A study on Mobile Communication Devices

Dr. JATINDER KUMAR

Assistant Professor
A.S College, Khanna. Punjab (INDIA)
PG Department of Computer Science and Applications

Abstract

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link. This tutorial will give an overview of Mobile Computing and then it will take you through how it evolved and where is the technology headed to in future along with the classifications and security issues involved.

Mobile Computing is a technology that allows transmission of data, voice and video via a computer or any other wireless enabled device without having to be connected to a fixed physical link.

Keywords: android, wi-fi, smart phone, CDMA, 3G, 4G

Mobile Computing Device (MCD)

Mobile computing devices are generally modern-day handheld devices that have the hardware and software required to execute typical desktop and Web applications. Mobile computing devices have similar hardware and software components as those used in personal computers, such as processors, random memory and storage, Wi-Fi, and a base operating system. However, they differ from PCS in that they are built specifically for mobile architecture and to enable portability.

Among the common examples of mobile computing devices is a tablet PC, which has a built-in processor, memory and operating system (OS), and executes most applications built for a comparable PC.

The Difference Between a Cell Phone, Smartphone and PDA

Falling under the category of mobile devices, today's consumer electronics serve multiple purposes. Years ago, cellular phones, also called cell phone or mobile phone, served one purpose only: They let you send and receive voice communications. Today, mobile phones and similar devices are equipped with customized software, Internet access, digital cameras, portable music players, GPS functions and many more options.

Once again technological advancements make common terminology such as mobile phone, smart phone, PDA and PDA phone difficult to decipher as each type of device changes constantly and features traditionally belonging to one type of device are now found on others. Here we will explore the popular category of mobile communication devices, the similarities and differences between some of the popular products.

What Is a Mobile Phone?

A mobile phone is more frequently called a cellular phone or cell phone. These communication devices connect to a wireless communications network through radio waves or satellite transmissions. Most mobile phones provide voice communications, Short Message Service (SMS), Multimedia Message Service (MMS), and newer phones may also provide Internet services such as Web browsing, instant messaging capabilities and e-mail.

What Is a PDA?

Short for personal digital assistant, this is the name given to small handheld devices that combine computing, telephone/fax, Internet and networking features. A typical PDA can function as a cellular phone, fax sender, Web browser and personal organizer. These devices are usually pen-based, which requires the use of a stylus rather than a keyboard for input. PDAs today are available in either a stylus or keyboard version. Traditionally, PDAs have not had phone or fax services.

What Is a Smartphone?

A smartphone is considered to be the combination of the traditional PDA and cellular phone, with a bigger focus on the cellular phone part. These handheld devices integrates mobile phone capabilities with the more common features of a handheld computer or PDA. Smartphones allow users to store information, e-mail, install programs, along with using a mobile phone in one device. A smartphone's features is usually more oriented towards mobile phone options than the PDA-like features. There is no industry standard for what defines a smartphone, so any mobile device that has more than basic cellphone capabilities can actually be filed under the smartphone category of devices.

What Is a PDA Phone?

It's definitely a lack of standardization that makes the category of mobile devices so confusing to the consumer. As technology changes, so do the functions that these different devices perform. Years ago, many people differentiated PDA and smartphone simply by looking for touch-screen capabilities. If it had a touch screen it was a PDA, if it didn't, it was a smartphone. The Sony Ericsson Smartphone, for example, offers users both a touch screen and a full QWERTY keyboard. Despite the fact that the manufacturer calls this product a smartphone, the generic term for a PDA oriented device with cellular phone capabilities is called a PDA phone.

Fuzzy Lines Between Smart Devices

In summing up the differences between these common mobile communications devices you could say that a PDA phone is more PDA than phone and a smartphone is more phone than PDA. And, of course, a cellular phone is more phone than anything else.

DID YOU KNOW...

The first cellular call was placed on April 3, 1973 by Martin Cooper who was the general manager of Motorola's Communications Systems Division. He made the call to his rival, Joel Engel, Bell Labs head of research.

Mobile technology is the technology used for cellular communication. Mobile code division multiple access (CDMA) technology has evolved rapidly over the past few years. Since the start of this millennium, a standard mobile device has gone from being no more than a simple two-way pager to being a mobile phone, GPS navigation device, an embedded web browser and instant messaging client, and a handheld game console. Many experts argue that the future of computer technology rests in mobile computing with wireless networking. Mobile computing by way of tablet computers is becoming more popular. Tablets are available on the 3G and 4G networks.

The main concept involves –

#Mobile communication #Mobile hardware #Mobile software

Mobile communication

The mobile communication in this case, refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. These would include devices such as protocols, services, bandwidth, and portals necessary to facilitate and support the stated services. The data format is also defined at this stage. This ensures that there is no collision with other existing systems which offer the same service.

Since the media is unguided/unbounded, the overlaying infrastructure is basically radio wave-oriented. That is, the signals are carried over the air to intended devices that are capable of receiving and sending similar kinds of signals.

Mobile Hardware

Mobile hardware includes mobile devices or device components that receive or access the service of mobility. They would range from portable laptops, smartphones, tablet Pc's, Personal Digital Assistants.

These devices will have a receptor medium that is capable of sensing and receiving signals. These devices are configured to operate in full- duplex, whereby they are capable of sending and receiving signals at the same time. They don't have to wait until one device has finished communicating for the other device to initiate communications.

Above mentioned devices use an existing and established network to operate on. In most cases, it would be a wireless network.

Mobile software

Mobile software is the actual program that runs on the mobile hardware. It deals with the characteristics and requirements of mobile applications. This is the engine of the mobile device. In other terms, it is the operating system of the appliance. It's the essential component that operates the mobile device.

Since portability is the main factor, this type of computing ensures that users are not tied or pinned to a single physical location, but are able to operate from anywhere. It incorporates all aspects of wireless communications.

Mobile computing has changed the complete landscape of our day-to-day life. Following are the major advantages of Mobile Computing –

Location Flexibility

This has enabled users to work from anywhere as long as there is a connection established. A user can work without being in a fixed position. Their mobility ensures that they are able to carry out numerous tasks at the same time and perform their stated jobs.

Saves Time

The time consumed or wasted while travelling from different locations or to the office and back has been slashed. One can now access all the important documents and files over a secure channel or portal and work as if they were on their computer. It has enhanced telecommuting in many companies. It has also reduced unnecessary incurred expenses.

Enhanced Productivity

Users can work efficiently and effectively from whichever location they find comfortable. This in turn enhances their productivity level.

Ease of Research

Research has been made easier, since users earlier were required to go to the field and search for facts and feed them back into the system. It has also made it easier for field officers and researchers to collect and feed data from wherever they are without making unnecessary trips to and from the office to the field.

Entertainment

Video and audio recordings can now be streamed on-the-go using mobile computing. It's easy to access a wide variety of movies, educational and informative material. With the improvement and availability of high speed data connections at considerable cost, one is able to get all the entertainment they want as they browse the internet for streamed data. One is able to watch news, movies, and documentaries among other entertainment offers over the internet. This was not possible before mobile computing dawned on the computing world.

Streamlining of Business Processes

Business processes are now easily available through secured connections. Looking into security issues, adequate measures have been put in place to ensure authentication and authorization of the user accessing the services.

Some business functions can be run over secure links and sharing of information between business partners can also take place. Meetings, seminars and other informative services can be conducted using video and voice conferencing. Travel time and expenditure is also considerably reduced.

Trends in mobile computing

Enterprise mobility is driven by the need for seamless access to information anytime, anywhere and from any device. However, mobility has far-reaching effects on the enterprise in areas such as security risk, use policies, manageability and governance. This three-part series on enterprise mobility trends discusses mobility drivers, risks and mobility governance issues and examines how workforce demographics can affect enterprise mobility.

Anytime, anywhere, any device

One of the biggest drivers for enterprise mobility is the need for seamless access to information. Employees have grown accustomed to having ubiquitous information access in their personal lives and expect the same in their professional lives. In the past, employees would try to compartmentalize their personal and work lives in order to protect their personal time from job encroachment. Now, the opposite is true. Many employees move seamlessly between work and personal life and expect that their employers will support this new work paradigm.

Some enterprises struggle to create a business case that quantifies productivity gains and calculates a return on investment for mobility technology. This is very difficult to do, however, and most enterprises simply accept the idea that mobility results in productivity improvement. For many employees, a mobile work environment is now an expectation, analogous to the expectation that their employer will provide a local area network and Internet access. Therefore, many enterprises often deploy mobility technology without any up-front justification or global planning.

Data Leakage

The most profound risk to enterprise mobility is data leakage on mobile devices. Once a user transfers sensitive data to a mobile device, that data can be compromised if the device is lost or stolen, or the data is transferred to another device. This concern is exacerbated by the fact that the design of most mobile devices is driven by the needs of consumers rather than businesses and therefore is often unsuitable for the enterprise. Lastly, the mobile device has become the new network perimeter, so enterprises can no longer simply rely upon firewalls in order to lock down their sensitive information.

Some organizations have a policy that requires users to encrypt sensitive data on a laptop hard drive, but few organizations encrypt sensitive data stored on handheld devices. This means that sensitive data on a handheld is often more vulnerable to theft. In the event of a lost or stolen mobile device, many enterprises will remotely "wipe" the device, thereby removing sensitive information. Some vendors, such as Research In Motion (RIM), enable the IT manager to remotely disable the mobile device and restore it to factory defaults. Some enterprises have invested in technology to find lost or stolen laptops, such as Computrace's LoJack for Laptops product.

Many organizations encrypt sensitive information that is transmitted between the mobile device and enterprise servers by using virtual private network (VPN) technology. This "in transit" encryption is typically performed while users communicate on the road or at home. A few organizations even enforce the use of VPNs while users communicate over the office wireless LAN (WLAN).

Although many organizations enforce the use of two-factor authenticationon laptops, handheld authentication policies lag behind laptop authentication policies. For example, many organizations require a simple four-digit personal identification number (PIN), or no password at all. If a handheld device does not have a password and is lost or stolen, any sensitive data stored on it is easily accessible. The small size of handheld devices makes it easy for them to fall out of a pocket or purse and thus to become a security risk.

Data leakage on mobile devices is a major risk for almost every enterprise. Unfortunately, handheld security policies often lag behind similar laptop security policies. This can result in security breaches and increased legal liability. Enterprises must carefully evaluate their risk tolerance and then secure sensitive information before granting mobile device access privileges to users.

Mobile policies and governance

Mobility governance refers to the people, processes and policies associated with mobility deployment within the enterprise. With few exceptions, enterprise mobility deployment is reactive and tactical. The lack of a corporate mobility strategy results in the deployment of incompatible point solutions, coordination issues and inconsistent policies.

In addition, most enterprises have no coordinated approach to mobility funding. This includes decisions to deploy a wireless LAN, purchase mobile devices, and select mobile cellular service plans. Some managers demand that business case analysis be applied to the decision-making process for such things as wireless deployment and social networking implementation. IT managers often express frustration over the difficulty of developing a business case for mobility products and services. Other managers go to the other extreme and simply mandate mobility technology deployment without any upfront analysis.

Personal-use policies on handheld devices often vary widely. Some enterprises prohibit personal calls, forcing employees to carry two phones -- one for business use, the other for personal calls. Others allow personal phone calls only if employees do not exceed their minutes-of-use plan. Some enterprises have a "no text messaging" policy, although it is unclear how that policy can be enforced if the employee owns the phone.

Similarly, handheld ownership policies vary widely. Most enterprises allow only company-owned devices to access the network. Some allow personal laptops to access the network when using an enterprise-provided USB key that contains an approved bootable image.

Enterprises often struggle to balance the needs of IT staff to secure and manage mobile devices with the desire of employees to use mobile devices whenever and wherever they want. Some organizations opt for a laissez-faire approach that provides users with broad device usage and ownership flexibility. However, this approach often exposes the enterprise to inordinate security and legal risk. Alternatively, concerns over insufficient mobility security and management, coupled with the lack of coherent mobility governance, cause many IT organizations to simply reject user demands for greater mobility solutions. This approach can lead users to find ways to bypass the IT staff and enterprise policies.

Some enterprises are using the Information Technology Infrastructure Library (ITIL) for mobility service management. ITIL is a widely adopted framework for IT service management. ITIL can help organizations create a mobility strategy, personal-use policies, security best practices, and funding procedures.

Recommendations

Enterprises should consider the following recommendations:

Embrace mobility as a strategic initiative rather than simply a technology purchase decision.

Consider applying the ITIL concepts and policies to the challenge of enterprise mobility.

Consistently adhere to security best practices, and avoid making exceptions to security policies.

Enterprises often deploy mobility in an ad hoc, department-by-department fashion, in much the same way that local area network technology was deployed in the mid-1980s. Such an approach results in coordination issues, incompatible point solutions, inconsistent policies, increased security risk, and costly mistakes. Enterprises can avoid many of these problems if they embrace mobility as a strategic initiative, consider applying ITIL concepts, and consistently adhere to security best practices.

References:

- *Pahlavan, Kaveh; Levesque, Allen H (1995). Wireless Information Networks. John Wiley & Sons.* ISBN 0-471-10607-0.
- *Geier, Jim (2001). Wireless LANs. Sams.* ISBN 0-672-32058-4.
- Murthy, M. V. R. (2008). Mobile based primary health care system for rural India. W3C workshop on Role of Mobile Technologies in Fostering Social Development, Jun 2008

- Security of the Internet (The Froehlich/Kent Encyclopedia of Telecommunications vol. 15. Marcel Dekker, New York, 1997, pp. 231–255.
- Security Threat Mitigation and Response: Understanding CS-MARS, Dale Tesch/Greg Abelar, Cisco Press, Sep. 26, 2006