INTERNET PAMETINIH UREĐAJA

prof. dr Dejan S. Aleksić

Prirodno-matematički fakultet, Niš

07. БЕЗБЕДНОСТ ПОДАТАКА И СИСТЕМА У IOT

ШТА ЈЕ КРИПТОГРАФИЈА У IOT-У

Криптографија у IoT-у је примена математичких метода за заштиту комуникације и података између паметних уређаја, сервера и корисника, прилагођена хардверским ограничењима тих уређаја.

Три главна задатка криптографије у IoT-у:

1. Поверљивост (Confidentiality):
   Шта ради: Претвара читке податке у шифровани текст.
   Пример: Комшија не може да види снимак са ваше паметне камере, иако „хвата" ваш Wi-Fi сигнал.
2. Интегритет (Integrity):
   Шта ради: Гарантује да подаци нису измењени на путу од сензора до сервера.
   Пример: Сензор шаље температуру „20°C". Нападач не може да пресретне поруку промени је у „200°C" да би изазвао лажну узбуну на пожарном систему.
3. Аутентичност (Authenticity):
   Шта ради: Доказује идентитет пошиљаоца.
   Пример: Када паметна брава добије команду „Откључај", она криптографски проверава да ли је команда стигла од стварног власника или од хакера који стоји испред врата.

УВОД У ИЗАЗОВЕ БЕЗБЕДНОСТИ IOT СИСТЕМА

Аутентификација (Ко си ти?)	**Ауторизација (Шта смеш да радиш?)**
Дефиниција: Процес провере и потврђивања идентитета корисника или уређаја.	**Дефиниција:** Процес додељивања или провере права приступа ресурсима након успешне идентификације.
Кључно питање: Да ли си онај за кога се представљаш?	**Кључно питање:** Да ли имаш дозволу да приступиш овом фајлу/соби/серверу?
Примери: Лозинка, отисак прста, скенирање лица, дигитални сертификат.	**Примери:** Администраторска права, дозвола за читање (Read-only), приступ ВИП зони.

„Аутентификација увек претходи ауторизацији."

Не можемо знати шта смеш да радиш док не знамо ко си.

1. Аутентификација:
   На пасошкој контроли показујете пасош. Службеник проверава ко сте ви. Ако је пасош валидан, прошли сте аутентификацију.

2. Ауторизација:
   Показујете карту за укрцавање (Boarding pass). Она каже где смете да идете (смете у авион за Рим, али не у авион за Лондон, и смете у економску класу, али не у пилотску кабину). То је ауторизација.

УВОД У ИЗАЗОВЕ БЕЗБЕДНОСТИ IOT СИСТЕМА

- **Ограничења ресурса:**
  IoT чворови (као крајњи уређаји) засновани су на микроконтролерима са малом процесном снагом, ограниченим капацитетом меморије и ограниченим изворима напајања.
  Није увек изводљиво извршавати сложене криптографске алгоритме, као што је RSA са дугим кључевима, на таквим платформама, обично због неприхватљивог времена обраде података или превелике потрошње енергије
- **Хетерогеност протокола:**
  Недостатак стандардизације довео је до фрагментације екосистема. Тешко је осмислити јединствену безбедносну политику (због хетерогене и често некомпатибилне имплементације различитих комуникационих протокола (ZigBee, LoRa, Bluetooth, MQTT, CoAP)) и то је учинило архитектуру система сложеном, а сама сложеност система продубљује овај проблем и по својој природи ствара услове за појаву озбиљнијих безбедносних пропуста.

УВОД У ИЗАЗОВЕ БЕЗБЕДНОСТИ IOT СИСТЕМА

Модел противника и класификација претњи

Да би се пројектовао безбедан систем, није довољно само имплементирати криптографске алгоритме; неопходно је прво јасно дефинисати од кога и од чега се систем брани. У теорији информационе безбедности, ово се формализује кроз модел противника (енгл. Adversary Model).

Стандардни модел који се користи у анализи безбедносних протокола је Долев-Јао модел.

Према овом моделу, нападач има потпуну контролу над комуникационим каналом и способан је да:

- Пресретне сваку поруку која се шаље кроз мрежу.
- Измени садржај поруке или редослед пакета.
- Обрише или блокира поруке (напад ускраћивањем комуникације).
- Убаци лажне поруке које изгледају као валидне.
- Сними валидну поруку и пошаље је касније (напад поновним слањем).

Модел противника стога мора укључити и могућност напада заробљавањем чвора (node capture attack), где нападач физички приступа уређају, анализира његову меморију и покушава да екстрахује криптографски материјал.

УВОД У ИЗАЗОВЕ БЕЗБЕДНОСТИ IOT СИСТЕМА

Пасивни напади подразумевају неовлашћено праћење и прислушкивање комуникације без измене података. Циљ нападача је прикупљање информација.

- Прислушкивање (Eavesdropping): Пресретање садржаја порука ради крађе осетљивих података (нпр. лозинки или сензорских очитавања).
- Анализа саобраћаја: Чак и ако су подаци шифровани, нападач анализом метаподатака (ко шаље, коме, колико често и које величине су пакети) може закључити много о понашању система и навикама корисника. Пасивне нападе је изузетно тешко детектовати јер не нарушавају функционалност мреже.

Активни напади укључују директну интеракцију са системом ради измене његовог стања или ометања рада.

- Маскарада (Spoofing): Нападач се лажно представља као легитиман уређај или сервер како би стекао неовлашћени приступ или убацио лажне податке.
- Напад поновним слањем (Replay attack): Нападач снима валидну поруку (нпр. команду за откључавање врата) и касније је поново шаље како би изазвао исту акцију, иако не познаје садржај саме шифре.
- Модификација порука: Измена садржаја контролних команди или мерних података у транзиту, чиме се нарушава интегритет система.

УВОД У ИЗАЗОВЕ БЕЗБЕДНОСТИ IOT СИСТЕМА

Спољашње и унутрашње претње

- Посебан изазов представљају унутрашње претње.
- Док спољашњи нападач мора да пробије криптографску заштиту да би ушао у мрежу, унутрашњи нападач је легитиман чвор мреже који је компромитован (нпр. хакован сензор).
- Пошто овај чвор поседује валидне кључеве и права приступа, он може неометано слати лажне податке или нападати друге чворове изнутра, што традиционалне одбрамбене механизме попут заштитних зидова чини неефикасним.

АРХИТЕКТУРА БЕЗБЕДНОСТИ И ПОВРШИНЕ НАПАДА

Концепт површине напада (енгл. Attack Surface) односи се на скуп свих тачака у систему („праваца напада”) преко којих неовлашћени корисник може покушати да унесе податке или извуче информације.

У традиционалним системима, површина напада је често била ограничена на спољни мрежни интерфејс.

У IoT окружењу, површина напада је драстично увећана и обухвата:

- Физичке интерфејсе: Дијагностички портови (JTAG, UART), USB прикључци и слотови за SD картице на самом уређају, који омогућавају директан приступ хардверу.
- Бежичне интерфејсе: Радио комуникација (Wi-Fi, Bluetooth, Zigbee, LoRaWAN) која је због своје емисионе природе инхерентно отворена за прислушкивање и ометање.
- Мрежне сервисе: Отворени портови и сервиси који су активни на уређају (нпр. веб сервер за иницијалну конфигурацију или SSH сервис са подразумеваним лозинкама).
- Апликативне интерфејсе (API): Тачке комуникације са „Cloud” платформом и мобилним апликацијама које могу бити подложне манипулацији подацима.
- Људски фактор: Подложност корисника техникама социјалног инжењеринга, посебно приликом процеса упаривања уређаја или конфигурације приступа мрежи.

минимизација површине напада

АРХИТЕКТУРА БЕЗБЕДНОСТИ И ПОВРШИНЕ НАПАДА

Анализа рањивости према слојевима архитектуре

Детаљна анализа захтева сагледавање специфичних претњи на сваком од три основна слоја IoT архитектуре:

- слоју перцепције,
- мрежном слоју и
- апликативном слоју.

АРХИТЕКТУРА БЕЗБЕДНОСТИ И ПОВРШИНЕ НАПАДА

Слој перцепције (Физички слој)

Ово је најрањивији део система јер су уређаји често физички доступни нападачима у неконтролисаном окружењу.

Кључне рањивости укључују:

- Физичко заробљавање чворова: Нападач може отуђити уређај и директним повезивањем на интерфејсе преузети садржај меморије (firmware extraction). Уколико криптографски кључеви нису смештени у заштићеном делу хардвера безбедност целог система може бити нарушена.
- Напади путем бочног канала: Ово је софистицирана класа напада где нападач не напада сам алгоритам шифровања, већ његову физичку имплементацију. Анализом потрошње енергије, електромагнетног зрачења или времена извршавања операција, могуће је реконструисати тајне кључеве.
- Ометање сигнала: Емитовањем снажног радио-сигнала наградној фреквенцији уређаја, нападач може спречити комуникацију, изазивајући ефекат ускраћивања услуге на физичком нивоу.

АРХИТЕКТУРА БЕЗБЕДНОСТИ И ПОВРШИНЕ НАПАДА

Мрежни и транспортни слој

Овај слој је задужен за пренос података прикупљених на слоју перцепције до система за обраду.

С обзиром на то да се комуникација често одвија бежичним путем, она је подложна пресретању.

Доминантни безбедносни проблеми су:

- Напади на рутирање: У мрежама где чворови учествују у преносу туђих података (тзв. mesh топологије, карактеристичне за Zigbee или 6LoWPAN), малициозни чвор може одбацивати пакете (напад „црна рупа” - Black Hole) или их преусмеравати како би изазвао загушење мреже или исцрпљивање батерија суседних чворова.
- Напади „Човек у средини” (Man-in-the-Middle): Уколико комуникација није обострано аутентификована, нападач се може позиционирати између пошиљаоца и примаоца, пресрећући и потенцијално мењајући поруке пре него што оне стигну на одредиште.

АРХИТЕКТУРА БЕЗБЕДНОСТИ И ПОВРШИНЕ НАПАДА

Слој апликације и обраде података

Овај слој обрађује податке и пружа услуге крајњем кориснику.

Овде се фокус помера са хардверских на софтверске рањивости:

- Небезбедни API интерфејси: Апликативни програмски интерфејси којима уређаји комуницирају са сервером често немају адекватну контролу приступа, што омогућава нападачима слање неауторизованих команди.

- Инјекција малициозног кода: Уколико систем не врши валидацију улазних података, нападач може унети малициозни скрипт или SQL упит који ће се извршити на серверу или самом уређају

АРХИТЕКТУРА БЕЗБЕДНОСТИ И ПОВРШИНЕ НАПАДА

Повезаност површина напада и последице пробоја

- Важно је разумети да површине напада нису изоловане.
- Успешан напад на једном слоју често служи као основа за напад на друге делове система (тзв. Pivot attack).
- На пример, компромитовањем једног сензора (слој перцепције) због лоше заштићеног бежичног протокола, нападач може добити приступ локалној мрежи, а одатле покушати да приступи серверима или другим повезаним системима.
- Стога се саветује да приликом пројектовања система усвоји принцип „одбране у дубину” (Defense in Depth).
- Овај принцип налаже да отказивање једног механизма заштите не сме резултирати потпуним нарушавањем сигурности система, већ морају постојати додатни слојеви одбране који ће зауставити или успорити нападача

КРИПТОГРАФСКИ МЕХАНИЗМИ У УСЛОВИМА ОГРАНИЧЕНИХ РЕСУРСА

- Имплементација криптографске заштите на уређајима са ограниченим ресурсима представља инжењерски компромис између нивоа:
  - безбедности,
  - брзине обраде и
  - потрошње енергије.

- IoT уређаји често располажу са свега неколико килобајта RAM меморије и раде на батерије које морају трајати годинама.

- Стандардни алгоритми заштите, пројектовани за моћне рачунарске системе, често превазилазе могућности оваквог окружења.

- Да би се одговорило на ове изазове, користи се комбинација **оптимизованих стандардних алгоритама** и наменски развијених „**лаких**” (lightweight) криптографских решења.

КРИПТОГРАФСКИ МЕХАНИЗМИ У УСЛОВИМА ОГРАНИЧЕНИХ РЕСУРСА

- **Симетрична криптографија**
  - Криптографија тајног кључа

- **Асиметрична криптографија**
  - Криптографија јавног кључа

КРИПТОГРАФСКИ МЕХАНИЗМИ У УСЛОВИМА ОГРАНИЧЕНИХ РЕСУРСА

Симетрична криптографија (Криптографија тајног кључа)

Ово је најстарији и најједноставнији облик заштите.

Принцип: Пошиљалац и прималац користе исти кључ (један једини тајни кључ) и за шифровање и за дешифровање.

Аналогија: Замислите сеф. Ако ја закључам сеф одређеним кључем и пошаљем вам тај сеф, ви морате имати копију тог истог кључа да бисте га отворили.

Главни проблем: Дистрибуција кључа. Како да вам пошаљем тајни кључ преко небезбедног интернета (нпр. имејлом), а да га неко успут не пресретне? Ако нападач украде кључ, читава комуникација је компромитована.

Предности: Изузетно је брза и ефикасна. Процесори је лако обрађују.

Примена у IoT: Шифровање велике количине података (нпр. видео стрим са камере или континуирани подаци са сензора). Примери алгоритама: AES, DES, ChaCha20.

КРИПТОГРАФСКИ МЕХАНИЗМИ У УСЛОВИМА ОГРАНИЧЕНИХ РЕСУРСА

Асиметрична криптографија (Криптографија јавног кључа)

Настала је да би решила проблем размене кључева.

Принцип: Користи се пар кључева:

1. Јавни кључ (Public Key): Дели се свима слободно (као ваша имејл адреса). Служи за шифровање.
2. Приватни кључ (Private Key): Чува се у строгој тајности (само га власник зна). Служи за дешифровање.

Математичка веза: Оно што се закључа јавним кључем, може се откључати само одговарајућим приватним кључем. Чак ни сам јавни кључ не може да откључа поруку коју је управо шифровао.

Аналогија: Замислите поштанско сандуче са отвором за убацивање писама. Свако може да убаци писмо унутра (коришћење јавног кључа). Али само поштар (власник) који има кључ од вратанца може да извади и прочита писма (коришћење приватног кључа).

Друга примена: Дигитални потпис. Процес се може обрнути. Ако шифрујем нешто својим приватним кључем, свако то може отворити мојим јавним. То не штити тајност, али доказује да сам баш ја (једини власник приватног кључа) послао поруку. То је основа дигиталног потписа.

Мане: Спорија је (1000x) од симетричне криптографије и захтева више процесорске снаге.

Примери алгоритама: RSA, ECC (Елиптичке криве).

КРИПТОГРАФСКИ МЕХАНИЗМИ У УСЛОВИМА ОГРАНИЧЕНИХ РЕСУРСА

Симетрична криптографија у IoT системима

Симетрична криптографија, где пошиљалац и прималац деле исти тајни кључ, чини основу заштите поверљивости података у IoT мрежама због своје брзине и ефикасности.

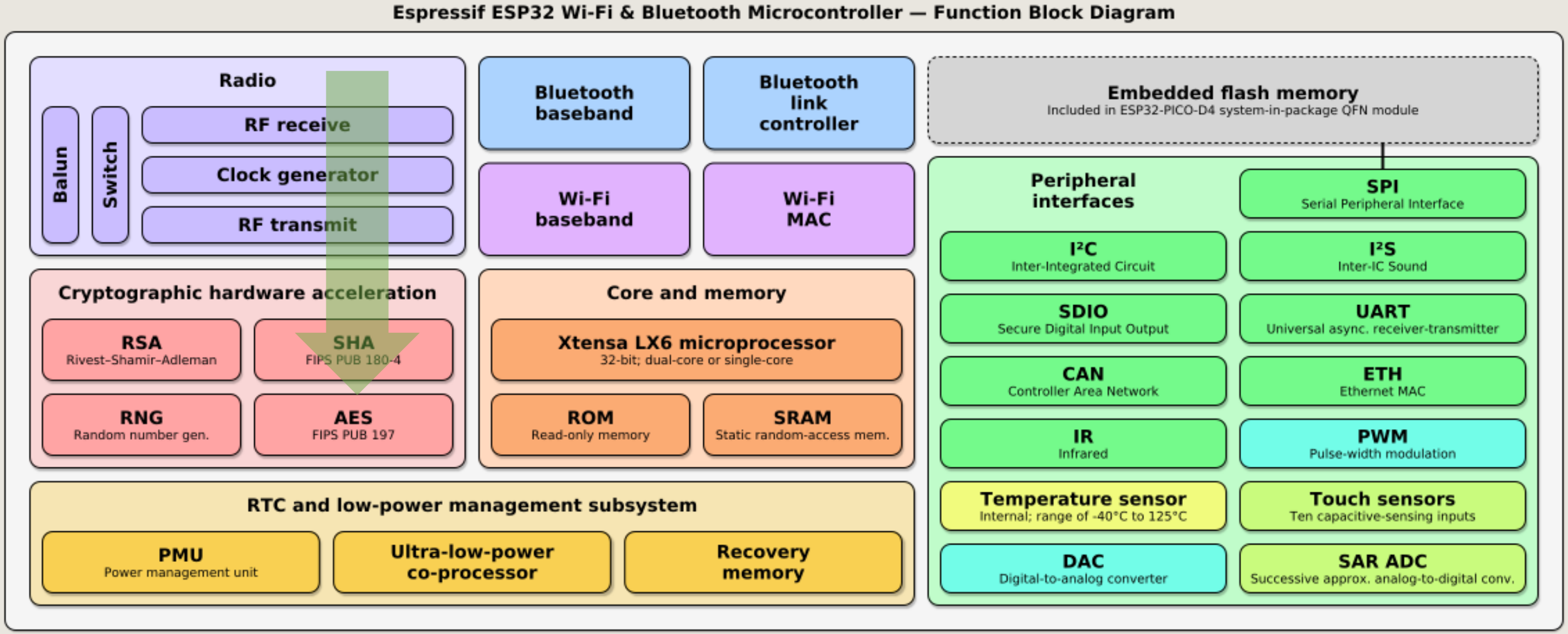
- AES и режими рада

  Напредни стандард за шифровање (AES - Advanced Encryption Standard) је данас де факто стандард и у IoT свету.
  Иако је AES релативно захтеван, већина модерних микроконтролера (нпр. ESP32, STM32 серије) поседује хардверске акцелераторе за AES инструкције. Ово омогућава шифровање уз минимално оптерећење главног процесора.

- Лаки симетрични алгоритми

  За екстремно ограничене уређаје (нпр. пасивни RFID тагови или 8-битни микроконтролери без хардверске акцелерације), користе се алгоритми пројектовани за минималну хардверску сложеност (gate count) и ниску потрошњу струје.

КРИПТОГРАФСКИ МЕХАНИЗМИ У УСЛОВИМА ОГРАНИЧЕНИХ РЕСУРСА



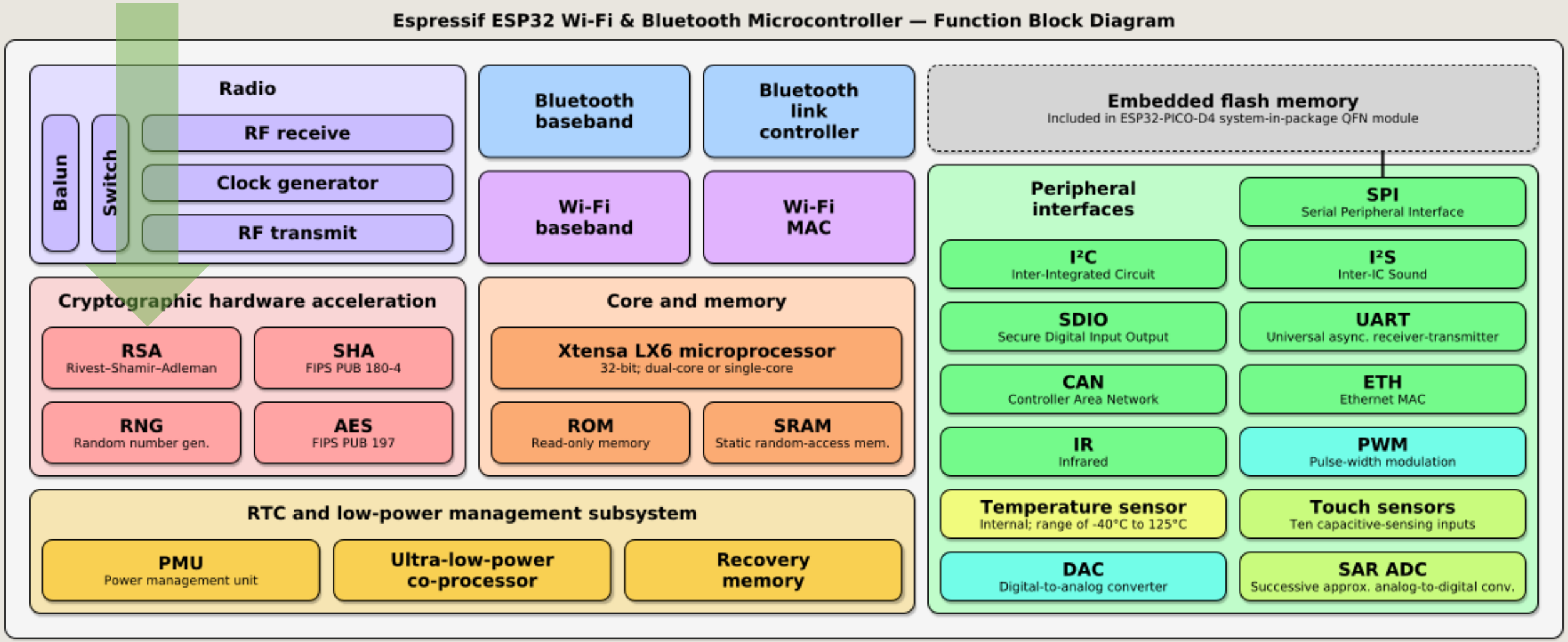
https://upload.wikimedia.org/wikipedia/commons/thumb/9/92/Espressif_ESP32_Chip_Function_Block_Diagram.svg/1143pxEspressif_ESP32_Chip_Function_Block_Diagram.svg.png

КРИПТОГРАФСКИ МЕХАНИЗМИ У УСЛОВИМА ОГРАНИЧЕНИХ РЕСУРСА

Асиметрична криптографијау IoT системима

- Асиметрична криптографија је неопходна за безбедну размену кључева и дигитално потписивање (аутентификацију уређаја). Док је **RSA** алгоритам доминирао деценијама, он је неподобан за већину IoT уређаја због дужине кључева и сложености прорачуна.
- Данашњи индустријски стандард у IoT-у је криптографија елиптичких кривих (**ECC** - Elliptic Curve Cryptography).
- Безбедност ECC-а заснива се тежини решавања проблема дискретног логаритма елиптичке криве, што је математички „тежи” проблем од факторизације бројева на којој се заснива RSA.
- Ово омогућава коришћење драстично краћих кључева за исти ниво безбедности.

КРИПТОГРАФСКИ МЕХАНИЗМИ У УСЛОВИМА ОГРАНИЧЕНИХ РЕСУРСА



https://upload.wikimedia.org/wikipedia/commons/thumb/9/92/Espressif_ESP32_Chip_Function_Block_Diagram.svg/1143pxEspressif_ESP32_Chip_Function_Block_Diagram.svg.png

КРИПТОГРАФСКИ МЕХАНИЗМИ У УСЛОВИМА ОГРАНИЧЕНИХ РЕСУРСА

Асиметрична криптографијау IoT системима

Ниво безбедности (симетрични кључ)	RSA дужина кључа	ECC дужина кључа
80 бита	1024	160-192
112 бита	2048	224
128 бита	3072	256
256 бита	15360	512

Поређење дужине кључева: RSA наспрам ECC

КАКО МЕРИМО БЕЗБЕДНОСТ: „БИТОВИ СИГУРНОСТИ” НАСПРАМ ДУЖИНЕ КЉУЧА

- Када у криптографији кажемо да је неки алгоритам „безбедан”, ми заправо говоримо о времену и енергији потребним да се он разбије.

- Основна јединица мере није сама дужина лозинке коју видите, већ ниво безбедности у битовима (Security Level).

- Ово је често збуњујуће јер, као што видите у табели, 80 бита безбедности не значи увек да је кључ дугачак 80 бита.

КАКО МЕРИМО БЕЗБЕДНОСТ: „БИТОВИ СИГУРНОСТИ” НАСПРАМ ДУЖИНЕ КЉУЧА

1. **Ниво безбедности (Симетрични кључ)** - „Златни стандард”
   Ово је наша референтна тачка. Код симетричних алгоритама (попут AES-а), ако кажемо да имамо 128-битну безбедност, то значи да нападач мора да изврши 2^{128} операција да би „грубом силом” (brute-force) погодио кључ.
   Ту важи правило: Дужина кључа ≈ Ниво безбедности.

Ниво безбедности (симетрични кључ)	RSA дужина кључа	ECC дужина кључа
80 бита	1024	160-192
112 бита	2048	224
128 бита	3072	256
256 бита	15360	512

КАКО МЕРИМО БЕЗБЕДНОСТ: „БИТОВИ СИГУРНОСТИ” НАСПРАМ ДУЖИНЕ КЉУЧА

2. RSA (Асиметрична криптографија)

RSA је базиран на тежини факторизације великих бројева.
Међутим, математичари су открили пречице за факторизацију.
То значи да 1024-битни RSA кључ није 2^{1024} пута тежак за разбијање.
Много је слабији.

Ниво безбедности (симетрични кључ)	RSA дужина кључа	ECC дужина кључа
80 бита	1024	160-192
112 бита	2048	224
128 бита	3072	256
256 бита	15360	512

КАКО МЕРИМО БЕЗБЕДНОСТ: „БИТОВИ СИГУРНОСТИ” НАСПРАМ ДУЖИНЕ КЉУЧА

3. ECC - Елиптичке криве (Асиметрична криптографија)

Криптографија елиптичких кривих (ECC) је модерна асиметрична метода. Она користи сложенију математику која не дозвољава лаке „пречице” нападачима.
Зато је ECC кључ много краћи, а пружа исту заштиту.

Ниво безбедности (симетрични кључ)	RSA дужина кључа	ECC дужина кључа
80 бита	1024	160-192
112 бита	2048	224
128 бита	3072	256
256 бита	15360	512

ПРЕГЛЕД ЕВОЛУЦИЈЕ БЕЗБЕДНОСТИ

- 80 бита безбедности (Застарело):
  - Ово је био стандард пре 2010. године.
  - RSA кључ од 1024 бита се данас сматра небезбедним за озбиљне примене јер модерни суперкомпјутери и клауд (cloud) кластери могу да га угрозе.
- 112 бита безбедности (Минимум):
  - RSA скаче на 2048 бита. Ово је тренутно најчешћи кључ који видите на интернету (HTTPS сертификати), али се полако напушта.
  - ECC овде користи само 224 бита.
- 128 бита безбедности (Данашњи стандард):
  - Ово је ниво који препоручују агенције које се баве безбедношћу података.
  - Кључни моменат за IoT: Уместо да користите тешки RSA кључ од 3072 бита који троши батерију, ви користите брзи ECC кључ од 256 бита.
- 256 бита безбедности (Војни ниво):
  - Користи се за строго поверљиве податке и заштиту од будућих квантних рачунара (донекле).
  - Овде RSA постаје апсурдан – кључ од 15.360 бита је превелик за већину мрежних пакета и процесора. ECC остаје компактан на 512 бита.