

Състояние и проблеми на сигурността в
киберпространството на България

Криптографска сигурност

Владимир Кожухаров

Дефиниции

- **Криптографска сигурност** - система от криптографски методи и средства, които се прилагат с цел защита на класифицираната информация от нерегламентиран достъп при нейното създаване, обработка, съхраняване и пренасяне (ЗЗКИ) .

Криптографските методи и средства са съвкупности от криптографски механизми, чиите основни елементи са криптографските алгоритми.

- **INFOSEC** – съвкупност от мерки за защита поверителността, интегритета и наличността (достъпността) на информацията, обработвана, съхранявана или пренасяна от комуникационни, информационни и други електронни системи, а също интегритета и наличността на самите системи.
- **Information Assurance** – система от мерки за достигане на определено ниво на увереност, че информацията и системите, които я обработват, съхраняват или транспортират, са защитени по отношение на поверителност, интегритет, достъпност, автентификация и неотричане на авторство.

Криптографски алгоритми

Криптографски алгоритъм е математическа функция и нейните параметри за сигурност. Една част от параметрите се променят във времето и се наричат **ключове**.

Алгоритмите биват:

- **симетрични** - състоят се от две функции – за криптиране и декриптиране, притежаващи едни и същи секретни ключове;
 - **Поточни** – информацията се обработва побитово (посимволно);
 - **блокови** - информацията се разбива на блокове, които се обработват;
- **Асиметрични** - двете функции използват различни ключове, единият от които е секретен (частен), а другият – публичен.

Опазването на секретните ключове от нерегламентиран достъп е от основно значение за сигурността на защитаваната информация, поради което се отделя специално внимание на производството, разпределението и съхранението им.

Част от параметрите могат да служат за обособяване на групи потребители. Параметрите, уникални за дадена група, се наричат потребителски.

Криптографски механизми

Дефиниция – хардуерна или софтуерна имплементация на един или няколко криптографски алгоритми и съпътстващите ги аларми, проверки и други процеси, необходими за ефективна и сигурна обработка.

Примери:

- Хеш функция – която преобразува входните данни в блок данни (хеш) с определена дължина по такъв начин, че да е практически невъзможно по даден хеш да се определи кои са били входните данни или да се намерят два блока входни данни с еднакъв хеш;
- Електронен подпис – механизъм, използващ асиметричен алгоритъм, чрез който с помощта на секретния ключ се извършва криптиране (подписване) на данни, които получателят може да провери чрез декриптиране с помощта на публичния ключ;
- Блоково или поточно шифриране;
- Key wrap – механизъм за криптиране и хеширане на ключове с цел съхраняването им по безопасен начин.

Разработката на криптографските механизми (и тяхната проверка) изисква познания в различни области от математиката, програмирането, изчислителната техника и др.

Изисквания към криптографските механизми

От какво се обуславят:

- Многообразието на технологиите за реализация – преход от електромеханични през електронни чипове до софтуерни реализации върху различни платформи;
- Многообразието на механизмите, осигуряващи поверителност, интегритет, автентификация, достъпност, невъзможност за отричане на авторство;
- Разнообразната среда, в която действат механизмите.

Зависят от :

- Величината на вредата, която би настъпила при тяхното компроментиране;
- Заплахите към тях от страна на средата, в която са реализирани.

Изисквания към криптографските механизми (2)

- Към алгоритмите по отношение на:
 - Начина на тяхното проектиране и съхранение;
 - Дължината на ключовете;
 - Потребителските параметри.
- Към реализацията на алгоритмите:
 - Начина на реализация -дискретни елементи, чипове, програмируеми матрици (FPGA), софтуер;
 - Дублиране на критичните за сигурността функции;
 - Осигуряване на интегритета на криптографските функции и параметри.
- Към останалите елементи, засягащи сигурността
 - Разработката, производството, употребата, ремонта;
 - Конфигурационния контрол;
 - Управлението на ключовете.

Осигуряване правилна реализация на механизмите

- Контрол на производството;
- Контрол на разпределението и съхранението;
- Контрол на процеса за проверка на реализацията;
- Конфигурационен контрол на продукта при употребата му.

Съвместимост на криптографските продукти

Разработка на изисквания и спецификации за съвместимост към:

- Комуникационните устройства на въоръжение в НАТО и страните – членки - Secure Communications Interoperability Protocol (SCIP). Обхваща управление на ключовете, речева компресия, криптиране, трансмисия;
- Следващата генерация на IP устройства в рамките на НАТО и страните - членки - NATO Networked Information Infrastructure IP Network Encryption (NINE), базиран на IPSec.

Състояние и проблеми на криптографската сигурност у нас

- Нормативна уредба
- Производство и внос
- Проблеми на органа за криптографска сигурност

Нормативна уредба

- Няма съществена актуализация от момента на създаването си – не е отразено участието ни в ЕС и НАТО (частично).
- Част от текстовете на Наредбата за криптографската сигурност (НКС) въвеждат протекционистка политика, противоречаща на европейската практика:
 - чл.14, ал. 2 дава предимство на националните криптографски средства при еднакви показатели,
 - чл. 14, ал. 3 ограничава използването само на национални средства в областта на задграничните комуникации,
- Въведени са ограничения към класификационното ниво на информацията, обработвана от криптографските средства (чл.25 ал.2)
- чл. 80, ал.1, разрешавайки проблема със закупените до влизането в сила на НКС криптографски средства от неутрални страни, дава възможност за закупуване на нови, произведени извън ЕС или НАТО, въпреки политиката на тези две организации в тази област.

Нормативна уредба (2)

Одобрение за прилагане на криптографски средства (НКС гл. 5)

- Да се синхронизира чл. 71, ал.2 с исканата от органите на ЕС и НАТО документация при одобрение на КС.
- Да се разделят процесът на разработка от процеса на одобрение. При непълна документация и при неправилна реализация процедурата за одобрение да се прекратява.
- Да се прецени необходимостта от заплащане на процедурата за одобрение от страна на фирмите. В момента тя е безплатна, поради което те използват ОКС като безплатна лаборатория за тестване на устройството.
- Да се прецизира процедурата по одобрение:
 - Да се прецени дали да се облекчи процедурата за одобрение на криптографски средства, вече одобрени от органите на ЕС и НАТО;
 - да се прецени дали е необходимо да се предоставя криптографски алгоритъм на фирмите (чл. 85, т. 2);
 - Да се прецени дали ОКС трябва да консултира частни фирми (чл.86).

(Част от горните проблеми могат да се разглеждат като държавна помощ за фирмите)

Производство и внос на криптографски средства

- Слаб интерес към производството, обществените поръчки за разработки са единици. Общият брой на одобрените български устройства е символичен.
- Практика е фирмите да не спазват чл. 87, ал. 1 и още по време на разработката да подават заявление по чл. 70 от НКС.
- Вноството е основно от една фирма от държава извън ЕС и НАТО, което увеличава рисковете.
- Интересът на фирми от страни-членки на ЕС и НАТО е малък:
 - Трябва да имат български представител (чл. 69);
 - Трябва да ни предоставят информацията по чл. 71.

Проблеми на органа за криптографска сигурност

- Малък щат, невъзможност за наемане на изявени специалисти, след като натрупат опит, част от специалистите напускат.
- Проверките отнемат много време и средства (писане на програми, подготовка на стендове за изпитване със скъпоструващи уреди, изискване на допълнителна информация...), а е невъзможно да бъдат отказани.
- Собствените разработки (по чл.42, ал. 1 от ЗДАНС) крият рискове поради малкия щат и липсата на независим контрол.
- ОКС структурно е разположен в дирекция, чиито приоритети са съвсем различни – липсва интерес към развитието на дейността.

Въпроси?

Владимир кожухаров

E-mail: vladoko@yahoo.com