Scopri cosa c'è dentro al tuo *smartphone*

Giovanni Zorzoni

Mynet

Negli anni ‘80 e ‘90..

Off-the shelf / merchant silicon

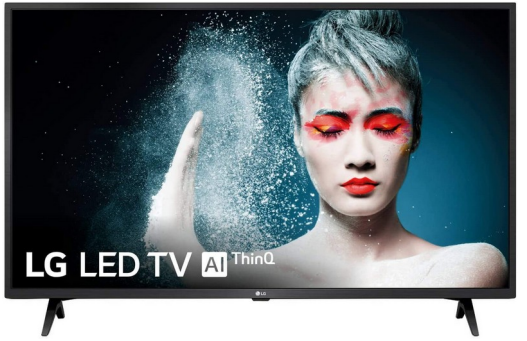
Verticalmente integrato

Da metà anni 2000: ibridazione

Limitato livello di integrazione verticale

Alto contenuto di integrazione verticale

Oggi, 2022



Oggi, 2022: comune denominatore

ARM® POWERED

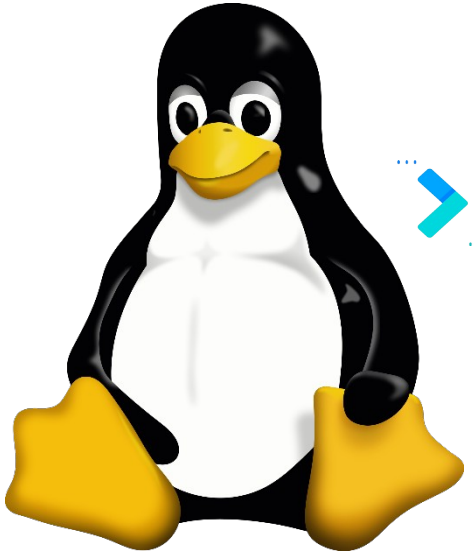
UNIX

00011110 00011110 00011110 00011110 00011110 00011110 00011110 00011110

NetBSD

Oggi, 2022: comune denominatore

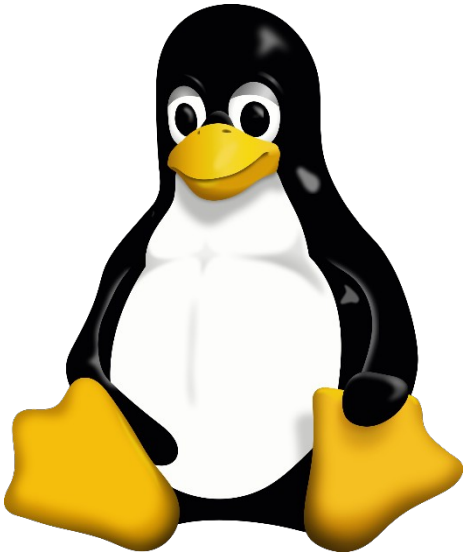
- Il 90% dei processori in tutti i dispositivi sono derivati ARM



- Il 90% di tutti i dispositivi basati su ARM usano sistemi operativi basati su Linux

LUGMan

Cos’è Linux?

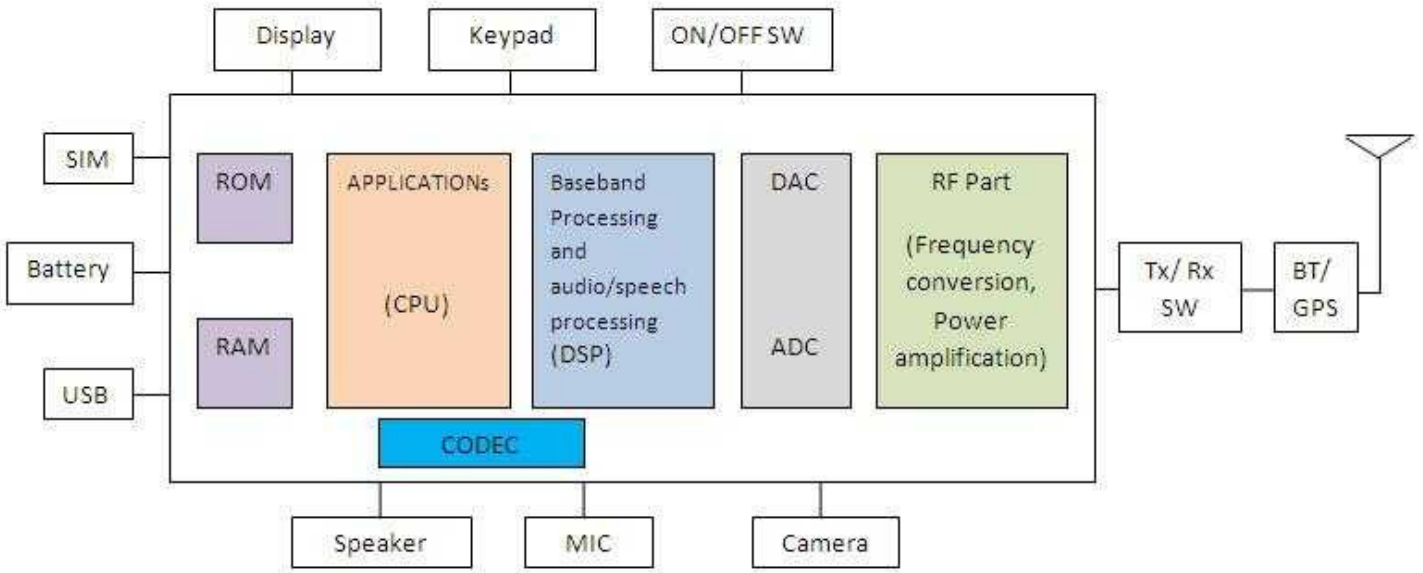


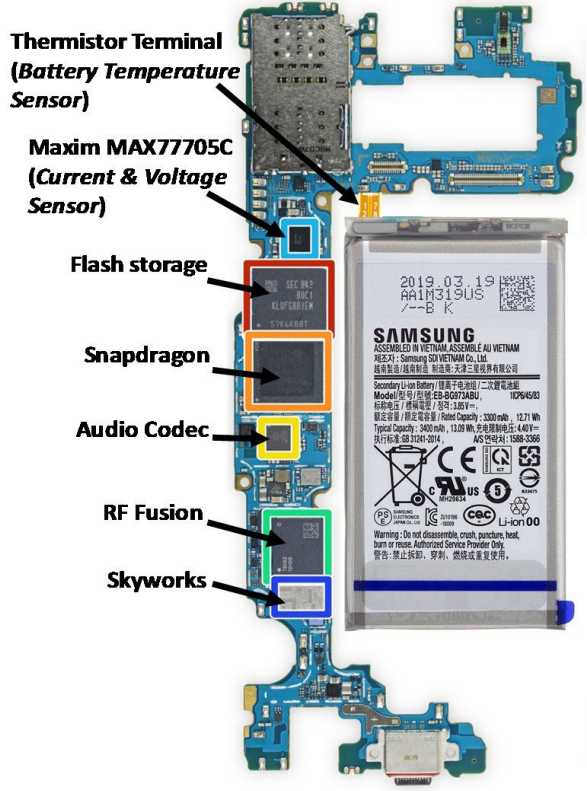
E’ un kernel, base di un sistema operativo, una sorta di «primo programma» che permette a tutti gli altri programmi di funzionare, di non darsi fastidio, e di collaborare al fine di garantire le funzionalità desiderate di un dispositivo complesso.

Linux è presente su forni a microonde, telefoni, router ad alta velocità per Internet, televisori, cruscotti e sistemi di intrattenimento per auto, set-top box (Sky, Amazon Stick, Nvidia Shield), oscilloscopi……

……e… smartphone Android!

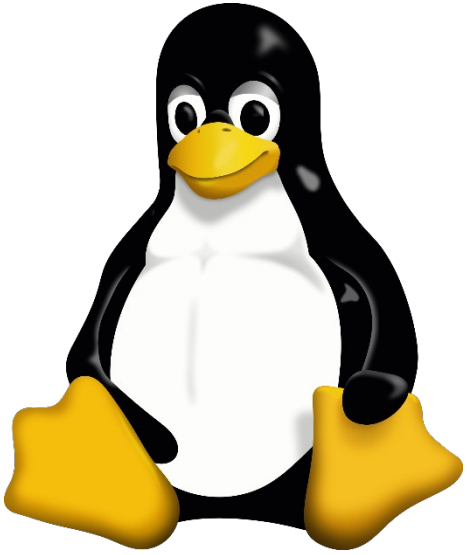
Dai telefoni DCT3 Nokia agli smartphone di oggi: in 25 anni nulla è cambiato





L’evoluzione hardware permette sistemi operativi più complessi

E’ stato possibile abbandonare le tastiere fisiche, introdurre fotocamere e schermi migliori, innovazioni degli standard 3GPP (3G, 4G e LTE+, 5G da BTS e da microwave, ..), WLAN e bluetooth avanzati, sistemi di sicurezza.



I sistemi complessi sono sempre meno personalizzabili dagli utilizzatori

L’uso distorto del «gratis» (tracer, GPS, applicazioni che salvano sempre il contenuto dei dati altrove), sistemi a controllo vocale (quasi) always on, il fingerprint degli utenti..

Come riprendere il controllo?

Jaibraking o Rooting!
(e, per piccoli risultati, side-loading)

Rooting

Da Wikipedia, l'enciclopedia libera.

Il **rooting** è un processo informatico che permette agli utenti di smartphone, tablet o altri dispositivi dotati di sistema operativo Android di ottenere controlli privilegiati (conosciuti come permessi di root) su vari sottosistemi Android. Poiché il sistema utilizza il kernel Linux, *rootare* un dispositivo Android offre l'accesso ai permessi amministrativi (superutente) come se ci trovassimo su Linux o su qualsiasi altro sistema operativo Unix-like, ad esempio FreeBSD o MacOS.

Il rooting viene generalmente eseguito per superare i limiti che gli sviluppatori ed i tecnici hardware hanno impostato sul dispositivo. In questo modo l'utente è in grado di modificare le impostazioni di sistema, installare app che richiedono permessi da amministratore, rimuovere o sostituire il sistema operativo ed eseguire ogni altra operazione altrimenti inaccessibile per un normale utente Android.[1]

Sideloading

From Wikipedia, the free encyclopedia

Sideloading describes the process of transferring files between two local devices, in particular between a personal computer and a mobile device such as a mobile phone, smartphone, PDA, tablet, portable media player or e-reader.

Sideloading typically refers to media file transfer to a mobile device via USB, Bluetooth, WiFi or by writing to a memory card for insertion into the mobile device, but also applies to the transfer of apps from web sources that are not vendor-approved.

When referring to Android apps, "sideloading" typically means installing an application package in APK format onto an Android device. Such packages are usually downloaded from websites other than the official app store Google Play. For Android users sideloading of apps is only possible if the user has allowed "Unknown Sources" in their Security Settings.[1]

When referring to iOS apps, "sideloading" means installing an app in IPA format onto an Apple device, usually through the use of a computer program such as Cydia Impactor,[2] Xcode, on the actual device using a jailbreak method or using a signing service instead of through Apple's App Store. On modern versions of iOS, the sources of the apps must be trusted by both Apple and the user in "profiles and device management" in settings; except when using jailbreak methods of sideloading apps. Sideloading is not allowed by Apple except for internal testing and development of apps using the official SDKs. [3]

- Eliminare la pubblicità sulle vostre smart-TV in sovraimpressione durante i programmi
- Eliminare la pubblicità su Youtube sui vostri smartphone
- Mettere in atto una serie di modifiche del sistema operativo per disattivare molti dei sistemi di «telemetria» presente sui dispositivi
- Dare nuova vita e funzionalità a vecchi dispositivi (es. un vecchio smartphone può diventare una security cam, un termostato smart, ..)
- Accertarvi che terze parti non abbiano inserito dei software malevoli nel dispositivo

https://rada.re/

Sweet, old
GNU Debugger

```
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from zte-led...
(No debugging symbols found in zte-led)
(gdb) b main
Breakpoint 1 at 0x10645
(gdb) disassemble
Dump of assembler code for function main:
   0x00010645 <+0>:     mov    $0x0,%ch
   0x00010647 <+2>:     scas   %es:(%edi),%eax
   0x00010648 <+3>:     and    %cl,0x7b(%ebx)
   0x0001064b <+6>:     inc    %esp
   0x0001064c <+7>:     sbb    %al,0x8(%esi)
   0x0001064f <+10>:    lock inc %edi
   0x00010651 <+12>:    cld
   0x00010652 <+13>:    add    %ah,(%ecx)
   0x00010654 <+15>:    dec    %edi
   0x00010655 <+16>:    hlt
   0x00010656 <+17>:    add    %eax,-0x1(%eax)
   0x00010659 <+20>:    notl   -0x1(%edx)
   0x0001065c <+23>:    add    %esp,(%eax)
   0x0001065e <+25>:    adc    $0x1bfc41f0,%eax
   0x00010663 <+30>:    dec    %ebx
   0x00010664 <+31>:    jnp    0x106aa <main+101>
   0x00010666 <+33>:    sbb    %al,0x8(%esi)
   0x00010669 <+36>:    lock cmp %ah,%bh
   0x0001066c <+39>:    dec    %edi
   0x0001066d <+40>:    hlt
   0x0001066e <+41>:    gs inc %eax
   0x00010670 <+43>:    push   %edi
--Type <RET> for more, q to quit, c to continue without paging--
```

Hey, *objdump* anyone?

A software reverse engineering (SRE) suite of tools developed by NSA's Research Directorate in support of the Cybersecurity mission

https://ghidra-sre.org/

Cercate su Internet e troverete un mondo da esplorare.. e veniteci a trovare più spesso per qualche esperimento insieme..