WILLIAM & MARY

CHARTERED 1693

CSCI 445:
Mobile Application Security

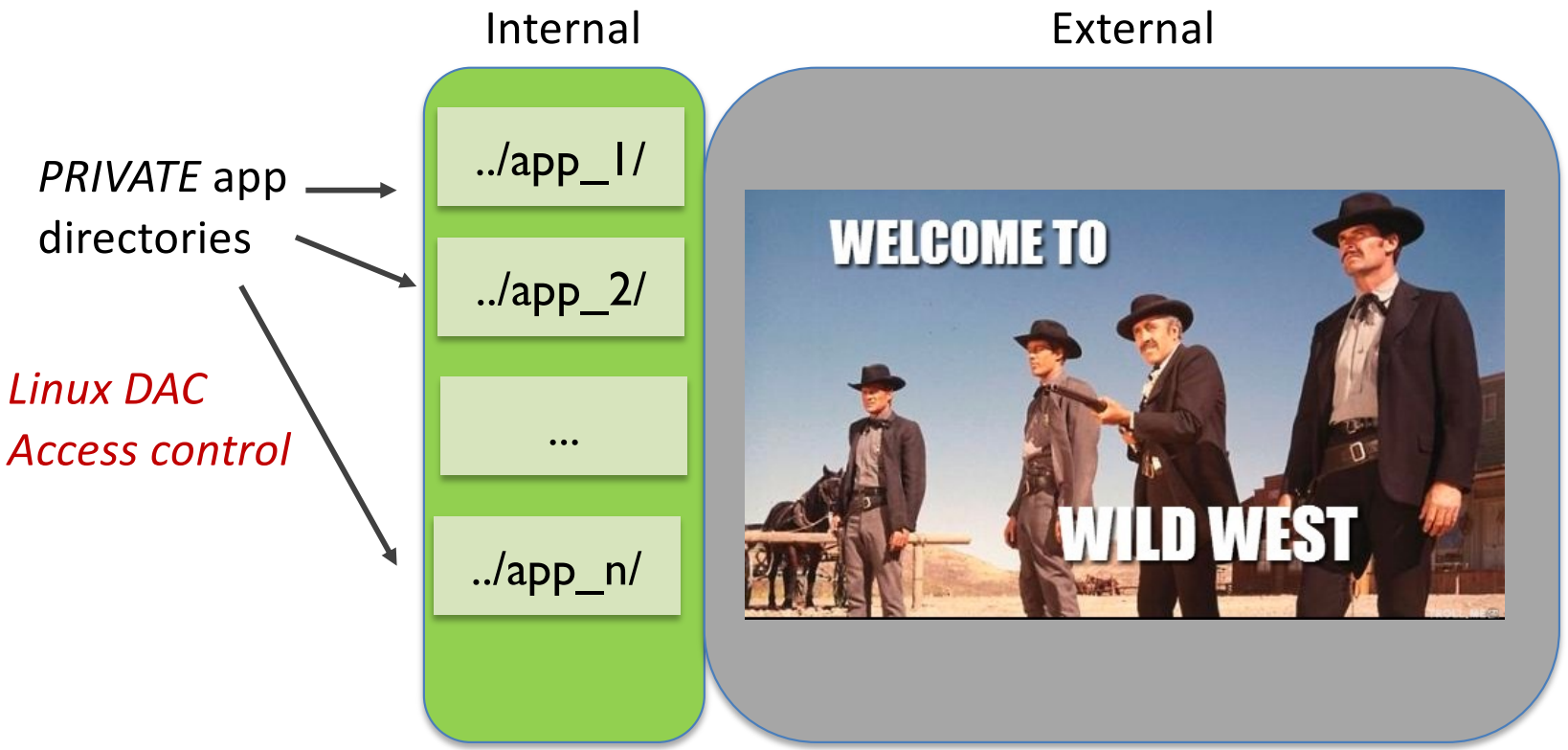
Lecture 10

Prof. Adwait Nadkarni

Android's storage architecture

App Storage on Android

Q: *Why do apps need external storage (sdcard)?*



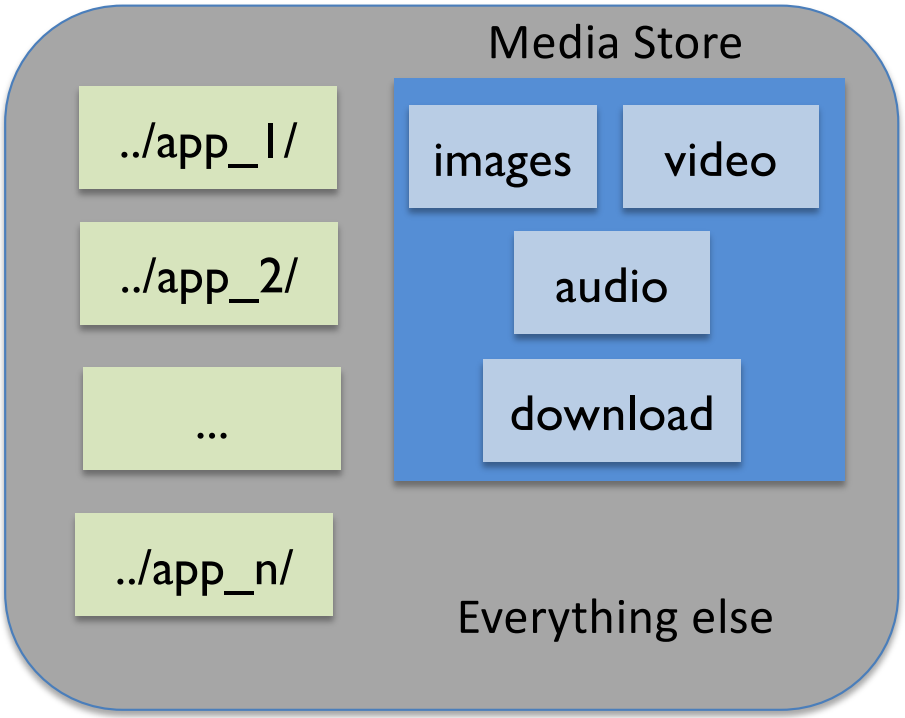
Any app with READ/WRITE_EXTERNAL STORAGE can access all data! (but this is changing)

Towards better external storage

- Apps need to read/write files on external storage
  - How can we facilitate access without abuse?
    - *Do all apps need **broad** storage access?*
- Two kinds of apps:
  1. Apps that want to offload their data
  2. Apps that want to *manage* data (e.g., file managers)
     - Insight: *Only the latter need broad storage access!*

External storage (now)

Apps need no permission to access their dirs



Apps need media-specific runtime permissions

- Apps with READ/WRITE_EXTERNAL_STORAGE permissions can still access everything. *So how does this new design help?*
- *Apps that do not need broad storage access can function with none or media-specific permissions!*

External Storage (future)

- *Scoped Storage* all the way!
  - Apps will *only* be able to access their own private directories on external storage
  - Read/write external storage permissions will not be widely granted
- *What about file managers?*
  - *Apps will need to specially request Google for broad storage permissions*
- *Does this solve the problem of abuse of broad storage access?*

Protecting Data at Rest

Storing Sensitive Data (1)

- Applications often require the use of sensitive data such as user credentials
- The attacker may try to access this data on storage.
- *Option 1:* Do not store it on the device

Storing Sensitive Data (2)

- Applications often require the use of sensitive data such as user credentials
- *Option 2:* Store it in the app's private directory
  - /data/data/<app-package-name>

```
//API to read/write files in the PRIVATE path, i.e.,/data/data/<app_packagename>/files/
FileInputStream fis = openFileInput("input.txt");

//Note: NEVER use MODE_WORLD_READABLE/WRITABLE unless there is no other option.
FileOutputStream fos = openFileOutput("output.txt", MODE_PRIVATE);
int ch;
while((ch = fis.read())!=-1){
      fos.write(ch);
}
```

Other Useful APIs:
getFilesDir(), getDir(), deleteFile(), fileList()

Thankfully deprecated in Android N, but still found in some apps

Storing Sensitive Data (3)

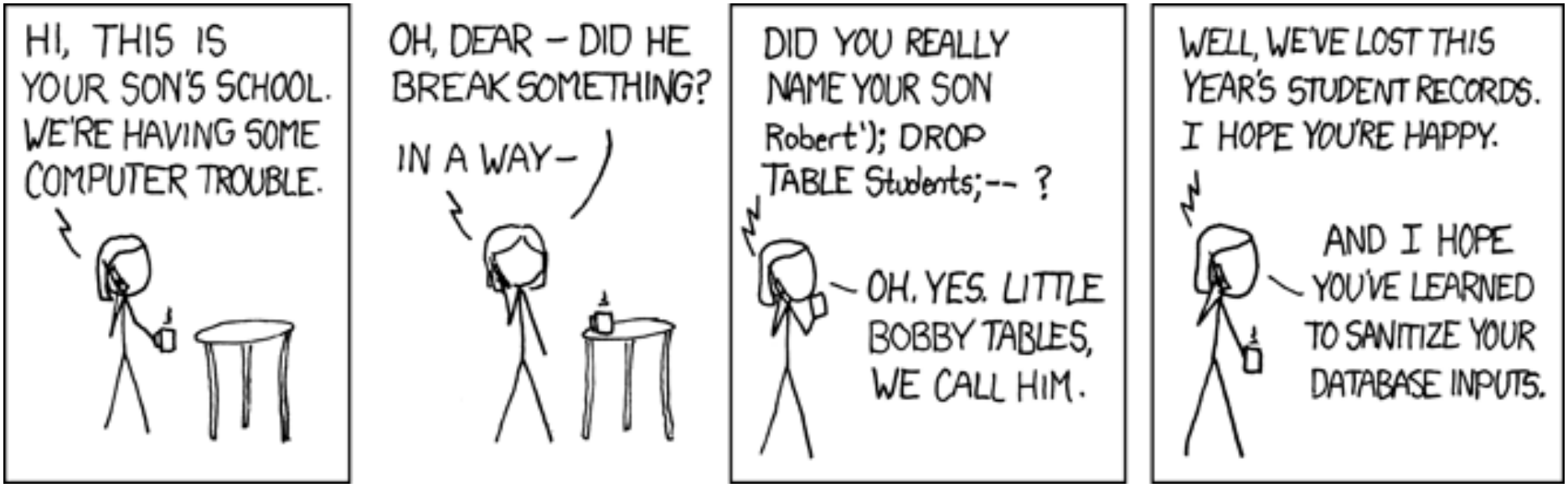
- Applications often require the use of sensitive data such as user credentials
- *Option 3*: Encrypt it!
  - Use the *Android KeyStore* for key generation and storage

```
KeyPair generateKeys() throws Exception {
    Calendar cal = Calendar.getInstance();
    Date now = cal.getTime();
    cal.add(Calendar.YEAR, 1);
    Date end = cal.getTime();

    KeyPairGenerator kpg = KeyPairGenerator.getInstance("RSA", "AndroidKeyStore");
    kpg.initialize(new KeyPairGeneratorSpec.Builder(context).setAlias(alias)
                        .setStartDate(now).setEndDate(end)
                        .setSerialNumber(BigInteger.valueOf(1))
                        .setSubject(new X500Principal("CN=SampleCN")).build());

    return kpg.generateKeyPair();
}
```

And finally...


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

Prevent SQL Injection

- *SQL injection*: user provides a substring for an SQL query that changes the query entirely (e.g., add SQL operations to query processing)

```
SELECT fieldlist FROM table
 WHERE field = 'anything' OR 'x'='x';
```

```
SELECT UserId, Name, Password FROM Users WHERE UserId = 105 or 1=1;
```

- Use *parameterized SQL* methods for the implementation of query, insert, etc.

```
// Partial Implementation of the Content Provider's query method.
public Cursor query(Uri uri, String[] projection, String selection, String[] selectionArgs) {
    // Query the underlying database using the SQLiteDatabase query method,
    //Instead of calling rawQuery(String sqlQuery, String[] selectionArgs);
    SQLiteDatabase db = dbHelper.getWritableDatabase();
    SQLiteQueryBuilder qb = new SQLiteQueryBuilder();
    return qb.query(db, projection, selection, selectionArgs, null, null, orderBy);
}
```

Takeaways

1

Use default APIs

- getFilesDir()/getExternalFilesDir()
- MediaStore APIs

2

Move to scoped storage, adhere to least privilege

3

Encrypt credentials w/ Keystore

Security Research Methods I

Derived from slides by William Enck

Reading papers …

- What is the purpose of reading papers?
- How do you read papers?

Understanding what you read

- Things you should be getting out of a paper
  - What is the central idea proposed/explored in the paper?
    - Abstract
    - Introduction
    - Conclusions

    } *These are the best areas to find an overview of the* ***contribution***

  - How does this work fit into others in the area?
    - Related work - often a separate section, sometimes not, every paper should detail the relevant literature. Papers that do not do this or do a superficial job are almost sure to be bad ones.
    - An informed reader should be able to read the related work and understand the basic approaches in the area, and how they differ from the present work.

Understanding what you read (cont.)

- What scientific devices are the authors using to communicate their point?
- Methodology - this is how they evaluate their solution.
  - Theoretical papers typically validate a model using mathematical arguments (e.g., proofs)
  - Experimental papers evaluate results based on test apparatus (e.g., measurements, data mining, synthetic workload simulation, trace-based simulation).
  - Empirical research evaluates by measurement.
  - Some papers have no evaluation at all, but argue the merits of the solution in prose (e.g., design papers)

Understanding what you read (cont.)

- What did they find?
  - Results - statement of new scientific discovery.
    - Typically some abbreviated form of the results will be present in the abstract, introduction, and/or conclusions.
    - Note: *just because a result was accepted into a conference or journal does necessarily not mean that it is true. Always be circumspect.*
- What should you remember about this paper?
  - Take away - what general lesson or fact should you take away from the paper.
  - Note that really good papers will have take-aways that are more general than the paper topic.

The best papers are the ones that teach you something

Tips for reading a paper

- Everyone has a different way of reading a paper.
- Here are some guidelines I use:
  - Always have a copy to mark-up. Your margin notes will serve as invaluable sign-posts when you come back to the paper (e.g., "here is the experimental setup" or "main result described here")
    - Digitally: Zotero, Mendeley
  - After reading, write a summary of the paper containing answers to the questions in the preceding slides. If you can't answer (at least at a high level) these questions without referring to the paper, it may be worth scanning again.
- Over the semester, try different strategies for reading papers and see which one is the most effective for you.

Reading a systems security paper

- What is the security model?
  - Who are the participants and adversaries
  - What are the assumptions of trust (trust model)
  - What are the relevant risks/threats
- What are the constraints?
  - What are the practical limitations of the environment
  - To what degree are the participants available
- What is the solution?
  - How are the threats reasonably addressed
  - How do they evaluate the solution
- What is the take away?
  - key idea/design, e.g., generalization (not solely engineering)
- Hint: I will ask these questions when evaluating course project.

The End