فصلنامه علمی-ترویجی پدافند غیرعامل
سال ششم، شماره ۴، زمستان ۱۳۹۴، (پیاپی ۲۴): صص ۲۲ -۱۵

یک مدل کنترل دسترسی زمان‌دار مبتنی بر اهداف برای ارتقاء حفظ حریم خصوصی

محمدباقر عرفانی[۱]، محمدعلی جوادزاده[۲]، محمدرضا کنگاوری[۳]

تاریخ دریافت: ۹۳/۰۷/۲۰
تاریخ پذیرش: ۹۴/۰۳/۲۷

چکیده

صاحبان اطلاعات، بر اساس اهدافی اطلاعاتشان را انتشار می‌دهند؛ و استفاده از اطلاعات باید در جهت همان هدفی باشد که انتشار یافته است. بنابراین، وجود یک روشی برای کنترل دسترسی به اطلاعات انتشاریافته، لازم و ضروری است. این مدل از یک سو به سازمان‌ها و شرکت‌ها کمک می‌کند که بتوانند مشتری‌های مرتبط با فعالیت کسب‌وکار خود را جذب کنند و از سوی دیگر، به صاحبان اطلاعات این امکان را می‌دهد که بتوانند جمع‌آوری‌کنندگان اطلاعات (شرکت‌ها و سازمان‌ها) را در استفاده از اطلاعات شخصی خود محدود کنند. اهداف به دو نوع، اهداف مجاز و اهداف غیرمجاز تقسیم می‌شوند؛ و صاحبان اطلاعات، مجاز یا غیرمجاز بودن آن ها را تعیین می‌کنند. این مدل به اهدافی که صاحبان اطلاعات تعیین می‌کنند یک پارامتر زمان اضافه می‌کند تا انتشار اطلاعات خود را محدودتر کنند؛ یعنی اینکه صاحبان اطلاعات، برای اهدافی که انتخاب کرده‌اند محدوده زمانی را تعیین می‌کنند که در این محدوده زمانی، استفاده از اطلاعات امکان‌پذیر است. وجود محدوده زمانی در انتشار اطلاعات، باعث ارتقاء حفظ حریم خصوصی افراد می‌شود. با توجه به اینکه انتشار اسناد محرمانه، فوق محرمانه، سری و به‌کلی سری در پدافند غیرعامل از اهمیت ویژه‌ای برخوردار است؛ این مدل، با تعیین محدوده زمانی، از انتشار اسناد ملی و نظامی در زمان نامناسب جلوگیری می‌کند.

کلیدواژه‌ها: کنترل دسترسی زمان‌دار، اهداف دسترسی، اهداف مجاز، اهداف غیرمجاز، حفظ حریم خصوصی.

۱- کارشناس ارشد دانشگاه جامع امام حسین (ع) -mb.erfani@yahoo.com- نویسنده مسئول
۲- مربی و عضو هیئت علمی دانشگاه جامع امام حسین(ع)
۳- دانشیار، دانشگاه علم و صنعت ایران

۱- مقدمه

شرکت‌ها، سازمان‌ها، وب‌سایت‌های شخصی و تجاری و مانند آن، با اهداف[1] گوناگون اقدام به جمع‌آوری اطلاعات شخصی افراد در پایگاه‌های داده خود می‌کنند و از این اطلاعات برای اهداف خاصی بهره می‌برند که در مواردی از این اطلاعات استفاده‌هایی می‌شود که مدنظر و خواست صاحب آن اطلاعات نیست. ازاین رو افراد در ثبت و افشاء اطلاعات شخصی خود بیمناک بوده و در اغلب موارد با بی‌اعتمادی نسبت به جمع‌آوری کنندگان اطلاعات، اطلاعات خود را در اختیار آن‌ها قرار نمی‌دهند. طبق مطالعه‌ای که گروه تجارت فدرال آمریکا انجام داده است، ۹۷ درصد از وب‌سایت-ها برای ثبت‌نام کاربران خود، حداقل نام، نام خانوادگی، آدرس پست الکترونیکی و یا آدرس پستی را از مشتریان خود درخواست می‌کنند که این اطلاعات در حوزه حریم خصوصی افراد است[۵]. افراد برای اینکه حریم خصوصی خود را حفظ کنند با ثبت نکردن اطلاعات، خود را از یکسری خدمات محروم می‌کنند و از طرف دیگر، جمع‌آوری‌کنندگان اطلاعات که اغلب، شرکت‌ها می‌باشند زیان می‌بینند. برای حفظ حریم خصوصی با اهداف دسترسی، کارهای قابل‌توجهی صورت گرفته است. ازجمله کارهای صورت گرفته، مدل کنترل و دسترسی مبتنی بر اهداف [۶] می‌باشد که بر اساس مدل کنترل دسترسی نقش مبنا[2] است که با تعیین نقش‌ها، دسترسی به اطلاعات را کنترل می‌کند. از دیگر مقالات ارائه شده، طراحی یک مدل کنترل دسترسی مبتنی بر اهداف [۲] توسط Buyn و همکارانش است. بدین‌صورت که درختی از اهداف توسط شرکت‌ها تعیین می‌شود و مشتری‌ها استفاده از اطلاعاتشان را در اهداف تعیین‌شده، مشخص می‌کنند و این امکان برای مشتری ها به‌وجود می‌آید که از انتشار اطلاعاتشان در اهدافی که خواست آن‌ها نیست، جلوگیری کند و یا برای اهدافی که مدنظر و خواست آن‌هاست، انتشار یابد. مثلاً اطلاعات در بخش تبلیغات (به‌عنوان یک هدف) استفاده نشود، ولی در بخش آموزش مورد استفاده قرار گیرد [۲،۳،۴]. در سال ۲۰۰۹، kabir و wong با افزودن شروطی به اهداف دسترسی، مدل Byun را ارتقا داده و جمع‌آوری اطلاعات توسط شرکت‌ها را با در نظر گرفتن حریم خصوصی افراد بیشتر کردند[۱]. بدین ترتیب که اهدافی که مشتری به‌صورت کلی از انتشار آن‌ها جلوگیری کرده است را با جزییات بیشتر و انتخاب را برای مشتری بیشتر می‌کند. به‌عنوان مثال، ممکن است مشتری اطلاعات را در تبلیغات خارج از کشور منع کند، ولی مایل به استفاده از اطلاعاتش در تبلیغات داخل کشور باشد. ما در این مقاله سعی داریم به اهدافی که مشتری تعیین کرده است یک پارامتر زمان اضافه کنیم تا محدودیتی برای استفاده از اطلاعات انتشاریافته ایجاد کنیم. لذا دسترسی محدود به اطلاعات شخصی افراد و همچنین اسناد طبقه‌بندی، باعث ارتقاء حریم خصوصی می‌شود. بدین ترتیب که یک مشتری ممکن است بخواهد برای حفظ حریم خصوصی خود و برای اهداف تعیین‌شده، محدوده زمانی معینی را مشخص کند؛ مانند استفاده از اطلاعات با اهداف «تبلیغاتی» تا ساعت ۲۴:۰۰ تاریخ ۰۱/ ۱۰/ ۱۳۹۶ امکان‌پذیر است و بعدازاین زمان، امکان‌پذیر نیست. در ادامه دو طرح را برای کاربرد این مدل پیشنهاد می‌دهیم. اولی در مورد مدیریت کاربران تلفن همراه است و دومی بر مبنای چالشی است که در پدافند غیرعامل حائز اهمیت است. حفاظت از اسناد با ارزش و طبقه‌بندی‌شده در سطح ملی و نظامی از اهمیت ویژه‌ای برخوردار است. اگر در زمان نامناسب انتشار پیدا کنند و یا افراد غیرمجاز به آن‌ها دسترسی پیدا کنند، می‌تواند زیان‌های جبران‌ناپذیری را وارد کند.

۲- ادبیات موضوع

در این مقاله، از درخت اهداف برای بیان مقاصد انتشاردهندگان اطلاعات استفاده می‌شود. هر گره نشان‌دهنده هدف است که می‌تواند به‌عنوان هدف مجاز(اعلان مجوز بهره‌برداری) و یا هدف غیرمجاز به‌عنوان عدم انتشار اطلاعات بیان شود. لبه‌ها رابطه سلسله‌مراتبی بین دو هدف را مشخص می‌کنند. R_i و R_j گره های درخت هستند که اگر مسیر رو به پایین وجود داشته باشد، گره R_i والد گره R_j است و گره R_j فرزند گره R_i است (شکل ۱).

در اینجا ما یکسری موضوعات داریم که توسط استفاده‌کنندگان ارائه می‌شود که می‌خواهند اطلاعات مشتری را برای آن مقاصد مورد بهره‌برداری قرار دهند که به آن‌ها ((اهداف)) می‌گوییم و از بین این اهداف، در هنگام جمع‌آوری صاحبان اطلاعات انتخاب می‌کنند که اطلاعاتشان برای چه اهدافی استفاده شود؛ به این‌گونه اهداف، اهداف مشتری می‌گوییم.

اهداف مجاز[3] (AIP): اهدافی که مشتری مشخص می‌کند که اطلاعاتش برای این اهداف استفاده شود؛ یعنی مجوز بهره‌برداری را برای استفاده‌کنندگان صادر می‌کند.

اهداف غیرمجاز[4] (PIP): اهدافی که مشتری مشخص می‌کند که اطلاعاتش برای این اهداف استفاده نشود. برای مشتری مهم است که اطلاعاتش برای این اهداف انتشار نیابد.

در این مقاله مجموعه اهداف را با ω نشان می‌دهیم و در قالب

1– Purpose
2– Role base access control(RBAC)
3– Allowable Intended Purpose
4– Prohibited Intended Purpose

درخت، Ω نشان‌دهنده اهداف به‌صورت سلسله مراتبی (شکل ۱) است.

مثال ۱:

ω={اهداف عمومی{مدیر{پروفایل، گزارش‌ها}،{حمل‌ونقل}، {خرید}، {تبلیغات {مستقیم{ایمیل{ویژه‌ها، خدمات به‌روزرسانی}، تلفن}، {باواسطه{ایمیل واسط، آدرس پستی واسط}}}}}

روابط اهداف:

$AIP \subseteq w,\ PIP \subseteq w$

$IP^{1} = \{AIP, PIP\}$

$IP^{*} = AIP^{\downarrow} - PIP^{\downarrow}$

$AIP^{\downarrow}$: مجموعه‌ای از تمام گره‌های (اهداف) مجاز و فرزندان آن گره را شامل می‌شود.

$PIP^{\downarrow}$: مجموعه‌ای از تمام گره‌های (اهداف) غیرمجاز و فرزندان آن گره را شامل می‌شود.

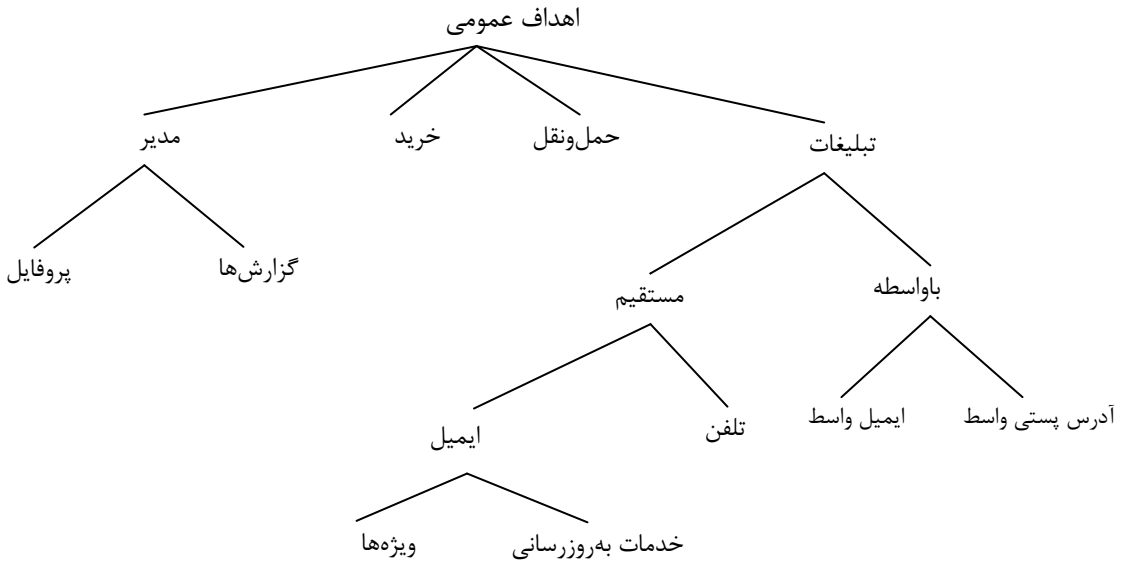
برای مثال اگر داشته باشیم ({ایمیل} {مدیر، مستقیم}) =IP آنگاه:

{{تلفن} مستقیم، {گزارش‌ها، پروفیل} مدیر} = IP* می‌شود [۱، ۲، ۷ و ۸].

اهداف دسترسی (AP): در درخت اهداف (Ω)، اگر داشته باشیم $IP=\{AIP,PIP\}$ و $IP^{*}=AIP^{\downarrow}-PIP^{\downarrow}$، اهداف دسترسی مجموعه‌ای از اهداف قابل‌استفاده در درخت Ω ($IP \Leftarrow_{\Omega} AP$) اگر و فقط اگر $AP \in IP^{*}$ باشد.

۳- پارامتر زمان

زمان دسترسی اهداف (T): زمانی است که مشتری برای هر هدف تعیین می‌کند و زمان دسترسی به هدف را مشخص می‌کند. همان‌طور که گفته شد، مشتری از بین اهداف، دو نوع هدف، اهداف مجاز و اهداف غیرمجاز را مشخص می‌کند. اگر پارامتر T را صفر (Ø) قرار دهیم، نشان‌دهنده عدم استفاده از این هدف در هیچ زمانی است و اگر پارامتر T را بی‌نهایت(∞) قرار دهیم، نشان‌دهنده استفاده از این هدف در هرزمانی است. ما در این مقاله سه حالت ممکن برای زمان دسترسی اهداف (AIP) در نظر گرفته‌ایم، حالت اول t_s[۲]، دسترسی اهداف تا زمان T تعیین می‌شود ($T \leq AIP$)، حالت دوم t_g[۳]، دسترسی یا عدم دسترسی به اهداف بعد از زمان T تعیین می‌شود ($AIP \leq T$) و حالت سوم t_b، دسترسی یا عدم دسترسی به اهداف در محدوده زمانی خاصی تعیین می‌شود ($T_1 \leq AIP \leq T_2$). اهداف در این حالت‌ها قابل‌دسترس هستند و در غیر این صورت اهداف غیرقابل دسترس می‌باشند و حالت PIP دارند.



شکل ۱- درخت اهداف Ω [۱، ۲، ۷ و ۸]

1– Intended Purpose

2– Accessible Purpose
3– Smaller than
4– Greater then

جدول۱. درخت اهداف

نام	age	tel	$name_{ip}$	age_{ip}	tel_{ip}
علی	۴۰	۲۲۷۷۸۸۰۱	{{G, t_g };{ S, t_g }}	{{A, t_∞ };{M, t_b }}	{{G, t_s };{ M, ø }}
عادل	۱۸	۳۳۴۰۰۰۴۰	{{G, t_g };{ P, ø }}	{{G, t_g };{M, t_g }}	{{G, t_g };{M, t_g }}
ثمین	۲۲	۸۸۲۸۸۲۳۲	{{G, t_s };{ M, ø }}	{{G, t_s };{M, t_b }}	{{G, t_s };{P, t_b }}
رویش	۲۹	۵۵۴۹۴۹۵۶	{{G, t_b };{ S, ø }}	{{G, t_s };{M, ø }}	{{G, t_b };{P, t_b }}

G={General purpose}, A={Admin purpose}, S={Shipping purpose}, P={Purchase purpose}, M={Marketing purpose}, ip={Intended purpose}={AIP, PIP}, t =Time

به‌عنوان‌مثال، دسترسی علی برای اهداف عمومی و حمل‌ونقل زمان مشخصی تعیین شده که بعد از این زمان، قابل‌دسترس است. دسترسی به سن علی برای اهداف عمومی برای همیشه مجاز تعیین شده و دسترسی به سن علی برای اهداف تجارت در محدوده زمانی خاصی تعریف‌شده که خارج از این محدوده، قابل‌دسترس نیست. دسترسی به تلفن علی برای اهداف عمومی تا زمان خاصی قابل‌دسترس است و بعدازاین زمان قابل‌دسترس نیست و دسترسی به سن علی برای تجارت در هرزمانی منع شده و قابل دسترس نیست.

۴- پیاده‌سازی

برای پیاده‌سازی این روش، بر اساس زبان پرس‌وجو (SQL) در پایگاه داده لازم است، روشی را برای ذخیره‌سازی درخت اهداف داشته باشیم و سپس بتوانیم بر اساس این ذخیره‌سازی پرس‌وجوهای لازم را اجرایی کنیم. اگر به آنچه داریم، نگاهی بیندازیم شامل یک درخت اصلی است که مشتری‌ها بر اساس آن تعیین می‌کنند که کدام اهداف مجاز و کدام غیرمجاز هستند و زمان استفاده را بر اساس پارامتر $\{t_g, t_s, t_b, ø\}$برای هر هدف مشخص کند.

پیشنهاد می‌شود برای هریک از مؤلفه‌های ذکرشده به صورت جداگانه مثلاً در یک جدول پایگاه داده ذخیره شوند، مانند آنچه در جدول (۲) می‌بینیم. چون مجاز بودن یا نبودن اهداف، وابسته به پارامتر زمان است. پس کنترل اصلی در اینجا بر اساس پارامتر T صورت می‌گیرد. بدین‌صورت که برای اهداف غیرمجاز همیشه T=0 است، پس‌نیازی به ذخیره‌سازی آن نداریم. ولی برای اهداف مجاز، پارامترهای دسترسی $\{t_g, t_s, t_b\}$ می‌بایست بررسی شوند. در جدول (۲) نمونه‌ای از ذخیره‌سازی را مشاهده می‌کنیم.

جدول ۲. نحوه ساخت درخت اهداف

P_id	P_name	Parent	Code	PIP	$AIP\_T_۱$	$AIP\_T_۲$
۱	A	-	øx۲۰۰	øx۳FF	Ø	Ø
۲	B	۱	øx۱۰۰	øx۳۳۰	۱۳۹۳/۰۱/۰۱-۲۴۰۰	۲۴۰۰-۱۳۹۶/۰۱/۰۱
۳	C	۱	øx۰۸۰	øx۲۸۰	∞	∞
۴	D	۱	øx۰۴۰	øx۲۴F	۱۳۹۳/۰۱/۰۱-۲۴۰۰	Ø
۵	E	۲	øx۰۲۰	øx۳۲۰	۱۳۹۴/۰۱/۰۱-۲۴۰۰	۲۴۰۰-۱۳۹۵/۰۱/۰۱
۶	F	۲	øx۰۱۰	øx۳۱۰	۱۳۹۳/۰۱/۰۱-۲۴۰۰	∞
۷	G	۴	øx۰۰۸	øx۲۴B	۱۳۹۳/۰۱/۰۱-۲۴۰۰	∞
۸	H	۴	øx۰۰۴	øx۲۴۴	۱۳۹۴/۰۱/۰۱-۲۴۰۰	۲۴۰۰-۱۳۹۹/۰۱/۰۱
۹	I	۷	øx۰۰۲	øx۲۴A	۱۳۹۲/۰۱/۰۱-۲۴۰۰	Ø
۱۰	J	۷	øx۰۰۱	øx۲۴۹	∞	∞

برای عمل پرس‌وجو ما همواره نیاز داریم تمام حالت‌های لازم را بررسی کنیم (()comp check در جدول ۳). در حالت t_g ،t_s و t_b اهداف مجاز را بررسی می‌کنیم. بررسی اهداف مجاز، بر اساس مقایسه تاریخ و زمان سرور و با مقدار T صورت می‌گیرد و هر بار که نیاز باشد، پرس‌وجو اجرا می‌شود (()Modifying_Query در جدول ۳) تا برای یک هدف بر اساس قوانین حریم خصوصی تصمیم گرفته شود.

۵- تاثیر پارامتر زمان در حفظ حریم خصوصی

اگر T_∞ برابر زمان بی‌نهایت باشد (مشتری برای هدف، محدودیت زمانی تعیین نکرده باشد) و اگر T_T برابر است با یک مقدار زمانی (زمانی ثابت برای استفاده از هدف) و $T_\emptyset$ برابر مقدار زمانی صفر است (مشتری دسترسی به این هدف را منع کرده است)؛ و از طرفی خدمات (اهداف شرکت‌ها) را با AIP نشان دهیم. بررسی می‌کنیم که چه تأثیری بر حفظ حریم خصوصی دارد.

اگر هدفی برابر T_∞ باشد $AIP= T_\infty$ است بدین معنی است که پارامتر زمان، تأثیری بر محدودیت اهداف ندارد و می‌توان تا بی‌نهایت زمانی از آن استفاده کرد؛ مانند آنچه در مدل BYUN [۲] می‌بینیم.

اگر هدفی برای اطلاعات یک مشتری برابر $T_\emptyset$ باشند، $AIP=T_\emptyset$ بدین معنی است که حفظ حریم خصوصی‌اش را بر خدمات ترجیح می‌دهد.

اگر هدفی برای اطلاعات یک مشتری برابر $T_{T(g,s,b)}$ باشد، بیانگر این است که مشتری در زمان محدودی خدمات را بر اطلاعات شخصی‌اش ترجیح می‌دهد؛ بنابراین، افزودن پارامتر زمان نشان می‌دهد که در یک زمان‌های خاصی مشتری اجازه استفاده از اطلاعاتش را می‌دهد و در زمان‌های دیگر این اجازه را سلب می‌کند، یعنی $T_T<T_\infty$ و می‌توان نتیجه گرفت که زمان محدود برای استفاده از یک هدف به حفظ حریم خصوصی کمک می‌کند.

۶- دو پیشنهاد برای استفاده از این مدل

پیشنهادهایی که در زیر مطرح‌شده‌اند از جنبه تجاری و امنیتی حوزه فناوری اطلاعات در حوزه پدافند غیرعامل است.

پیشنهاد اول: با رشد فنّاوری ارتباطات و همه‌گیر شدن استفاده از تلفن‌های همراه، ارسال پیامک‌های تبلیغاتی چالش‌هایی را، هم

جدول ۳. پرس‌وجو بر روی جدول اهداف

```
Comp_check (ap, AIP_T1, AIP_T2){
Returns Boolean
if((ap&AIP_T1) ≠۰ && AIP_T2 =∞ && (ap&AIP_T1) ≤ ∞)
Return true;// T∞
if((ap&AIP_T1) ≠۰ && AIP_T2 =0 && (ap&AIP_T1) ≤ Server(Datetime))
Return true;//Ts
elseif((ap&AIP_T1) ≠۰ && (ap&AIP_T2) =∞ && (ap&AIP_T1) ≥ Server(Datetime))
Return true;//Tg
elseif((ap&AIP_T1) ≠۰ && (ap&AIP_T1) ≥ Server(Datetime) && (ap&AIP_T2) ≤ Server(Datetime)))
Return true;//Tb
Else false;
                                                                    }

Modifying_Query (Query Q)
Returns a modified privacy-preserving query Q
Let R1,…, Rn be the relations referenced by Q
Let P be the predicates in WHERE clause of Q
Let a1,…, am be the attributes referenced in both
the projection فهرست and P
Let AP be the access purpose encoding of Q
for each Riwhere i=1,n do
if (Comp_Check (AP, Ri_aipt1, Ri_aipt2))=False then
return ILLEGAL-QUERY;
end if;
end for;
return Q without modified P;
```

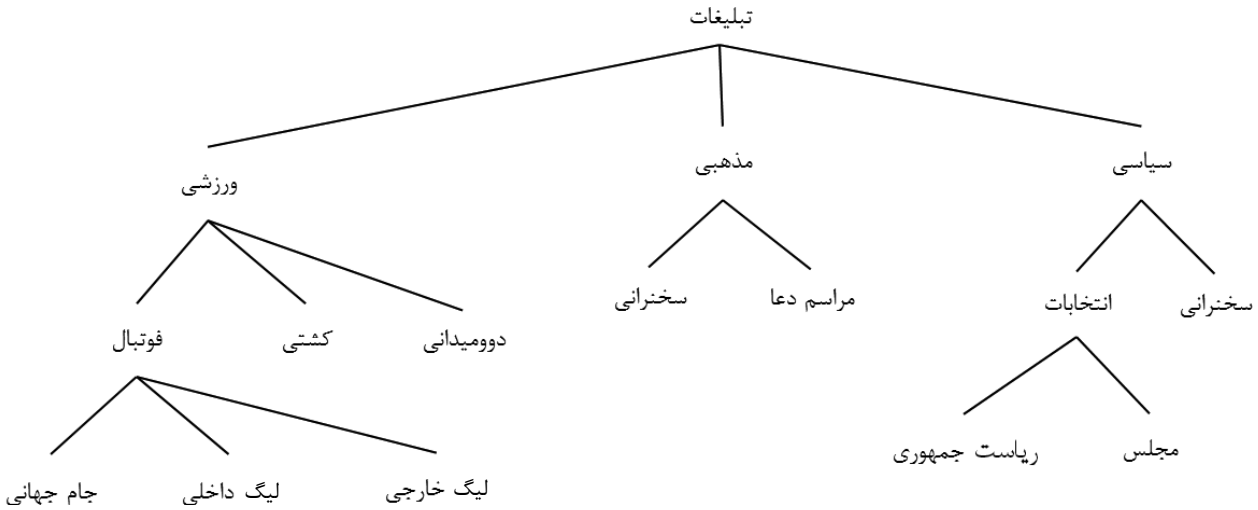
برای اپراتورهای تلفن همراه و هم برای مشترکین مشکلاتی را به وجود آورده است. از طرفی اپراتورها نمی‌توانند از سود سرشار تبلیغات بگذرند و اینکه اطلاعات مشترکین خود را در اختیار شرکت‌ها و سازمان‌ها قرار دهند، منع قانونی دارد و از طرفی پیامک‌ها برای مشترکین این اپراتورها مشکل‌ساز و آزاردهنده شده است. به‌طوری‌که حریم خصوصی آن‌ها مورد تعرض قرار می‌گیرد. با استفاده از این مدل، مشترکین اهداف {PIP، AIP} و زمان اعتبار این اهداف را مشخص می‌کنند. با این روش اولاً مشترکین با توجه به نیازمندی که دارند تبلیغات را دریافت می‌کنند. ثانیاً صاحبان تبلیغات به جامعه هدف خود، تبلیغ ارسال می‌کنند و از ارسال پیامک‌های بی‌اثر جلوگیری می‌شود. ثالثاً شرکت‌های تلفن همراه از چالش‌های قانونی که باعث نقض حریم خصوصی می‌شود، رهایی پیدا می‌کنند.

نمونه کوچکی از اهداف تبلیغات در شکل (۲) نمایش داده شده است.

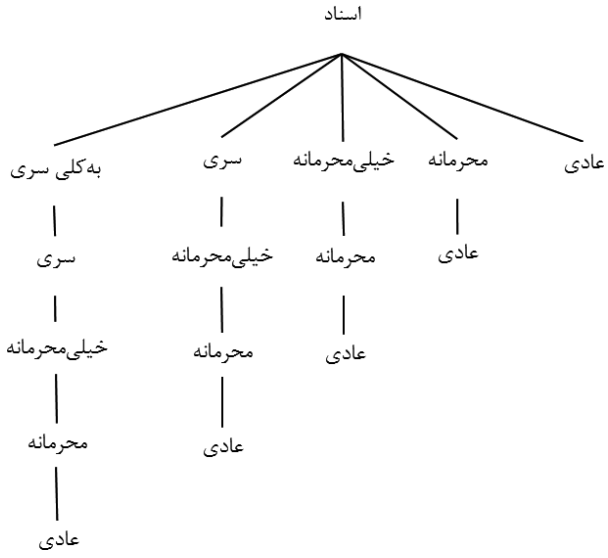
اپراتورها با روش‌های گوناگون می‌توانند از نظرات مشترکین خود مطلع شوند. مثلاً فرم حریم خصوصی مخصوص تبلیغات را در پورتال خود قرار دهند تا مشترک بر اساس نیاز خود آن را پرکنند، یا از روش‌های ارتباطی تلفنی مثل پیامک استفاده شود و یا از ترکیب این دو روش و روش‌های دیگر بهره ببرند. در ضمن امکان حذف و ویرایش را برای مشترکین خود فراهم نمایند. از هر روشی که استفاده می‌شود، می‌بایست اهداف (تبلیغات) را مشخص کرده (با جزئیات در نظر گرفتن سلسله‌مراتب) و در این حال مشترک بتواند زمان پایان یک تبلیغ را بر اساس {T،∞}مشخص کند. با این تدبیر، ضمن اینکه تبلیغات به‌وسیله اپراتورها شکل قانونی به خود می‌گیرد، حفظ حریم خصوصی مشترکین نیز در نظر گرفته می‌شود که خود نوعی تبلیغ است. شکل (۲) نمونه‌ای از درخت اهداف بدین منظور است.

پیشنهاد دوم: اسناد ملی و نظامی از لحاظ ماهیتی که دارند، انتشار آن‌ها بر اساس یک سیاست مشخص انجام می‌گیرد. خصوصیت انتشاراتی، به‌طور معمول در قالب طبقه‌بندی عادی، محرمانه، سری و به‌کلی سری قرار می‌گیرد که هرکدام در سازمان‌های مختلف تعریف خاص خود را دارند. انتشار اسناد دارای طبقه‌بندی برای کسانی که حق دسترسی به آن را ندارند، می‌تواند عواقب خطرناکی در سطح ملی و سازمانی داشته باشد؛ و از طرفی انتشاردهنده اگر ناخواسته یک سند دارای طبقه‌بندی را انتشار دهد ممکن است ازلحاظ حقوقی دچار مشکل شود. مطابق با قانون انضباطی نیروهای مسلح جمهوری اسلامی، اسناد طبقه‌بندی شده باگذشت زمان معین، از ارزش و اعتبار آن ها کاسته شده و قابل‌تبدیل شدن به سطوح پایین‌تر هستند [۹]. مثلاً اسناد محرمانه بعد از گذشت مدتی بنا بر ابلاغیه درون‌سازمانی به عادی قابل تبدیل و انتشار آن مجاز است. استفاده از این مدل می‌تواند با تعیین سیاست‌ها، جلوی انتشار اسناد طبقه‌بندی را از زمان ایجاد تا زمانی که این سند مجوز انتشار نداشته باشد، بگیرد.

در این ساختار، اهداف مجاز{AIP} برای انتشار (با توجه به سیاست سازمان) به‌حق دسترسی افراد وابسته است. مثلاً کسی که حق دسترسی به اسناد سری را دارد، حق انتشار اسناد سری و پایین‌تر را دارد و بالعکس حق انتشار اسناد بالاتر (به‌کلی سری) را



شکل ۲- درخت اهداف تبلیغات



شکل ۳– درخت اهداف اسناد

ندارد. در کنار حق دسترسی به اسناد، سطوح طبقاتی دارای مدت اعتبار نیز می‌باشند، یعنی سطوح دسترسی اسناد بعد از مدتی تقلیل پیدا می‌کنند. مثلاً بعد از هفت سال، سطح ((به‌کلی سرّی)) به سرّی بعد از پنج سال، سطح سری به محرمانه و همین‌طور تا آخر که یک سند به سطح عادی برسد و انتشار آن عمومی گردد. گره‌های درخت اهداف، برای عده‌ای قابل‌انتشار است و برای عده‌ای غیرقابل انتشار و هر گره دارای مدت اعتبار مشخص است که پس از اتمام این مدت، سطح دسترسی آن یک پله تنزل پیدا می‌کند و برای افرادی که سطح دسترسی پایین‌تری دارند، دسترس پذیر می‌شود.

همان‌طور در جدول (۴) مشاهده می‌شود، اسناد دارای زمان اتمام یک طبقه‌بندی خاص است، مثلاً سند A در درخت اسناد دارای سطح یک و نوع ((به‌کلی سری)) است که در زمان AIPend این سند از حالت ((به‌کلی سری)) به ((سری)) تبدیل می شود و زمان جدید که مربوط به سری بودن سند است، به آن اختصاص می‌یابد و کاربری که مجوز دسترسی به این سند را دارد بتواند از آن بهره ببرد؛ و به همین ترتیب این به‌روز رسانی انجام می‌گیرد تا یک سند فاقد طبقه‌بندی شود و مجوز انتشار عمومی گردد.

۷- نتیجه‌گیری

همان‌طور که مشاهده شد درخت اهداف برای حفظ حریم خصوصی صاحبان اطلاعات تشکیل می‌شود و اگر پارامتر زمان به این درخت افزوده شود در شرایطی که زمان برای اهداف مجاز با بی‌نهایت مقداردهی نشده باشد، یعنی زمانی برای پایان استفاده از اهداف مشخص‌شده باشد، می‌تواند حفظ حریم خصوصی صاحبان اطلاعات را ارتقاء دهد. حفظ حریم خصوصی ضمن احترام به مشتری، استفاده‌کنندگان اطلاعات را در شناخت مشتریان خود تقویت می‌کنند و مشتری‌های مرتبط با هدف را انتخاب می‌کنند. حفاظت از اسناد ملی و حفظ حریم خصوصی که از مباحث امنیت است در پدافند غیرعامل دارای اهمیت بسزایی است. همان‌طور که در این مدل دیده شد، حفاظت اسناد دارای طبقه بندی‌شده و انتشار این اسناد در زمان مناسب با دسترسی افراد مجاز می‌تواند در سطوح ملی و نظامی به‌کار گرفته شود.

جدول ۴. ساختار ذخیره‌سازی اسناد دارای طبقه‌بندی

P_id	DOC	CODE	AIP_{pub}	AIP_{End}	LEVEL	TYPE
۱	A	øx۲۰۰	۱۳۹۰/۰۱/۰۱-۲۴۰۰	۱۴۰۲/۰۱/۰۱-۲۴۰۰	۱	به‌کلی سری
۲	B	øx۱۰۰	۱۳۸۹/۰۱/۰۱-۲۴۰۰	۱۳۹۰/۰۱/۰۱-۲۴۰۰	۱	محرمانه
۳	C	øx۰۸۰	۱۳۹۳/۰۱/۰۱-۲۴۰۰	۱۴۰۰/۰۱/۰۱-۲۴۰۰	۲	خیلی محرمانه
۴	D	øx۰۴۰	۱۳۹۳/۰۱/۰۱-۲۴۰۰	Ø	۲	عادی
۵	E	øx۰۲۰	۱۳۹۳/۰۱/۰۱-۲۴۰۰	۱۳۹۶/۰۱/۰۱-۲۴۰۰	۲	محرمانه
۶	F	øx۰۱۰	۱۳۹۰/۰۱/۰۱-۲۴۰۰	۱۴۰۲/۰۱/۰۱-۲۴۰۰	۲	سری
۷	G	øx۰۰۸	۱۳۹۳/۰۱/۰۱-۲۴۰۰	۱۴۰۲/۰۱/۰۱-۲۴۰۰	۳	سری
۸	H	øx۰۰۴	۱۳۸۰/۰۱/۰۱-۲۴۰۰	Ø	۳	عادی
۹	I	øx۰۰۲	۱۳۹۲/۰۱/۰۱-۲۴۰۰	۱۳۹۹/۰۱/۰۱-۲۴۰۰	۱	خیلی محرمانه
۱۰	J	øx۰۰۱	۱۳۹۳/۰۱/۰۱-۲۴۰۰	۱۳۹۶/۰۱/۰۱-۲۴۰۰	۳	محرمانه

۸- مراجع

1. K. Mdenamul and W. Hua, “Conditional Purpose Based Access Control Model for Privacy Protection,” Department of Mathematics and Computing University of Southern Queensland, Toowoomba, Queensland 4350, Australia, 2009.
2. J. Byun, E. Bertino, and N. Li, “Purpose based access control of complex data for privacy protection,” In: 10th ACM Symposium on Access Control Model And Technologies, pp. 102-110, Stockholm 2005.
3. J. Byun, E. Bertino, and N. Li, “Purpose based access control for privacy protection in relational database systems,” The VLDB Journal The International Journal on Very Large Data Bases vol. 17, Issue 4, July 2008.
4. E. Bertino, J. Byun, and N. Li, “Privacy preserving database system,” in `FOSAD', pp. 178-206, 2005.
5. Federal Trade Commission, “Privacy online: Fair information practices in the electronic marketplace: A report to congress,” May 2000. Available:www.ftc.gov/reports/privacy2000/ privacy2000.pdf.
6. Y. Naikuo, B. Howard, and Z. Ning, “A purpose-based access control model,” Journal of information assurance and security, vol. 1, pp. 51-58, 2008.
7. B. Elisa, “Purpose Based Access Control for Privacy Protection in Database Systems,” 10th International Conference, DASFAA 2005, Beijing, China, April 2005.
8. W. Hua, S. Lili, and V. Vijay, “Purpose-based access control policies and conflicting analysis,” published in Security and Privacy - Silver Linings in the Cloud Springer (Ed.), pp. 217-228, 1393.

۹. قانون مجازات جرائم نیروهای مسلح جمهور اسلامی ایران، ماده ۲۴، مصوب ۱۳۸۲/۱۰/۰۹.

A Timed Access Control Model Based on Purposes to Amplify Privacy

M. B. Erfani*

M. A. Javadzadeh

M. R. Kangavari

Abstract

Information owners, based on their publication purposes their information and use of information for the same purpose, which is to be published. So there is a way to control access to published information, is essential. This model on the one hand to help organizations and companies so that customers related with your business activity and attract the other hand, this allows information to owners who are able to collect information (companies and organizations) in the use personal information your limit. Two purposes, purposes allowed and purposes unauthorized divided, and the owners of the information, whether allowed or unauthorized define them. This model purposes to determine a time parameter adds information owners to publication their information limit; This means that owners of information, for purposes that have chosen to set time range addressing. The use of information is possible in this time frame. There is time range on the release of information will amplify privacy. Since the publication of confidential documents, secret, secretive completely passive defense is important, this model, to determine the time of publication of national documents and military passes at the wrong time stop. Since the release of confidential documents, secret, secret and completely passive defense is very important series, this model, by specifying a time range of national and military documents to prevent the wrong time.

Key Words: *Timed Access Control, access Purposes, Purposes allowed, Purposes unauthorized, privacy.*

* Imam Hussein Comprehensive University - (mb.erfani@Yahoo.com)-Writer-in-Charge