Механика Транспорт Комуникации

Научно списание

ISSN 1312-3823

брой 3, 2008 г.

статия № 0333

http://www.mtc-aj.com

СЪВРЕМЕННИ АСПЕКТИ И ПРОБЛЕМИ НА ЕЛЕКТРОННАТА ЗАЩИТА И СИГУРНОСТ ПРИ РАЗВИТИЕТО НА ЕВРОПЕЙСКАТА ИНФОРМАЦИОННА СТРУКТУРА

Антонио АНДОНОВ

andonov@vtu.bg

ВТУ „Тодор Каблешков", „Гео Милев"158, София 1574

БЪЛГАРИЯ

Резюме: *В съвременното информационно общество, на база на интернет и информация от ново поколение, настъпват промени в общоприетата търговия и обществената администрация. Информационните технологии и криптографията играят решаваща роля.*

В предложената статия се разглеждат основните принципи на синхронизация на криптографската политика и международните стандарти за създаване на средства за шифриране.

Ключови думи: *информационна сигурност, електронна защита, криптография*

1.Увод

В нарастващата конкурентна глобална икономика Европа заяви своята регионална роля чрез определянето и реализирането на Европейска информационна инфраструктура [1]. Тя се разглежда като комплекс от мрежи и услуги, които дават възможност за достъп до всякакъв вид информация и улесняват мобилността на работната сила, обмена на стоки, развитие на електронна търговия и банкиране. От особено значение за Европейска информационна инфраструктура е философията на Internet, която отдава голямо значение на базовия минимален набор на стандарти и се основава на свободното разпространение на софтуерни приложения. Докато компютърните мрежи за данни съществуват от много години, появата на Internet като повсеместна транспортна услуга, е последният феномен. Увеличаването на броя на потребителите стимулира развитието на нови услуги. Досега Internet беше съществена свободна среда за предлагане и използване на информационни услуги. Превръщането на Internet в среда, която предлага голям брой обществени, търговски и чисто информационни услуги, поставя ударението върху редица специфични въпроси, като право за достъп, защита, конфиденциалност и информационна сигурност, като стимулира нови технологични изследвания и развитие за тяхното решаване.

Затова неслучайно защитата на даннити в информационната инфраструктура е най-сериозният проблем на съвременните информационни технологии.

2. Проблемът за сигурността при трансфер на информация.

Още великият английски философ Франсис Бейкън е написал: „Знанието е сила". Това е причината, поради която е толкова важно да се предотврати достъпът до определена информация на хора, които може да манипулират с нея, или да злоупотребяват със силата на знанието.

В днешното време на електронните медии поверителната информация се предава по информационните канали под различни форми: радиопредаване, телефонни и телефаксни връзки, компютърни мрежи и мрежи за обмен на данни и т.н. Тъй като тези комуникационни канали не могат да бъдат контролирани като изолирани от потребителя, съдържанието им трябва да бъде защитено.

При този проблем и други подобни, общото е използването на криптографията,

или по-точно криптоподобни методи за преобразуване на информацията. Това са технически средства, които позволяват на една или повече страни, познаващи секретните части на информацията, които с голяма вероятност могат да бъдат възпроизведени, да я защитят от тези, които не познават съответните секретни ключове. Криптографията не е само способ за скриване на поверителни послания. Друг важен неин аспект е автентификацията. Електронният подпис е гаранция за самоличността на подателя на даден документ и показва убедително точното време на създаване на документа. Като се използват само няколко основни инструмента, могат да се създадат сложни схеми и протоколи, които да позволяват използването на електронните пари, например. Също можем да докажем, че знаем някаква информация, без да я разкриваме, или да разделим и кодираме една тайна така, че не по-малко от трима или петима души да са необходими, за да я възстановят. Криптографията е в основата на онлайн-икономиката, понеже осигурява така необходимата поверителност и сигурност на отношенията търговец-клиент. Без криптография схемите, работещи с електронни пари, не могат да се реализират. Чрез нея е възможно да се легитимира потребител пред банка или друга институция, да се шифрират числата, които представляват виртуални пари, така, че никой освен банката да не може да оперира с тях, да се изпращат данни по обществени комуникационни линии, или интернет, да се подписват документи от разстояние. На криптиращи алгоритми се опират онлайн-магазините, борсите, търговете и ауксионите, работата с кредитни карти, компаниите с офиси по целия свят, когато трябва да си предават документация бързо и сигурно. Всеки потребител, който има желание да подобри сигурността на системата си, може да използва криптиран софтуер за събраната информация или трафика на данни.

3. Социално-политически, юридически и финансови проблеми при използването на криптографията.

Криптографията е необичайна наука. Повечето учени се стремят първи да публикуват своите разработки, тъй като по пътя на разпространението работите им добиват ценност. Обратно, най-голямата ценност на криптографията се осигурява чрез минимизиране на достъпа на информация. Затова професионалните криптографи обикновено работят в затворени съобщества, където е възможно да се създадат условия за нормално професионално взаимодействие за целите на гарантиране на качество, и в същото време да се съхрани секретността на разработките. Разкриването на тези секрети се разрешава само с оглед историческата точност, едва след като е ясно, че полза от по-нататъшна секретност не може да бъде извлечена.

Развитието на информационното общество все в по-голяма степен зависи от способността да се защитава информацията при нейното предвижване в глобалния свят, т.е. определя се от възможностите на криптографията. В този смисъл шифрирането може да се разглежда като ключ на информационния век. В продължение на хилядолетия, шифрирането е било от значение само за правителствата, във военните и дипломатическите дела. Днес то се прилага както в бизнеса, така и защита на личните дела. За щастие в началото на информационния век бе създадено изключително устойчиво шифриране. Това е появата криптографията с открит ключ и в частност на шифъра RSA. Обаче криптографията има и негативна страна. Тя може да се използва за защита на информация за терористични и престъпни цели. През двадесет и първи век основната дилема, стояща пред криптографията, се състои в това, да се намери способ, даващ възможност да се ползва шифриране в обществения живот и бизнеса и същевременно непозволяващ ползването на шифриране за престъпни цели.В настояще време протичат активни работи [2, 3] за най-добрите пътища за решаване на дадения проблем. Значителна част от тези дискусии са вдъхновени от историята на Цимерман [4], човекът, създал общодостъпния в интернет шифър PGP, който по своята ефективност е устойчив на усилията да бъде разбит от всички дешифрователни центрове в света. Разпространението на PGP заставя криптографите, борците за граждански права, сътрудниците на правозащитните органи сериозно да се замислят за последствията от широко приложение на криптоустойчивото шифриране. Огромна част от обществото, както и самият Цимерман, считат, че използването на криптоустойчиво шифриране е благо за обществото, тъй като гарантира на всички конфиденциалност при използване на

цифровите комуникации. Против тях са тези, които считат, че шифрирането е заплаха за обществото, тъй като престъпници и терористи могат да се свързват тайно, без да могат да бъдат разкрити. Основният въпрос се състои в това, длъжни ли са правителствата да забранят криптография по законодателен път, или не. Възможно ли е това?!

Но освен с вътрешната политика този въпрос е свързан и с националната сигурност. Например, известно е, че Агенцията за национална сигурност на САЩ, задно с Англия, Австрия, Канада, Нова Зенландия и др., ползват системата „Ешалон"- глобална система за прехващане, която е способна да осъществи сканиране на електронни писма, факсове, телефони и работи в съответствие с речници подозрителни думи, които разпознават в реално време. Обаче „Ешалон" би била безполезна, ако съобщенията станат шифрирани и влизащите в нея държави губят важна разузнавателна информация за политически интриги и терористични атаки. Независимо, че сътрудниците на правозащитните органи доказват, че шифрирането трябва да бъде забранено, тъй като то ще направи „Ешалон" неефектива, борците за граждански права заявяват, че шифрирането е необходимо точно за това. Свои интереси имат и големите корпорации – от една страна информационна сигурност в електронната търговия и банкиране, от друга– възможност за укриване на сделки, данъци и неконтролируеми електронни пазари.

В настояще време политиката по отношение на криптографията е различна в различни региони на света и бързо се мени, под влияние на постоянно случващи се събития.

4. Заключение. Изводи.

Криптоустойчивото шифриране и неговите приложения се превръща в изключително важен международен проблем – глобален, корпоративен и персонален. Шифрирането може да нанесе както значителна вреда, така и полза на бизнеса и правовия ред. Държавната политика в това направление трябва да отчита не само заплахите за правоохранителни органи и разузнавателните операции, но и необходимостта от защита на интелектуалната собственост и икономическата конкуренция. Крипто-графската политика трябва да отговаря на нуждите на потребителите от шифриране и да отчита основните права на човека – гарантирането на право на личен живот. балансът на тези интереси е необикновено сложен.

ВТУ „Т. Каблешков" е едно от първите учебни заведения в РБ, в което проблемите на информационната сигурност се изучават, най-напред като избираема, а впоследствие като основна в магистърския курс на обучение на специалност „КОТ" дисциплина. Съвременното развитие, когато човечеството създава наред с физическия и виртуален свят, отново се изправя пред старите вечни проблеми, за които студентите трябва да са готови в условията на информационния век: как да се определи границата между свободата и отговорността, защитата на личния живот, свободата и властта; кака във виртуалната реалност да се създадат юрисдикции на реалното право.

Литература

[1] Андонов А., Г.Чернева. Информационна сигурност на комуникационните мрежи. С. 2004, ISBN 954-12-0102-4.

[2] Мэй Т. Криптоанархия. манифест криптоанархиста. М. Культура, 2005.

[3] Мнукин Дж. Виртуальное право. М. Культура, 2005.

[4] Американска криптологическа асоциация: http://www.und.nodak.edu/org/crypto .

CONTEMPORARY ASPECTS AND PROBLEMS OF ELECTRONIC PROTECTION AND SECURITY AT THE EUROPEAN INFORMATION INFRASTRUCTURE DEVELOPMENT

Antonio ANDONOV

Higher School of Transport "T. Kableshkov", Geo Milev Str. 158, 1574 Sofia BULGARIA

Abstract: *In the contemporary information society making use of the Internet and new generation information highways causes changes as well as replacement of conventional trade and public administration. Information technology and cryptography become a crucial international issue.*

The proposed article presents the basic principles for synchronization of the cryptography policy of various countries and international standards for the production of means of encryption

Key words *information security , electronic protection, cryptography*