

# **COMP5216** Assignment Project Exam Help

**Week 06**

**Semester 2, 2020**

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

Dr. Kanchana Thilakarathna  
School of Computer Science

# Announcements

- Project proposal submissions are due now.
- After marking the project proposals, I'll organize individual feedback sessions.
- Official moving of students between tutorials are not going to happen.
  - Due to restriction <https://eduassistpro.github.io/>
  - Timetable clashes

Add WeChat edu\_assist\_pro

# Special Consideration

- In case of **Illness or Misadventure**
  - You can apply for special consideration
- The first thing you do should be
  - **Let the coordinator know** (best by email and while still sick)
  - **Submit your as**
- Follow proper b <https://eduassistpro.github.io/>
  - Have professional practitioner sign **Add WeChat edu\_assist\_pro**, upload scans
  - Submit application for special consideratorm
  - Note you have only a quite short deadline for applying
- No special consideration for missing out a few days or being on holiday etc.
  - Take the responsibility of your time management
- University Policy:  
[http://sydney.edu.au/current\\_students/special\\_consideration/index.shtml](http://sydney.edu.au/current_students/special_consideration/index.shtml)

## Assessment - Late submission policy

- Suppose you hand in work after the deadline:
- If you have not been granted special consideration or arrangements
  - A penalty of 5% of the maximum marks will be taken per day (or part) late.
  - After ten days, f zero.
  - e.g. If an assignment is worth 40% and you are one hour late submitting, then the maximum possible marks would be 38%.
  - e.g. If an assignment is worth 40% and you are 28 hours late submitting, then the maximum possible marks would be 36%.
- Warning: submission sites get very slow near deadlines
- Submit early; you can resubmit if there is time before the deadline

# Academic Dishonesty & Plagiarism

- Academic Integrity
  - Plagiarism: NO
  - Outsourcing: NO
  - See more details on the course website in Assessment section
- “The University of Sydney is unequivocally opposed to, and intolerant of, plagiarism and academic dishonesty. Plagiarism is defined as ‘the presentation of work as one’s own work without appropriate acknowledgement of the source.’ [from site below]”
- Submitted work is compared against other work (from students, the internet, etc)
  - Turnitin for textual tasks (through Canvas), other systems for code
- Penalties for academic dishonesty or plagiarism can be severe
- University Policy: <http://sydney.edu.au/elearning/student/EI/index.shtml>

# Outline

- State of Mobile Security & Privacy
- What is Privacy ?
- Mobile Security threat models
- Security of Mobile Operating Systems
  - App sandboxin <https://eduassistpro.github.io/>
  - Permissions
  - Releasing apps [Add WeChat edu\\_assist\\_pro](#)
- Best Mobile Security Practices

# Security Challenge

- Exponential **growth of smart devices** and **third party apps**.
  - Leads to security & privacy threats:

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

- Theft of personal information.
- Increased risks of malware.

# Security concerns of smart devices

Healthcare challenges: Ransomware and the Internet of Things are the tip of the iceberg

BY LYSA MYERS POSTED 7 APR 2017 - 02:00PM

RANSOMWARE



If your mobile phone is running slowly or always losing battery, it might have been hacked to mine cryptocurrency – here's how to protect yourself

Ana Zarzalejos, Business Insider España 18h 14,090

Zero-day mobile malware surged 92% in last six months

Networks Asia staff | August 31, 2018

in Share

G+

Like 0

Tweet

share

Print

Email

In the last 6 months, Pradeo Lab has observed a massive 92% rise of zero-day malware on mobile devices, demonstrating that hackers are strongly focusing their attention on enterprise mobility and constantly innovating to overcome security forces.

## Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

"FITNESS AND MEDICAL DEVICES ARE OFTEN FULL OF SENSITIVE INFORMATION, YET SECURITY AND PRIVACY ARE OFTEN AN AFTERTHOUGHT."

### More Devices Means More Targets

First, we had to worry about the physical security of our computers. More recently, we have learned to worry about mobile phones and tablet devices. Now, according to CIO, "we have to worry about protecting our car, our home appliances, our wearables and many other IoT devices."

Simple but extremely effective: Inside the world's most prolific mobile banking malware

Asacub trojan has quietly been going about its business for years, stealing funds from hundreds of thousands of victims – but it can also be easily avoided.



By Danny Palmer | August 29, 2018 -- 14:28 GMT (00:28 AEST) | Topic: Security

# Security threats are expected to grow further...

- Advanced sensing - 3D, IR cameras, HR, Brainwaves, etc.

## Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

The screenshot shows a blog post with the following details:

- Tags: Culture, Ethics, Technology, Virtual Reality
- Title: Mixed Reality Comes With New Privacy Concerns
- Published: May 20
- Comments: 0 Comments
- Keywords: augmented reality privacy, mixed reality privacy, virtual reality privacy
- Content: "At this point, we're all fully aware that everything you do can be put online, and whatever's online can be seen by a lot of people (unless, of course, it's on this blog)."

# What is Privacy ?

- “Personal Information”
  - Any information that identifies you or could reasonably be used to identify you
    - E.g. name, address, financial details, opinions, memberships, ethnic origin, health information, criminal record, etc.
  - Not just demographic information
    - E.g. photos, IP address, Device history, Location, installed apps
- Carefully treat and protect personal information collection, use, storage and sharing through your service

# What is Privacy ?

- “Personal Information”
  - Any information that identifies you or could reasonably be used to identify you
    - E.g. name, address, financial details, photos, opinions, memberships, ethnic origin, health information, criminal record, etc.

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro



of us are **more concerned** about online privacy than we were **five years ago**

Australian Community Attitudes to Privacy Survey  
2017



<https://www.oaic.gov.au>

# What is Privacy ?

- “Personal Information”
  - Any information that identifies you or could reasonably be used to identify you
    - E.g. name, address, financial details, photos, opinions, memberships, ethnic origin, health information, criminal record, etc.

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro



of us are **more concerned** about online privacy than we were **five yrs ago**

Australian Community Attitudes to Privacy Survey

2017



Australian Government

Office of the Australian Information Commissioner

# What is Privacy ?

- Failing to protect privacy could also result in a breach of the Privacy Act
  - <https://www.oaic.gov.au/privacy-law/privacy-act/>
- EU General Data Protection Regulation (GDPR)
  - <https://www.eugdpr.org>
- Mobile Privacy – A
  - Developed in 201
    - <https://www.oaic.gov.au/privacy-law/guide-for-mobile-app-developers.pdf>

## Assignment Project Exam Help

Add WeChat edu\_assist\_pro

### Checklist

- Your privacy responsibilities
- Be open and transparent about your privacy practices
- Obtain meaningful consent despite the small screen challenge
- Timing of user notice and consent is critical
- Only collect personal information that your app needs to function
- Secure what you collect**

# Mobile Security Threat Models

- **Physical Attacks**
  - Circumvent authentication to unlock the device.
- **App Attacks**
  - Use malicious app to hijack the access to other apps, etc.
  - Code tampering
- **System Attacks**
  - Use mobile platform which impacts all apps installed on the device
- **Server/Cloud Attacks**
  - Data breaches
  - Common to all other web services
- **Network Attacks**
  - Use packet sniffing or spoofing
  - Man-In-the-Middle attacks
  - Common to all other web services

# Physical Attacks

- Current device unlocking methods - Passwords, PINs, Patterns, Biometrics
  - Once unlocks all apps are accessible
- What are the potential authentication attacks?  
Assignment Project Exam Help
- Smudge attacks
  - Entering pattern with various lighting techniques
  - Aviv, A. J., Gibson, K. L., Mossop, E., Blaze, M., & Smeets, B. (2013). Fingerprint Attacks on Smartphone Touch Screens. *Woot*, 10, 1.
- Fingerprint extraction
  - Many demos on YouTube



# Physical Attacks

- People choose common simple patterns
  - Low entropy – Faster brute force attacks
  - At most 1600 patterns with less than 5 strokes

Assignment Project Exam Help

- People often reu

<https://eduassistpro.github.io/>

- Security questions are often very predictable
  - Mother's maiden name? – depending on culture, try Smith, Chang, Kim, Schmidt, ...
  - First car? – try Golf, Yaris, Corolla, ...
  - Social networks help collect additional information about a person

Add WeChat [edu\\_assist\\_pro](https://edu_assist_pro)

# Physical Attacks



Assignment Project Exam Help

- Is our phones mobile biometric authentication? [https://eduassistpro.github.io/  
biometric  
Add WeChat edu\\_assist\\_pro  
to PIN](https://eduassistpro.github.io/Add_WeChat_edu_assist_pro_to_PIN)
  - Most (if not all) biometric authentication is based on PINs
  - No more secure than PIN
- Biometrics – if compromised, lost for ever
  - Can not be changed

# **App Attacks - Mobile Malware**

- Capable of performing System Attacks and/or App Attacks

**Assignment Project Exam Help**

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

# **App Attacks - Mobile Malware**

- Examples of threats on Google Play store in 2017

**Assignment Project Exam Help**

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

# App Attacks - Mobile Malware

- Ransomware example: Fake app for popular Chinese game King of Glory
  - Direct user to pay via WeChat, AliPay, QQ

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

# App Attacks - Mobile Malware



DEPARTMENT OF JUSTICE

FEDERAL BUREAU OF INVESTIGATION

FBI HEADQUARTERS

WASHINGTON DC DEPARTMENT, USA

AS A RESULT OF FULL SCANNING OF YOUR DEVICE, SOME SUSPICIOUS FILES HAVE BEEN FOUND AND YOUR ATTENDANCE OF THE FORBIDDEN GEOGRAPHIC SITES HAS BEEN FIXED. FOR THIS REASON YOUR DEVICE HAS BEEN LOCKED.

INFORMATION ON YOUR LOCATION AND SNAPSHOTS CONTAINING YOUR FACE HAVE BEEN UPLOADED ON THE FBI CYBER CRIME DEPARTMENT'S DATACENTER.

FIRST OF ALL, FAMILIARISE WITH THE POSITIONS STATED IN SECTION «THE LEGAL BASIS OF VIOLATIONS». ACCORDING TO THESE POSITIONS YOUR ACTIONS BEAR CRIMINAL CHARACTER, AND YOU ARE A CRIMINAL SUBJECT. THE PENALTY AS A BASE MEASURE OF PUNISHMENT ON YOU WHICH YOU ARE OBLIGED TO PAY IN A CURRENT OF THREE CALENDAR DAYS IS IMPOSED.

THE SIZE OF THE PENALTY IS \$500.00

ATTENTION!

DISCONNECTION OR DISPOSAL OF THE DEVICE OR YOUR ATTEMPTS TO UNLOCK THE DEVICE INDEPENDENTLY WILL BE APPREHENDED AS UNAPPROVED ACTIONS INTERFERING THE EXECUTION OF THE LAW OF THE UNITED STATES OF AMERICA (READ SECTION 1509 - OBSTRUCTION OF COURT ORDERS AND SECTION 1510 - OBSTRUCTION OF CRIMINAL INVESTIGATIONS). IN THIS CASE AND IN CASE OF PENALTY NON PAYMENT OF THE PENALTY OF THREE CALENDAR DAYS FROM THE DATE OF THIS NOTIFICATION, THE TOTAL AMOUNT OF PENALTY WILL BE TRIPLED AND THE RESPECTIVE FINES WILL BE CHARGED TO THE OUTSTANDING PENALTY. IN CASE OF DISSENT WITH THE INDICTED PROSECUTION, YOU HAVE THE RIGHT TO CHALLENGE IT IN COURT.

TO MAKE A PENALTY PAYMENT, GO TO SECTION «PAYMENT PENALTIES»

DIRECTOR JAMES COMEY  
FEDERAL BUREAU OF INVESTIGATION  
FBI DEPARTMENT OF JUSTICE, USA



- Types of Android Ransomware
  - Lock Screen Ransomware
  - Crypto
  - Send SMS
  - Steal sensitive information
  - Disable anti-vir <https://eduassistpro.github.io/>
- Advertisement Hijacking
  - Take a popular application & change the advertisement ID
  - Publish in a different app market
- For fun: Change scores in games/Skip levels

# System Attacks – OS vulnerabilities

- Android exploits and vulnerabilities

- Janus attack – 2017

<https://blog.trendmicro.com/trendlabs-security-intelligence/janus-android-app-signature-bypass-allows-attackers-modify-legitimate-apps/>

- Modify the APK (add extra bytes) without changing the signature
    - Exploited to pp without the knowledge

<https://eduassistpro.github.io/>

- Stagefright attack 2015

<https://www.androidcentral.com/stagefright>

- A video sent via MMS could be used to attack libStageFright mechanism which process video files
    - Exploited to do remote code executions

# System Attacks – OS vulnerabilities

- “**Rooting**” Android Devices
  - Enables “Root” access to the system
  - Allows to replace the existing OS with custom ROMs

Assignment Project Exam Help

- “**Jail Breaking**” i
  - Allows to bypass <https://eduassistpro.github.io/>
  - Exploited to download & install apps from outside Apple AppStore
- Popularity of jail breaking and rooting are going down
- Vendor are also keep making it difficult to hijack the OS

Assignment Project Exam Help  
**Securit** **Systems**  
<https://eduassistpro.github.io/>  
Add WeChat edu\_assist\_pro

# Operating Systems got you covered (mostly) ...



- Closed-source operating system based on Unix (Darwin)
- Apps are developed in Objective-C
  - Native development in Objective-C
  - **App Sandbox**
  - **User permission structure**
  - Vendor (Apple) **singed app release**
- Open-source operating system based on Linux (by Google)
  - Native development in Java
  - **App Sandbox**
  - **User permission structure**
  - Developer (self) **singed app release**

# Android OS Architecture

**Applications:** Users interact with the device via the apps. Can be either first party or third party.

**Android Framework:** Provides basic functions such as communication between apps, managing voice calls or managing app life cycles.

## Assignment Project Exam Help

<https://eduassistpro.github.io/> libraries that contain instructions to different types of data. E.g. Webkit,

Add WeChat [edu\\_assist\\_pro](#) Android R Dal Machine and Core Libraries.

**Hardware Abstraction Layer (HAL):** Converts the Java API calls to system calls that is understood by the Linux kernel.

**Linux Kernel:** A kernel built on top of Linux kernel2. Additional modifications done by Google to make it suitable for smartphones (E.g. power management). Handles all conventional operating system functions such as process management and memory management.

**Source:** Android developer documentation

# 1. Android App Sandbox

- Similar to user-based protection model in Linux
- 1. Each app runs with its own Dalvik Virtual Machine
- 2. Apps are not allowed to talk to each other
- 3. Limited access to the OS (Kernel)

Assignment Project Exam Help

- Apps must explicitly declare the required permissions for add <https://eduassistpro.github.io/> by the basic sandbox

Add WeChat edu\_assist\_pro

## 2. User Permission Structure

- App must get permission to do anything that
  - Uses data or resources that the app did not create
  - Uses network, hardware, features that do not belong to it
  - Affects the behaviour of the device
  - Affects the behaviour of other apps
- **If it isn't yours,** <https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

## 2. User Permission Structure

- **Normal** permissions do not directly risk the user's privacy
  - Example: Set the time zone
  - Android automatically grants normal permissions.
- **Dangerous** permissions risk the user's privacy
  - Example: Read the user's contacts
  - Android asks user to explicitly grant dangerous permissions

## 2. User Permission Structure

- Before Marshmallow (API 23)
  - Grant permission before installing
- After Marshmallow (API 23)
  - App must get runtime permission

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

## 2. User Permission Structure

- Before API 23 → Uninstall app !
- After API 23
  - Can revoke each permission at any time

Settings > apps > permissions

Assignment Project Exam Help

<https://eduassistpro.github.io/>

- Use Android Support Library to develop backward compatible permission structure

Add WeChat edu\_assist\_pro

### 3. Android app signing process

- The code we write is built to an Android Application Package (APK)
- **Developer (self) signed app release**

Assignment Project Exam Help

Managing  
your own key

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

Google Play  
App signing

# Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

# Best Practices for Privacy Aware Apps

- Do not ask “personal information” if not necessary
- **Privacy by Design**
  - Building privacy and data protection up front into the design specifications and architecture of information and communication systems and tec  
and data prote <https://eduassistpro.github.io/> compliance with privacy
- Make privacy y  
[Add WeChat edu\\_assist\\_pro](#)
- Draft a privacy policy (data management procedure) if you access sensitive information
- Beware of what you log. Android log can be read by other apps with **READ\_LOGS** permission

# Security Best Practices - Physical Attacks

- PIN or a pattern for individual apps (second layer of defence)
  - E.g. Perfect AppLock  
<https://play.google.com/store/apps/details?id=com.morrison.applocklite&hl=en>
- Use **Multi-Factor** <https://eduassistpro.github.io/>
  - Smartwatch, gla

Assignment Project Exam Help

Add WeChat edu\_assist\_pro

# Security Best Practices - Physical Attacks

- Two-factor authentication with SMS messages and OTC (one-time-code)

## Assignment Project Exam Help

- Is this secure? What <https://eduassistpro.github.io/>
  - **SMS interception/hijacking:** As a result of mobile networks
    - In 2017, attackers successfully intercepted German banks by creating a fake mobile network O2-Telefonica mobile network
  - **SIM-swap**
  - **Mobile number port-out**
  - **Interception by malware and trojans**
    - Check Point Ltd. discovered a trojan named “EuroGrabber” which carried out similar attacks in Eastern Europe and swiped approximately \$47 million from over 30,000 customers

# Security Best Practices - Physical Attacks

- Advanced SMS-based two-factor authentication with KeyMaps
  - Merging with the ZKPP (Zero-Knowledge Password Proof)



Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

- E.g. <https://www.tokenone.com>

# Security Best Practices - Physical Attacks

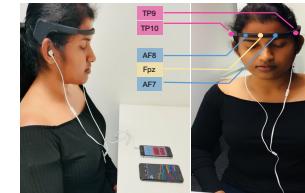
- Behavioural authentication for two-factor authentication
  - Nearly impossible to perfectly mimic behaviours, e.g. replay attacks.
- BreathPrint
  - Breathing acoustics for user authentication

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

- MusicID for smart headsets
  - Brainwave patterns for user authentication
- Follow NIST Digital Identity Guidelines
  - <https://pages.nist.gov/800-63-3/sp800-63-3.html>



# Security Best Practices - Permissions

- Only use permission that is necessary for the functionality of the app
- Beware of the permission requested by libraries
  - Users don't see
  - Review libraries <https://eduassistpro.github.io/> permission
- Explain the reason for requesting permission to the user
  - Add WeChat edu\_assist\_pro permission
- Indicate when you access sensitive information to the user

# Security Best Practices - Permissions

- Ask permission at the right time
  - E.g. Photo app (Camera Permission)
    - At the launch – Access to Camera
    - When user wants to share – Access to Contacts
- Ask the right (mi <https://eduassistpro.github.io/>)
  - E.g. Reducing the volume of audio receiving a call
  - READ\_PHONE\_STATE permission directly receiving a call
    - It also allows you to read Phone Hardware IDs, SIM, Incoming phone number, etc. → **Over permission ?**
  - Instead, use **AudioFocus**
    - Don't need any permission
    - <https://developer.android.com/guide/topics/media-apps/volume-and-earphones>

# Security Best Practices - Permissions

- Can you avoid using permission ?

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

# Security Best Practices - Permissions

- Can you avoid using permission ?
  - Use another app to perform the task you wanted... How ?

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

# Security Best Practices - Permissions

- Use another app to perform the task you wanted... How ?
- Example: Taking a Photo
  - With CAMERA Permission
    - Allows your application to take photos
    - You have to add the permission `android.permission.CAMERA` to your manifest file
    - Only prompt the permission request once
  - With Intent type `MediaStore.ACTION_IMAGE_CAPTURE`
    - You do not have to design the UI for taking a photo
    - User can pick the favorite app to take a photo
    - Your app will not have direct access to Camera
    - Selection prompt appears every time user invoke this action

# Security Best Practices - IDs

- Don't store user names and passwords on the device
- Use user name and passwords for the initial authentication

**Assignment Project Exam Help**

- Use a hash or no transmit sensitive <https://eduassistpro.github.io/>
  - E.g. use has if you plan to  
y, not the email address.

**Add WeChat edu\_assist\_pro**

- Hash function H are used to produce a hash h of fixed length given a message m:  $h = H(m)$ 
  - One-way function: computationally infeasible to find an input m that corresponds to an output h, whereas computing h from m is easy
  - Weak collision resistant: given an input m and an output h, it is infeasible to find another different input m' such that  $H(m) = H(m')$

# Security Best Practices - IDs

- User short-lived, service specific authorization tokens
  - Use the com.google.android.gms.iid InstanceID API.
  - Use randomUUID()
- For a unique identifier to track users across apps
  - Why ?
  - GUID (Globally Unique Identifier) <https://eduassistpro.github.io> Use IMEI or phone number
  - Create a large unique number [Add WeChat edu\\_assist\\_pro](#)
- For a unique identifier to track users across apps
  - For Advertising and Analytics
  - Use the Advertising Identifier available from the AdvertisingIdClient.Info class via the getId() method
  - <https://developers.google.com/android/reference/com/google/android/gms/ads/identifier/AdvertisingIdClient>

# Security Best Practices - Storage

- Three methods to save files
  - Internal Storage
  - External Storage
  - Content Providers

Assignment Project Exam Help

## Internal Storage <https://eduassistpro.github.io/>

- Only accessible to the app, good e t of the apps
- For more sensitive data, you can e
  - Do not make keys accessible to the app
  - Encrypt with KeyStore -  
<https://developer.android.com/reference/java/security/KeyStore>
- If you want to share data with another app...

# Security Best Practices - Storage

- If you want to share data with another app...
  - Use Content Provider
  - Avoid the MODE\_WORLD\_WRITEABLE or MODE\_WORLD\_READABLE modes

Assignment Project Exam Help

## External Storage

- Don't store sensitive data in external storage
  - External storage can be readable by every app
  - External storage can be removed
- Perform input validation before receiving data from the external storage
  - <https://developer.android.com/training/articles/security-tips#InputValidation>

# Security Best Practices – Web content access

- Carefully use WebView due to common exploits with HTML and JavaScript
  - E.g. Cross-Site Scripting
  - If your app does not use JavaScript, do not call `setJavaScriptEnabled()`
  - Carefully use Allow JavaScript to allow JavaScript to perform like a <https://eduassistpro.github.io/>
    - Only for web sites that can trust
  - If sensitive data was exchanged, Add WeChat edu\_assist\_pro

# Security Best Practices - Networking

- Minimize networking activities
- Authenticated, encrypted socket-level communication via SSLSocket class

## Assignment Project Exam Help

- Avoid writing new protocols
- Never write new code
- Do not use SMS for sensitive information
  - SMS are not encrypted
  - Not strongly authenticated
  - Can be read by any application with READ\_SMS permission
- Use HTTPS over HTTP wherever, whenever possible
  - When is it not possible to use HTTPS ?

Add WeChat edu\_assist\_pro

# Security Best Practices - Why HTTPS (HTTP over TLS) ?

- If somebody can capture the network traffic generated by the previous app, he will be able to see what words you are looking for? <https://eduassistpro.github.io/>
- Who potentially capture the traffic generated by the smartphone? [Add WeChat edu\\_assist\\_pro](#)
- Solution: End to End Encryption → HTTPS

# Security Best Practices - Encryption

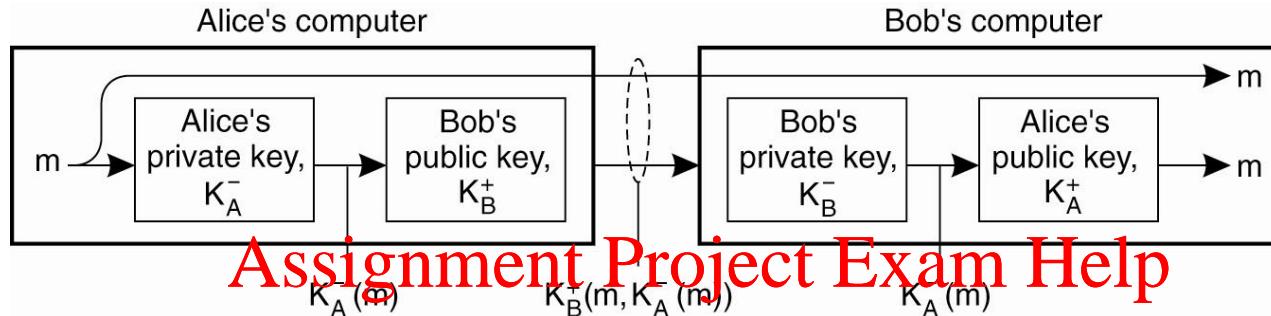
## Public key signature

- Alice sends a message  $P$  to Bob
  - 1. Alice encrypts it with her private key  $K_A^-$  and sends it off to Bob
  - 2. She can use Bob's public key  $K_B^+$  to keep the message secret and sends  $K_B^+(P, K_A^-(P))$ , com  
ed
  - 3. Bob decrypts the s <https://eduassistpro.github.io/> with Alice's public key. If the message is the same as the non-signed s been sent by Alice.

Add WeChat edu\_assist\_pro

Is this provide enough integrity?

# Security Best Practices - Encryption



<https://eduassistpro.github.io/>

## Issues with public key signatures

- Alice's signature is valid only until her private key remains a secret
- If Alice wants to bail out, Alice could claim that her private key was stolen
- Alice can change her private key
- Central authority may be required to keep track of keys

# Security Best Practices - Validation of Certificates

- A certificate is a simple text file containing some information such as Company Name, the domain name, and a public key.
- Anybody can ~~Assignment Project Exam Help~~ create a server pretending to be somebody
  - <https://eduassistpro.github.io/>
- Answer is Certificate Authorities
  - Add WeChat edu\_assist\_pro
    - Android comes with the set of CAs in the phones list, if you receive a certificate from a server & if it says it is issued by a trusted CA in the phones list, Android can verify the certificate.
- Example CAs are Comodo, Symantex, DigiCert, and Entrust.

# Security Best Practices - Trusted CA in Android

- If you go to Settings →  
Additional Settings → Security  
& Privacy → Trusted  
credentials.

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu\_assist\_pro

# Security Best Practices – Releasing the App

- You can use Android Studio to sign your app
- Sign up as a developer (Need to pay a subscription fee).
  - <https://play.google.com/apps/publish/signup/>

## Assignment Project Exam Help

- Go to the developer console
  - <https://play.google.com/apps/publish/signup/>
- **Google App Security Addons** <https://eduassistpro.github.io/>
- **Google Play Protect** <https://developer.android.com/google/play/assistant>
  - A good way to identify malicious third-party libraries
- **Launch Checklist**
  - <https://developer.android.com/distribute/best-practices/launch/launch-checklist>
  - Week 11 Tutorial

# Summer Research Projects/Honours Projects

## CS2020/23 Unravelling the Nascent Privacy Risks of 3D Spatial Mixed Reality Data

**Supervisor:** Kanchana Thilakarathna

**Eligibility:** The ability and desire to experiment with real devices, e.g. Oculus and HoloLens; and knowledge in applied machine learning.

**Project Description:**

Augmented, virtual, and/or mixed reality technology (AR/VR/MR) is increasingly becoming popular. From face filters to virtual pets or monsters that seemingly inhabit the physical-world, various MR applications are now widely accessible to most users.

MR platforms require spatial understanding of objects or surfaces, including their structural and photo-metric (e.g. colour and texture) attributes. Aside from objects being detected, spatial information also reveals the location of the user with high specificity, e.g. in which part of environment which poses additional holistic experimental validation of the project. In light of that, this project focuses on quantifying and detect the extent of privacy leakage in mixed reality environments, e.g. Oculus, and measures to mitigate it. The project will involve developing a system to detect privacy leakage in mixed reality environments, e.g. Oculus, and measures to mitigate it. The project will involve developing a system to detect privacy leakage in mixed reality environments, e.g. Oculus, and measures to mitigate it.

**Requirement to be on campus:** No

Assignment Project Exam Help  
<https://eduassistpro.github.io/>

Related Reading:

- [1] J. A. de Guzman, Jaybie A., Kanchana Thilakarathna, and A. Seneviratne. "A First Look into Privacy Leakage in 3D Mixed Reality Data." *European Symposium on Research in Computer Security (ESORICS)*, pp. 149-169, 2019.
- [2] J. A. de Guzman, K. Thilakarathna, and A. Seneviratne. Safemr: Privacy-aware visual information protection for mobile mixed reality. In *2019 IEEE 41st Conference on Local Computer Networks (LCN)*. IEEE, 2019.
- [3] J. A. De Guzman, K. Thilakarathna, and A. Seneviratne. Security and privacy approaches in mixed reality: A literature survey. *ACM Comput. Surv.*, 52(6):110:1–110:37, Oct. 2019.
- [4] J. A. de Guzman, K. Thilakarathna, and A. Seneviratne. Conservative plane releasing for spatial privacy protection in mixed reality. *arXiv preprint arXiv:2004.08029*, 2020.

- Please contact me if you are interested.

Add WeChat `edu_assist_pro`

# Privacy and Security of XR



- Multi-layer 3D point cloud mapping of surroundings



Spatial generalizations



- We were the first to reveal spatial privacy risks of MR devices.

- Reveal and quantify priv with mobile AR/MR devic 3D point clouds.
- Development of privacy preserving transformation of spatial data.

<https://eduassistpro.github.io/>

Add WeChat **edu\_assist\_pro**

- We are one of the 5 research groups in the world working with **Facebook Reality Labs** in developing privacy-aware MR solutions.

- <https://research.fb.com/blog/2020/09/announcing-the-winners-of-the-explorations-of-trust-in-ar-vr-and-smart-devices-request-for-proposals/>

# Summer Research Projects/Honours Projects

## CS2020/33 Efficient Streaming of 360 Degree Videos by Deep Video Content Analysis

**Supervisor:** Kanchana Thilakarathna

**Eligibility:** Knowledge on applied machine learning and computer networking basics are desirable. Mobile programming (iOS or Android) experience will be an added advantage. **Project Description:**

360° videos are a popular application of virtual reality. However, streaming 360-videos requires high bandwidth consumption. Tile-based streaming, which partitions a video frame into tiles and sends selected tiles based on user field-of-view (FoV) can fail if user FoVs are not available in real-time. This project aims to predict future user FoVs by analysing content features and using these predictions for efficient tile partitioning. Firstly, you will investigate different psychological factors that affect visual attention such as the contextual relationships between objects. Existing research shows that humans tend to be attracted to faces and text. However, there is plenty of untapped psychological research such as developing a novel content-based tile partitioning method. You will then focus on developing a novel content-based tile partitioning method for tiles leveraging methods such as DNNs. Finally, you will evaluate the performance of your proposed method on a 360-video streaming platform.

**Requirement to be on campus:** No

<https://eduassistpro.github.io/>

Related Reading:

- [1] Constantin, Mihai Gabriel, et al. "Computational understanding of visual attention beyond semantics: literature survey and analysis of covariates." *ACM Computing Surveys (CS)* 51, no. 1 (2019): 25.
  - [2] Qian, Feng, et al. "Flare: Practical viewport-adaptive 360-degree video streaming for mobile devices." *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. ACM, 2018.
  - [3] He, Jian, et al. "Rubiks: Practical 360-degree streaming for smartphones." *Proceedings of the 16th Annual International Conference on Mobile Systems, Applications, and Services*. ACM, 2018.
- Please contact me if you are interested.

# Networking Challenge of XR

## Assignment Project Exam Help

- 80 times more bandwidth to <https://eduassistpro.github.io/>
  - Ultra small latency to avoid
  - Large scale measurement and quantification of the quality of service offered by current mobile networks
  - Development of field of view aware video encoding mechanism
  - Development of tile-based video streaming framework
- Add WeChat **edu\_assist\_pro**

Partners:



# Summer Research Projects/Honours Projects

## CS2020/24 Real-time Encrypted Network Traffic Profiling with Deep Learning

**Supervisor:** Kanchana Thilakarathna

**Eligibility:** Knowledge on applied machine learning and computer networking basics are desirable.

**Project Description:**

Providers of large, enterprise-class networks find it hard to track hosts, servers and other vulnerable assets in their networks. Network profiling systems provide valuable insights to the assets on a network and their purpose. A network profiler in the provider's better consider how configuration changes will impact networks, and security administrators to identify suspicious activity. However, effective network profiling under real world constraints such as high-speed networking and ubiquitous encryption is challenging. The primary focus of this research is to develop means to address issues such as high-speed network profiling method based on deep learning operating at high speed. In collaboration with Data61-CSIRO.

**Requirement to be on campus:** No

Assignment Project Exam Help

<https://eduassistpro.github.io/>

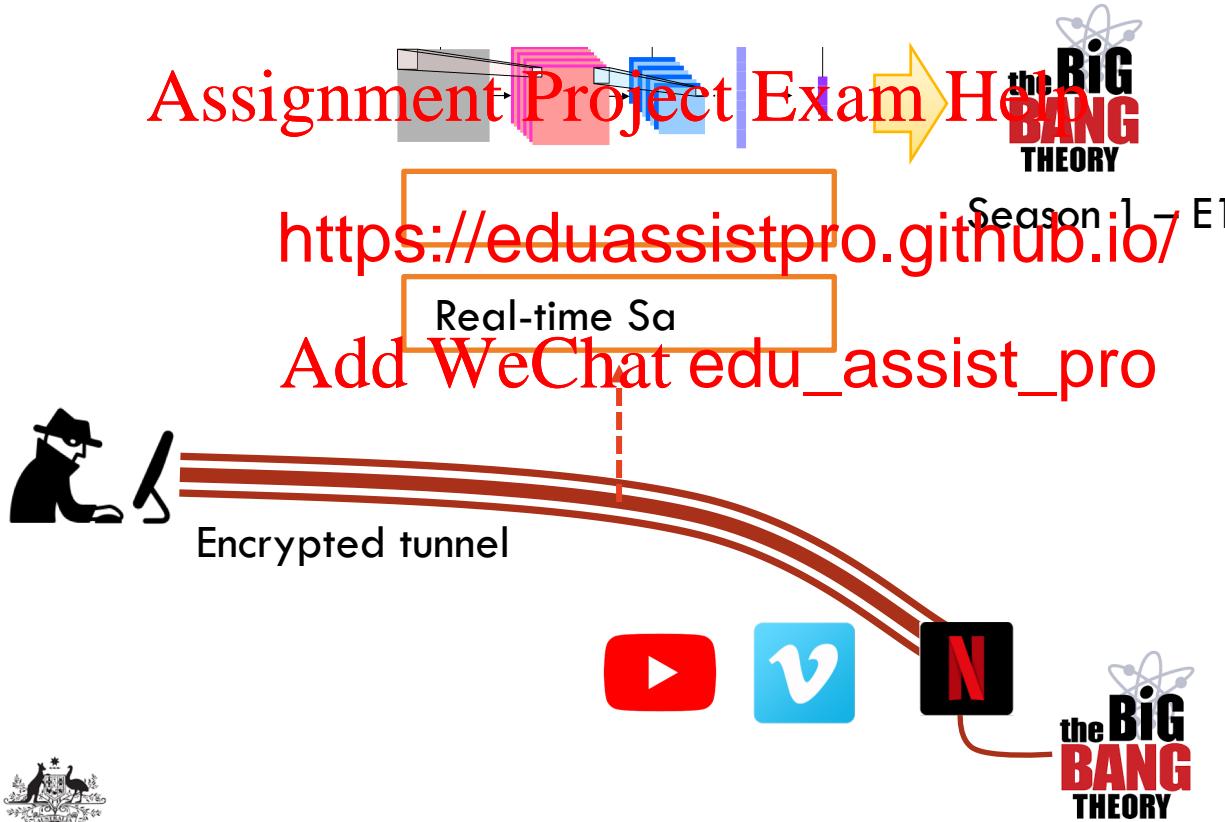
Related Reading:

- [1] Li, Y., Huang, Y., Xu, R., Seneviratne, S., Thilakarathna, K., Cheng, A., ... & Jourjon, G. (2018, November). Deep Content: Unveiling Video Streaming Content from Encrypted WiFi Traffic. In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)* (pp. 1-8). IEEE.
  - [2] Zhang, Xiaokuan, Jihun Hamm, Michael K. Reiter, and Yinqian Zhang. "Statistical Privacy for Streaming Traffic." In NDSS. 2019.
- Please contact me if you are interested.

Add WeChat `edu_assist_pro`

# Side-channel information leaks

- Deep Bypass: Clear & Dark Real-time Traffic Profiling with Deep Learning



# What's Next ?

- Start working on your project
- Tutorial 6 – Assignment Project Exam Help
- Next week – Bes https://eduassistpro.github.io/  
rgy and Cloud Computing Add WeChat edu\_assist\_pro
- See you all next week !