پدافند غیر عامل در حوزه

شبکه ارتباطات ثابت

فهرست

مقدمه

تلفن ثابت نخستین بار در سال ۱۲۶۹ هجری شمسی، چهارده سال پس از اختراع آن، در تهران راه‌اندازی شد . از زمان اختراع تلفن در سال ۱۸۷۶، این وسیله برای بیش از یک قرن، نقش منحصر به فردی را در دنیای ارتباطات ایفا کرده است. امروزه هر چند شیوه‌های جدید ارتباطی همچون تلفن همراه ظهور کرده‌اند، اما همچنان تلفن ثابت، به دلیل داشتن مزایای خاص از جایگاه ویژه‌ای در ارتباطات هزارهٔ سوم برخوردار است. برخورداری از امنیت نسبی در مقایسه با شیوه های نوین ارتباطی از جمله مزایای شبکه تلفن ثابت است. با این وجود، این شبکه نیز در معرض تهدیدات مختلفی است. لذا در ادامه ابتدا به مرور کلی ساختار شبکهٔ تلفن ثابت پرداخته و سپس برخی تهدیدات این شبکه و راهکارهای مقابله با آن ها را از منظر پدافند غیرعامل بررسی می کنیم.

فصل ۱

آشنایی با شبکه تلفن ثابت

سرویس‌های شبکه تلفن ثابت به چند دسته قابل تقسیم است: سرویس هایی که توسط شبکه PSTN[1] ارائه می‌شود، سرویس‌های شبکه هوشمند، سرویس‌های شبکه ISDN[2]، سرویس پیجینگ و سرویس‌هایی که به‌واسطه شبکه WLL[3] ارائه می‌شود. با توجه به گستردگی و فراگیری شبکه PSTN نسبت به شبکه های دیگر، در ادامه این فصل به بررسی مؤلفه ها و سرویس های این شبکه خواهیم پرداخت و در انتها شرح مختصری در خصوص سایر شبکه ها ارائه خواهد شد.

---

[1] Public Switched Telephone Network
[2] Integrated Services Data Network
[3] Wireless Local Loop

شبکه تلفن ثابت PSTN

شبکه تلفنی سوییچ عمومی یا PSTN، یک ابرشبکه متشکل از شبکه‌های تلفنی سوییچ مداری در سراسر دنیا است. این شبکه برخلاف شبکه اینترنت که یک شبکه مبتنی بر IP[1] است، بر پایه سوییچینگ مداری بنا شده است.

در ادامه برخی مؤلفه‌های مهم و مفاهیم اساسی این شبکه معرفی می‌شوند.

- سیگنالینگ

سیگنالینگ به بیان ساده عبارت است از انتقال اطلاعات کنترلی در شبکه تلفنی. این اطلاعات شامل سیگنال‌های لازم برای برقراری ارتباط، امتداد و پایان آن است. در شبکهٔ تلفن ثابت دو نوع سیگنالینگ CAS[2] و CCS7[3] (SS7[4]) متداول است. به طور کلی، استفاده از CAS، علاوه بر محدود کردن ظرفیت ارتباطی کشور، باعث ایجاد محدودیت در ارای ه سرویس‌ها و فناوری‌های جدید مخابرات نیز می‌شود. از جمله مزایای CCS7 نسبت به CAS می‌توان به افزایش سرعت برقراری ارتباط، کاهش زمان اشغال بودن خطوط، امکان استفاده از شبک ه فعلی برای پیاده‌سازی شبکه‌های نسل جدید و امکان مزاحم‌یابی سریع اشاره کرد.

---

[1] IP Based
[2] Channel Associated Signaling
[3] Common Channel Signaling 7
[4] Signaling System 7

- شماره‌گذاری

اساساً دو روش برای شماره‌گذاری در شبکهٔ تلفن ثابت وجود دارد. روش بسته[1] یا نامنظم و روش باز[2] یا منظم. در روش بسته، کل کشور شامل یک منطقهٔ شماره‌گذاری است. به این معنی که، برای آغاز هر مکالمه، شماره‌گیری ملی به صورت کامل صورت می‌گیرد. در روش باز، کل کشور به چند منطقهٔ جغرافیایی تقسیم می‌شود. در این حالت، برای مکالمات محلی، شماره‌گیری به صورت محلی و برای مکالمات بین‌منطقه‌ای، شماره‌گیری ملی به صورت کامل صورت می‌گیرد.

روش بسته عمدتاً در آمریکای شمالی و روش باز در اروپا و آسیا متداول است. شماره‌گیری متداول در کشور ما نیز مبتنی بر روش باز است. هرکدام از این روش‌ها، مزایا و معایب خاص خودش را دارد. به عنوان مثال، روش بسته دارای شماره‌های با طول یکسان برای کلیهٔ مکالمات و نیز شماره‌های قابل حمل است. از سوی دیگر، روش باز دارای شماره‌های با طول کمتر برای مکالمات محلی نسبت به مکالمات بین‌منطقه‌ای است.

- همزمانی

به بیان ساده، «همزمانی» به معنی استفاده از یک ساعت واحد در نقاط مختلف شبکهٔ مخابراتی است. مسألهٔ همزمانی سامانه‌های سوئیچ و انتقال مخابراتی واقع در نقاط مختلف شبکه با توجه به دگرگونی شبکه‌های تلفنی و تغییر سامانه‌های انتقال در این شبکه‌ها از حالت رقومی به دیجیتال و عملکرد این سامانه‌ها با نرخ بیت مشخص، اهمیت ویژه می‌یابد. به عنوان

1 Closed method
2 Open method

مثال، عدم رعایت همزمانی در سامانه‌های مخابراتی باعث بروز نویز شنوایی در سرویس‌های صوت و از بین رفتن اطلاعات در سامانه‌های سیگنالینگ و داده می‌گردد.

معرفی دیگر شبکه های ارتباطات کابلی وثابت

در ادامه چند شبکه دیگر ارتباطات کابلی و ثابت به اختصار معرفی خواهد شد.

- شبکه هوشمند [1]

شبکه هوشمند، شبکه‌ای است که در لایهٔ بالایی شبکه مخابراتی قرار می‌گیرد. در این شبکه، انواع و اقسام سرویس‌ها به‌راحتی و با انعطاف‌پذیری زیاد قابل تعریف و ارائه هستند. برای تحقق یک شبکه هوشمند، باید نقاط هوشمند در تعامل با نقاط فعلی شبکه به ساختار شبکه افزوده شوند. ارتباط این نقاط هوشمند با یکدیگر و نیز با سایر نقاط شبکه بر روی بستر CCS7 صورت می‌گیرد.

- مزایای شبکه هوشمند

مزایای بهره‌گیری از شبکه هوشمند در شبکه ارتباطات ثابت شامل این موارد است:

۱. جداسازی اعمال مربوط به سرویس از سوئیچ‌های تلفنی به منظور یکنواخت کردن نحوه استفاده از آن‌ها
۲. ارائه سریع‌تر سرویس‌ها
۳. بالا بردن درصد مکالمات موفق

[1] Intelligent Network

۴. استفاده مؤثر از منابع شبکه
۵. مدیریت قابل انعطاف بر روی سرویس‌ها
۶. امکان کنترل پارامترهای ارایه سرویس از طریق مشترک

- شبکه ISDN[1]

از دهۀ ۷۰ میلادی، ایجاد شبکۀ داده جهت استفادۀ عموم مردم آغاز شد. با گسترش این شبکه در کنار شبکۀ تلفنی، نیاز به یکپارچه‌سازی آن در دهه ۸۰ میلادی احساس و منجر به ایجاد شبکۀ ISDN شد. این شبکه، به‌دلیل توانمندی‌های خود، ضمن یکپارچه‌سازی سرویس‌های صوت، تصویر و داده، اثرات ترافیکی هر یک از شبکه‌های مذکور را بر یکدیگر از بین می‌برد و سرویس‌های ارزش‌افزوده متنوعی را ارائه می‌دهد.

شبکه ISDN امکان ارائه سرویس‌های جدید مخابراتی را که برای پشتیبانی آن‌ها کانال های ۶۴ کیلوبیت برثانیه و یا مضربی از آن تا دومگابیت بر ثانیه مورد نیاز است، فراهم می آورد.

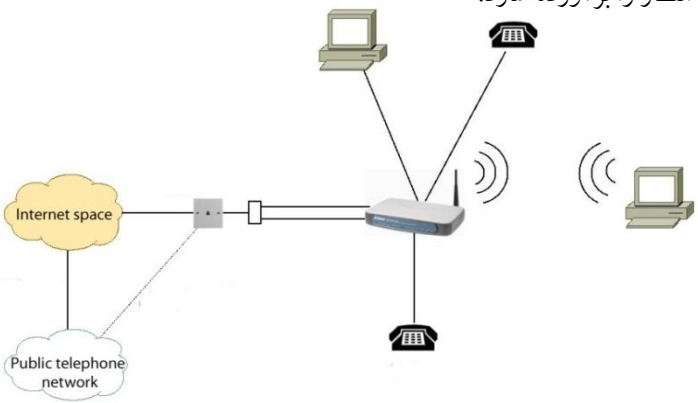
- شبکه WLL[2]

شبکه WLL، مجموعه‌ای از تجهیزات، واسط‌ها و امکانات مخابراتی است که تأمین‌کننده دسترسی رادیویی به شبکه PSTN است. با استفاده از این نوع دسترسی بی‌سیم ، تقریباً می توان هر سرویسی را که قابل ارائه به مشترکین PSTN است، به مشترکین این سامانه نیز ارائه کرد.

[1] Integrated Services Data Network
[2] Wireless Local Loop

- سرویس صوت مبتنی بر IP (VoIP[1])

نسل بعدی ارتباطات صوتی VoIP است. این سرویس انتقال صوت از طریق شبکه های سوئیچ بسته‌ای [2] و شبکه اینترنت را ممکن می‌سازد. پیاده‌سازی موفق این فناوری نیازمند راهکارهای امنیتی قوی است. اگر یک شبکه VoIP دارای امنیت لازم نباشد نمی‌تواند کیفیت و اعتبار مورد انتظار را برآورده سازد.



در این روش با کمک اینترنت کاربر با مراجعه به سایت های خاص شماره مد نظر خود را در کشور هدف به صورت ظاهری کرایه می کند. درواقع اینترنت با ایجاد ارتباط ارزان قیمت و سریع به سرعت در مخابرات کشورها نفوذ نموده است. [3] چالش های امنیتی مرتبط با شبکه‌های مبتنی بر IP مقوله محافظت از این شبکه ها را در مقابل تهدیدات، بسیار پیچیده تر و دشوارتر از شبکه‌های انتقال صوتی سنتی می کند. به عنوان مثال VoIP در برابر حملات مختص شبکه‌های IP نظیر کرم‌ها، ویروس‌ها و یا حمله

[1] Voice over Internet Protocol
[2] Packet Switch
[3] مقاله امنیت سیستم های ارتباطی ثابت و همراه– ناصر نامخواه

DoS[1] بسیار آسیب پذیر است. یکی دیگر از دلایل آسیب پذیری بیشتر VoIP در مقایسه با شبکه‌های سنتی وجود نرم افزارها و اجزاء بیشتر است. در واقع VoIP به لحاظ ساختاری، ابزارهای درگیر و مرتبط با IP را دو برابر می‌کند و این به معنی دو برابر شدن نقاط دسترسی مهاجمین به شبکه خواهد بود. با توجه به اینکه امروزه نفوذ به اغلب سرویس های اینترنتی توسط هکرها به سهولت قابل انجام است، در این روش کاربر عملاً تماس های خود را از طریق اینترنت با تمام اینترنتی ها مشترک نموده است!![2]

[1] Denial of Service

فصل ۲

تاریخچه شبکه تلفن ثابت

برقراری ارتباط در شبکه تلفن ثابت ابتدا تنها به صورت نقطه به نقطه امکان پذیر بود. این شبکه از یک زنگ ساده و یک دستگاه فرستنده-گیرنده در دو طرف خط، جهت سیگنالینگ قبل از تماس و یک دستگاه سوئیچ به نام switch hook جهت برقراری تماس‌ها تشکیل می شده است. در ادامه و در سال های بعد هر تلفن به دستگاهی به نام سامانه تبادل تلفن محلی [۱] متصل شد. این سامانه ها توسط یک معبر مشترک [۲] به هم متصل شدند. به همین ترتیب با اتصال تسلسلی شبکه‌های محلی تشکیل شده، شبکه‌های شهرها، کشورها و قاره‌ها ایجاد شدند. سپس از طریق سامانه های خودکارسازی [۳]، شماره‌گیری پالس [۴] بین دستگاه های تلفن و مبدل‌ها و بعدها بین خود مبدل ها ایجادشد.

---

[1] Local telephone exchange
[2] Trunk
[3] Automation
[4] Pulse dialing

در ادامه توسعه روش های سیگنالینگ، آدرس دهی چند فرکانسی[1] مطرح گردید. استفاده از این روش در شبکه‌های تلفنی در اواخر قرن بیستم بوسیله روش SS7 به اوج خود رسید.

در ابتدای توسعه شبکه های تلفن ثابت از جمله مسائل مطرح در برقراری ارتباط موضوع میزان کیفیت سرویس های ارائه شده در این شبکه ها بود. در این زمینه ارلانگ[2] از اولین فعالانی بوده است که با بررسی مشکلات شبکه تلفن ثابت، برای تضمین سطح خاصی از کیفیت سرویس های ارائه شده ، گام‌هایی برداشته است.

شبکه PSTN نیز اولین نمونه از سامانه های طراحی شده به وسیله مهندسی ترافیک[3] به منظور تضمین کیفیت خدمات ارائه شده [4] به حساب می آید. این شبکه در ابتدا به صورت رقومی و مبتنی بر خطوط ثابت بود در حالیکه امروز سرویس های آن به‌صورت کاملاً دیجیتال ارائه می‌شود.

هم‌اکنون تعداد زیادی از شبکه‌های خصوصی وجود دارند که به شبکه PSTN جهانی متصل نیستند و معمولاً برای مقاصد نظامی از آن ها استفاده می‌شود. برخی از شبکه‌های خصوصی نیز با استفاده از دستگاه هایی موسوم به دروازه محدودکننده [5]، به PSTN جهانی متصل می‌شوند. نمونه‌ای از این دستگاه‌ها PBX[6] نامیده می‌شود.

---

[1] Multi Frequency
[2] A. K Erlang
[3] Traffic Engineering
[4] Quality of Service
[5] Limiter Gateway
[6] Public branch Exchange ابزاری به منظور ایجاد یک سامانه تلفنی سازمانی است به طوریکه به هر کارمند یک خط برای تماس های داخلی اختصاص داده شده و به صورت همزمان تعدادی خط خارجی بین کارمندان به اشتراک گذاشته می شود.

فصل ۳

انواع تهدیدات و حملات در شبکهPSTN

در این فصل به بیان برخی حملات و تهدیدهای مطرح روی شبکه های PSTN خواهیم پرداخت. شایان ذکر است مواردی همچون تهدیدات حوزه الکترومغناطیس و دسترسی فیزیکی نیز در این زمینه مطرح هستند که با توجه به ارائه این موارد در کتابچه های منتشرشده و عمومیت آن ها در اغلب حوزه های زیرمجموعه فناوری اطلاعات و ارتباطات از مطرح نمودن مجدد آن‌ها صرف‌نظر می‌شود.

فعال‌سازی نقاط ضعف امنیتی

فعال‌سازی و استفاده از نقاط ضعف امنیتی و درهای پشتی[1] ناشناخته موجود در پروتکل‌های مخابراتی و تجهیزات سخت‌افزاری و نرم‌افزاری شبکه ارتباطات ثابت که توسط شرکت‌ها و کشورهای سازنده در آن ها گنجانده شده است از

[1] Back door

مهم‌ترین تهدایداتی است که امنیت و پایداری کل شبکه را در معرض خطر قرار می‌دهد. این موضوع نیازمند عزم جدی در شناسایی و تولید محصولات راهبردی این حوزه به صورت بومی و دقت نظر مضاعف در نحوه و چگونگی بکارگیری تجهیزات و پروتکل‌های غیر بومی در شبکه‌های داخلی است.

عدم پشتیبانی مطلوب تجهیزات

یکی از مهم‌ترین آسیب‌پذیری‌های زیرساخت شبکه مخابراتی در کشور را می‌توان وابستگی به شرکت ها و کشورهای بیگانه در ارائه خدمات پشتیبانی تجهیزات بکارگیری شده در این شبکه به دلیل عدم تولید و پشتیبانی داخلی این تجهیزات دانست. از سوی دیگر کیفیت و میزان دسترسی شرکت‌های فروشنده این تجهیزات به اجزای شبکه، کنترل نشده و بعضاً بسیار زیاد است. بدیهی است هر کدام از این موارد می تواند امنیت و پایداری شبکه ملی را با چالش و خطر جدی روبرو نماید.

حمله به شبکه سیگنالینگ

اصولاً سامانه‌های سیگنالینگی ITU-T قبل از SS7 بسیار آسیب‌پذیر بودند. نتیجه ضعف این سامانه ها حملات متعددی از جمله BlueBoxing، GoldBoxing، BlackBoxing، RedBoxing ... بود که به شبکه ثابت انجام می‌شد. در بررسی امنیت شبکه سیگنالینگ SS7 نیز تهدیدهای مختلفی را می‌توان نام برد و در کل، شبکه SS7 (CCS7) به عنوان یک شبکه نا امن شناخته شده است. از آنجا که شبکه PSTN، خود از شبکه سیگنالینگ SS7 استفاده می‌کند پس تهدیدهای SS7 و حملاتی که ممکن است به آن انجام شود کل شبکه را هدف قرار می دهد.

به طورکلی گرچه امروزه دستکاری و تغییر اطلاعات این شبکه ها برای نفوذگران دشوار است ولی این موضوع، به تنهایی برای تضمین امنیت اطلاعات روی این شبکه ها، خصوصاً در شرایط مخاصمات موجود بین المللی کافی نیست.

حمله میانی[1]

این حمله پایه‌ای، به منظور دسترسی به خط مشترک شبکه تلفن ثابت مورد استفاده قرار می‌گیرد. این حمله می تواند زمینه ای برای سایر حملات نظیر دستکاری[2] تماس و اطلاعات، نمایش جعلی[3] و شنود[4] باشد. در این حالت خط مشترک قطع شده و یک دستگاه سخت افزاری که دارای دو درگاه زوج سیم ورودی و خروجی است، بر روی آن نصب می‌شود. در چنین حالتی می‌توان دستکاری‌های زیادی بر روی اطلاعات کاربر انجام داد.

فرض کنید کاربر بخواهد مبلغی را از یک حساب به حساب دیگر واریز کند در این صورت مهاجم منتظر می‌ماند تا کاربر اطلاعات مربوط به تأیید هویتش را بر روی خط بفرستد. سپس کنترل تماس را در اختیار گرفته و مبلغ مورد نظر را به حساب خود منتقل می‌کند!

سوء استفاده از سرویس[5]

سوء استفاده از سرویس می‌تواند ابعاد گوناگونی داشته باشد. فرض کنید که نفوذگر می‌خواهد هزینه زیادی را به صورت‌حساب یک مشترک تحمیل کند. او می‌تواند بارترافیکی تماس ها و یا داده‌های قربانی را افزایش داده و یا تماس‌های راه دور برقرار کند. اکثر این سوءاستفاده‌ها با اهداف مالی صورت می گیرد.

---

[1] Man-in-the-Middle
[2] Manipulation
[3] Misrepresentation
[4] Eavesdropping
[5] Service Abuse

فصل ۴

راهکارهای مقابله با تهدیدات

در این فصل به ارائه راهکارهای مقابله با تهدیدات و حملات شبکه های ارتباط ثابت، مبتنی بر اصول پدافند غیر عامل پرداخته شده است.

اصل اختفاء

رمز نگاری داده‌های در حال مبادله مهمترین وجه اختفاء در ارتباطات تلفن ثابت است. البته اختفاء در این زمینه مصادیق دیگری دارد که در زیر به آنها اشاره شده است:

- تغییر مکان منطقی اجزاء با کارکردهای مشخص
- شبکه‌های خصوصی مجازی
- اختفای اماکن از طریق تلفیق اماکن با کارکردهای گوناگون در یک مکان جغرافیایی

- اختفای تماس‌ها از طریق تغییر مشخصات قراردادی
- استفاده مناسب از تنوع کاربری، و ایجاد و برقراری تماس ها در کلاف‌هایی از تماس های عمومی که توسط مهاجم به سهولت قابل تشخیص و رویت نباشد
- حذف نقاط با ارزش از روی نقشه‌هایی که به دلیل خاص ی باید در رسانه‌های گروهی منعکس شود
- اختفای مشخصات تجهیزات و توصیفات اجزای با ارزش شبکه و نیز توصیفات دارایی‌های با ارزش موجود در شبکه تلفن ثابت

اصل استتار

استتار در شبکه تلفن ثابت دارای مصادیقی است که در ادامه به بخشی از آن ها اشاره می‌شود:

- استتار درون‌شبکه‌ای: عبارت است از اینکه در درون شبکه دارایی های با ارزش تا حد امکان مشابه دیگر دارایی‌ها جلوه داده شوند.

هدف اصلی در این روش استتار آن است که نقش و جایگاه یک دارایی از دید عناصر شبکه به خوبی قابل شناسایی و حدس زدن نباشد. به عنوان مثال یک مشترک نباید بتواند به راحتی تشخیص دهد که مرکز مخابراتی وی یک مرکز محلی، منطقه‌ای یا ملی است. همچنین بر اساس اصل دسترسی افراد به اطلاعات در حد لزوم، این استتار حتی در قبال پرسنل فنی شبکه نیز توصیه می‌شود به عنوان مثال در مواقعی می‌توان به گونه‌ای عمل کرد که مشخصات فنی ارتباطات مهم، حساس وحیاتی در هر

موقعیت از شبکه مشابه مشخصات فنی عموم ارتباطات موجود در آن منطقه محلی باشد.

- استتار برون شبکه‌ای: عبارت است از اینکه دارایی های با ارزش از دید خارج از شبکه قابل تمییز از دارایی‌های عادی نباشد.

از دید خارج از شبکه مجموعه‌ای از پارامترها از قبیل مشخصات مربوط به ترافیک ارتباطات، تدابیر امنیتی که ذینفعان شبکه جهت حفاظت از آن اتخاذ می کنند و دامنه و کیفیت مخاطبین و مراجعات انسانی به یک عنصر، توصیف گر سطح اهمیت آن در شبکه است. یکی از مهم ترین ابزارهایی که در حصول به چنین پارامترهایی مورد استفاده قرار می‌گیرد، تحلیل‌های آماری ترافیک است. به همین دلیل لازم است تدابیری اتخاذ شود که یا امکان تحلیل آماری از دشمن گرفته شود و یا با تحت تأثیر قرار دادن داده‌ها سعی در گمراه نمودن دشمن در تحلیل آماری شود. از این رو یکی از روش های ارائه داده غلط به دشمن اینست که داده‌های ترافیک به گونه‌ای تنظیم شود که تحلیل‌های آماری روی تماس های مهم، حساس و حیاتی مشابه سایر تماس ها باشد. همچنین با توجه به این استدلال که معمولاً میزان اهمیت یک دارایی نسبت منطقی با میزان تدابیر امنیتی مربوطه دارد؛ لذا یک رویکرد صحیح اینست که تدابیر امنیتی که برای حفاظت از دارایی های مهم، حساس و حیاتی اتخاذ می‌شود مشابه تدابیر امنیتی عمومی به نظر برسد.

اصل استحکامات و موانع

در شبکه تلفن ثابت از گونه‌های مختلفی از استحکامات و موانع می‌توان بهره برد. از استحکامات فیزیکی گرفته تا روش‌های نرم‌افزاری کنترل دسترسی ها که در ادامه به برخی از آنها اشاره می گردد.

- استفاده از انواع سازوکارهای دفاعی نرم افزاری از جمله:
  - دیواره‌های آتش
  - سامانه‌های کنترل دسترسی
  - کشف و توقیف رفتارهای نامتعارف
  - سامانه‌های تشخیص حمله و نفوذ
- استفاده از فاصله

این روش به انواع تدابیری اشاره دارد که فاصله ابزارهای موجود در دست دشمن را از ابزارهایی که به واقع می‌تواند شبکه را مورد تهدید قرار دهد، زیاد می کند. به عنوان مثال بومی‌سازی قراردادهای شبکه‌ای باعث ایجاد فاصله شبکه با معیارهای استاندارد و به همین تناسب دشواری شناخت شبکه توسط دشمن می‌شود.

- استفاده از توپوگرافی

این روش شامل استفاده از پتانسیل های ماهوی در شبکه تلفن ثابت که برخاسته از الگوهای استفاده محلی از این شبکه است؛ می شود.

- استفاده از زیستگاه‌ها

در این روش از تجمع‌های مفید دارایی های معمولی جهت محافظت از دارایی‌های مهم، حساس و حیاتی بهره‌گیری می شود. به عنوان مثال

ارتباطات مهم، حساس و حیاتی با خارج از کشور، می‌تواند از طریق شماره‌هایی صورت پذیرد که در محدوده شماره‌های مناطقی از کشور است که مهاجرین بیشتری در خارج از کشور دارد.

اصل پراکندگی

به طور کلی ایجاد پراکندگی در دارایی های مهم، حساس و حیاتی از لحاظ فیزیکی و منطقه‌ای به عنوان یک اصل دفاعی ضرورت دارد. به عنوان مثال لازم است:

- حتی‌المقدور تأسیسات مهم، حساس و حیاتی شبکه از جمله مراکز منطقه‌ای و ملی به صورت پراکنده در جغرافیای کشور قرار داده شود.
- ارتباط‌های با ارزش دارای پراکندگی زمانی یا مکانی باشند.

اصل توزیع‌شدگی

توزیع‌شدگی در شبکه تلفن ثابت به معنای ایجاد شرایطی برای توزیع ارزش دارایی‌ها، و نیز حمایت عملکردی اجزاء شبکه از یکدیگر در شرایط بحران است. توزیع شدگی مصادیق متعددی دارد از جمله:

- توزیع تماس‌ها از طریق استفاده از خطوط تماس متعدد
- توزیع داده تماس‌هایی مثل نمابر بر روی تماس‌های توزیع شده
- توزیع تجهیزات و اجزاء به منظور ایجاد افزونگی پشتیبان
- ایجاد افزونه برای انباره‌های داده‌ای
- نیروهای انسانی متعدد برای مدیریت و نگهداری اماکن و تجهیزات خاص

اصل فریب

این اصل شامل قرار دادن ساز وکارهایی در جهت شناسایی هدف های اشتباه و اتلاف انرژی مهاجمین می‌شود. از جمله مکانیزم های این روش می توان به موارد ذیل اشاره کرد:

- ایجاد مکانیزم های ظرف عسل[1]
- تنظیم اطلاعات اشتباه در پیغام‌های امضای تجهیزات
- مهم جلوه دادن اطلاعات بی‌ارزش

[1] Honey Pot سیستم یا قسمتی از یک سیستم است که برای فریب دادن کاربر غیر مجاز به صورت عمدی گذاشته می شود.