iOS ENCRYPTION CONT
Lecture 20a

COMPSCI 702
Security for Smart-Devices

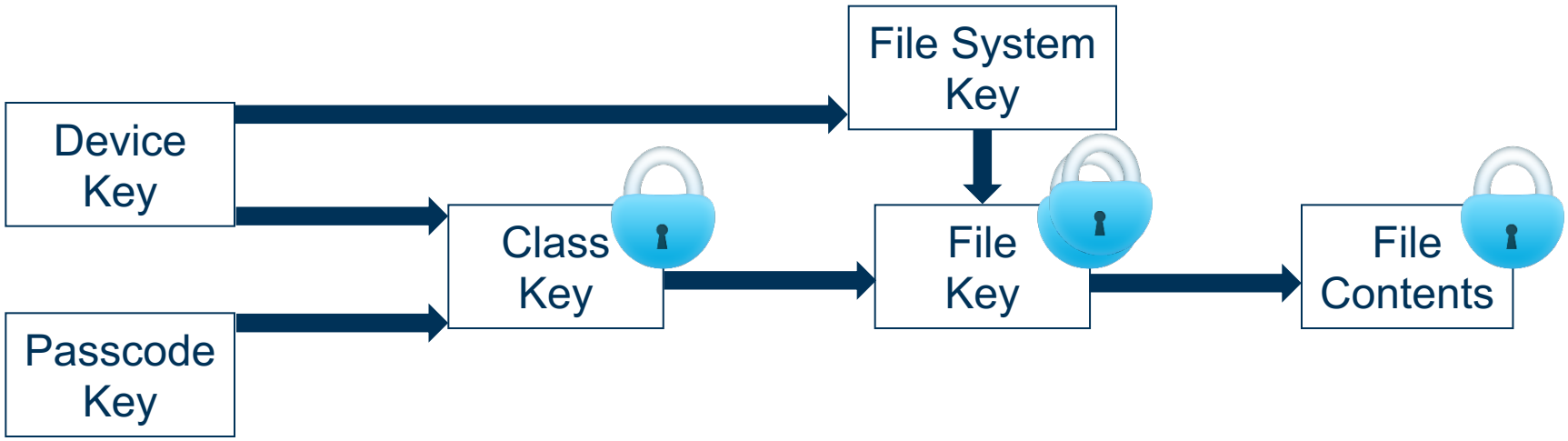
Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

April 28, 2021

FILE SYSTEM KEY

- An additional layer to protect file keys, used for remote wipe out
- It is created when
  - iOS is installed or
  - The device is wiped by the user



WHY LAYERED KEYS

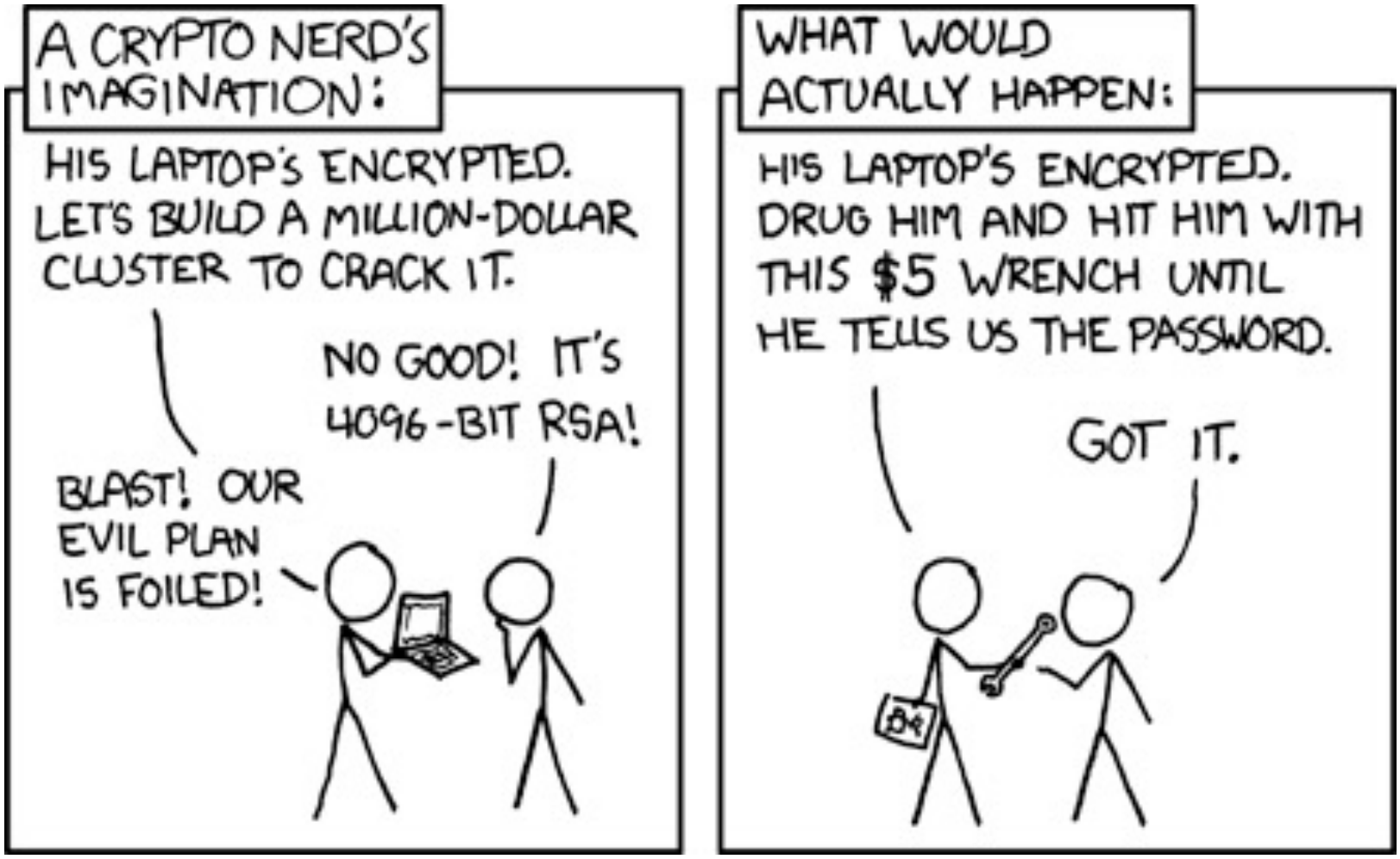
- The entire filesystem can be rendered useless by wiping the file system key
- Modifying a passcode just rewraps the class key
- Changing a file's class only requires rewrapping of the file key
- Deleting a file will require throwing away the file key
- If the device key is used, files or keychain items could only be restored using the same device

KEYCHAIN ITEM PROTECTION CLASSES – (FOR PASSWORDS ETC.)

Protection Class	Description
kSecAttrAccessible **When Unlocked**	Accessed when the device is unlocked
kSecAttrAccessible **After First Unlock**	Protected unless the passcode is entered
kSecAttrAccessible **Always**	Not protected and always accessible (default)
kSecAttrAccessible **When Unlocked – This Device Only**	Same as when unlocked, but non-migratory
kSecAttrAccessible **After First Unlock – This Device Only**	Same as after first unlock, but non-migratory
kSecAttrAccessible **Always – This Device Only**	Same as always, but non-migratory

SUMMARY

- Use complex passcodes
- Sensitive information should be protected as much as possible
- iOS enables protection of files and keychain items
- A lost device is subject to recovery unless a remote wipe command is sent
- Data could be read from jailbroken devices



Source: xkcd.com

RESOURCES

- **White Paper on iOS Security**
  https://www.apple.com/business/docs/iOS_Security_Guide.pdf
- **iOS Hacker's Handbook**
  Charlie Miller, Dionysus Blazarkis, Dino Dai Zovi, Stefan Esser,Vincenzo Iozzo, Ralf-Philipp Weinmann
  John Wiley & Sons, Inc., 2012
- **Apple iOS 4 security evaluation**
  Dai Zovi and Dino A.
  Black Hat USA 2011
  http://media.blackhat.com/bh-us-11/DaiZovi/BH_US_11_DaiZovi_iOS_Security_WP.pdf
- **Bypassing iPhone 3G[s] Encryption**
  http://www.zdziarski.com/blog/?p=516

ACKNOWLEDGEMENT

- Last few slides are based on the presentation shared by Robert Sheehan, thanks to him!

Questions?

Thanks for your attention!