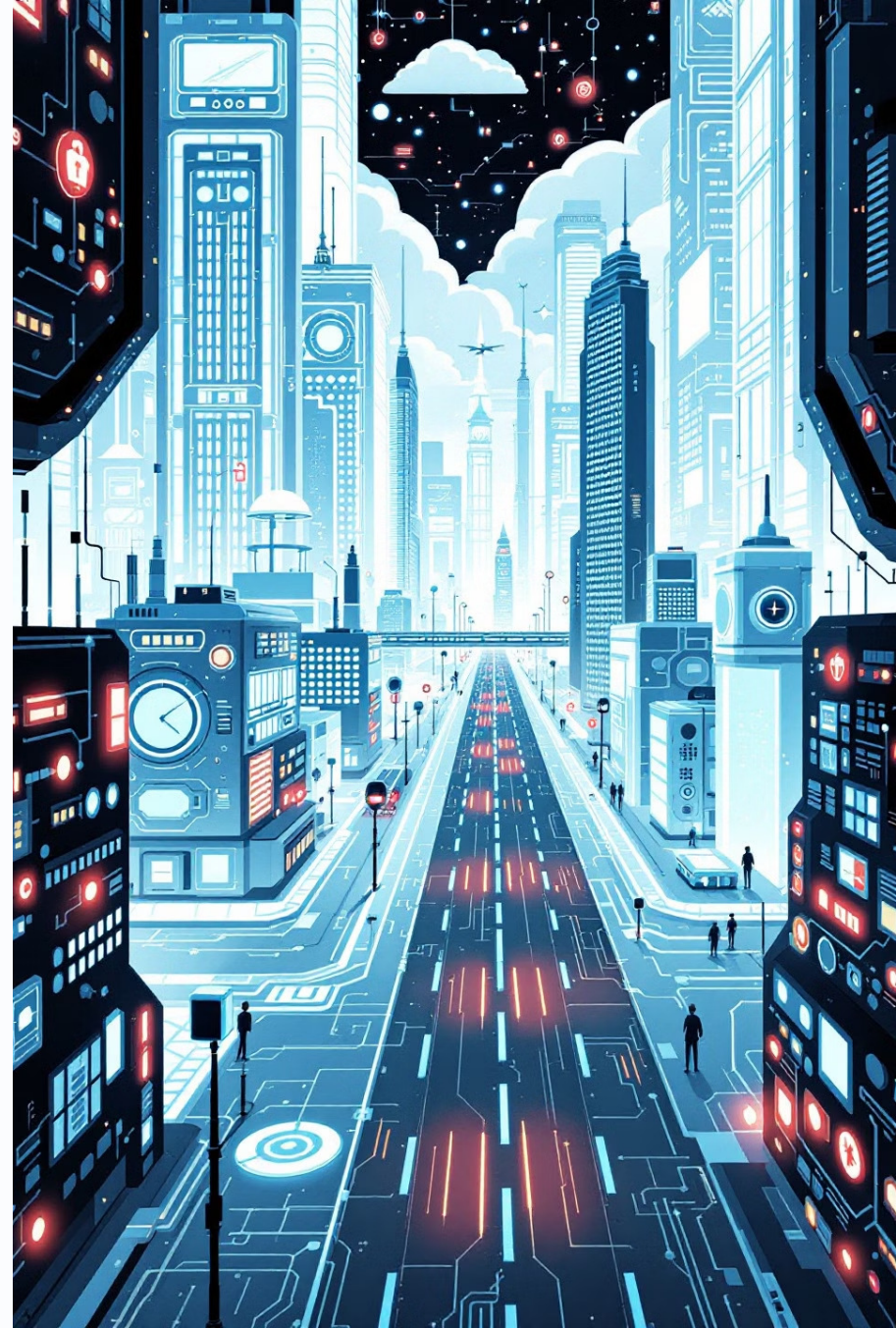


IoT Жүйелерінің Қауіпсіздігі: Шифрлеу және Аутентификация Әдістері

Бұл презентация IoT жүйелерінде шифрлеу және аутентификация әдістері арқылы қауіпсіздікті арттырудың негізгі әдістерін қарастырады. Біз қауіпсіздік тәуекелдерін, шифрлау түрлерін, аутентификация құралдарын және IoT қорғаудың техникалық шараларын талқылаймыз.



IoT Құрылғыларының Қауіпсіздігі Мәселелері

Қауіпсіздік Бос орындары

IoT құрылғыларының көбінесе әлсіз қауіпсіздік конфигурациясы бар.

Әлсіз парольдер және әлсіз шифрлау оларды зиянкестер үшін осал етеді.

Деректерге Қол жеткізу

IoT құрылғылары тұтынушылар туралы сезімтал ақпарат жинайды.

Бұл деректердің осалдығы жеке өмірдің бұзылуына әкелуі мүмкін.

Топтық Шабуылдар

IoT құрылғыларының көп санын бақылау DDoS шабуылдарын қоса, ірі масштабты шабуылдарды жасауға мүмкіндік береді.

Қауіпсіздік Тәуекелдерінің Жіктелуі

1 Жауапсыз бағдарламалық жасақтама

Жауапсыз бағдарламалық жасақтама қорғаныссыздық осалдықтар жасайды, оларды зиянкестер пайдалана алады.

2 Фишинг және Әлеуметтік инженерия

Бұл шабуылдар IoT құрылғыларына кіру үшін пайдаланушыларды алдауға бағытталған.

3 DDoS шабуылдары

Бұл шабуылдар IoT құрылғыларын қолдана отырып, серверлерді немесе желілерді артық жүктеу арқылы қызметтің тоқтауына әкелуі мүмкін.

4 Кіру осалдықтары

Әлсіз парольдер мен аутентификация әдістері IoT құрылғыларына рұқсатсыз кіруге мүмкіндік береді.



Симметриялық Шифрлау Әдістері

AES

Advanced Encryption Standard (AES) - бұл IoT құрылғылары үшін кең таралған симметриялық шифрлау алгоритмі.

DES

Data Encryption Standard (DES) - бұл ескірген, бірақ кейбір IoT құрылғыларында әлі де қолданылатын симметриялық шифрлау алгоритмі.

3DES

Triple DES (3DES) - DES алгоритмінің жетілдірілген нұсқасы, қорғаныс деңгейін арттырады.

Blowfish

Blowfish - бұл IoT құрылғыларында қолданылатын жылдам және сенімді симметриялық шифрлау алгоритмі.

Асимметриялық Шифрлау Әдістері



RSA

RSA - бұл кең таралған асимметриялық шифрлау алгоритмі, ол жеке және ашық кілттерді пайдаланады.



ECC

Elliptic Curve Cryptography (ECC) - бұл RSA-ға қарағанда аз есептеу ресурстарын қажет ететін асимметриялық шифрлау әдісі. ECC IoT құрылғыларына өте қолайлы.



DSA

Digital Signature Algorithm (DSA) - бұл сандық қолтаңбаларды жасау және тексеру үшін қолданылатын асимметриялық шифрлау алгоритмі.

Аутентификация және Авторизация Құралдары

1

Парольдер

IoT құрылғыларына кіру үшін пайдаланылатын парольдер күшті және ерекше болуы керек.

2

Екі факторлы аутентификация (2FA)

2FA қосымша қауіпсіздік қабатын қосады, бұл парольден басқа қосымша идентификаторды қажет етеді.

3

Токендер

Токендер - бұл IoT құрылғыларына рұқсатсыз кіруді болдырмауға көмектесетін кіруді басқару жүйелерінің бөлігі.

4

Биометриялық аутентификация

Бұл әдіс саусақ іздерін, бетті тануды немесе көздің торлы қабығын сканерлеу сияқты биометриялық деректерді пайдаланады.

IoT Бағдарламалық Жасақтама Қауіпсіздігі



Кластерлік Криптография және Биометриялық Аутентификация

1

Кластерлік Криптография

Кластерлік криптография IoT құрылғыларында деректерді шифрлаудың таратылған әдісі. Бұл әдіс кілттерді бірнеше құрылғыларға бөлу арқылы кілттердің осалдығын азайтады.

2

Биометриялық Аутентификация

Биометриялық аутентификация саусақ іздерін, бетті тануды немесе көздің торлы қабығын сканерлеу сияқты биометриялық деректерді пайдаланады.

3

Құрылғылардың арасындағы коммуникацияны шифрлау

IoT құрылғыларының арасындағы барлық деректер алмасуы шифрлау арқылы қорғалуы керек.

4

Қауіпсіздік саясатын қалыптастыру

IoT жүйелерінде қауіпсіздікті қамтамасыз ету үшін нақты қауіпсіздік саясатын қалыптастыру маңызды.

IoT Жүйелерін Қорғаудың Техникалық және Ұйымдастырушылық Шаралары

1

Қауіпсіздік бағдарламалық жасақтамасы

IoT құрылғыларында вирусқа қарсы бағдарламалық жасақтаманы қолдану қажет.

2

Желілік қауіпсіздік

Желілік қауіпсіздік шараларын, мысалы, брандмауэрлер мен VPN-ді қолдану қажет.

3

Қауіпсіздік мониторингі

IoT жүйелеріндегі қауіпсіздік оқиғаларын үнемі бақылау қажет.

4

Қауіпсіздік оқыту

IoT қауіпсіздігі туралы пайдаланушыларға оқыту беру маңызды.