Пакеттік коммутациялы сандық желілер

Дәріс 10: Сандық желілердің қауіпсіздігі және заманауи даму бағыттары

ДӘРІСКЕР: PhD, доцент м.а.
Сқабылов Әлішер Әлиұлы

Дәрістің мақсаты:

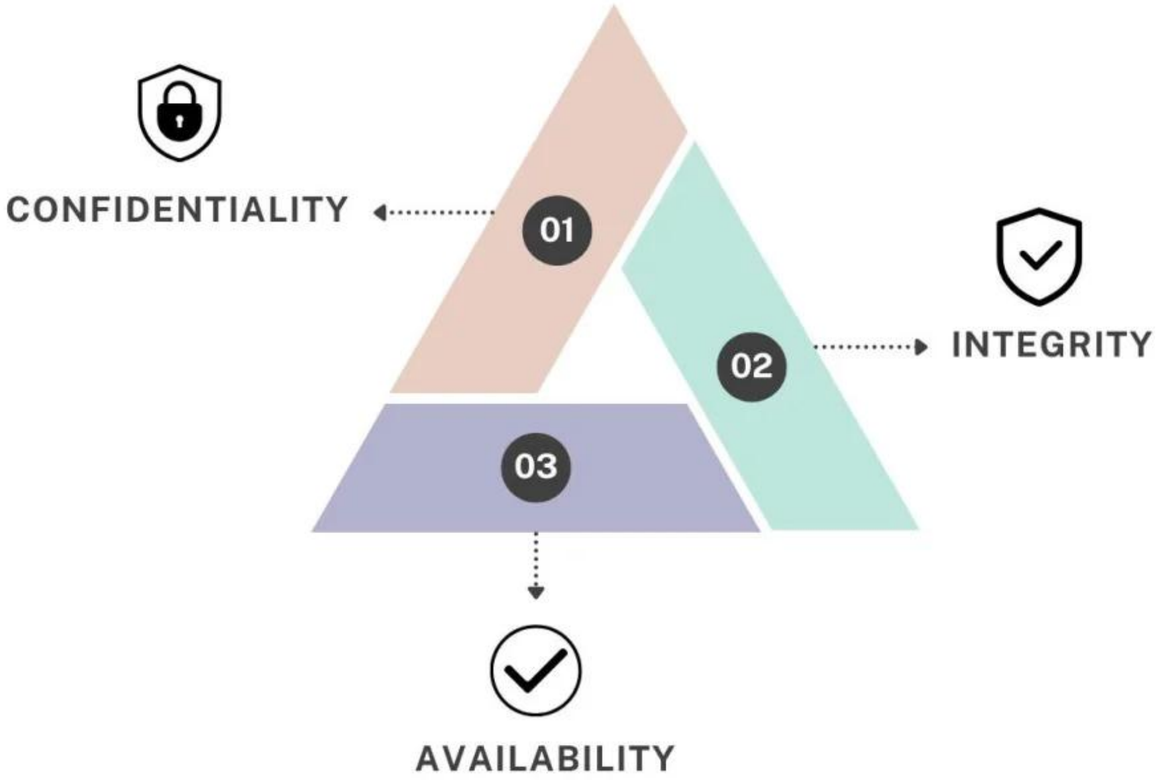
Желілік қауіпсіздіктің негізгі принциптерін, қауіптер мен шабуыл түрлерін, қорғау құралдары мен криптографиялық тетіктерді түсіндіру. Сонымен қатар сандық желілердің заманауи даму бағыттарын қарастыру.

Ақпараттық қауіпсіздік негіздері

Ақпараттық қауіпсіздік — ақпаратты рұқсатсыз қолжетімділіктен, өзгертуден және жоғалтудан қорғау. Қауіпсіздіктің негізгі моделі — **CIA үштігі:**

Қасиет	Сипаттамасы	Қорғау тәсілдері
Құпиялылық (Confidentiality)	Ақпаратты тек рұқсаты бар тұлғалар көреді	Шифрлау, аутентификация
Тұтастық (Integrity)	Деректер рұқсатсыз өзгертілмейді	Хэш, цифрлық қолтаңба
Қолжетімділік (Availability)	Ақпарат пен қызметтер қажет кезде қолжетімді болады	Резервтеу, DDoS-тан қорғау

CIA Triad



Ақпараттық қауіпсіздік негіздері

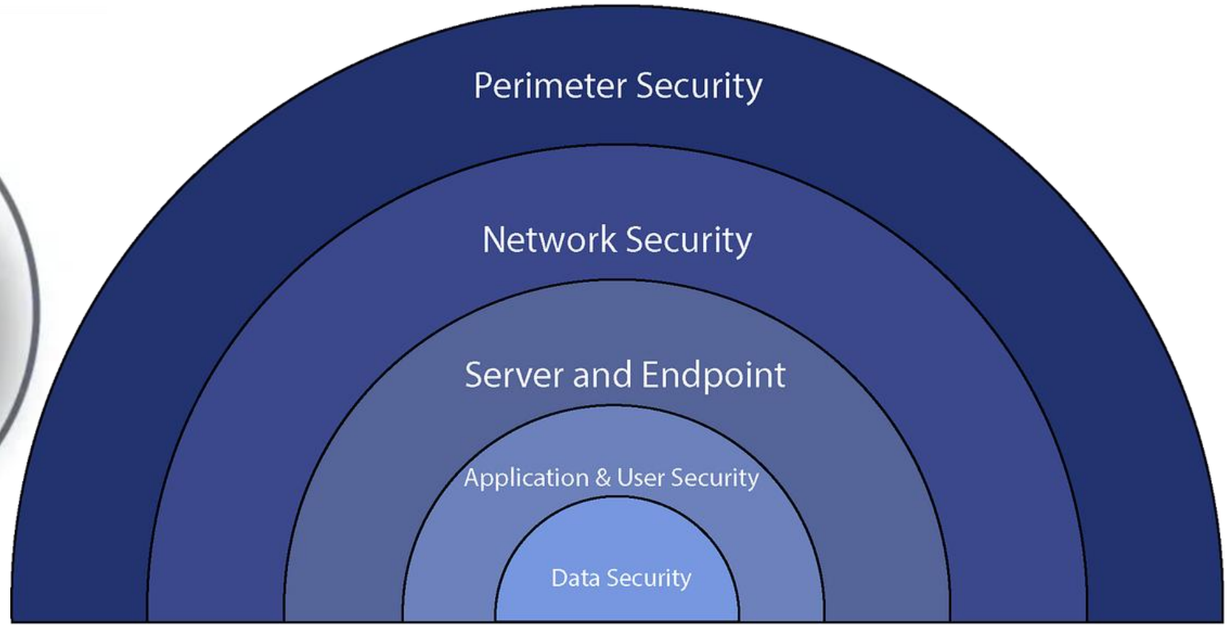
Қосымша қауіпсіздік тетіктері — **AAA**:

- Authentication — пайдаланушының кім екенін растау.
- Authorization — қолжетімділік құқықтарын беру.
- Accounting — пайдаланушы әрекеттерін тіркеу.

AAA RADIUS және TACACS+ арқылы жүзеге асырылады.

Эшелонды қорғаныс (Defense in Depth) — бірнеше қорғаныс деңгейін біріктіру принципі.





Желілік қауіптер мен шабуылдар

Желілік шабуылдар **екі негізгі топқа** бөлінеді:

- **Пассивті** шабуылдар — трафикті тыңдау және ақпарат жинау. Негізгі мақсаты — деректерді байқатпай алу.
- **Белсенді** шабуылдар — трафикті өзгерту, жалған деректер жіберу немесе желі қызметін тоқтату.

Шабуыл	**Сипаттамасы**
Sniffing	Желілік трафикті тыңдау
MAC flooding	Коммутатордың MAC-кестесін жалған мекенжайлармен толтыру
ARP spoofing	Жалған ARP жауаптары арқылы трафикті бұру
DoS / DDoS	Желі ресурстарын шамадан тыс жүктеу
Фишинг	Жалған хаттар мен сайттар арқылы деректерді алдау жолымен алу
Зиянды БҚ	Вирус, құрт және ransomware
Брутфорс	Парольді көптеген комбинацияларды тексеру арқылы табу

Желілік шабуылдардан қорғану шаралары

Шабуыл	Қарсы шаралар
Sniffing	TLS, SSH, VPN шифрлауы
MAC flooding	Port Security
ARP spoofing	Dynamic ARP Inspection, DHCP Snooping
DoS / DDoS	Трафикті сүзу, CDN, Rate Limiting
Фишинг	Пайдаланушыларды оқыту, MFA
Зиянды БҚ	Антивирус, жаңартулар, резервтік көшірме
Брутфорс	Күрделі пароль, MFA, әрекеттер санын шектеу

Криптографиялық қорғау негіздері

Криптография — ақпаратты шифрлау және оның қауіпсіздігін қамтамасыз ету әдістерінің жиынтығы. **Негізгі криптографиялық тетіктер:**

1. Симметриялық шифрлау (AES-128/256)

- Шифрлау мен дешифрлауға бір кілт қолданылады.
- Жылдам жұмыс істейді.
- Негізгі мәселесі — кілтті қауіпсіз жеткізу.

2. Асимметриялық шифрлау (RSA, ECC)

- Ашық және жабық кілт жұбы қолданылады.
- Кілт алмасу және цифрлық қолтаңба үшін пайдаланылады.
- Симметриялық шифрлауға қарағанда баяу.

Криптографиялық қорғау негіздері

3. Хэш-функциялар (SHA-256)

- Кез келген көлемдегі деректерден тұрақты ұзындықтағы хэш қалыптастырады.
- Деректер тұтастығын тексеруге қолданылады.
- Бір бит өзгерсе де, хэш нәтижесі айтарлықтай өзгереді.

4. Цифрлық қолтаңба

- Хабардың жіберушісін және тұтастығын тексеруге мүмкіндік береді.

5. Сертификат және PKI (X.509)

- Ашық кілттің белгілі тұлғаға немесе ұйымға тиесілігін сенімді орталық (CA) растайды.

Гибридті шифрлау және TLS жұмысы

Іс жүзінде симметриялық және асимметриялық шифрлау бірге қолданылады. Бұл әдіс **гибридті шифрлау схемасы** деп аталады.

Жұмыс істеу принципі:

1. Асимметриялық криптография арқылы сессиялық кілт келісіледі.
2. Екі тарап ортақ симметриялық кілтті қолданады.
3. Деректер AES сияқты симметриялық шифр арқылы қорғалады.
4. Қабылдаушы алынған деректерді сессиялық кілтпен дешифрлайды.

Артықшылықтары:

- Асимметриялық криптография кілт алмасуды қорғайды.
- Симметриялық шифрлау деректерді жылдам өңдейді.
- Қауіпсіздік пен өнімділік үйлеседі.

TLS — осы тәсілді қолданатын қорғалған байланыс хаттамасы.

Жіберуші → асимметриялық кілт алмасу → ортақ сессиялық кілт → AES арқылы шифрланған деректер → қабылдаушы.

Желілік қауіпсіздік құралдары

Құрал	Негізгі қызметі
ACL және Firewall	IP, порт және хаттама бойынша трафикті сүзу
DMZ	Сыртқа ашық серверлерді ішкі желіден бөлу
IDS	Шабуылдарды анықтау
IPS	Шабуылдарды анықтау және тоқтату
VPN	Қорғалған туннель арқылы қашықтан қосылу
NAC / IEEE 802.1X	Желіге қосылар алдында құрылғыны аутентификациялау
Port Security	Коммутатор порттарына қосылған құрылғыларды шектеу
SIEM	Қауіпсіздік оқиғаларының журналдарын жинау және талдау

Қауіпсіздік хаттамалары

Желілік байланыс пен деректерді қорғау үшін арнайы хаттамалар пайдаланылады. **IPsec режимдері:**

- Transport mode — деректердің пайдалы бөлігін қорғайды.
- Tunnel mode — IP пакетін толық инкапсуляциялап қорғайды.

Хаттама	**Қызметі**
TLS 1.3 (RFC 8446)	Қорғалған байланыс орнатады; HTTPS негізі
IPsec	Желілік деңгейде деректерді қорғайды; VPN үшін қолданылады
SSH (22 порт)	Қашықтан басқарудың қорғалған арнасы
WPA3	Wi-Fi желісіндегі шифрлау мен аутентификацияны қамтамасыз етеді
DNSSEC	DNS жауаптарының түпнұсқалығын цифрлық қолтаңба арқылы растайды

Zero Trust қауіпсіздік моделі

Zero Trust — «ешкімге сенбе, әрқашан тексер» принципіне негізделген желілік қауіпсіздік моделі.
Дәстүрлі тәсілде ішкі желі сенімді, ал сыртқы желі сенімсіз деп қарастырылады. Zero Trust бұл қағидадан бас тартады.

Негізгі принциптері:

- Әрбір пайдаланушы мен құрылғыны тексеру.
- Қолжетімділікті орналасуына қарамастан бағалау.
- Ең аз құқық принципін қолдану.
- Әрбір сұраныстың қауіпсіздігін қайта тексеру.
- Пайдаланушының, құрылғының және қосылу жағдайының сенімділігін бағалау.

Мақсаты: Рұқсатсыз қолжетімділікті азайту және ішкі желідегі қауіптердің таралуына жол бермеу.

Заманауи желілердің дамуындағы жаңа технологиялар

Бағыт	Мәні	Артықшылығы
Wi-Fi 6/7	Жоғары өткізу қабілеттілігі бар сымсыз байланыс	Тығыз ортада тұрақты жұмыс
QUIC / HTTP/3	UDP негізіндегі заманауи транспорттық хаттама	Жылдам веб-қосылым
AI және Intent-based Networking	Желі ақауларын болжау және ниет бойынша баптау	Автоматты оңтайландыру
Постквантты криптография	Кванттық компьютерлерге төзімді алгоритмдер	Ұзақ мерзімді құпиялылық

Технологиялардың өзара байланысы:

- 5G желілері SDN/NFV негізінде құрылуы мүмкін.
- IoT құрылғыларын қорғауда Zero Trust қағидалары қолданылады.
- AI желідегі ақаулар мен қауіптерді ерте анықтауға көмектеседі.
- Постквантты криптография болашақтағы криптографиялық қауіптерге қарсы бағытталған.

Білімді бекітуге арналған сұрақтар:

1. CIA үштігінің негізгі қасиеттерін түсіндіріңіз.
2. AAA тетігі дегеніміз не және ол қандай қызмет атқарады?
3. Пассивті және белсенді шабуылдардың айырмашылығы неде?
4. ARP spoofing және MAC flooding шабуылдарынан қалай қорғануға болады?
5. DoS және DDoS шабуылдарының айырмашылығы қандай?
6. Симметриялық және асимметриялық шифрлауды салыстырыңыз.
7. Хэш-функция мен цифрлық қолтаңба қандай міндеттерді атқарады?
8. Firewall, IDS және IPS құралдарының айырмашылығын түсіндіріңіз.
9. TLS, IPsec және SSH хаттамаларының негізгі қызметтері қандай?
10. SDN мен IPv6 технологияларының мәні мен артықшылықтарын атаңыз.

Әдебиеттер тізімі:

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. — СПб.: Питер, 2020.
2. Таненбаум Э., Уэзеролл Д. Компьютерные сети. 5-е изд. — СПб.: Питер, 2012.
3. Kurose J.F., Ross K.W. Computer Networking: A Top-Down Approach. 8th ed. — Pearson, 2021.
4. Stallings W. Data and Computer Communications. 10th ed. — Pearson, 2014.
5. Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. — Pearson, 2020.
6. RFC 8446 — The Transport Layer Security (TLS) Protocol Version 1.3.
7. RFC 8200 — Internet Protocol, Version 6 (IPv6) Specification.
8. NIST SP 800-207 — Zero Trust Architecture, 2020.
9. NIST FIPS 203, 204, 205 — Post-Quantum Cryptography Standards, 2024.
10. Cisco Networking Academy — netacad.com.