مقدمه‌ای بر پدافند غیرعامل درحوزه شبکه‌های ارتباطات سیار

فهرست

مقدمه

شبکه‌های ارتباطات سیار به عنوان یکی از زیرساخت‌های مهم کشور، بستری برای بهره‌برداری‌های گوناگون ارتباطی، اطلاع‌رسانی، تجاری، سیاسی و فرهنگی در کشور است و روز به روز بر کاربردهای آن افزوده می شود. عدم توجه به امنیت شبکه‌های ارتباط سیار در کنار مزایای غیرقابل انکار حاصل از آن، می‌تواند معضلات مهم و غیر قابل جبرانی را در سطح کشور ایجاد نماید.

شناخت جامع مشکلات امنیتی حاصل از شبکه‌های ارتباطات سیار و اقدام جهت مرتفع نمودن معضلات عمده این حوزه نقش قابل ملاحظه‌ای در ارتقاء امنیت، ایمنی و پایداری زیرساخت ارتباطات سیار ایفا می‌نماید و گامی در راستای تأمین اهداف پدافند غیر عامل در این خصوص بشمار می‌آید.

فصل ۱

نسل های شبکه های ارتباطات سیار

سامانه‌های همراه طی نسل‌های مختلف تکامل یافته و در جهت بهبود سرویس‌دهی تغییر نموده‌اند. در جدول ذیل فهرستی از استانداردهای صوتی و داده‌ای بر مبنای نسل‌های شبکه‌های ارتباطات سیار دسته‌بندی و ارائه شده‌است. در بخش های بعد برخی از این نسل ها بصورت اجمالی بررسی خواهندشد.

جدول استاندارد های صوتی و داده‌ای نسل‌های شبکه‌های ارتباط سیار

<table>
<tr>
<td>۰G
PTT
MTS
IMTS
AMTS</td>
<td rowspan="2">۲G
GSM
iDEN
D-AMPS
IS-۹۵/cdmaOne
PDC
CSD
PHS</td>
<td rowspan="2">۳G
W-CDMA
UMTS (۳GSM)
FOMA
۱xEV-DO/IS-۸۵۶
TD-SCDMA
GAN/UMA</td>
</tr>
<tr>
<td>۰.۵G
Autotel/PALM
ARP</td>
</tr>
<tr>
<td rowspan="2">۱G
NMT
AMPS
Hicap
CDPD
Mobitex
Data Tac</td>
<td>۲.۵G
GPRS
HSCSD
WiDEN</td>
<td>۳.۵G
HSDPA</td>
</tr>
<tr>
<td>۲.۷۵G
CDMA۲۰۰۰۱xRTT/IS-۲۰۰۰
EDGE (EGPRS)</td>
<td>۳.۷۵G
HSUPA
۴G</td>
</tr>
</table>

نسل «۱»

فناوری نسل«۱» یا 1G براساس سیگنال‌های آنالوگ و سامانه‌های سوئیچینگ مداری[1] است و تنها برای انتقال صدا کاربرد دارد. سامانه پیشرفته تلفن همراه[2] در آمریکای شمالی و سامانه ارتباطی سراسری[3] در اروپا از مهمترین سامانه‌های بهره‌برداری شده برمبنای این نسل بشمار می‌آیند.

شبکه‌های ارتباطی نسل اول دارای ضریب امنیتی بسیار پایینی هستند و در آنها امکان کلاهبرداری‌های مختلفی وجود دارد. بطور مثال می توان به مبادله واضح و بدون رمزنگاری اطلاعات روی این شبکه‌ها اشاره نمود، که علاوه بر ایجاد امکان شنود غیر مجاز مکالمات، امکان شناسایی اعضای شبکه را نیز فراهم می‌آورد، به این ترتیب در این نسل مهاجمین به راحتی می توانستند با استفاده از هویت یک عضو مجاز، مکالمات خود را با هزینه وی انجام دهند. طبق گزارش مؤسسه مهندسین برق انگلستان[4] حدود ۵٪ از مکالمات صورت گرفته این نسل در سال ۱۹۹۵ غیرمجاز بوده‌اند. بنابراین سامانه‌های ارتباطی آنالوگ نسل اول کاملاً نامطمئن است.

---

[1] Circuit Switch: در سوئیچینگ مداری ارتباط به صورت پیوسته فعال نگه داشته می شود.

[2] Advance Mobile Phone System

[3] Total Access Communication System

[4] The Institution of Electrical Engineers in United Kingdom

نسل «۲»

نیاز به نرخ داده بالاتر و سرویس بهتر، همچنین فراهم کردن امنیت بیشتر برای کاربران موجب شد تا نسل«۲» شبکه‌های تلفن همراه ارائه گردد. سامانه‌های منطبق بر استانداردهای این نسل، اوایل دهه ۱۹۹۰ به بهره‌برداری رسیدند.

نسل«۲» یا 2G از مخابرات دیجیتال استفاده می‌کند و بیشینه نرخ ارسال داده در آن ۹/۶کیلو بیت بر ثانیه است. ارتباطات در این نسل براساس سیگنال‌های داده دیجیتال بوده و مهمترین شبکه این نسل، GSM[۱] است که در حال حاضر ترین شبکه تلفن‌همراه در جهان می‌باشد. مزایای نسل«۲» چه از نظر فناوری و چه از نظر ارائه خدمات عبارتند از:

- ارائه سرویس‌های داده در کنار سرویس‌های صوتی؛ مانند دورنما و سرویس پیام کوتاه
- پوشش‌دهی مناسب در محیط‌های بسته توسط میکروسلول‌ها[۲]
- کاهش ابعاد و وزن گوشی‌ها و سایر تجهیزات
- ارزان‌بودن سرویس‌ها و خدمات در مقایسه با سامانه‌های آنالوگ
- کدگذاری و رمز نگاری

---

[۱] Global System for Mobile Communication

[۲] شبکه‌های GSM از سامانه‌های سلولی استفاده می‌کنند. در این شبکه‌ها تقریباً در مرکز هر سلول یک ایستگاه مبنا (BS) وجود دارد که شامل آنتن، یک کنترلگر و تعدادی فرستنده و گیرنده برای برقراری ارتباط روی کانال‌هایی که به آن سلول اختصاص داده شده است می‌باشد. دستگاه‌های موبایل فعال در یک سلول با BS در تماس هستند و هر BS به یک مرکز سوییچ ارتباطات موبایل (MTSC) متصل است.

نسل «۲/۵»

نسل«۲/۵» یا $2G^{+}$ به دلیل گسترش اینترنت و تقاضای فزاینده برای دسترسی به اطلاعات و با توجه به محدودیت‌های سرعت سامانه‌های مبتنی بر TDMA[۱]، شکل گرفت. در این نسل، ارتباطات مبتنی بر بسته[۲] بوده و سرعت انتقال داده تا ۳۸۴kbps افزایش یافته‌است. مهمترین شبکه این نسل، GPRS[۳] می‌باشد. این شبکه در حال حاضر، در اپراتور اول و دوم کشور مورد بهره‌برداری قرار گرفته است.

نسل «۳»

نسل«۳» بدلیل وجود برخی مشخصات و قابلیت‌های امنیتی نسبت به 1G و 2G از امنیت بالاتری برخوردار است. در ادامه به برخی از مزایای افزوده شده به فناوری نسل«۳» نسبت به نسل«۲» اشاره می شود.

- کانال‌های ترافیک دیجیتالی
- استفاده بهینه از طیف فرکانسی
- ارسال با نرخ بالا و متناسب با نیاز مشترک
- ارائه سرویس‌های متنوع داده و چندرسانه‌ای
- رمزنگاری قدرتمندتر و امنیت بیشتر با استفاده از فناوری CDMA[۴]

---

[۱] Time-Division Multiple Access فناوری است که در فرکانس‌های ۹۰۰ هرتز و ۱۸۰۰ هرتز کار می‌کند.

[۲] Packet

[۳] General Packet Radio Service

[۴] Code Division Multiple Access

- امکان تشخیص و تصحیح خطا که منجر به بهبود کیفیت صدا و وضوح بیشتر آن می‌شود.

نسل «۴»

شبکه‌های مخابراتی سیار نسل«۴» سعی دارند شبکه‌های مخابراتی، اینترنت و سرویس‌هایشان را بصورت یکپارچه ارائه کنند. معماری شبکه مخابراتی استانداردهای نسل«۴» بر مبنای فناوری بیسیم دسترسی با برد کوتاه-سرعت بالا و استانداردهای اینترنت است. این شبکه‌ها از طریق انواع مختلف پایانه‌ها و تجهیزات، قابل دسترسی هستند.

با توجه به اهمیت شبکه GSM و GPRS در فصل آتی به شرح بیشتر در مورد این دو شبکه پرداخته خواهد شد.

فصل ۲

آشنایی با شبکه ارتباط سیار GSM

مهم‌ترین و پراستفاده‌ترین شبکه ارتباطات سیار در جهان، شبکه GSM است. هم‌اکنون ۹۵ درصد از کشورهای جهان و بیش از ۷۰ درصد از مشترکان تلفن همراه دنیا از این سامانه استفاده می‌کنند. شبکه GSM در سال ۱۳۷۳ در ایران و در شهر تهران راه‌اندازی و مورد بهره برداری قرار گرفت و تاکنون همه اپراتورهای فعال در عرصه ارتباطات سیار کشور آن را پیاده‌سازی کرده اند.

در اوایل دهۀ ۱۹۸۰ شبکه‌های تلفن همراه آنالوگ در اروپا به سرعت شروع به رشد کرد. هر کشور برای خود شبکه‌ای پیاده‌سازی نمود و در مدت زمان کوتاهی در اروپا شبکه‌های متعددی ایجاد شدند که با یکدیگر سازگار نبودند. با پیشرفت فناوری، شبکه‌های دیجیتال برای ارتباطات سیار ایجاد گردید. شبکه GSM یکی از مشهورترین پیاده‌سازی‌های نسل«۲» شبکه‌های ارتباط سیار است. این شبکه نسبت به شبکه های آنالوگ مزایای بسیاری را در حوزه‌های مختلف از جمله امنیت، عرضه کرده است.

همان‌طور که گفته‌شد مهم‌ترین و پر استفاده‌ترین استاندارد نسل«۲» ارتباطات سیار، GSM می‌باشد که در بیشتر کشورهای جهان پیاده‌سازی شده است. در کشور ما نیز در حال حاضر از این شبکه استفاده می‌شود بنابراین به بررسی جزئی‌تر آن می‌پردازیم.

ویژگی‌های شبکه GSM

شبکه‌های GSM دارای ویژگی‌های بسیاری از جمله موارد ذیل هستند:

- سیار بودن کامل

برای کاربر این مزیت وجود دارد که در حین مسافرت به کشورهای دیگر امکان برقراری ارتباط با دستگاه تلفن همراه خود را داشته باشد.

- ظرفیت بالا و طیف قابل تخصیص اختیاری

شبکه‌های GSM نسبت به شبکه‌های نسل«۱»، ظرفیت تماس‌های بیشتری ارائه کرده‌اند و پهنای باند را به صورت مؤثرتری اختصاص می‌دهند.

- امنیت

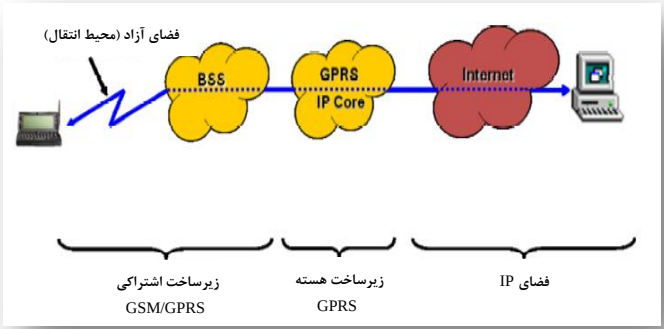
سرویس‌های امنیتی اضافه‌شده به این شبکه شامل ناشناسی[۱]، تشخیص هویت[۲] و حفظ محرمانگی[۳] در برابر شنود به روش‌های معمول است.

[۱] Anonymity
[۲] Authentication
[۳] Confidentiality

فصل ۳

آشنایی با شبکه ارتباط سیار GPRS

شبکه‌های GPRS مبتنی بر سوئیچینگ بسته‌ای[۱] بوده و به عنوان یک امکان جنبی برای شبکه‌های GSM که برپایه سوئیچینگ مداری عمل می‌کنند، طراحی شده‌اند. بنابراین اجزای اصلی معماری GSM در GPRS مورد استفاده قرار گرفته اند.



نمودار مفهومی شبکه GPRS

[۱] Packet Switching: در این روش، صرفاً در زمان ارسال اطلاعات، ارتباط فعال خواهد شد.

ویژگی های شبکه GPRS

ویژگی‌های شبکه GPRS بطور خلاصه عبارتند از:

- سرعت

در تئوری، بیشینه سرعت در این شبکه ۱۷۱/۲ Kbps است که سه‌برابر سریع تر از شبکه مخابراتی ثابت و ده برابر سریع‌تر از سرویس‌های GSM است.

- بلادرنگی[۱]

GPRS امکان ارتباط آنی را فراهم کرده‌است بنابراین داده‌ها می‌توانند هر لحظه که لازم باشد ارسال یا دریافت شوند. این مزیت در کاربردهایی مثل تعیین صلاحیت کارت‌های اعتباری حائز اهمیت است. همچنین GPRS قادر است بطور کامل سرویس‌های مبتنی بر اینترنت را پشتیبانی نماید.

[۱] Realtime

- امنیت

در GPRS علاوه بر سرویس‌های امنیتی GSM شامل احرازهویت و محرمانگی داده‌ها و سیگنال‌ها؛ امنیت زیرساخت GPRS هم مورد توجه قرار گرفته‌است.

مهم‌ترین تغییر در جهت ارتقاء امنیت GPRS نسبت به GSM اولیه، جایگزینی الگوریتم رمز A۵، مربوط به لایه اول رادیویی با الگوریتم رمز GEA در لایه سوم شبکه رادیویی می‌باشد.

فصل ۴

مشکلات امنیتی شبکه های ارتباطی GSM و GPRS

در این فصل مشکلات و آسیب‌پذیری های شبکه های ارتباطی GSM و GPRS به تفکیک بررسی خواهد شد.

مشکلات امنیتی شبکه GSM

آشکارترین آسیب‌پذیری معماری امنیتی در GSM آن است که هیچ‌گونه اقدام امنیتی در زمینه محافظت از صحت داده یا پیام درآن پیش‌بینی نشده و تنها احراز هویت و حفظ محرمانگی مورد بررسی قرارگرفته است. عدم وجود ساز و کارهای محافظت از صحت داده و پیام بدین معناست که دریافت‌کننده نمی‌تواند دست‌بردن یا نبردن در پیام را تایید کند. این آسیب‌پذیری، راه تغییرات گوناگون با حملات دستکاری در میان راه را در شبکه GSM باز می‌گذارد.

آسیب‌پذیری مهم دیگر در معماری امنیت GSM، دامنه محدود رمزنگاری است. تنها لینکی که از نظر رمزنگاری در شبکه GSM محافظت می‌شود، رابط بیسیم BTS–ME است، بنابراین دیگر بخش‌های شبکه می‌تواند براحتی در معرض حمله قرار گیرد.

نکته دیگر در مورد محرمانگی آنست که معماری امنیتی GSM انعطاف ناپذیر است؛ به بیانی دیگر، جایگزینی الگوریتم موجود در رمزنگاری (A۵) با الگوریتم کارآمدتر یا افزایش طول کلیدی که در الگوریتم رمزنگاری A۵ به کار می رود، بسیار مشکل است. بنابراین، می توان گفت که شبکه های GSM محدود به الگوریتم‌های A۵ هستند.

آسیب‌پذیری مهم دیگر در معماری امنیتی GSM آن است که این معماری از شناسایی یک‌سویه درتأیید هویت کاربر به‌وسیله شبکه استفاده می کند.

یکی از حمله‌های واقعی به شبکه GSM با نام SIM cloning شناخته شده است. هدف از این حمله، استحصال کلید رمزنگاری[۱] از سیم‌کارت[۲] است. پس‌از به‌دست‌آوردن کلید،نه‌تنهامی‌توان‌از‌آن‌برای‌شنود تماس‌های برقرار شده از سیم کارت استفاده کرد، بلکه برای قراردادن تماس‌های دیگر در صورت حساب مشترک نیز می‌توان از آن بهره برد. نحوه اجرای حمله SIM cloning بسیار متنوع است. بعنوان نمونه در یک رهیافت، مهاجم به سیم‌کارت و رایانه شخصی، که برای برقراری ارتباط با آن مورد استفاده قرار می‌گیرد، دسترسی فیزیکی دارد.

---

[۱] حداکثر با یک دقیقه دسترسی به سیم کارت می‌توان کلید را از الگوریتم COMP۱۲۸ که به عنوان الگوریتم مرجع در ویژگی‌های GSM مشخص شده است، استخراج کرد.

[۲] SIM Card

مشکلات امنیتی شبکه GPRS

شبکه GPRS همانطور که قابلیت‌های زیادی برای مشترکان ایجاد می‌کند، مشکلات امنیتی خاص خود را نیز بر شبکه ارتباطات سیار تحمیل می‌نماید. اتصال گوشی‌های تلفن‌همراه به شبکه اینترنت از یک طرف و گسترش امکانات و قابلیت های این گوشی‌ها -که آنها را به رایانه‌های کوچکی تبدیل کرده است- از طرف دیگر، تهدیدات بسیار زیادی، اعم از تهدیدات شبکه‌های IP را متوجه شبکه ارتباطات سیار می‌کند.

آسیب‌پذیری‌های شبکه GPRS را می‌توان در دو مرحله بررسی کرد. مرحله اول مواردی که ممکن است در فاز پیاده‌سازی شبکه باعث ایجاد ضعف‌هایی در سامانه شوند و مرحله دوم، حملات بالقوه‌ای که شبکه در معرض آن‌ها است. مشکلات مرتبط با فاز پیاده‌سازی شبکه GPRS عبارتند از:

- بکارگیری یک شبکه مدیریت و نگهداری (O&M) برای هر دو بخش صدا و IP
- یکسان بودن شبکه «مدیریت و نگهداری» و شبکه‌های رایانه‌ای اپراتور تلفن همراه
- اشتراک در شبکه‌های بیلینگ[۱] و شبکه ارتباطات سیار متصل به سایر شبکه‌ها[۲] یا به عبارت دیگر عدم طراحی یک یا چند GGSN[۳] مجزا برای محدودسازی داده های خاص اپراتور

---

[۱] Billing

[۲] Roaming

[۳] Gateway GPRS Support Node

- عدم طراحی ابزار همزمان سازی و ثبت وقایع جامع در شبکه

مخاطرات بالقوه در زمان استفاده از شبکه عبارتند از:

- عدم وجود سیاست امنیتی مشخص و مدون اپراتور برای امنیت شبکه GPRS
- لحاظ نکردن ملاحظات امنیتی در قراردادهای پیاده‌سازی و خدمات میان اپراتور و سازندگان و یا سرویس‌دهندگان
- ضعف فناوری و دانش مرتبط با امنیت در اپراتور تلفن همراه
- ضعف امنیت شبکه زیرساخت
- مشکلات مربوط به فناوری WAP مانند ضعف WAP ۱.x Gateway که در آن تنها امنیت انتها به انتها وجود دارد.

یکی از مهم‌ترین آسیب‌پذیری زیرساخت شبکه مخابراتی در کشور را می‌توان عدم تولید و پشتیبانی داخلی تجهیزات شبکه ارتباطات سیار دانست. در حال حاضر بجز بخش‌های جزئی شبکه BSS (شامل BTS و BSC) و تعداد کمی از SMSC[۱]ها که توسط شرکت‌های داخلی ساخته می شود، دیگر اجزای شبکه از بعضی شرکت‌های خارجی خریداری می‌گردد، لذا کشور در زمینه تعمیرات اساسی و پشتیبانی فنی آنها نیز همواره وابسته به این شرکت‌ها است. همچنین کیفیت و میزان دسترسی شرکت‌های فروشنده این تجهیزات به اجزای شبکه، کنترل نشده و بعضاً در

[۱] Short Message Service Center

سطح بسیار بالایی است. بدیهی است هر کدام از این موارد می تواند امنیت و پایداری شبکه ملی را با چالش و خطر جدی روبرو نماید.

فصل ۵

معیارها و راهکارهای امنیتی در شبکه های ارتباطات سیار

در این فصل به راهکارهای پدافند غیرعامل به منظور امن، ایمن و پایدار نمودن شبکه ارتباطات سیار در دو سطح طراحی- معماری و پیاده‌سازی، پرداخته می‌شود. در این راستا ابتدا معیارها و محورهای پدافند غیرعامل تشریح و سپس راهکارهایی برای مقابله با حملات و مشکلات شبکه ارتباطات سیار، براساس این محورها توصیه می گردد.

محورهای دفاع غیرعامل در شبکه‌های ارتباطات سیار

پدافندغیرعامل بمنظور امن، ایمن و پایدارسازی شبکه‌های ارتباطات سیار محورهای ذیل را دنبال می کند:

- استفاده از شبکه‌های جایگزین به صورت منطقه‌ای و یا سراسری
- کاهش امکان حمله به نقاط حیاتی، حساس و مهم شبکه
- کاهش میزان خسارات ناشی از حمله به نقاط مهم، حساس و حیاتی شبکه

- کاهش هزینه و افزایش سرعت و سهولت بمنظور جبران خسارات وارد شده به نقاط مهم، حساس و حیاتی شبکه و بازسازی شبکه با اندیشیدن تمهیدات لازم
- ایجاد امکان شناسایی دشمن و کشف نفوذ به شبکه ارتباطات سیار در صورت هرگونه حمله یا نفوذ
- محدود سازی گستره حملات به شبکه ارتباطات سیار

راهکارهای پدافند غیرعامل در شبکه‌های ارتباطات سیار

در این بخش به بیان راهکارهای پدافند غیرعامل به منظور تـأمین امنیـت، ایمنـی و پایداری شبکه‌های ارتباطات سیار مبتنی بـر محورهـای ذکـر شـده در بخـش قبـل پرداخته می‌شود. هدف از این راهکارهای امنیتی بالابردن مقاومت شبکه، کـاهش میزان خسارات و تسهیل بازسازی شبکه در حملات و شرایط بحران ومخاصـمات بین‌الملل است. در یک دسته‌بندی راهکارهـای امـن، ایمـن و پایـدارسـازی شـبکه ارتباطات سیار در برابر حملات و آسیب‌پذیری‌ها را می‌تـوان بـه دو بخـش تقسـیم نمود:

الف) راهکارهای مربوط به طراحی شبکه: راهکارهایی که کلان‌تر و غالباً از جنس معماری و طراحی بوده و لازمه برخی از آنها تغییرات گسترده و زیربنایی در شبکه‌های ارتباطات سیارمی‌باشد.

ب) راهکارهای مربوط به پیاده‌سازی: راهکارهایی که اجرایـی‌تـر و جزئـی‌تـر هسـتند و برخـی از آنهـا روش‌هـایی هسـتند کـه راهکارهـای طراحـی را عملـی می‌سازند.

راهکارهای طراحی شبکه

همانطور که اشاره شد، راهکارهای طراحی عموماً کلان‌تر و غالباً از جنس معماری و طراحی می‌باشند. این راهکارها براساس اصول راهبردی و مبتنی بر محورهای دفاعی بیان شده در بخش قبل تدوین شده است. اصول کلی حاکم بر راهکارهای این بخش پیشگیری از حمله و نفوذ، جلوگیری از انتشار و تشدید، شناسایی و بازسازی تا حد ممکن است. این راهکارها شامل موارد ذیل می‌باشد:

۱. محرمانه و مخفی نگهداشتن اطلاعات ساختار، طراحی و پیاده‌سازی شبکه و نیز اطلاعات مربوط به نقاط مهم، حساس و حیاتی شبکه که تأثیر بسزایی در امنیت شبکه و جلوگیری از نفوذ و دسترسی دشمن دارد. مثالی از آن طبقه‌بندی محرمانه برای اطلاعات جداول مسیریابی صدا در شبکه است.

۲. مستقل‌سازی حداکثری بخش‌های مختلف شبکه ارتباطات سیار از شبکه‌های دیگر مخابراتی و رایانه‌ای.

۳. اجرای اصول و راهکارهای امنیتی در طراحی و پیکربندی زیرشبکه‌ها جهت جلوگیری از حمله و نفوذ به شبکه.

۴. رعایت اصول طراحی منطقه‌ای در شبکه ارتباطات سیار بگونه‌ای که حملات به یک مرکز (یا منطقه) صرفاً منجر به اختلال یا دسترسی غیرمجاز به همان مرکز (منطقه) شود و یا کمترین میزان مشترکین را تحت تاثیر قرار دهد. یکی از اصول مهم در این راهکار، طراحی شبکه بصورت مجموعه‌ای از زیرشبکه‌های نسبتاً مستقل است.

۵. رعایت اصول طراحی لایه‌ای در شبکه ارتباطات سیار به صورتی که نفوذ یا صدمه به یک لایه وسیله‌ای برای گسترش نفوذ و صدمه به لایه‌های دیگر نشود.
۶. طراحی شبکه بگونه‌ای که تا حد ممکن اختلال و یا دسترسی به یک کاربرد یا سرویس، به سایر خدمات صدمه‌ای وارد ننماید.
۷. معماری و طراحی شبکه ارتباطات سیار به گونه‌ای که در صورت گسترش خسارت به مراکز، لایه‌ها و کاربردهای دیگر، خسارت مستهلک و میرا شود، نه اینکه تشدید گردد.
۸. طراحی و معماری بگونه‌ای که در حوادث و حملات، بصورت نظام مند و به سرعت مکان، نوع، عامل و سطح تأثیر شناسایی شود.
۹. طراحی دفاع در شبکه ارتباطات سیار بگونه‌ای که دشمن برای حمله، به دانش سطح بالا و متنوع، هزینه زیاد، ابزار و تجهیزات متعدد، پیشرفته و پیچیده نیاز داشته باشد.

استفاده از راهکارهای بومی و نوآورانه امن، ایمن و پایدارسازی شبکه و عدم استفاده از پیشنهادات، روش‌ها و الگوریتم‌های امنیتی شناخته‌شده می‌تواند منجر به چنین نتایجی شود.

راهکارهای پیاده‌سازی شبکه

راهکارهای پیاده‌سازی، اجرایی‌تر و جزئی‌تر بوده و برخی از آنها در واقع روش‌هایی برای عملیاتی کردن راهکارهای طراحی ارائه شده در بخش قبل هستند. این راهکارها به دو گروه قابل تقسیم هستند. که در ادامه فصل به آنها می پردازیم.

۱. راهکارهای امنیتی فناورانه

در این بخش مجموعه‌ای از راهکارهای ایمن‌سازی شبکه ارتباطات سیار که بیشتر در حوزه پیاده‌سازی است، بیان شده است.

- اعمال اصول امنیتی در نصب تجهیزات و راه‌اندازی شبکه

راه‌اندازی مراکز و نصب تجهیزات شبکه (**NE**[۱]) باید در مناطقی که احتمال وقوع حمله یا حوادث غیر مترقبه کمتر و یا شرایط برای جبران خسارات احتمالی مناسب‌تر باشد، انجام پذیرد.

- اجرای اصول اختفا[۲]، استتار[۳] و فریب[۴] در نصب تجهیزات و ایجاد و راه‌اندازی مراکز

اختفا به‌معنی مخفی‌سازی از دید دشمن، استتار به معنای مشابه‌سازی اهداف (تجهیزات، کابل‌ها و مراکز) با زمینه قرارگیری و فریب به معنی به اشتباه انداختن دشمن در مورد اهداف واقعی است که این سه راهکار به عنوان سه اصل مهم پدافندغیرعامل باید در پیاده‌سازی شبکه‌های ارتباط سیار در نظر گرفته شود.

- پراکندگی حداکثری مراکز و تجهیزات

یکی دیگر از روش‌های دفاعی در پدافند غیرعامل، پراکنده سازی مکانی حداکثری تجهیزات مهم، حساس و حیاتی

---

[۱] Network Elements

[۲] Concealment

[۳] Camouflage

[۴] Deception

شبکه ارتباطات سیار است. البته ماهیت شبکه ارتباطات سیار پراکنده بوده که این خود یک حسن به حساب می‌آید ولی بخش‌های مهم متمرکز شبکه همچون نظارت و مدیریت از مراکز آسیب پذیر شبکه ارتباطات سیار محسوب می‌شود.

- مقاوم سازی مراکز و ارتباطات

با امن‌سازی شبکه‌های ارتباطات سیار می‌توان از برخی از حملات نرم پیشگیری نمود. به همین خاطر الزام اپراتورهای تلفن همراه به مقاوم‌سازی امنیتی و پیاده‌سازی استانداردها، رویه‌ها و راهکارهای فنی امنیتی برای حفظ امنیت شبکه ارتباطات سیار تحت مدیریت خود نقش به‌سزایی در بالا بردن مقاومت شبکه‌های تلفن‌همراه در هنگام حملات دشمن و حوادث غیر مترقبه خواهد داشت.

- راه‌اندازی مراکز پاسخگویی به حوادث امنیتی

در کنار ایجاد مؤسسات ملی امداد و نجات برای شبکه‌ها سامانه‌های رایانه‌ای **CERT** ملی، بطور خاص برای شبکه‌های ارتباطات سیار نیز باید گروه‌ها و مراکز پاسخگو به حوادث امنیتی (**IRT**[1]) راه‌اندازی شود.

- تدارک تجهیزات و اجزای جبرانی در شبکه ارتباطات سیار

[1] Incident Response Team

به منظور بازسازی سریع شبکه ارتباطات سیار، باید به میزان قابل قبولی اجزای شبکه و قطعات جانبی برای جایگزینی وجود داشته باشد.

- رعایت اصول راه‌اندازی سریع

جهت بازسازی، ترمیم و راه‌اندازی مجدد شبکه آسیب دیده، باید اصول و مواردی رعایت شود تا محل و نحوه ذخیره‌سازی تجهیزات و لینک‌های جایگزین، شیوه‌های حمل و نقل آنها، روش نصب و تعمیر آنها، سریع و آسان باشد.

- توسعه توان تولید و پشتیبانی داخلی در تجهیزات شبکه

تا حد امکان قابلیت ساخت و تعمیرات اساسی تجهیزات در داخل کشور و توسط شرکت‌ها و نیروهای داخلی فراهم آید.

- بالابردن کیفیت و قابلیت اعتماد[1] تجهیزات شبکه

استفاده از اجزای با طول عمر بالا و با کیفیتی که در شرایط آب و هوایی و سایر شرایط نامساعد نیز بخوبی کار خود را انجام دهند و بکارگیری شیوه‌هایی که باعث طولانی شدن زمان تعمیرات اساسی تجهیزات شود لازم به نظر می‌رسد. همچنین، قابلیت اعتماد به تجهیزات و اتصالات کابلی یا رادیویی در شرایط عادی در برابر خطای اپراتور انسانی، حرارت محیط، شرایط جوی غیر حاد و ... نیز باید وجود داشته باشد.

---

[1] Reliability

نکته دیگری که در اینجا لازم به ذکر است، تلاش برای کاهش هزینه تولید، تعمیر و نصب تجهیزات شبکه به منظور بالا بردن صرفه و امکان مالی برای بازسازی خسارت محتمل زمان حادثه است. شاید یکی از روش‌ها نیز استفاده از توان داخلی برای تولید و پشتیبانی تجهیزات شبکه باشد.

۲. راهکارهای امنیتی مربوط به فرایندها و روال‌ها

در این بخش راهکارهای امنیتی که در مباحث پیاده‌سازی شبکه‌های ارتباطات سیار و در حوزه مرتبط با فرایندها و روال‌های سازمانی است، بیان می‌گردد. این موارد به طور مستقیم قابل تست و پیاده‌سازی نیستند، بلکه به منظور تدوین دستورالعمل‌ها، رویه‌ها، قوانین و دوره‌های آموزشی مورد بررسی قرار می‌گیرند.

- بالا بردن اولویت امنیت نزد اپراتورهای تلفن همراه

اپراتورهای تلفن همراه باید روال‌های درون و برون سازمانی را که امنیت شرکت و شبکه تلفن همراه را تقویت می‌کنند، اجرا نمایند.

- رعایت روال‌های امنیتی مرتبط با مشترکان

در روال‌های مربوط به خرید، صدور و تخصیص SIM به مشترک، باید اصول امنیتی جهت فاش نشدن این اطلاعات مراعات گردد.

- معتمد و آگاه بودن مجریان و مدیران شبکه

یکی از مسائلی که تاثیر بسزایی در امنیت شبکه ارتباطات سیار دارد، معتمد بودن و داشتن آگاهی و دانش امنیتی کافی مجریان و

مدیران شرکت‌های اپراتور تلفن همراه است، بگونه‌ای که ایشان در مواجهه با برخی معضلات امنیتی و یا مشکلات پیش‌بینی نشده در شرایط عادی و یا بحرانی بتوانند به خوبی عکس‌العمل نشان دهند. همچنین وضعیتی اتفاق نیفتد که خودشان خواسته یا ناخواسته، عامل و یا تشدید کننده حملات دشمن شوند. طبق آمارهای بین‌المللی اکثر حملات و نفوذها به شبکه‌ها با واسطه یا بی واسطه از طریق کارکنان داخل سازمان است و نه هکرهای خارجی.

از جمله مسائلی که باید رعایت شود، اینست که تا حد ممکن، نصب، راه‌اندازی و نگهداری تجهیزات مراکز مهم و بطور خاص، حساس و حیاتی توسط افراد مورد اعتماد و تایید شده صورت پذیرد. در صورتی که چاره‌ای جز بکارگیری افراد خارجی و یا ناشناخته نیست، این افراد باید تحت نظارت و کنترل کامل افراد معتمد باشد.

همچنین مدیران و متولیان آگاه شبکه‌های ارتباطات سیار باید نظارت، بازدید و تست‌های دوره‌ای و مرتب در مراکز و لایه‌های شبکه بر روی طراحی‌ها، سخت‌افزار و نرم‌افزار شبکه داشته باشند.

- مراعات کنترل دسترسی و امنیت فیزیکی

رفت و آمدها به مراکز و اماکن مهم، حساس و حیاتی شبکه ارتباطات سیار، همچنین دسترسی‌های فیزیکی و غیر فیزیکی به سخت‌افزارها و نرم‌افزارها باید طبق اصول امنیتی از پیش تعریف شده و کاملاً مطابق با آن باشد. همچنین کلیه دسترسی‌ها نیز به طرق مختلف باید تحت کنترل و نظارت و قابل بررسی باشد.

- ایجاد روال‌های امن در مورد اطلاعات شبکه

اطلاعات ساختاری، طراحی و عملیاتی شبکه ارتباطات سیار، تعداد و نوع تجهیزات و سیستم‌ها، جداول مسیریابی، ظرفیت اجزای شبکه، نسخه نرم‌افراز و سخت‌افزار، وضعیت حال حاضر و برنامه آینده توسعه شبکه، ایرادات و مشکلات فعلی شبکه ارتباطات سیار باید تحت طبقه‌بندی صحیح و منطبق با اصول پدافند غیرعامل قرار گیرد.

- ایجاد ساختار اطلاع‌رسانی عمومی

بسیاری از نفوذها به شبکه‌ها، ویروس‌های مخرب در شبکه، حملات از کار انداختن تجهیزات، مشکلات ناشی از شبکه اینترنت در GPRS، از ورودی گوشی و SIM مشترک حاصل می‌شود. با گسترش قابلیت‌های حافظه‌ای و پردازشی گوشی‌های تلفن همراه، روز به روز بر این تهدیدات افزوده می‌شود. به عنوان مثال غالب ویروس‌های شناخته شده موبایل که می‌تواند ترافیک و سیگنالینگ شبکه را تحت تاثیر قرار دهد، از طریق بلوتوث منتقل می‌شود که ارتباطی با شبکه ارتباطات سیار ندارد. آموزش عمومی کاربران تلفن همراه، گسترش و بالا بردن سطح اطلاعات عمومی مشترکین از تهدیدات و مشکلات و عوارض امنیتی ممکن در مورد تلفن همراه، تدوین دوره‌های آموزشی و اطلاع‌رسانی و تبلیغاتی از جمله راهکارهایی هستند که می توانند نقش مؤثری در کاهش این مشکلات داشته باشند.