Journal of New Achievements in Electrical, Computer and Technology
Vol. 2, No. 3, Jun-Sep 2022,(1-7)
WWW.JNAECT.IR

مجله دستاوردهای نوین در برق،کامپیوتر و فناوری
دوره ۲، شماره۳، تابستان ۱۴۰۱ (۷-۱)

مزایای فنی و امنیتی طرح ریجستری موبایل

مهرداد قادری[1*]

۱- کارشناسی ارشد مکاترونیک، دانشکده فنی ومهندسی دانشگاه محقق اردبیلی،اردبیل، Mehrdadghaderi254315@gmail.com

چکیده

امروزه تکنولوژی روزبه روز درحال پیشرفت میباشد. که دنیای ارتباطات بخش عظیمی از تکنولوژی را در دل خود قرار می دهد. اینترنت، شبکه های اجتماعی، تماس تلفنی، جزوی از دنیای ارتباطات محسوب میشوند. که مهمترین واصلی ترین بخش از این موارد دستگاه موبایل میباشد. این پیشرفت نیز دارای جوانب امنیتی زیادیاست. که در این مقاله ما قصد داریم در خصوص کدIMEIموبایل را مورد بررسی قراردهیم. و طرح ریجستری موبایل در ایران را از نظر جوانب امنیتی مورد بررسی کنیم که دارای چه مزایا و معایبی میباشد. همچنین استفاده از یک چارچوب مدیریت هویت غیر متمرکز را برای پیاده سازی سیستمی برای مقابله با جعل تلفن‌های هوشمند بررسی می‌کند که ویژگی‌های ایجاد هویت و انتقال مالکیت را همراه با قابلیت سریع و ایمن ارائه می‌کند. و ازطرفی گزارش وسایل دزدیده شده و افراد نا امن کننده بستر ارتباطات در کوتاه ترین زمان مورد پیگیری قرار میگیرد.

واژه‌های کلیدی: ریجستری موبایل، امنیت ارتباطات،IMEI

.

۱. مقدمه

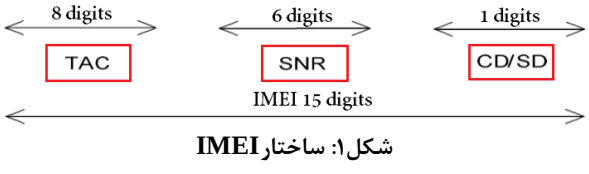
پیشرفت‌های فناوری در صنعت دستگاه‌های تلفن همراه منجر به استقرار گسترده آن و تکیه بر آنها در انجام اکثر کارهای روزمره مانند گشت و گذار در اینترنت، خواندن ایمیل، خرید و حتی انجام تراکنش‌های بانکی شده است. به دلیل اهمیت محتویات آنها نسبت به حجم کم و همچنین قیمت بالای آنها، هدف سرقت هایی قرار گرفته اند که به مرور زمان در حال افزایش است. از طرفی نیز افراد سود جو و مختل کنندگان آرامش زندگی مردم یا اصطلاحا مزاحمان تلفنی یکی از روش های که برای جلوگیری از شناسایی خود استفاده میکنند این است که قبل از شناسایی موبایل خود را عوض میکنند. تا رد پایی از خود نگذارند. همچنین علیرغم تلاش زیاد برای بازیابی موبایل های دزدیده شده، بسیاری از دستگاه های سرقتی پیدا نشدند، زیرا هویت (IMEI) دستگاه دزدیده شده معمولاً توسط سارق تغییر می کند. اگرچه تغییر شماره IMEI در برخی از کشورها مانند انگلستان یا داشتن ابزارهای مورد استفاده برای این منظور جرم قابل مجازات تلقی می شود. همچنین، کشورهای دیگر مانند کلمبیا برای تأیید اعداد IMEI در شکل، به یک پایگاه داده متمرکز و سیستم تأیید تکیه می کنند. ۱ تعداد دستگاه هایی را نشان می دهد که در بازه زمانی ۲۰۱۶ تا ۲۰۱۷ مسدود شده اند[۱]. با این حال، تغییر IMEI تلفن های همراه، و ردیابی گوشی های گم شده و ردیابی مجرمان و نا امن کنندگان را به موضوعی حیاتی و چالش برانگیز برای ادارات امنیتی تبدیل می کند. بنابراین، وجود روشی برای جلوگیری هرچه بیشتر موارد امنیتی. این مقاله به شرح طرح ریجستری وموارد پیرامون آن تنظیم شده است.

۱-۲- پیشینه:

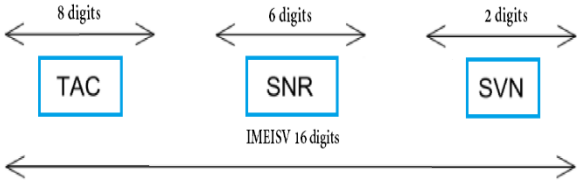
اولین سوال این است که کد IMEIچیست؟

شناسه بین المللی تجهیزات موبایل یا شماره سریال گوشیInternational Mobile Equipment Identity که به اختصار(IMEI) گفته میشود. یک شناسه منحصر به فرد است که همه دستگاه های تلفن همراه در جهان را شناسایی می کند. که شامل ۱۵ رقم اعشاری است که بسته به تعداد اسلات های سیم کارت ممکن است ۱یا۲ یا تعداد بیشتریIMEIداشته باشد که مشخص می کند: مبدا تلفن، مدل تلفن و شماره سریال تلفن. شناسه تجهیزات بین‌المللی موبایل و شماره نسخه نرم‌افزار (IMEISV)، که از ۱۶ رقم اعشاری تشکیل شده است، همچنین می‌تواند به عنوان هویت تلفن همراه مورد استفاده قرار گیرد[۱][۲].

در تصاویر۱و۲ زیر به ترتیب ساختار IMEI و IMEISV را نشان داده شده است. علاوه بر این، ما هر بخش از هر دو ساختار را در تصویر۳توصیف کرده ایم. همچنین به ساختاری که شامل این بخش است اشاره کرده ایم[۳][۴].



شکل۱: ساختار IMEI



شکل۲: ساختار IMEISV

Part	IMEI/IMEISV		
	Description	*IMEI*	*IMEISV*
TAC	Type Allocation Code: مدل دستگاه را مشخص می کند	✓	✓
SNR	یک شماره منحصر به فرد است.که هر دستگاه را درTACشناسایی میکند	✓	✓
CD/SD	Check Digit/Spare Digit برای اعتبار سنجی شمارهIMEI دریافتی استفاده میشود	✓	×
SVN	Software Version Number شماره نسخه نرم افزار تجهیزات موبایل را مشخص می کند	×	✓

شکل۳: تشریح بخش های IMEI/IMEISV

کد های IMEIموبایل را می توان بر روی جعبه بسته بندی آنها دید همچنین در تمامی مدل های موجود در بازار با شماره گیری کد#06#*میتوان بصورت اتوماتیک شمارهIMEIموبایل را مشاهده کرد که درشکل۴نشان داده شده است[۱][۵].

شکل۴:نحوه شماره گیری کد#06#*

همچنین روش های دیگر برای بدست آوردن کد هایIMEIوجود دارد که یکی دیگر از این روش ها ورود به قسمت تنظیمات گوشی و سپس ورود به قسمت اطلاعات موبایل میباشد.

موارد استفاده از IMEI را میتوان به موارد زیر اشاره کرد:

- این شناسه در موقعیت‌هایی استفاده می‌شود که نیاز به تعریف منحصربه‌فردی از دستگاه تلفن همراه دارد، از جمله موارد زیر:

برای شناسایی منحصر به فرد دستگاه های متصل به یک شبکه سلولی برای تنظیم انتقال داده بین دستگاه های شبکه استفاده می شود.

- به اپراتورها کمک می کند تا تعیین کنند که نرم افزار کدام دستگاه ها باید برای بهبود عملکردشان به روز شوند یا نیاز به فراخوانی دارند .
- توسط IMEI می توان دستگاه دزدیده شده را پیدا کرد یا از استفاده از خدمات شبکه تلفن همراه جلوگیری کرد .
- برخی از برنامه ها از IMEI برای شناسایی مکان دستگاه تلفن همراه و وضعیت اینترنت استفاده می کنند.
- می توان از آن برای توسعه راه حل های احراز هویت قوی استفاده کرد.

درموارد ذکر شده مختصری از موارد استفاده از شماره سریال گوشی های همراه را بیان کردیم[۶][۱][۷].

-راه حل های پیشنهادی امنیتی

برخی از محققان، پیشنهاد کرده اند که ساختار IMEI را تغییر داده و بر اساس کشور برای کمک به یافتن دستگاه های گمشده تخصیص داده شود. همچنین، پیشنهاد دادند که به یک سیستم GPS یک شناسه منحصر به فرد داده شود. سپس آن دو شناسه را نقشه برداری کنید و یک چک جمع را محاسبه کنید که در یک ثبات قابل برنامه ریزی ذخیره می شود. با این حال، ما معتقد نیستیم که تغییر ساختار IMEI یک ایده عملی است زیرا اعمال آن برای دستگاه هایی که در حال حاضر در دست مصرف کننده هستند، دشوار است. اما شناسایی جی پی اس برای یافتن گوشی گمشده در صورتی که سارق سیم کارت را خارج کند مفید خواهد بود[۱][۴].

علاوه بر این، آنها پیشنهاد کردند که شناسه GPS در کنار IMEI در پایگاه داده GSM ذخیره شود. جایی که ادعا می کنند که اگردزد IMEI را تغییر می دهد، سیستم می تواند آن را شناسایی کرده و اطلاعات خود را به پلیس اطلاع دهد. اما اگر دزد راهی برای تغییر شناسه GPS پیدا کند چه می شود[۱۰].

همچنین پیشنهاد بهبود الگوریتم Luhn را پیشنهاد کردند که برای اعتبارسنجی IMEI یا شماره کارت اعتباری استفاده می‌شود. آنها پیشنهاد کردند که یک رقم چک جمع در انتهای IMEI یا شماره کارت اعتباری اضافه شود. همچنین، آنها پیشنهاد کردند یک مرحله دیگر به الگوریتم برای تأیید چک‌سوم اضافه شود. آنها ادعا می کنند که پیشنهاد آنها نیاز به شخص ثالث برای انجام فرآیند تأیید را برطرف می کند. با این حال، همانطور که قبلا ذکر کردیم، تغییر ساختار شماره IMEI یک راه حل غیر عملی است[۱۱].

همچنین برخی از محققین دیگر نیز ثبت شماره IMEI و اثر انگشت هر گوشی را در پایگاه داده سازنده آن پیشنهاد کرد. این پایگاه داده برای تأیید اعتبار شماره IMEI هر بار که کاربر سعی می کند به شبکه تلفن همراه پیوند دهد، مورد اعتماد است. با این حال، پایگاه داده مرکزی ممکن است خراب شده باشد، و داده های ارسال شده در طول فرآیند تأیید نیز می توانند دستکاری شوند[۱۰].

به طور مشابه، برخی دیگر از محققان ایجاد پایگاه داده ای را توصیه کردند که اعداد IMEI را برای تلفن های همراه با قابلیت های مشترکشان حفظ کند. این پایگاه داده برای تأیید جعلی نبودن دستگاه مورد اعتماد است. با این حال، نویسندگان قادر به تصمیم گیری در مورد فرآیند اجرای پایگاه داده نیستند. آنها اشاره کردند که دو راه وجود دارد: ۱) ایجاد یک راه جدید اما جمع آوری اطلاعات از فروشندگان دشوار خواهد بود. ۲) استفاده از پایگاه داده فعلی IMEI اما اطلاعات کافی ندارد.

بر همین اساس برخی دیگر از نویسندگان ادعا می کنند که روش پیشنهادی آنها اولین روشی است که اعداد IMEI جعلی را با بررسی تصویر روی بسته بندی موبایل تشخیص می دهد. این روش واریانس و وزن اجزای رنگ تصویر را تخمین می‌زند تا مکان‌هایی را که در تصویر IMEI دستکاری شده‌اند و تقلبی بودن آن‌ها را تشخیص دهد. این کار فقط بر روی شناسایی دستگاه‌های تقلبی از طریق بررسی تصویر IMEI روی بسته‌بندی دستگاه متمرکز بود و به شناسایی شماره‌های IMEI تقلبی متصل به شبکه تلفن همراه کمکی نمی‌کند[۱۲].

همچنین نویسندگان در[۱۳] ادعا می کنند که روش پیشنهادی آنها اولین روشی است که اعداد IMEI جعلی را با بررسی تصویر روی بسته بندی موبایل تشخیص می دهد. این روش واریانس و وزن اجزای رنگ تصویر را تخمین می‌زند تا مکان‌هایی را که در تصویر IMEI دستکاری شده‌اند و تقلبی بودن آن‌ها را تشخیص دهد. این کار فقط بر روی شناسایی دستگاه‌های تقلبی از طریق بررسی تصویر IMEI روی بسته‌بندی دستگاه متمرکز بود و به شناسایی شماره‌های IMEI تقلبی متصل به شبکه تلفن همراه کمکی نمی‌کند.

۳-طرح ریجستری در ایران چگونه است؟:

در این بخش میخواهیم در خصوص نحوه ریجستری کردن تلفن های همراه بحث نماییم.

هدف از طرح رجیستری، مبارزه با قاچاق و واردات غیر قانونی گوشی های هوشمند است. از آنجایی که درصد بالایی از گوشی های هوشمند موجود در بازار ایران به صورت قاچاق وارد کشور می شدند، طرح رجیستری وارد میدان شد تا بتوان با این معضل مقابله کرد. در این طرح، تنها گوشی هایی که از طریق گمرک وارد ایران شده اند، فعال خواهند شد. با اجرایی شدن این طرح گوشی هایی که از طریق گمرک وارد کشور می شوند، صاحب یک کد IMEI می شوند. در این شرایط فقط گوشی های موبایلی که کد IMEI آن ها در سامانه همتا ثبت شده باشد با سیم کارت های داخلی فعال می شوند. گوشی های قاچاق غیر فعال شده و دیگر قابل استفاده نیستند.

سامانه همتا را میتوان ازسه طریق استفاده نمود:

- سایت به آدرس:

https://hamta.ntsw.ir

شکل۵-سامانه همتا

- کد دستوری USSD

*7777#

- استفاده از نرم افزار اندروید وIOSجهت فعال کردن سریال موبایل.

۴- نتایج:

همانطور که در این تحقیق بررسی شد گوشی های همراه یکی از موارد بسیار پر اهمیت جهت کلاهبرداری و دیگر مسال امنیتی میباشند.که در طرح ریجستری تا حدودی خلا های امنیتی کامل شده است. و ادارات امنیتی راحت تر میتوانند که موبایل های دزدیده شده را ردیابی کرد. از انجایی که اکثرا افراد خلافکار بدلیل ارزان بودن سیمکارت تلفن، به راحتی میتوانند خط تلفن خود را عوض کنند. اما امروزه بدلیل گران بودن تلفن های همراه عوض کردن خط تلفن برای این افراد دشوار است. لذا طرح ریجستری موبایل میتواند تا حد زیادی از سو استفاده های که از طریق موبایل صورت میگرد جلوگیری به عمل آید. همچنین با اجرایی شدن این طرح پیگیری ها و رد یابی ها راحت تر انجام میشود.

۱-۳-جرائم مرتبط به کد های IMEI و موارد سریال های جعلی:

سرقت پول و فعالیت های مخربی همچون فیشینگ از طریق اینترنت سیمکارت و IMEI. این زمانی اتفاق می افتد که به سایت بانک مخرب دسترسی پیدا می کنید که درخواست شماره IMEI تلفن را برای هکر ارسال می کند و او نیز به نوبه خود گزارش می دهد که تلفن برای دریافت سیم کارت جدید از دست رفته است. پس از آن، هکر یک تلفن شبیه سازی شده خواهد داشت که می تواند پیام های تایید را برای دسترسی به حساب بانکی قربانی دریافت کند

برخی از برنامه ها و اپلیکشن ها اطلاعات مربوط به دستگاه های تلفن همراه، از جمله IMEI، شماره تلفن و شناسه سیم کارت را به صورت قانونی یا غیرقانونی جمع آوری می کنند. با این حال، این اطلاعات توسط اشخاص غیرمجاز افشا خواهد شد ومورد سواستفاده قرار میگیرد که منجر به ایجاد خلل های حریم خصوصی وامنیت میشود[۴][۵][۸].

از طرفی دستکاری شماره های سریال موبایل باعث شده است افراد سودجو بفکر گوشی های دزدی باشند و با این روش شماره سریال ها را تغیر می دهند وکه همین عمل منجر شده است یک بازار سیاه جهت فروش موبایل های سرقتی ایجاد شود.که البته شناسای شماره سریال های تقلبی نیز روش های شناسایی خاص به خود را دارد[۹].

هدف وتمرکز مطالعه مانیز در این مقاله بر همین اساس است که طرح ریجستری در ایران از دید امنیتی چه مزایای در برخواهد داشت.

مراجع

[1] S. J. Alsunaidi and A. M. Almuhaideb, “The Security Risks Associated with IMEIs and Security Solutions,” *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, pp. 1–5, 2019, doi: 10.1109/CAIS.2019.8769521.

[2] S. P. Rao, S. Holtmanns, I. Oliver, and T. Aura, “Unblocking stolen mobile devices using SS7-MAP vulnerabilities: Exploiting the relationship between IMEI and IMSI for EIR access,” *Proc. - 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust. 2015*, vol. 1, pp. 1171–1176, 2015, doi: 10.1109/Trustcom.2015.500.

[3] T. E. Wei, A. B. Jeng, H. M. Lee, C. H. Chen, and C. W. Tien, “Android privacy,” *Proc. - Int. Conf. Mach. Learn. Cybern.*, vol. 5, pp. 1830–1837, 2012, doi: 10.1109/ICMLC.2012.6359654.

[4] M. La Polla, F. Martinelli, and D. Sgandurra, “A survey on security for mobile devices,” *IEEE Commun. Surv. Tutorials*, vol. 15, no. 1, pp. 446–471, 2013, doi: 10.1109/SURV.2012.013012.00028.

[5] C. Miller, “Mobile attacks and defense,” *IEEE Secur. Priv.*, vol. 9, no. 4, pp. 68–70, 2011, doi: 10.1109/MSP.2011.85.

[6] G. Farrell, “Preventing phone theft and robbery: The need for government action and international coordination,” *Crime Sci.*, vol. 4, no. 1, pp. 1–11, 2015, doi: 10.1186/s40163-014-0015-0.

[7] M. A. Khan, A. Tripathi, and M. Dixit, “All time tracking system for recovering stolen devices even in power-off state,” *Proc. - 7th Int. Conf. Commun. Syst. Netw. Technol. CSNT 2017*, pp. 262–266, 2018, doi: 10.1109/CSNT.2017.8418549.

[8] W. Enck *et al.*, “TaintDroid: An information-flow tracking system for realtime privacy monitoring on smartphones,” *ACM Trans. Comput. Syst.*, vol. 32, no. 2, 2014, doi: 10.1145/2619091.

[9] S. J. Alsunaidi and A. M. Almuhaideb, “Security Methods Against Potential Physical Attacks on Smartphones,” *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, pp. 1–6, 2019, doi: 10.1109/CAIS.2019.8769458.

[10] V. Ilango and N. Acram N, “Advanced IMEI and Credit Card Validation Techniques using Layered based LUHN ’ s Algorithm,” *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 6, no. April, pp. 166–171, 2018.

[11] R. D. Cutkosky and R. S. Davis, “Simple control circuit for temperature regulation and other bridge applications,” *Rev. Sci. Instrum.*, vol. 52, no. 9, pp. 1403–1405, 1981, doi: 10.1063/1.1136782.

[12] A. Figueiredo Loureiro, D. Gallegos, and G. Caldwell, “Substandard cell phones: Impact on network quality and a new method to identify an unlicensed IMEI in the network,” *IEEE Commun. Mag.*, vol. 52, no. 3, pp. 90–96, 2014, doi: 10.1109/MCOM.2014.6766091.

[13] P. Shivakumara, V. Basavaraja, H. S. Gowda, D. S. Guru, U. Pal, and T. Lu, “A new RGB based fusion for forged IMEI number detection in mobile images,” *Proc. Int. Conf. Front. Handwrit. Recognition, ICFHR*, vol. 2018-Augus, pp. 386–391, 2018, doi: 10.1109/ICFHR-2018.2018.00074.

Technical and security advantages of mobile registry

Mehrdad Ghaderi [1] *
[1] Master of Mechatronics, Faculty of Engineering, Mohaghegh Ardabili University, Ardabil

Abstract:

Today, technology is advancing day by day. That the world of communications embraces a huge part of technology. The Internet, social networks, and telephone calls are part of the world of communication. The most important part of these cases is the mobile device. This development also has many security aspects. In this article, we are going to examine the mobile IMEI code. And let's examine the mobile registry plan in Iran in terms of security aspects, what are its advantages and disadvantages. It also examines the use of a decentralized identity management framework to implement a system to combat counterfeit smartphones, which provides features of identity creation and transfer of ownership along with fast and secure capabilities. On the other hand, reports of stolen equipment and insecure people in the communication platform will be followed up in the shortest time.

Keywords: MobileRegistry ,CommunicationSecurity ,IMEI