Tu Lam

CS 373 (Defense Against the Dark Arts)

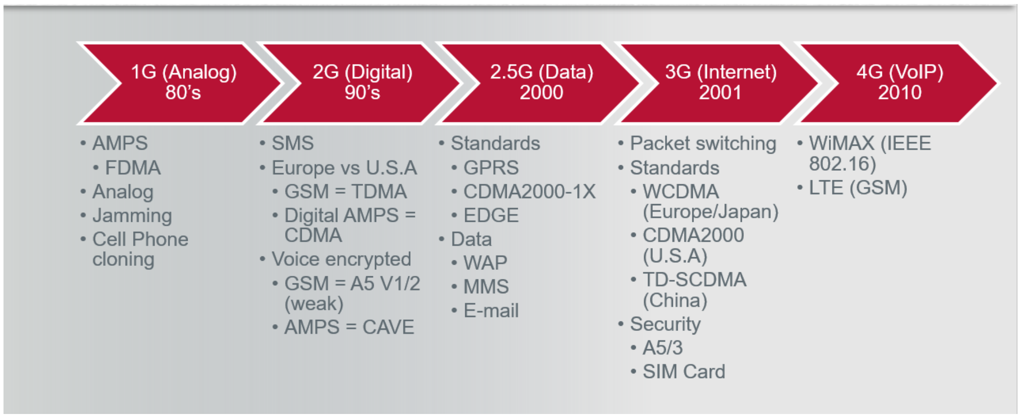
Dr. Bram Lewis

November 22nd, 2021

Homework #9-10 Write-Up

Week #9-10 of the class have a special guest; their name is Fernando Ruiz, and they work at McAfee as a Mobile Malware Researcher. Through this week lecture, we are diving into the concept of ***mobile security***. Moving on from the PC threat, we are looking into that malware threat can be presented through non-PC devices as well, which in this case is our smartphone or tablet. Throughout this week, we will look more into the Android malware and other that might be in store for us.

First, we dive into the ***evolution of mobile device*** and learning about the history of it. We first talk about the Motorola handheld phone in 1973. Then, the first smartphone was released to the public back in 1984 costing a whopping $3,995. Then, we dive into the history of the usage of data and how the first 1G data a started till now with 4G data (This lecture was written back in 2015 as 5G data was not present yet). Below is a screenshot of how the data evolve throughout the timeline.



1G (Analog) 80's
- AMPS
  - FDMA
- Analog
- Jamming
- Cell Phone cloning

2G (Digital) 90's
- SMS
- Europe vs U.S.A
  - GSM = TDMA
  - Digital AMPS = CDMA
- Voice encrypted
  - GSM = A5 V1/2 (weak)
  - AMPS = CAVE

2.5G (Data) 2000
- Standards
  - GPRS
  - CDMA2000-1X
  - EDGE
- Data
  - WAP
  - MMS
  - E-mail

3G (Internet) 2001
- Packet switching
- Standards
  - WCDMA (Europe/Japan)
  - CDMA2000 (U.S.A)
  - TD-SCDMA (China)
- Security
  - A5/3
  - SIM Card

4G (VoIP) 2010
- WiMAX (IEEE 802.16)
- LTE (GSM)

<u>Figure #1</u>: [**From Lecture**] *The timeline of the data usage evolution*

To the next topic, we look at the ***OS (Operating system)*** development, below is an attachment of the timeline of how OS has evolved throughout time and how it changes throughout the year.

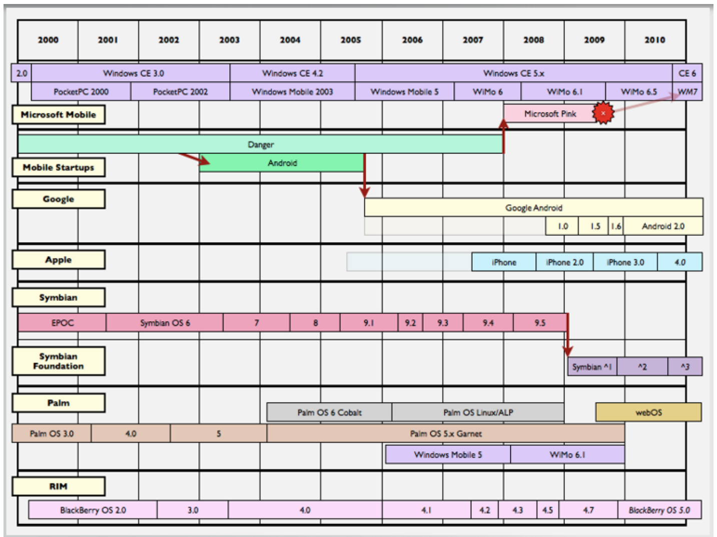


Figure #2: [**From Lecture**] *Timeline of OS system*

OS has been in the game for most of the 21st century in the smartphone world. First, we have the ***iOS*** which came from Apple in 2007, then Microsoft developed their own OS with ***Android***, and there are other competitor's OS such as ***Firefox OS***, ***Tizen***, ***Ubuntu Touch***, and more. With these OS in mind, we will look at ways that hacker uses these OS to break in and modify to the way that they wanted to operate. First, looking at Apple's ***jailbreak*** method, this method purpose is to run software/code not authorized by Apple on their devices. This open the backdoor to their system and make it easy to modify the software on the device. On the Android side, we have ***rooting*** which is a method of getting root privileges in the system. Below is a screenshot laying out how much security has evolved for the Android side with their OS system.

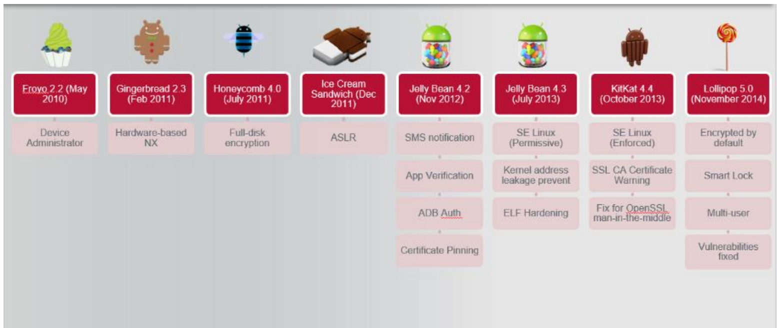
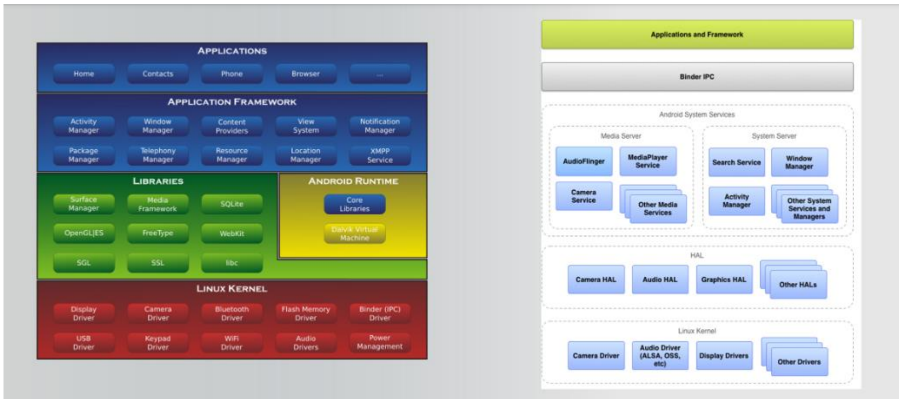

Eroyo 2.2 (May 2010)
Device Administrator
Gingerbread 2.3 (Feb 2011)
Hardware-based NX
Honeycomb 4.0 (July 2011)
Full-disk encryption
Ice Cream Sandwich (Dec 2011)
ASLR
Jelly Bean 4.2 (Nov 2012)
SMS notification
App Verification
ADB Auth
Certificate Pinning
Jelly Bean 4.3 (July 2013)
SE Linux (Permissive)
Kernel address leakage prevent
ELF Hardening
KitKat 4.4 (October 2013)
SE Linux (Enforced)
SSL CA Certificate Warning
Fix for OpenSSL man-in-the-middle
Lollipop 5.0 (November 2014)
Encrypted by default
Smart Lock
Multi-user
Vulnerabilities fixed

Figure #3: [**From Lecture**] *Timeline of Android security evolution*

Moving to ***mobile malware genesis***, we were given a history timeline of malware genesis evolve throughout the early 2000s. Then, we discover more time ranging from the year 2006-2008 with more malwares presenting in those year and then thing subside for a bit in 2008-2010. With the OS software running on mobile devices, the company who created this updated their security to protect against malware genesis, but thing can't be block easily as there were couple of cases of malware presented through those OS as well. We have ***IKEE***, the first iOS malware where its job is to jailbroken iPhones and ask a $5 ransom to remove the malware which discover in November of 2009. Other we can mention on the Android side is the attack of ***FakePlayer***, a malware pretends to be a media player and there is ***Tapsnake*** which involved in tracking GPS coordinates and sends to a remote server. Finally, we then move onto learning about the first Botnet that was found in Android in 2011 which is called ***Geinimi***.

Next, we learn about the ***Android fundamental***, where we learn the basic of Android operation. Below is a representation of how the Android architecture is layout and it layer of functionality wise. Next, we move onto the runtime of Android machine when running a version of 4.4 or greater. In this we see that Android use something called ***Ahead-of-time (AOT)*** compilation to run their software, and added other stuffs on there to improve the Android overall. When using an Android, the application has couple main components that they serve when they are dealing with the public. Those four are ***activities (UI), services, broadcast receivers, and content providers***. Through this we can see the dynamic power of Android and it integrated system when it comes to operating with user and how it works.



<u>*Figure #4*</u>: [**From Lecture**] *Architecture layout of Android*

Through this week, we learn the basic fundamental of mobile security. Learning about their evolution of the mobile devices and how they change throughout the year. Next, we learn about couple malware that was introduce to these mobile devices and how they were a threat to our own system. And finally, discovering way to protect themselves with their own OS system. The content was a good grasp about cybersecurity throughout our every device and we should pay more attention when we are using them so we don't have this problem arise.

References

1. Ruiz, F. (2015, March 11). Mobile Security. Canvas. Retrieved November 22, 2021, from https://canvas.oregonstate.edu/courses/1877198/pages/module-9-10-learning-materials?module_item_id=21556829.