طراحی پروتکل احراز هویت بر مبنای لگاریتم گسسته

جوادصابری– دانشگاه هوایی شهید ستاری

javad_sattari_iut@yahoo.com

محمد با قری– دانشگاه امام حسین (ع)

mbaghery2000@yahoo.com

چکیده

شبکه های کا مپیوتری کاربرد های زیادی در زندگی روز مره دارندویکی از مسائل مهم که در استفاده از شبکه باید مد نظر قرار گیرد احراز هویت یا شناسایی کاربرا نی است که قصد استفاده از اطلاعات شبکه را دارند.

احرازهویت یا شناسایی کاربران برای دسترسی به انواع اطلاعات مانند اطلاعات تجاری،اسنادنظامی،اطلاعات بانکی و غیره لازم و ضروری است.

در این مقاله در ابتدا به معرفی و ضرورت احراز هویت میپردازیم. سپس طرح شنر[1] و اکاموتو [2]را معرفی میکنیم آنگاه طرح بهبود یا فته ای که ترکیبی از این دو طرح و مبنای امنیتی آن حل ناپذیری لگاریتم گسسته[3] ا ست را مطرح میکنیم .

واژه های کلیدی: طرحهای شناسایی ، طرح شنر، طرح اکا موتو، لگاریتم گسسته

[1] Schnorr
[2] Okamoto
[3] Discrete Logarithms

۱-معرفی طرح احراز هویت

احراز هویت یا شناسایی یعنی یک کاربر هویت واقعی خود را به طرف مقابلش اثبات کند، یعنی فرد کاربر که قصد استفاده از ا طلاعات را دارد به طرف مقابل خود اثبات میکند که او واقعا همان کسی است که ادعا میکند.

به عنوان مثال وقتی شما بخواهید از یک کامپیوتر استفاده کنید یا به حساب بانکی از دستگاه خود پرداز دسترسی پیدا کنید باید احراز هویت شوید . یک راه معمول که در این موارد استفاده میشود وارد کردن کلمه عبور به کا مپیوتر یا دستگاه خود پرداز است . اما میدانیم جعل کردن کلمه عبور بسیار آسان است و هر کسی با دانستن کلمه عبور میتواند خود را به عنوان فرد موجه به سیستم معرفی کند و از اطلاعات سیستم استفاده کند .

یک طرح شناسایی زمان و ا قعی[۱] است و بعد از اجرای پروتکل شناسایی و شناخته شدن فرد اجازه دسترسی به منبع اطلاعاتی صادر میشود .

هر طرح شناسایی دارای دو مولفه است .

الف–اثبات کننده [۲]

ب–تصدیق کننده[۳]

در طرح شناسایی، اثبات کننده تلاش میکند خود را به تصدیق کننده بشناساند و به او اثبات کند او همان کسی است که ادعا میکند.

طرح شناسایی باید دارای خصوصیات زیر باشد .

الف–وقتی اثبات کننده و تصدیق کننده هر دودرستکارباشنداثبات کننده قادر است به طور موفقیت آمیزی خودش را به تصدیق کننده احراز هویت کند .یعنی تصدیق کننده پروتکل شناسایی را با پذیرش مشخصه اثبات کننده کامل میکند.

ب– انتقال پذیری[۱]

[1] Realtime
[2] Prover
[3] Verifier

تصدیق کننده نمیتواند یک تبادل شناسایی را که با اثبات کننده انجام داده استفاده کند تا خودش را به عنوا ن شخص سوم c به جای اثبات کننده(p) به تصدیق کننده(v)اثبات کند.

ج-جعل پذیری [۲]

احتمال اینکه شخص سومی مثل c بجای اثبات کننده p پروتکل شناسایی را انجام دهد و نقش p را بازی کند و باعث شود v مشخصه اش را به عنوان p بپذیرد ناچیز ا ست.

اکثر طرحهای شناسایی که ارائه شده اند از ریاضیات رمز نگاری کمک میگیرند. این طرحها بر اساس مسائل سخت ریا ضی که هنوز راه حلی برای آنها ارائه نشده ا ست بنا شده اند. که سه مساله معروف آنها در ذیل آمده ا ست.

الف- مساله تجزیه اعداد [۳]

ب-حل مساله معکوس rsa

ج-مساله لگاریم گسسته [۴]

نمونه هایی از طرحهای شناسایی که تا کنون ارائه شده اند طرح شنر ،اکا موتو ، فیات شا میر[۵]،فیج فیات شا میر[۶] ،گویلو کویسکویتر[۷] ،انگ شنر[۸]هستند.

طرح شناسایی باید خواص زیر را داشته باشد .

الف-کا مل بودن [۹]:تصدیق کننده همیشه اثبات را می پذیرد اگر اثبات کننده فرد واقعی باشد و اثبات کننده و تصدیق کننده پروتکل را درست دنبال کنند .

ب-ساندنس[۱۰] :یعنی هر کس شانس اجرای موفقیت آمیز پروتکل شناسایی را داشته باشد باید کلید سری اثبا ت کننده را بداند یا قادر باشد آنرا در زمان چند جمله ای بد ست آورد .

---

[1] Transferability
[2] Impersonation
[3] Factoring
[4] Discrete Logarithm
[5] Fiat-Shamir
[6] Feige-Fiat-Shamir
[7] Guillou-Quisquator
[8] Ong-Schnorr
[9] Completeness
[10] Soundness

ج- امنیت [1] : در موقعی که یک اثبات کننده مشخصه ا ش را به تایید کننده در موقعیتهای مختلف اثبات میکند تایید کننده نمیتواند هیچ اطلاعاتی درباره مقدار کلید سری اثبات کننده با شرکت در تعدادی اجرای پروتکل و محاسبات چند جمله ای بد ست آورد .

در اینجا به طور مختصر مساله لگاریم گسسته را مطرح میکنیم.

۲-تعریف مساله لگاریتم گسسته[2] در گروه G:

برای یک عضو گروه g و یک عدد n تعریف میشود $g^n = g * g * .. * g$ (nبار)

مساله لگاریم گسسته به صورت زیر تعریف میشود.اگر یک عضو اولیه g در گروه G داده شده باشد و عضو h نیز متعلق به G باشد یک عدد صحیح x پیدا کنید که $g^x = h$ باشد.

طرح شنر[1,2] و اکاموتو[1,2] طرحهایی هستند که بر اساس مساله لگاریتم گسسته هستد ما با بررسی طرح شنر و اکا موتو طرح جدیدی بر اساس مساله لگاریتم گسسته را مطرح میکنیم .در اینجا به معرفی طرح پیشنهادی میپردازیم .

۳- تشریح طرح پیشنهادی

طرح پیشنهادی ما دارای سه مرحله است .

الف-تولید کلید

ب-بوجود آوردن گواهینامه

ج- اجرای پروتکل بین اثبات کننده و تصدیق کننده

۳-۱-مرحله تولید کلید

[1] Security
[2] DLP

در ابتدا یک مرجع مورد اعتماد [1] نیاز است که کارهای زیر را انجام میدهد.

مر جع مورد اعتماد پارا مترهایی برای طرحها به صورت زیر انتخاب می کند.

p : یک عدداول بزرگ ($p >= 2^{512}$) است که لگاریتم گسسته در Z_P حل ناپذیر است.

q : یک عدد اول بزرگ که مقسوم علیهی از $(p-1)$ و $q >= 2^{140}$ است.

$\alpha \in Z_p^*$: دارای مرتبه q است (چنین αای می تواند به عنوان $(p-1)/q$ امین توان یک عضو اولیه در Z_p^* محاسبه شود.

t: یک پارامتر بنحوی که $(q > 2^t)$وبرای بیشتر کاربرد ها $t = 40$ امنیت کا فی را فراهم می کند.

یک طرح امضای امن با الگوریتم ا مضای سری Sig_{TA}ویک الگوریتم تصدیق عمومی Ver_{TA} انتخاب میشود توجه داریم که پارامترهای p, q, α, Ver_{TA} به طور عمومی اعلام می شوند و توسط تمام افراد در شبکه قابل استفاده اند.

۳-۲- بوجود آوردن گواهینامه .

. مر جع مورد اعتماد یک رشته شناسایی $ID(prover)$ را پیشنهاد می کند .

.اثبات کننده به طور امنی سه اعداد تصادفی سری a, b, c را به عنوان کلید خصوصی ا ش انتخاب می کند که $0 \le a, b, c \le q-1$ و سپس کلید های عمومی v, q_a, q_b, q_cرا به صورت زیرمحاسبه می کند.

$$v = \alpha^{-abc} (\mathrm{mod}.p), q_a = \alpha^a (\mathrm{mod}\ p), q_b = \alpha^b (\mathrm{mod}\ p), q_c = \alpha^c (\mathrm{mod}\ p)$$

وآنگاه v, q_a, q_b, q_cرابه مر جع مورد اعتماد می فرستد.

. مر جع مورد اعتماد امضا s را تولید می کند

. $s = Sig_{TA}(ID(prover), v, q_a, q_b, q_c)$

.گواهینامه $C(prover) = (ID(prover), v, s)$به اثبات کننده داده می شود.

[1] Trusted Authority

۳-۳- اجرای پروتکل بین اثبات کننده و تصدیق کننده .

.اثبات کننده اعداد تصاد فی سری k_1, k_2 را انتخاب می کند که $0 \le k_1, k_2 \le q-1$ و $\gamma = \alpha^{k_1} \alpha^{2k_2} \pmod p$را محاسبه می کند.

. اثبات کننده $C(prover), \gamma$ را به تصدیق کننده می فرستد .

.تصدیق کننده امضای مر جع مورد اعتماد را روی گواهینامه اثبات کننده تصدیق می کند،در نتیجه کلید عمومی اثبات کننده را احراز هویت می کند .

. تصدیق کننده یک مقدار تصاد فی ω_1, ω_2 را انتغاب می کند که $1 \le \omega_1, \omega_2 \le 2^t$ و ω_1, ω_2 را به اثبات کننده می دهد.

. اثبات کننده مقادیر

$$y_1 = (k_1\omega_1 + (a+b+c+abc)\omega_2) (\mathrm{mod}.q)$$

و $$y_2 = (2k_2\omega_1 + (a+b+c+abc)\omega_2) (\mathrm{mod}.q)$$

را محاسبه می کند و y_1, y_2 را به تصدیق کننده می دهد.

. تصدیق کننده تصدیق می کند که $\alpha^{y_1+y_2}.v^{2\omega_2} = \gamma^{\omega_1}.(q_a.q_b.q_c)^{2\omega_2} \pmod{.p}$ می باشد.

اگر چنین شد تصدیق کننده پیام پذیرش مشخصه اثبات کننده را میدهد در غیر اینصورت تصدیق کننده در خروجی پیام عدم پذیرش مشخصه را میدهد.

۳-۴ بررسی خصوصیات پروتکل پیشنهادی .

الف- کامل بودن : اگر هر دو طرف درستکار باشندو محاسبات را درست اجرا کنند با محاسبه زیر مشخص است اثبات کننده قادر است خود را به تصدیق کننده اثبات کند.

$$\alpha^{y_1+y_2}.v^{2\omega_2} = \alpha^{(k_1+2k_2)\omega_1+2(a+b+c+abc)\omega_2}.\alpha^{-2abc\omega_2} = \alpha^{(k_1+2k_2)\omega_1}.\alpha^{(a+b+c)(2\omega_2)} = \gamma^{\omega_1}.(q_a.q_b.q_c)^{2\omega_2}$$

ب- شکستن طرح : لازمه شکستن طرح این است که، مقادیر کلید خصوصی a,b,c محاسبه شود و با توجه به اینکه فقط مقادیر q_a, q_b, q_c عمومی هستند و محاسبه a,b,c از آنها نیاز مند حل مساله لگاریتم گسسته

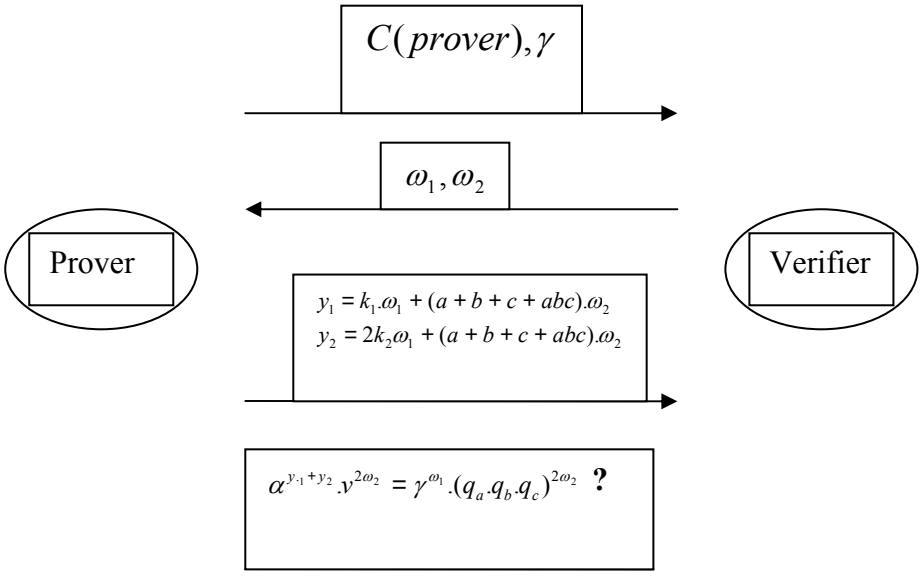
است یعنی سه مساله لگاریتم گسسته باید حل شود که در گروه Z_P با انتخاب مقدار مناسب P حل ناپذیر است . در ضمن یک حمله کننده فعال که می تواند مبادلات را مشاهده کند نمی تواند از مشاهداتش برای محاسبه a,b,c استفاده کند، زیرا با دانستن γ حتی با حل معادله لگاریتم گسسته که بسیار مشکل است مقدار $k_1 + 2k_2$ حاصل میشود که نمی تواند مقادیر k_1,k_2 را مشخص کند ، در نتیجه در معادلات زیر

$$y_1 = (k_1\omega_1 + (a+b+c+abc)\omega_2)(\mathrm{mod}.q)$$

$$y_2 = (2k_2\omega_1 + (a+b+c+abc)\omega_2)(\mathrm{mod}.q)$$

مقادیر k_1,k_2 مشخص نیست و از روی مقادیر مشخص $\omega_1,\omega_2,y_1,y_2$ نمی توان مقدار کلیدهای خصوصی a,b,c را محاسبه کرد و در نتیجه کلیدهای خصوصی قابل محاسبه نیستند.

توجه داریم با توجه و بررسی دقیق طرحهای شنر[1,2]و اکاموتو[1,2] این طرح جدید تمام محا سن هر دو طرح را دارد در ضمن ا مکان محاسبه کلید خصوصی را از حمله کننده فعال که تمام مبادلات را مشاهده می کند گرفته است.در شکل ۱ مراحل اجرای پروتکل به صورت گرافیکی نمایش داده شده است.



نتیجه گیری

در این مقاله ما به معرفی طرح احراز هویت جدیدی که بر اساس حل ناپذیری مساله لگاریتم گسسته است پرداختیم .در این طرح جدید طرحهای شنر واکاموتو را بهبود دادیم . این طرح ا مکان حمله غیر فعال وفعال را از دشمن میگیرد و محاسبه کلید خصوصی را غیر ممکن می سازد . در نتیجه ا مکان جعل را از حمله کننده میگیرد. در ضمن این طرح تمام محاسن طرحهای شنر واکا موتو دارد.

مراجع:

1-Douglas R.Stinson, Cryptography Theory And Practice ,Identification Scheme, pp 283,1995

2-Applied Cryptography,Bruce Schneier, Identification Scheme, pp 502,1996