№ 6 Зертханалық жұмыс. Деректерді шифрлау.

Негізгі теориялық ақпарат

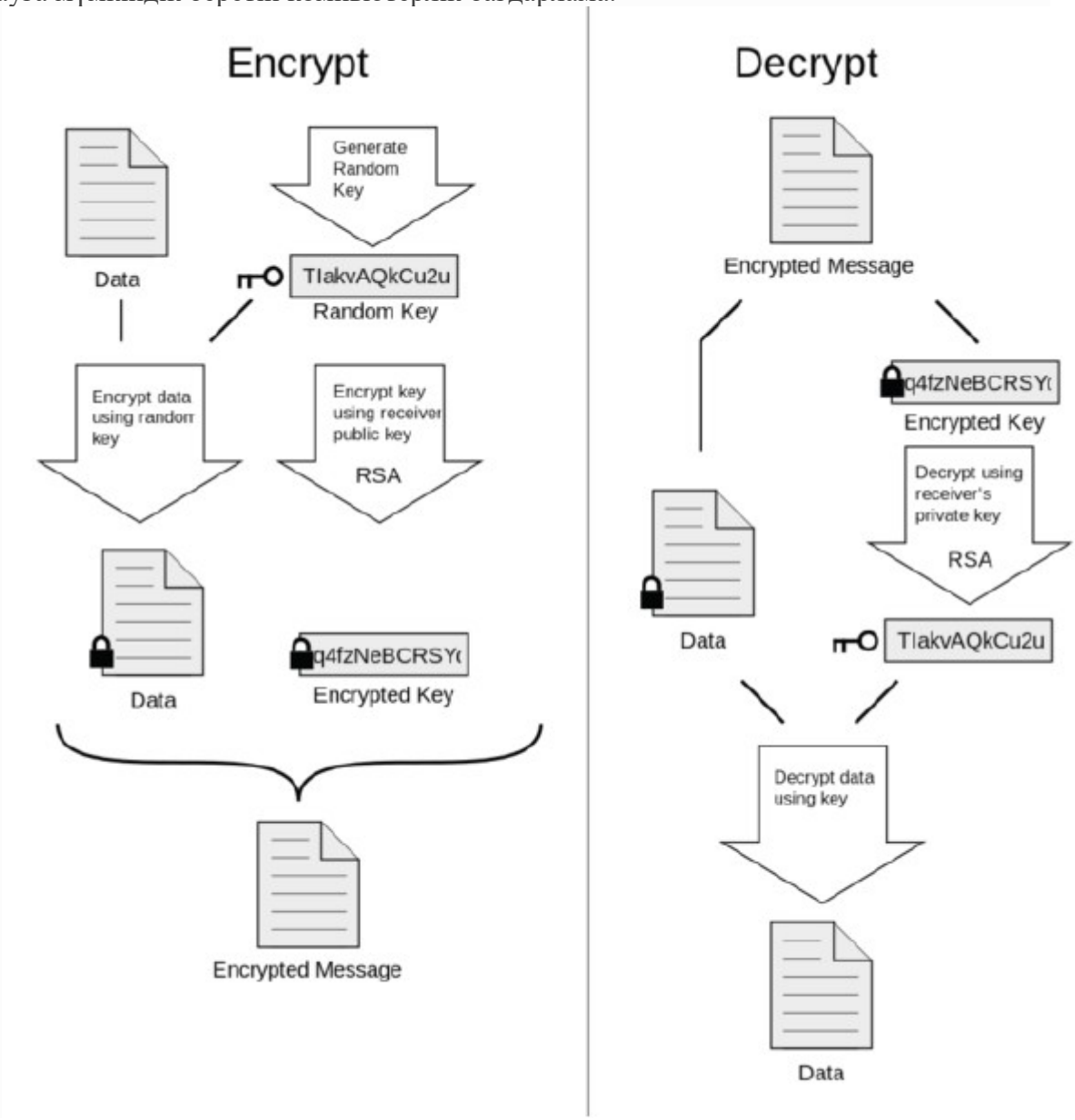
Мақсаты: деректерді шифрлаудың бағдарламалық құралдарымен жұмыс істеудің теориялық және практикалық дағдыларын алу.

Консоль командалары:

- **gpg** <параметры> - шифрлау және сандық қолтаңба құралы.
- **cryptsetup** <параметры> - dm-crypt ядро модулі негізінде жұмыс істейтін шифрланған диск бөлімдерін басқару бағдарламасы.
- **truecrypt** <параметры> - truecrypt көмегімен шифрланған диск бөлімдерін басқаруға арналған бағдарлама.
- **fallocate** <параметры> - файлдар үшін блоктарды қолмен бөлуге мүмкіндік беретін команда.

PGP

PGP (Pretty Good Privacy) — файлдарды немесе хабарламаларды, сондай-ақ электронды түрде ұсынылған басқа ақпаратты, соның ішінде сақтау құрылғыларындағы деректерді шифрлауды шифрлау/шифрын ашу және сандық қол қою операцияларын орындауға мүмкіндік беретін компьютерлік бағдарлама.



PGP-де шифрлау процесі бірнеше кезеңнен тұрады: хэштеу, деректерді қысу, симметриялы кілтпен шифрлау және ақырында ашық кілтпен шифрлау. Сонымен қатар, әр кезең әртүрлі алгоритмдерді қолдана алады. Осылайша, симметриялық шифрлау сеанс кілтіндегі жеті симметриялық алгоритмнің (AES, Blowfish, 3DES, CAST5, IDEA,Twofish, Camellia) бірін қолдану арқылы жүзеге асырылады. Сеанс кілті өз кезегінде криптографиялық тұрақты жалған кездейсоқ сандар генераторының көмегімен жасалады. Ол RSA немесе Elgamal алгоритмдерін қолдана отырып, алушының ашық кілтімен шифрланады (алушының бастапқы ашық кілтіне байланысты).

PGP бастапқыда клиенттік электрондық поштаны қорғау үшін жасалған, бірақ 2002 жылдан бастап қатты дискілерді, каталогтарды, файлдарды, жедел хабар алмасу бағдарламаларының сеанстарын шифрлауды, желілік қоймалардағы файлдар мен каталогтарды қорғауды, файлдарды пакеттік тасымалдауды және жаңа нұсқаларда HTTP сұраулары мен серверлік жауаптарды шифрлауды қамтиды және Клиент.

TrueCrypt

TrueCrypt — ең танымал деректерді шифрлау бағдарламаларының бірі. Арнайы криптоконтейнер файлы ретінде сақталған виртуалды шифрланған логикалық дискіні жасауға мүмкіндік береді. TrueCrypt көмегімен қатты диск бөлімін немесе USB дискісі сияқты кез-келген басқа медианы толығымен шифрлауға болады.

Жұмыс барысында бұл утилита компьютерде арнайы қорғалған аймақ жасайды. Операциялық жүйе өз кезегінде бұл аймақты файл немесе диск ретінде қабылдайды. TrueCrypt қорғалған кеңістігі мен кәдімгі дискінің айырмашылығы мынада: кәдімгі дискіде деректер әдетте ешқандай жолмен қорғалмайды және TrueCrypt деректерді "жылдам" шифрлайды, пайдаланушылар үшін мүлдем байқалмайды және осылайша арнайы манипуляцияларсыз ақпаратты сенімді қорғауды қамтамасыз етеді. Сонымен қатар, қорғалған аймақта TrueCrypt шифрланған ғана емес, сонымен қатар көзге көрінбейтін деректерді орналастыра алады.

TrueCrypt шифрланған виртуалды дискіні жасай алады:

- Файл контейнерінде онымен жұмыс істеуді жеңілдетеді — көшіру, тасымалдау (оның ішінде файл түріндегі сыртқы құрылғыларға), атын өзгерту немесе жою;
- Шифрланған диск бөлімі түрінде, бұл жұмысты ыңғайлы және өнімді етеді, 5.0 нұсқасынан бастап жүйелік бөлімді шифрлау мүмкіндігі пайда болды;
- USB дискісі сияқты құрылғының мазмұнын толық шифрлау арқылы (флоппи-дискілерге 7.0 нұсқасынан қолдау көрсетілмеді).

TrueCrypt қолдайтын шифрлау алгоритмдерінің тізіміне AES, Twofish және Serpent кіреді.

Шифрланған деректерге қол жеткізу үшін пароль (кілт сөз тіркесі), кілт файлы (бір немесе бірнеше), сондай-ақ олардың тіркесімдері қолданылады. Жергілікті, алынбалы, желілік дискілердегі кез-келген қол жетімді файлдарды кілт файлдары ретінде пайдалануға болады (алғашқы 1,048,576 байт қолданылады) немесе өзіңіздің кілт файлдарыңызды жасай аласыз.

TrueCrypt-тің қызықты мүмкіндіктерінің бірі-пайдаланушы құпия сөзді мәжбүрлі түрде ашқан жағдайда қажет шифрланған деректердің болуын жоққа шығарудың екі деңгейін қамтамасыз ету:

- Кәдімгі көлемге басқа құпия сөзді (немесе негізгі файлдар жиынтығын) орнатуға мүмкіндік беретін жасырын көлем жасаңыз. Бұл деректерге негізгі құпия сөзбен қол жеткізу мүмкін емес, ал жасырын көлемде өзінің файлдық жүйесі болуы мүмкін және ол негізгі көлемнің бос кеңістігінде орналасқан.
- TrueCrypt томдарының ешқайсысын анықтау мүмкін емес (TrueCrypt томдарын кездейсоқ деректер жиынтығынан ажырату мүмкін емес, сондықтан файлды TrueCrypt-пен немесе оны жасаған бағдарламамен, ешқандай формада және шеңберде байланыстыру мүмкін емес).

TrueCrypt-те Linux үшін графикалық интерфейс бар, бірақ шифрлауды консольден де басқаруға болады.

- Кілт файлын жасаңыз <truecrypt-create - keyfile /home/user/test/file> , мұнда файл-кілт файлының атауы. /Home/user / test каталогы болуы керек екенін ескеріңіз.
- Криптоконтейнер жасаңыз <sudo truecrypt-k /home/user/test/file-c /Dev/sda9>.
- Монтаждау <sudo mount / dev / mapper / truecrypt0 / mnt/ crypto > монтаждау каталогы (мұнда /MNT/crypto) бұрыннан бар болуы керек.
- Ажырату <truecrypt-d>.
- Ақпаратқа қайта қол жеткізу үшін контейнерді қосамыз <truecrypt-k /home/user/test/file /dev/hda9 /mnt/crypto>.

LUCKS/dm-crypt

LUKS (Linux Unified Key Setup) — бастапқыда Linux үшін ұсынылған, бірақ қазір бірқатар басқа операциялық жүйелерде қолдау көрсетілетін дискіні (немесе блоктық құрылғыны) шифрлау сипаттамасы. DM-crypt деп аталатын стандартты Linux ядросының шифрлау ішкі жүйесіне негізделген және tks1/TKS2 нұсқауларына сәйкес келеді.

Ерекшеліктері:

- Файл" контейнер " ретінде қолданылады. Оның мөлшері бекітілген. Өлшемнің өзгеруі мүмкін.
- Контейнердің" ішінде " сізге ыңғайлы кез-келген форматтағы файлдық жүйе жасалады.
- Пайдаланған кезде-кәдімгі бөлім сияқты орнатылады.
- Деректер кәдімгі файл / файлдық жүйе сияқты блоктарда сақталады. Яғни:
  - контейнер ішіндегі файлды өзгерту сол файл алып жатқан блоктардың қайта жазылуына әкеледі, бірақ бүкіл контейнер емес;
  - бір блоктың" жоғалуы/бүлінуі "" бұл блокта болған нәрсе " туралы ақпараттың жоғалуына әкеледі және басқа ештеңе жоқ.
  - контейнерді "бұлтқа" синхрондау кезінде-әдетте бүкіл файл қайта жазылмайды, бірақ трафиктің аз мөлшерін қажет ететін "өзгертілген бөлік".

Truecrypt-тен айырмашылығы:

- әдетте, деректерді өңдеу жылдамдығы жоғары (алгоритмге/кілт өлшеміне байланысты);
- кілттермен жұмыс істеу оңайырақ;
- "қос түбі" механизмі жоқ;
- "басқа ОЖ-дан"контейнерді пайдалану кезінде қиындықтар туындауы мүмкін

Зертханалық жұмыстарға арналған тапсырмалар

- Орнату PGP, GPG <sudo apt-get install pgpgpg>
- Ерікті файлдарға шифрлау және шифрын ашу операцияларын жасаңыз. Шифрлау үшін <gpg-c>пәрменін пайдаланыңыз. <Gpg –decrypt-file > шифрын ашу үшін (бұл жағдайда шифрланған файл каталогында шифры ашылады. Егер сізге транскрипцияланған мазмұнды экранға шығару қажет болса, <gpg –decrypt > пайдаланыңыз)
- Установить TrueCrypt. Нам потребуется версия 7.1a. Скачать её можно здесь или здесь.
- TrueCrypt Орнатыңыз. Бізге 7.1 нұсқасы қажет. Сіз оны осы здесь немесе осы здесь. жүктей аласыз.
- Криптоконтейнер жасаңыз, оны виртуалды диск ретінде бекітіңіз.
- Кейбір ақпаратты криптоконтейнерге салыңыз.
- Дискіні алып тастаңыз және криптоконтейнерді жылжытыңыз.
- Криптоконтейнерді виртуалды диск ретінде қайта орнатыңыз. Криптоконтейнердің өз бетінше берілуі және пайдаланылуы мүмкін екеніне көз жеткізіңіз.

- • LUKS/dm-crypt орнату <sudo apt-get update>, <sudo apt - get орнату cryptsetup>.
- Біз шифрланған деректерді сақтайтын файл жасаймыз. Ең оңай жолы <fallocate-l 512M / root /test1>, мұндағы / Root - файлды сақтау каталогы, test1 - Файл атауы. Сондай-ақ, бұл файлды жасау үшін dd пәрменін пайдалануға болады. <dd if=/dev/zero of=/root/test2 bs=1M count=512>. Үшінші әдіс-dd пәрменін пайдалану және файлды кездейсоқ деректермен толтыру. <dd if=/dev/urandom of=/root/test3 bs=1M count=512>.
- Криптоконтейнер жасаңыз. <cryptsetup-y luksFormat / root/test1 >(деректерді қайта жазуға және құпия сөзді орнатуға келісу керек).
- Контейнерді ашыңыз. <cryptsetup luksOpen /root/test1 volume 1>. (1 том-контейнердің аты, біз оны осы пәрменмен орнатамыз). Бұл /dev/mapper/volume1 файлын жасайды.
- Онда <mkfs файлдық жүйесін жасаңыз.ext4 -j /dev/mapper/volume 1>.
- <Mkdir /mnt/files > орнату қалтасын жасаңыз. Орнату <Mount / dev/mapper /volume1/mnt / files>
- Енді қандай файлдарды криптоконтейнерге жіберейік. Мысалы, /etc <CP-r /etc/* /mnt/files қалтасын көшіріңіз>.
- Орнату <umount / mnt / files>.
- Енді біз volume1-ді жабамыз. <cryptsetup luksClose volume1>. Осыдан кейін біздің деректер шифрланған.
- Оларды ашу үшін <cryptsetup luksOpen /root/test 1 Volume 1> және <mount /dev/mapper/Volume 1 /mnt/files>