Mobile Malware

BY: Rafay Sheikh, Afan Rasool, Md Enamul Kabir

What is Mobile Malware?

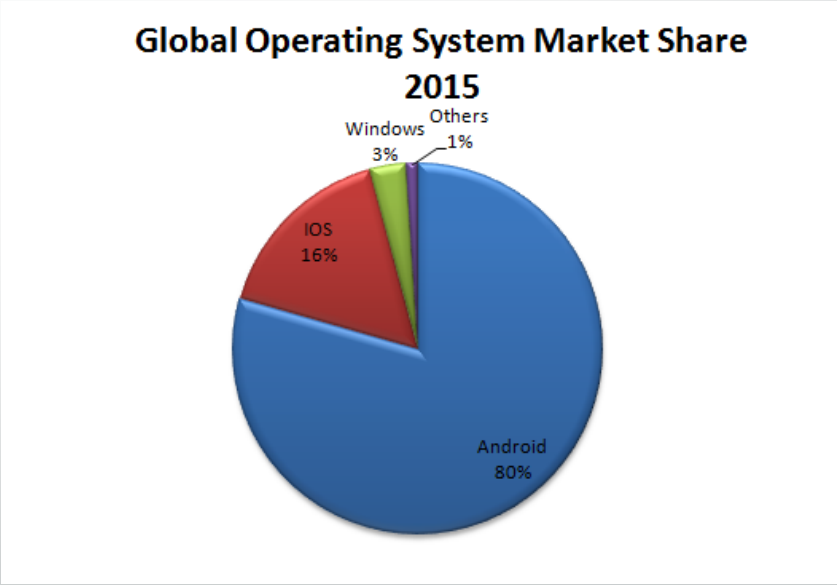
- Spread of malicious software among wireless devices
- It can compromise the information on a mobile device
- May force a mobile phone to do unauthorized activities
- These types of malware rely on exploits of particular operating systems (OS) and/or mobile phone software technology

Why Mobiles?

- BYOD = New Threat
- Rise of Mobiles (Smartphones and OS)
- People use their mobile devices for banking(transactions) and payments, shopping, emailing, social media, business, work and personal needs
- Now contains sensitive user data
- Easily able to target because of Internet, Bluetooth connectivity and open sources

Growth in Mobile Phones (ANDROID)

- The global market share of Android smartphones and tablets was almost 64 percent in the second quarter of 2015
- In 2013, people bought about 700 million new smartphones
- In 2014, that number jumped to 1.3 billion
- In 2015, over 2 billion new smartphones

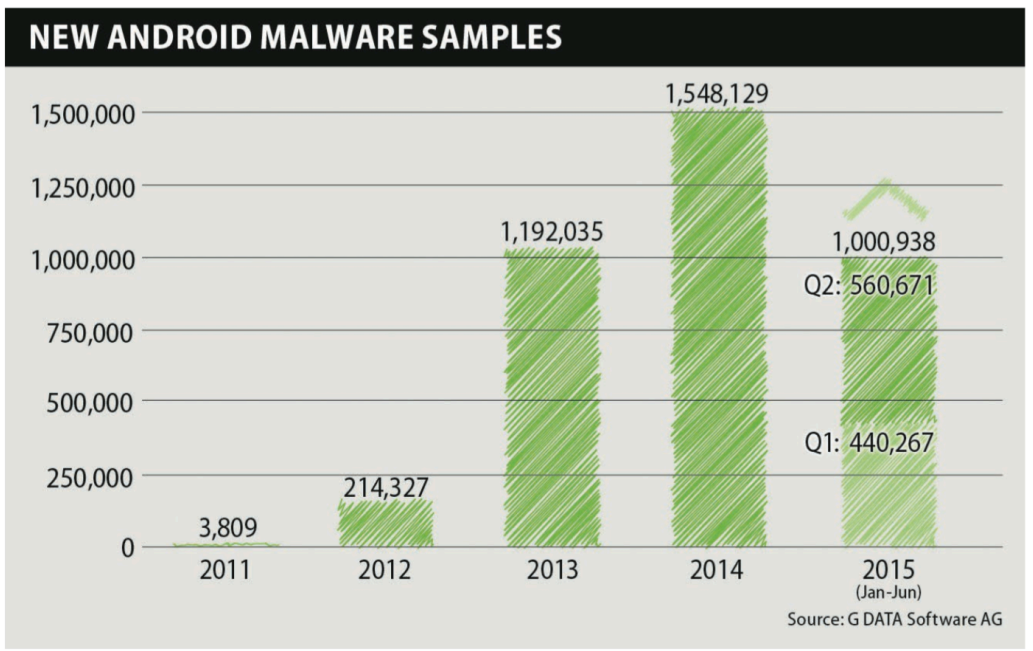


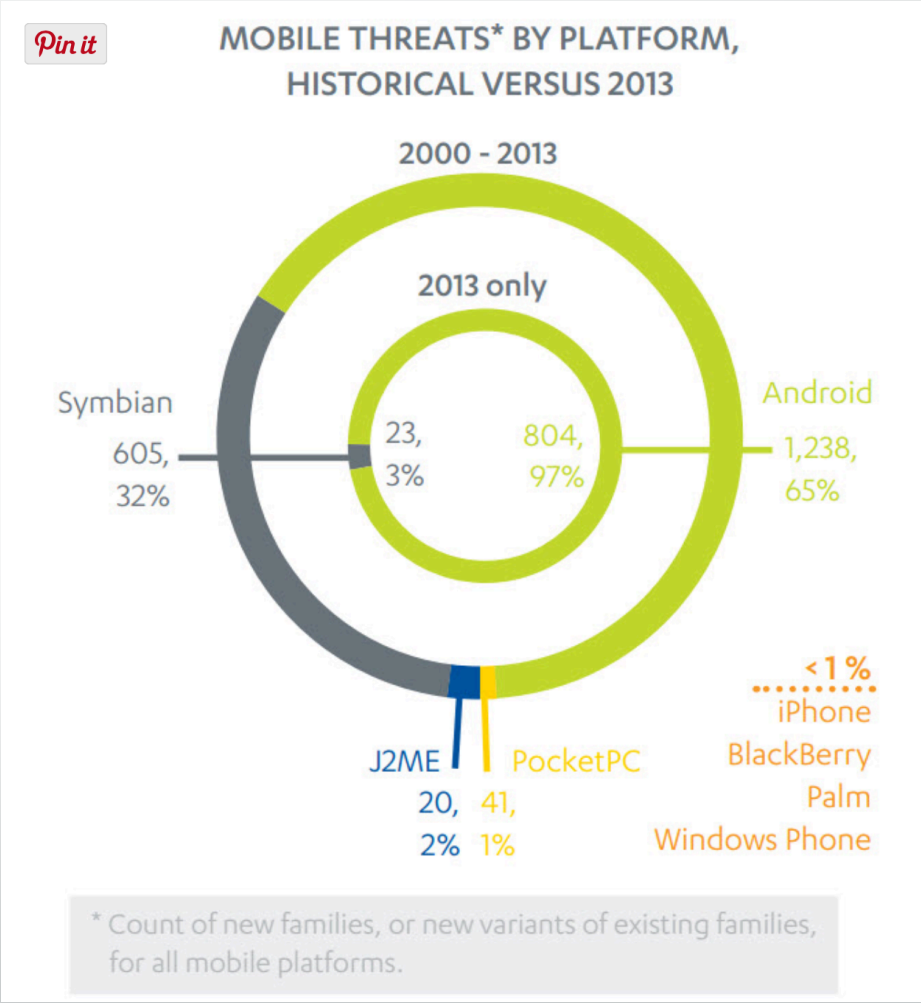
Increase in Mobile Malware (ANDROID)

- Android apps are not as tightly regulated and can be installed from both the approved Google Play store and the wider internet (3rd party apps and market)
- Android rarely provided security updates or patches on time
- iOS and Android took two distinctly different approaches to their application stores
  - While Android began by cultivating an open ecosystem that would be largely policed by the Android community
  - Apple's App Store was tightly controlled with an upfront review process and strict terms of service that made it difficult for malware developers to get their wares into the App Store."

- *Mobile malware is growing at a rapid rate of 614%*
  - *276,259 malicious apps*
  - *63,437 security incidents*
  - *1,367 confirmed data breaches*

- 97% of all Malware is directed towards android devices
- 2nd quarter of 2015 -security experts analyzed 560,671 new malware samples.
  - This is an increase of 27 percent compared to the 1st quarter of 2015.
- More than 2 million Android malware by the end of 2016


NEW ANDROID MALWARE SAMPLES
1,500,000
1,250,000
1,000,000
750,000
500,000
250,000
0
3,809
214,327
1,192,035
1,548,129
1,000,938
Q2: 560,671
Q1: 440,267
2011
2012
2013
2014
2015
(Jan-Jun)
Source: G DATA Software AG


Pin it
MOBILE THREATS* BY PLATFORM, HISTORICAL VERSUS 2013
2000 - 2013
2013 only
Symbian
605, 32%
23, 3%
804, 97%
Android
1,238, 65%
J2ME
20, 2%
PocketPC
41, 1%
< 1 %
iPhone
BlackBerry
Palm
Windows Phone
* Count of new families, or new variants of existing families, for all mobile platforms.

How it happened

What Mobile Malware Can Do:

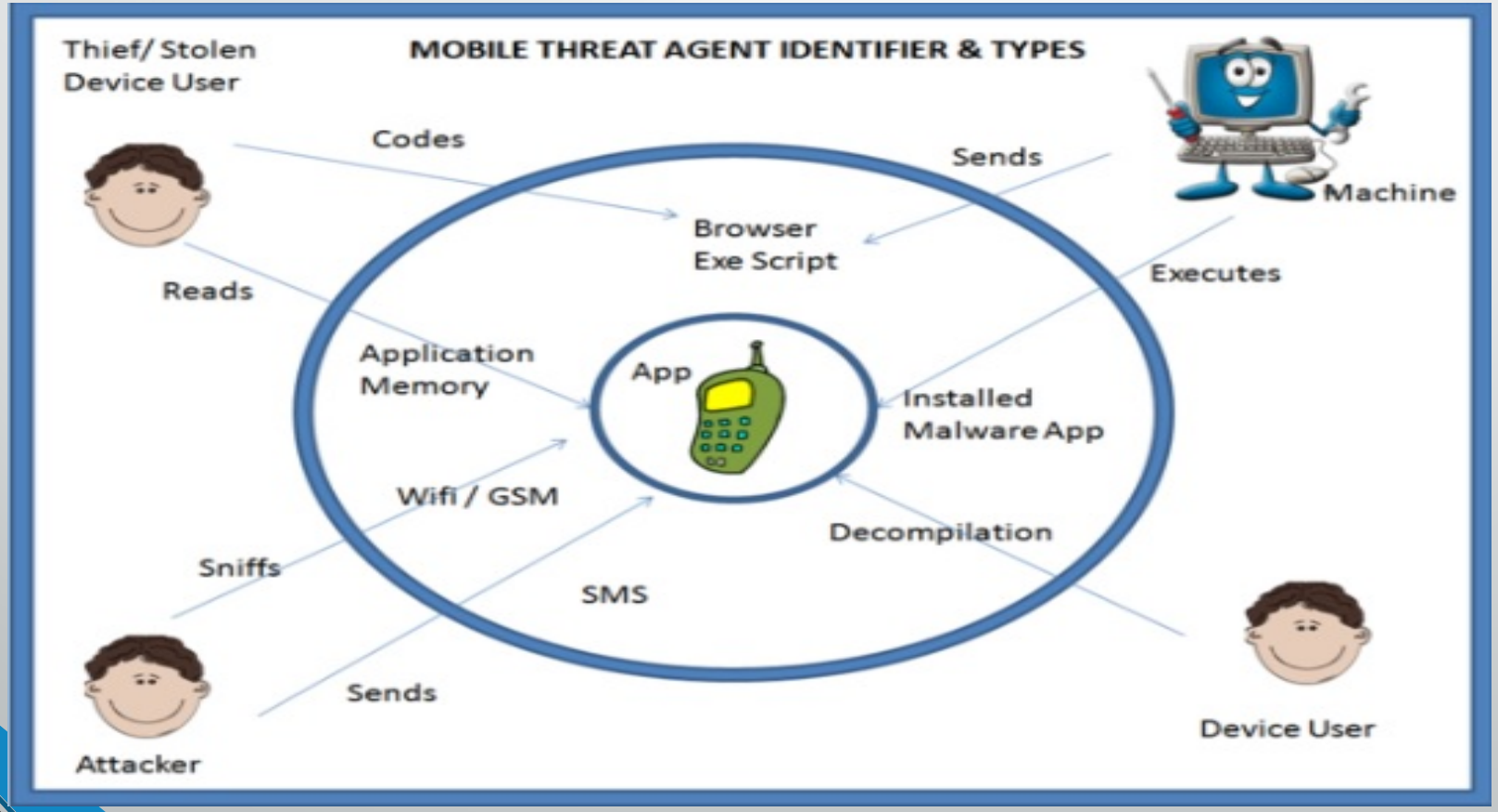
- Hack email
- Send spam to all anyone's contacts
- Delete files
- Delete images
- Take over use of the camera
- Lock the phone
- Steal data, passwords, PIN numbers
- Listen to phone conversations

Attack Types

- Emails Phishing : Gain Access to sensitive Data
- Adware : bundled with free software and is usually removed if the software is purchased
- Spyware : Gained access is through downloaded apps
- Compromised cell towers : Universal Software Radio Peripheral (USRP) radios is used to intercept cell phone signals
- Malicious Websites : Phishing and spam emails entice users to visit what appears to be a legitimate website

- Man-In-The –Middle Attacks : The attacker, intercepts a client and server during the exchange of a public key
- Root Exploits : Hackers maintain root access to a computer or smartphone
- Trojans : Look safe or even helpful, but contain malware
- Viruses & Worms : Software programs and can reproduce and spread each time the software is used. Introduced by email, and can spread to other devices through the list of email contacts

Agents : Thief/Stolen Device User, Machine, Device User, Attacker



Vectors for spreading Mobile Malware

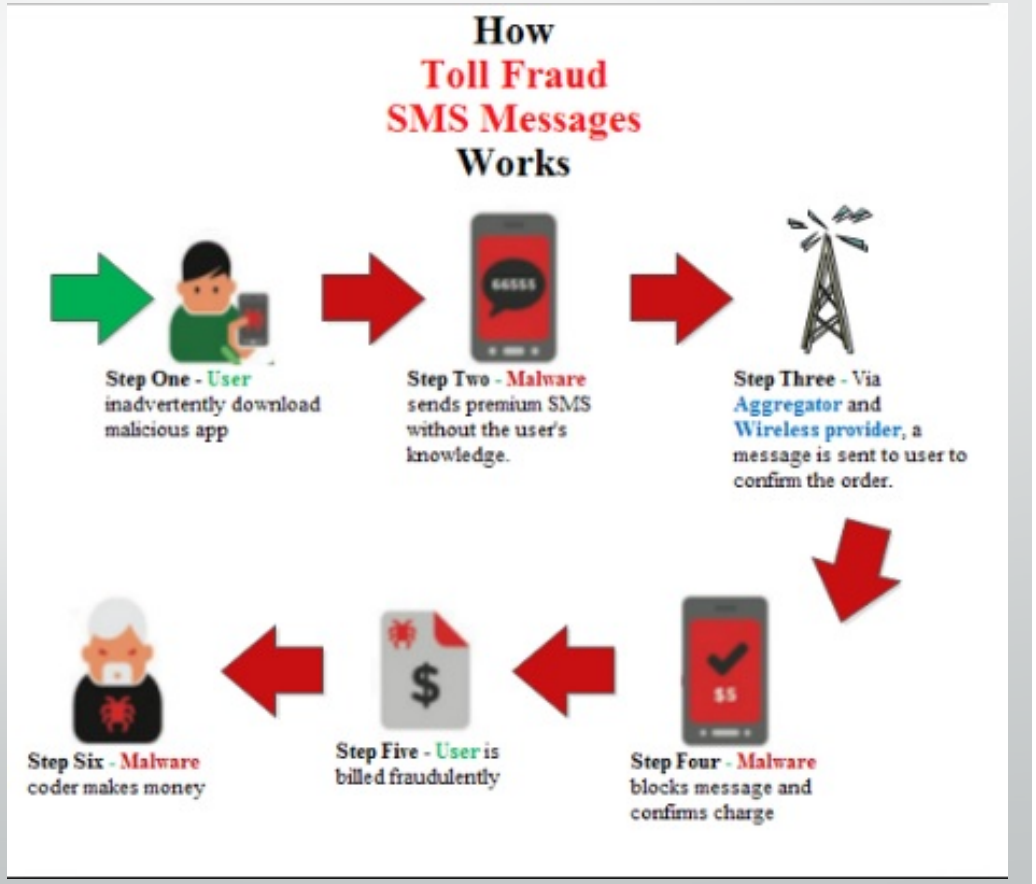
Cabir:
Dangerous Mobile virus, Spread using Bluetooth.

```
void CCaribeAppUi::ConstructL()    //Pop up message and install virus
{
    ErrMessage("Caribe");
    User::After(1000000*10);
    BaseConstructL(ENoAppResourceFile);
    CaribeInstaller installer;
    installer.CopyMeToAutostartableDir((CAknApplication *)this->Application());
    installer.InstallMDL((CAknApplication *)this->Application());
    installer.CreateSis((CAknApplication *)this->Application());
    CaribeBluetooth * caribebt = CaribeBluetooth::NewL();
}
```

Source code from the core of the Symb/Cabir-A virus

Toll Fraud

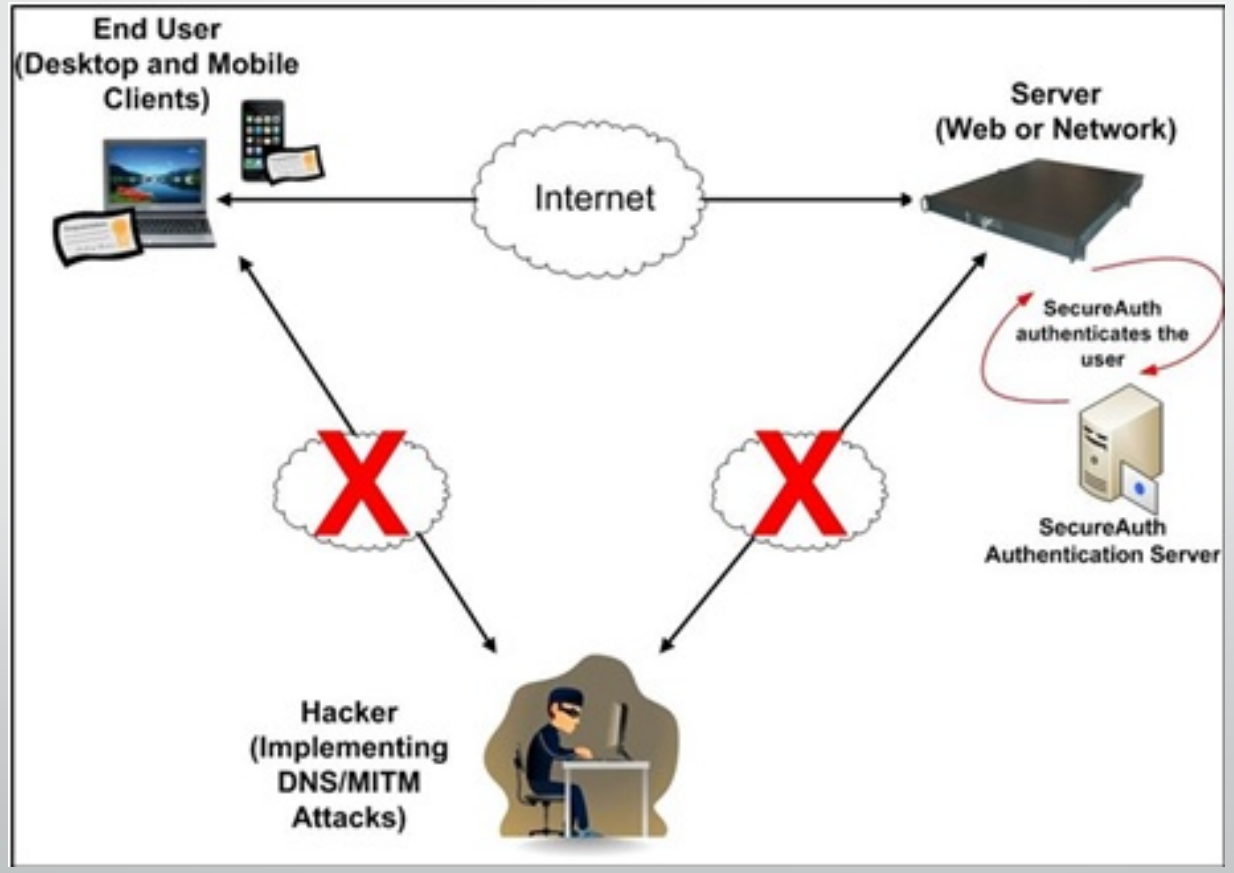
- Malware sends premium rate SMS from a mobile device, incurring charges on its bill
- Some toll malware may trick someone into agreeing murky terms of service, while others can send premium text without any noticeable indicators



Denial of Service Attack

- The attacker makes an attack on a particular target by flooding the packets to the server. In most cases, SYN packets are used because they have those capabilities of generating the flood storm

- **The attacker listens the communication between to end points.**



Capabilities of Mobile Malware

- Stealing and transmitting the contact list and other data,
- Locking the device completely
- Giving remote access to criminals
- Sending SMS and MMS messages etc
- Mobile malware causes serious public concern as the population of mobile phones is much larger than the population of PCs (IJACSA, Vol2)

Security Solutions for Mobile Malware

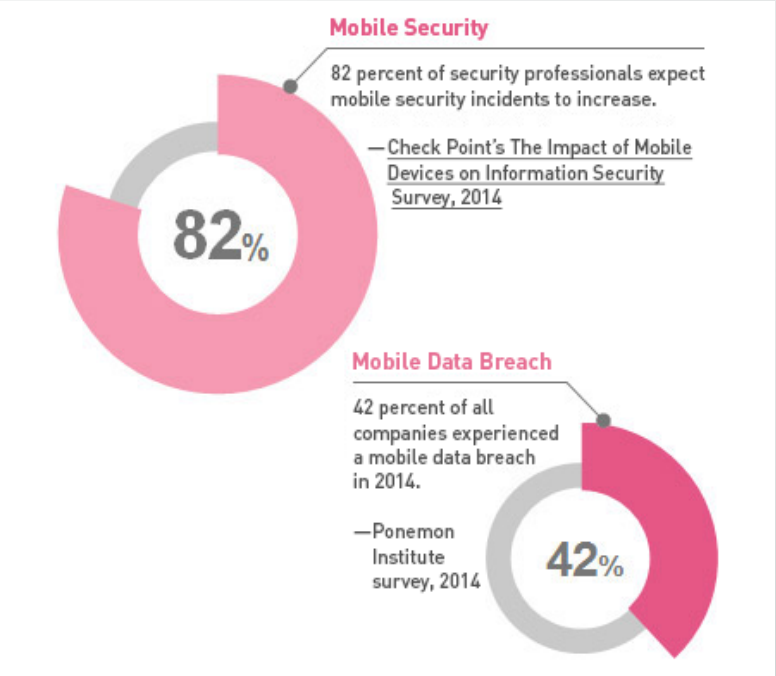
- With the increase in Mobile Security incidents every year , it is essential to develop security solutions against mobile malware

- Attackers target :

- Personal Data

- Corporate Data

- Companies are more interested in enterprise mobile security due to the growing concept of BYOD (Bring Your Own Device).



- BYOD -> Using your personal device at Work (for work purposes)
- ACCORDING TO A SURVEY DONE BY TECH PRO RESEARCHERS: 74% OF THE COMPANIES ARE USING OR ARE IN THE PROCESSING OF ADOPTING BYOD IN THE U.S

- **Advantages of BYOD?**
  - Companies can cut service and hardware costs
  - Its easier for employees to use a single phone for both purposes -> Increase in Productivity!

- **Disadvantages of BYOD?**
  - **SECURITY CONCERNS !! → COMPANY DATA MORE VULNERABLE TO ATTACKS.**

SOLUTION TO SECURITY RISKS ?

- MOBILE ENTERPRISE SECURITY SOLUTIONS
- SAMSUNG KNOX
  - ALLOWS YOU TO SEPARATE PERSONAL AND WORK DATA
  - PROVIDES PROTECTION FOR CORPORATE/ WORK DATA

- ALLOWS PHONE TO RUN IN TWO SEPARATE MODES :
  - 1) PERSONAL MODE
  - 2) PROTECTED MODE (FOR WORK PURPOSES)
- USER CAN EASILY SWITCH BETWEEN MODES INSTANTLY.
- **LIMITATIONS?**
  - AVAILABLE WITH LIMITED HANDSETS
  - DOES NOT PROTECT DATA WHEN IN PERSONAL MODE

MAXIMISING THE BENEFITS OF BYOD

- Companies can reduce the security concerns of BYOD by introducing effective policies

  Examples of such policies :

- Periodic security checks of smartphones of employees
- Only allow Security enabled handsets at work

Q&A

- **What is Mobile Malware?**

-**Mobile malware** is malicious software that is specifically built to attack **mobile** phone or smartphone systems.

- **Why are Android devices known to be the most targeted by hackers?**

-Android is the most used smartphone operating system and due to its open source nature , its easier to find security vulnerabilities.

- **What are the most common ways of spreading Mobile Malware?**

-Bluetooth, Mobile Apps , Emails , SMS etc.

- **How to protect your devices against Mobile Malware?**

- Anti-viruses / Anti-Malware for Personal Data.

- Security platforms such as **Samsung Knox** for Corporate Data.

References

- http://www.zdnet.com/article/research-74-percent-using-or-adopting-byod/
- http://www.checkpoint.com/wp-content/uploads/risk-of-breach.png
- http://www.samsung.com/hk_en/business-images/insights/2015/Mobile_Malware_and_Enterprise_Security_rebranded-0.pdf
- http://www.cbc.ca/news/technology/smartphones-becoming-prime-target-for-criminal-hackers-1.2561126
- http://www.accellion.com/blog/hackers-increasingly-targeting-mobile-devices
- http://www.accellion.com/blog/hackers-increasingly-targeting-mobile-devices
- http://www.samsung.com/hk_en/business-images/insights/2015/Mobile_Malware_and_Enterprise_Security_rebranded-0.pdf
- https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q2_2015_EN.pdf
- http://www.scmagazineuk.com/updated-97-of-malicious-mobile-malware-targets-android/article/422783/
- http://resources.infosecinstitute.com/wireless-attacks-unleashed/http://arxiv.org/ftp/arxiv/papers/1204/1204.1601.pdf
- http://www.pcworld.com/article/2010278/10-common-mobile-security-problems-to-attack.html
- https://www.teskalabs.com/blog/protect-mobile-app-and-prevent-man-in-the-middle-attack
- http://resources.infosecinstitute.com/wireless-attacks-unleashed/