CHANDIGARH UNIVERSITY

Discover. Learn. Empower.

INSTITUTE : UIE

DEPARTMENT : CSE

Bachelor of Engineering (Computer Science & Engineering)

WEB AND MOBILE SECURITY (Professional Elective-I)

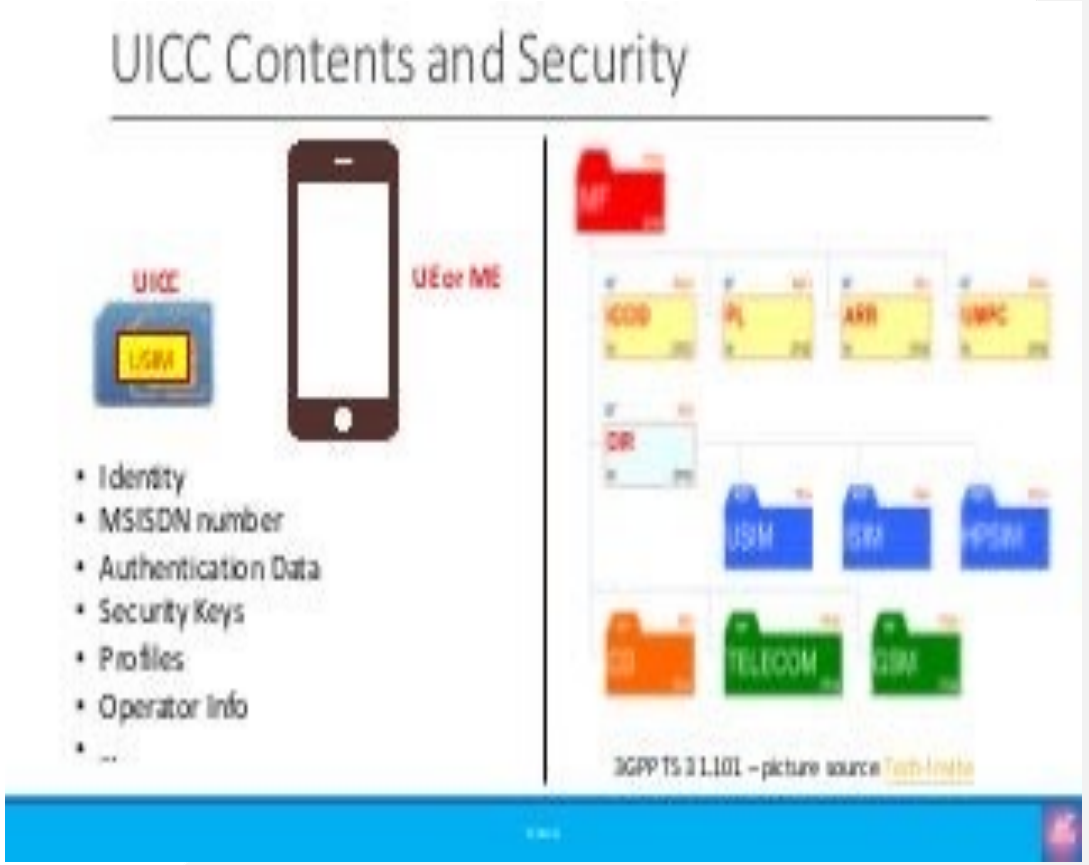
(20CST/IT-333)

TOPIC OF PRESENTATION:

SIM/UICC Security

Lecture Objectives

In this lecture, we will discuss:
SIM/UICC Security



UICC

- *UICC (Universal Integrated Circuit Card) is the hardware used in mobile devices that contains SIM and/or USIM applications enabling access to GSM, UMTS/3G and LTE networks.*
- *Embedded SIM is a UICC that supports "over the air" provisioning of an initial operator subscription and the subsequent change of subscription from one operator to another in accordance with the GSMA Embedded SIM specification. Use of the GSMA Embedded SIM Specification simplifies industrial and logistic processes for the distribution of M2M equipment.*

SIM

- A big differentiator and advantage of the UICC over the SIM is that it can have multiple applications stored on it because of its inherent processing power and larger storage capacity. The SIM card, on the other hand, is simply a storage device.
- One of the more important applications in the UICC is USIM (Universal SIM), which identifies the user and the device to the wireless service provider when using standards such as UMTS, HSPA and LTE. Other applications include CSIM (CDMA SIM) for enabling access to CDMA networks and ISIM (IP Multimedia Subsystem SIM) for securing access to multimedia services and non-telecom-related applications such as wireless and automatic payment

Vulnerabilities

- **1. Simjacker**
- In September 2019, security researchers at **AdaptiveMobile Security** announced they had discovered a new security vulnerability they called Simjacker. This complex attack carries out SIM card hacking by sending a piece of spyware-like code to a target device using an SMS message.
- If a user opens the message, hackers can use the code to spy on their calls and messages—and even track their location.

2. SIM card swapping

- Another SIM card security issue you may have heard of is **SIM card swapping**. Hackers used a variation of this technique to take over Twitter CEO Jack Dorsey's personal Twitter account in August 2019. This event raised awareness of how these attacks can be destructive. The technique uses trickery and social engineering, rather than technical vulnerabilities.
- To perform a SIM card hacking through a SIM card swap, a hacker will first call up your phone provider. They'll pretend to be you and ask for a replacement SIM card. They'll say they want to upgrade to a new device and, therefore, need a new SIM. If they are successful, the phone provider will send them the SIM

3. SIM Cloning

- Many times, people try to put SIM swapping and SIM cloning under that same umbrella. However, SIM cloning is more hands-on than the other option.
- In a SIM clone attack, the hacker first gains physical access to your SIM card and then creates a copy of the original. Naturally, for copying your SIM card, the hacker will first take out your SIM from the smartphone.

How to Keep Your SIM Card Safe

- **1. Protect Against Socially Engineered Attacks**
- **2. Set a SIM Card Lock**
- **3. Other Security Tips**
- As always, you should use strong and individually generated passwords. Don't reuse old passwords or use the same password on multiple accounts.
- Also, make sure your answers to password recovery questions aren't publicly available—such as your mother's maiden name.

https://www.makeuseof.com/tag/ways-sim-card-hacked/#:~:text=Set%20a%20SIM%20Card%20Lock,they%20need%20the%20PIN%20code.

Security practices

https://gesditel.es/en/sim-card-hacker/

- Put a PIN or password to unlock the SIM card.
- Do not share the PIN with absolutely no one.
- Keep the PIN and PUK number stored in a safe place.
- Use a PIN or key to unlock the SIM card.
- Encrypt our data.
- NEVER use SMS as a two-step authentication method.
- NEVER store sensitive information on your cell phone.
- Be very careful with the use of bank accounts on the cell phone.
- Use a VPN to browse from mobile or any other device.
- Do not open attachments that arrive in the mail or any messaging tool if you do not know the sender.
- Do not share personal information on the Internet.
- Install an antivirus or security tool on your cell phone.
- Do not link your bank account to your phone number.

References:

Books:

1. Hacking Exposed Mobile: Security Secrets & Solutions 1st Edition, Kindle Edition, by Neil Bergman, Mike Stanfield, Jason Rouse, and Joel Scambray
2. Hacking Exposed Web Applications, 3rd edition, Joel Scambray, Vincent Liu, Caleb Sima, Released October 2010, Publisher(s): McGraw-Hill

Reference Links:

1. https://justaskthales.com/en/what-uicc-and-how-it-different-sim-card/
3. https://www.makeuseof.com/tag/ways-sim-card-hacked/#:~:text=Set%20a%20SIM%20Card%20Lock,they%20need%20the%20PIN%20code.

Relevant Videos:

https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/
https://www.thalesgroup.com/en/markets/digital-identity-and-security/technology/sim
https://blog.3g4g.co.uk/search/label/UICC

THANK YOU