WELCOME TO OUR POWER POINT PRESENTATION

TOPIC: BLUETOOTH HACKING

[Security and Threats]

OVERVIEW

- BLUETOOTH INTRODUCTION
- BLUETOOTH ATTACKS
- SECURING BLUETOOTH DEVICES
- COUNTERMEASURES AND PREVENTIONS
- CONCLUSION

BLUETOOTH INTRODUCTION:

- Wireless networking technology
  - For short range devices
- Speed – 2.4Ghz
- Range is between 10 to 30m
- Data transfer rate is 1mbps
- Bluetooth SIG
  - Founded in 1998
  - Trade association
  - Owns and licenses IP

Hidden Dangers of using Bluetooth

BLUETOOTH ATTACKS:

- BLUEJACK ATTACK
- THE BLUESNARF ATTACK
- THE BLUEBUG ATTACK
- OTHER ATTACKS

  [TROJANS, VIRUSES, WORMS]

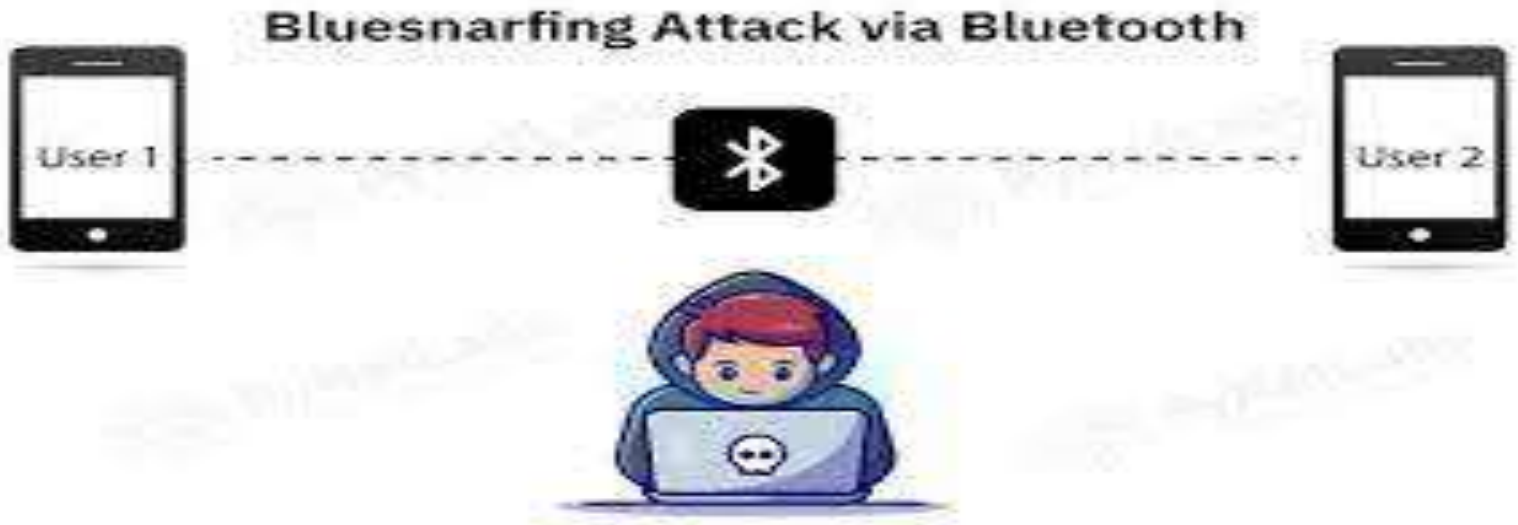
BLUEJACKING:

- OBEX push attack
  - Object exchange protocol for exchanging data with one another (data likes files,picture,business cards,calendar entries etc.)
- Commonly send ‘ business card ‘ with message via OBEX
- Variants
  - Bluetoothing
  - Bluechatting

- Modifying a remote mobile phone’s address book
- Bluespamming

THE BLUESNARFING ATTACK:

- Discovered by Marcel Holtmann
  - Published in October 2003
- BlueSnarf exploits weak OBEX implementation on mobile phones
- OBEX pull attack
  - Attacker involves the use of the OBEX protocal to forcibly pull sensitive data out of the victim's mobile phone
  - Extreme vulnerableand damage possible through bluesnarfing



- Can steal sensitive data without the knowledge of the victim
  - Address book,photographs
  - Music,videos,calendar,
  - IMEI, noReading/decoding sms messages etc.
- Adv connects to OBEX push profile
  - No authentication,no pairing needed

  →invisible connection

THE BLUEBUG ATTACK:

- Discovered by Martin Herfurt
  - Public field test – CeBIT 2004
- Full access to At Command set hence Full phone control
- Based on AT commands → not OBEX
- Typical use cases :-
  - Call control (turning phone into bug)
  - Intiating a new call to predefined no.

SECURING BLUETHOOTH DEVICES:

- A Device can implement three different security modes:
  - **Nonsecure**: A device will not initiate any security measures, so communication takes place without authentication or encryption.
  - **Service-level enforced security**: Two devices can establish an ACL link in a nonsecure manner. Security procedures are initiated when a L2CAP (Logical Link Control and Adaptation Protocal) channel request is made.
  - **Link –level enforced security** : Security procedures are initiated when the ACL Link is being established.

COUNTERMEASURES AND PREVENTION :

- One should not enable Bluetooth unless it is necessary.
- One should not accept files or business cards or any other incoming Bluetooth data from unknown people.
- Avoid using short pairing codes
- Change the default name.
- There is hardly any software available to prevent or detect blue-T-attacks.
- Turn off Bluetooth.
- Update your devices on regular basis.
- Change password when you come to know something wrong happening to your device.

CONCLUSION

- Low cost and power consumption technology.
- It may have great future if it should follow codes ethics.

THANK YOU…