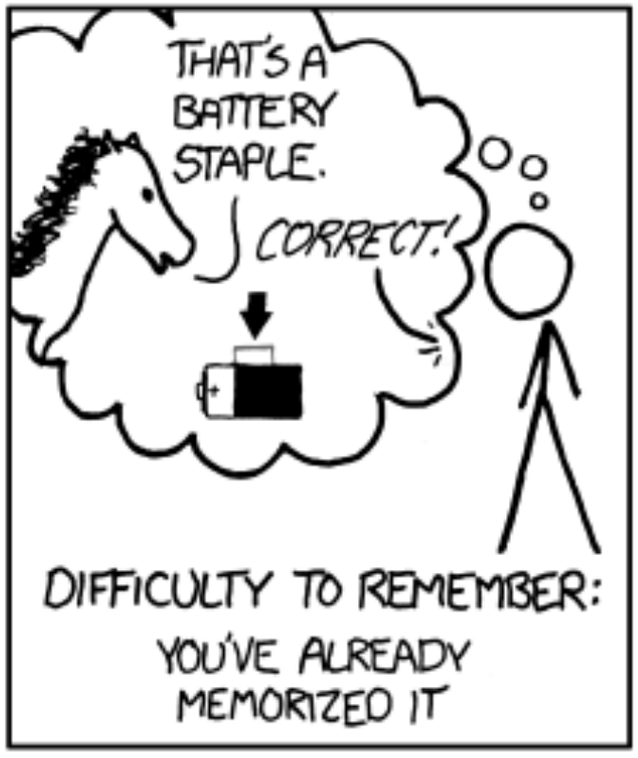
```
// zero and free those key bytes

-(void) dealloc {
    uint8_t *keyBytes = (void *)[keyData bytes];
//    NSLog(@"zeroing key");
    memset(keyBytes, 0, KEY_BYTES);
    [keyData release];
    [super dealloc];
}
```

Password Strength









THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

```
105   0
keylength   15
KeyStretchLoops   347514
KeyStretchTime    1.000
salt   911CE960669405E661FEA450563C310835BD031E1179166302343F
       D5B5D7E5A8
IV     1225076E665F69B967FAFD2BFD9E7389jRDfIAes156scwqNhod+lK
       5fP4oHPnMU

JLAvuFdEFIjPOnlk3gvEkuBO2FunrSpDrP65qO7wriL43r3y1GZGA==

wordlist 4k
wordwidth   12
words 4096

a
abandoned
ability
able
aboard
...
```