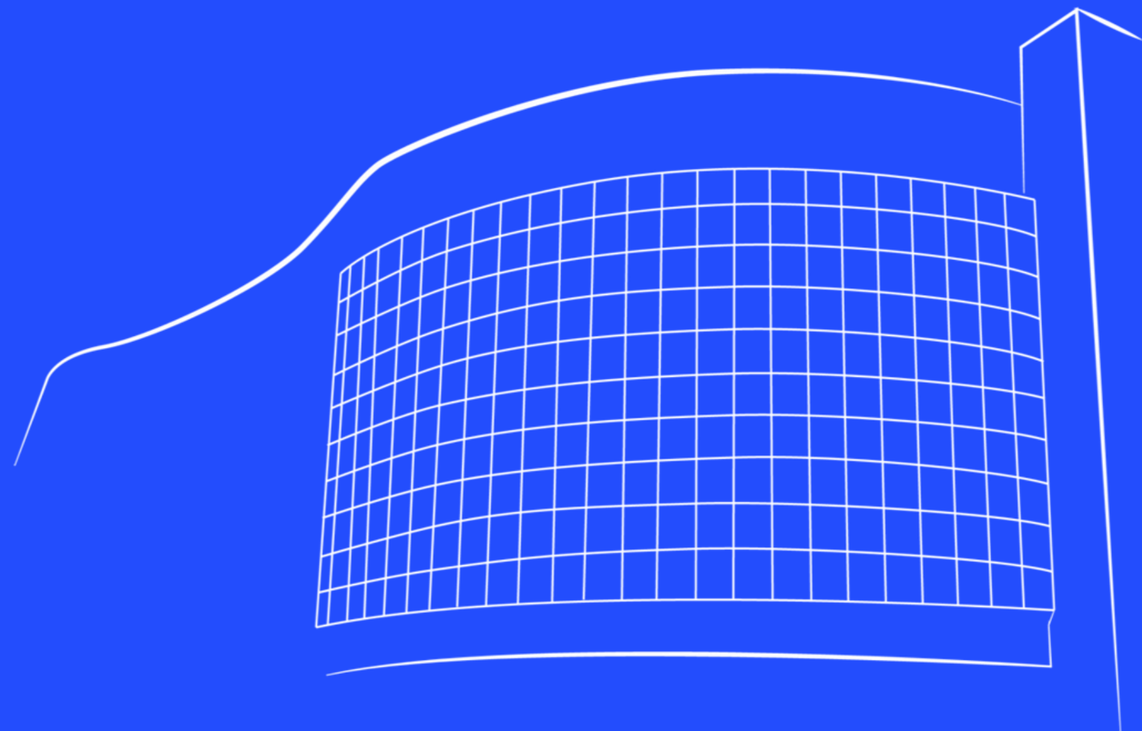
Segurança em Bluetooth Low Energy: Mecanismos, Vulnerabilidades, Ataques e Soluções aplicadas a Camada de Aplicação

SBrT 2025



CxSC Telecom
Centro de Segurança Cibernética

Inatel

Agenda

1. Fundamentos de segurança cibernética
2. Introdução ao Bluetooth Low Energy
3. Modelos de segurança e vulnerabilidades do Bluetooth Low Energy
4. Modelo de segurança proposto para Bluetooth Low Energy
5. Demonstração prática das vulnerabilidades do Bluetooth Low Energy

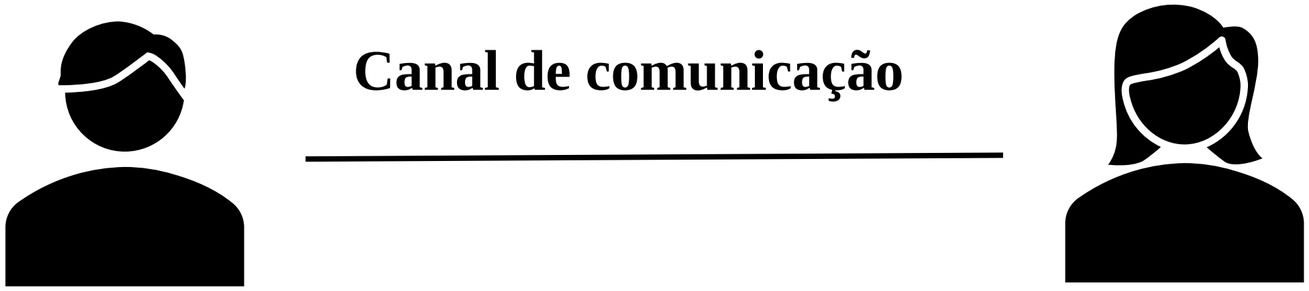
Agenda

1. Fundamentos de segurança cibernética
2. Introdução ao Bluetooth Low Energ
3. Modelos de segurança e vulnerabilidades do Bluetooth Low Energy
4. Modelo de segurança proposto para Bluetooth Low Energy
5. Demonstração prática das vulnerabilidades do Bluetooth Low Energy

Fundamentos de segurança cibernética
Conceitos iniciais

João deseja comunicar-se com Maria de forma segura. Como fazer isso, requer responder algumas perguntas:

- Como garantir à João que as mensagens dele serão lidas apenas por Maria?
- Como garantir para ambos que a mensagem recebida é de fato a transmitida?
- Como Maria tem certeza que é João quem se comunica com ela?
- Como podemos garantir que mensagens recebidas por Maria são de fato de João?



Fundamentos de segurança cibernética
Conceitos iniciais

As respostas para as questões anteriores podem ser respondidas por meio de cinco importante aspectos em uma comunicação segura:

- **Confidencialidade**: corresponde às informações estarem disponíveis somente a quem está devidamente autorizado a acessá-las
- **Integridade**: diz respeito à informação estar intacta, sem quebras e sem alterações não autorizadas
- **Autenticidade**: o remetente e o destinatário devem confirmar a identidade da outra parte envolvida na comunicação
- **Irretratabilidade**: impede que o emissor ou o receptor negue uma mensagem transmitida
- **Disponibilidade**: diz respeito à informação estar disponível para o usuário que à utiliza no momento em que se precisa dela

Fundamentos de segurança cibernética
Confiabilidade: Criptografia

Definição:

Área da criptologia que estuda princípios e técnicas para comunicação segura na presença de terceiros.

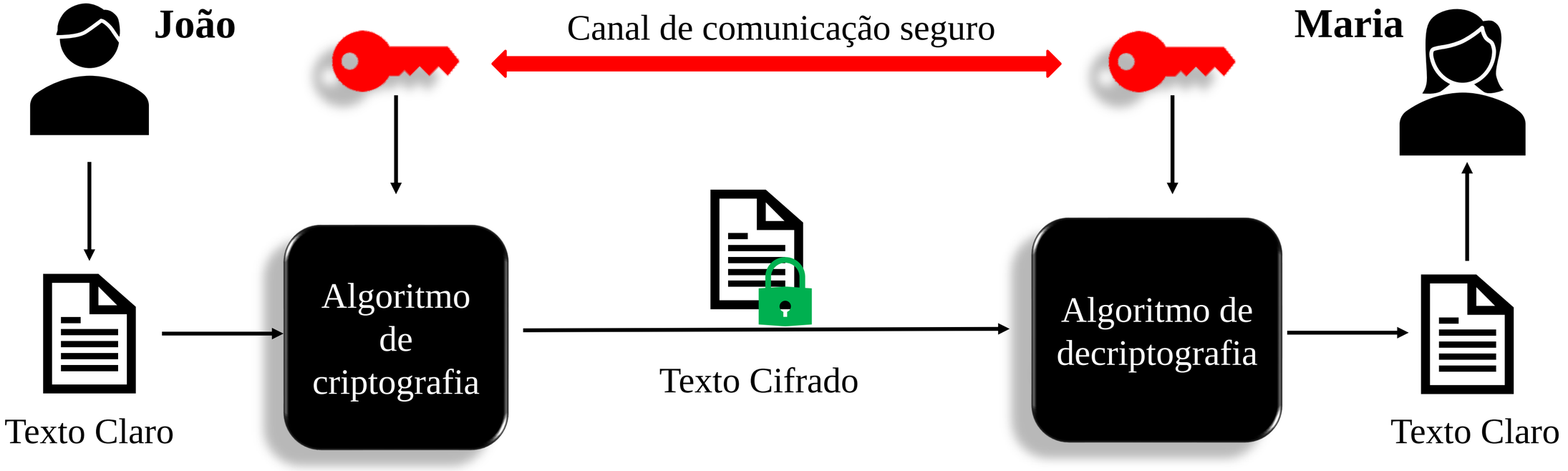
Grupos de técnicas de criptografia:

Criptografia simétrica: é uma forma de criptossistema que emprega a mesma chave secreta para realizar a criptografia e a decriptografia

Criptografia assimétrica: é uma forma de criptossistema que emprega um par de chaves (pública e secreta) para realizar a criptografia e a decriptografia, respectivamente.

Fundamentos de segurança cibernética
Confiabilidade: Criptografia Simétrica

A criptografia simétrica é uma forma de criptossistema em que a criptografia e a decriptografia são realizadas usando a mesma chave. Ela também é conhecida como criptografia convencional ou criptografia de chave única.



Fundamentos de segurança cibernética
Confiabilidade: Criptografia Simétrica e Padrões

Criptografia de Blocos:

- DES (*Data Encryption Standard*): Algoritmo criado pela *Federal Information Processing Standard* (FIPS) pelo EUA em 1976, sendo utilizado em larga escala internacionalmente.

- AES (*Advanced Encryption Standard*): Trata-se do atual padrão de criptografia dos EUA, utilizados em transações bancárias, redes Wi-Fi e no GPON.

Criptografia de Fluxo:

- RC4 (*Rivest Cipher*): Usado para criptografia WEP (*Wired Equivalent Privacy*) e WPA (*Wi-Fi Protected Access*)

Fundamentos de segurança cibernética
Confiabilidade: Criptografia Simétrica – Padrão DES

DES – *Data Encryption Standard*

- Algoritmo como *Federal Information Processing Standard* (FIPS) pelo EUA em 1976, sendo utilizado em larga escala internacionalmente.
- Inicialmente, o algoritmo possuía chave secreta de pequeno tamanho e suspeitas de um *backdoor* da Agência Nacional de Segurança (NSA)
- O padrão DES é um código de cifragem por blocos, onde o texto claro possui 64 bits e a chave secreta possui 56 bits utilizáveis de um total de 64 bits
- Uma chave de 56 bits possui 2^{56} chaves possíveis
- Ataque de força bruta levaria cerca de mil anos para quebrar a criptografia, considerando a análise de uma chave por microssegundo.

Fundamentos de segurança cibernética
Confiabilidade: Criptografia Simétrica – Padrão AES

AES – *Advanced Encryption Standard*

- Padrão de criptografia dos EUA, utilizado em transações bancárias, redes Wi-Fi e no GPON.
- O padrão se originou de um concurso realizado pelo NIST (*National Institute of Standards and Technology*)
- Esse algoritmo permite que o tamanho do bloco e o tamanho da chave possam ser especificados independentemente. As chaves podem assumir tamanhos de 128, 192 e 256 bits.
- Apresenta resiliência contra todos os ataques conhecidos e simplicidade de projeto

Tamanho da chave	128 bits	192 bits	256 bits
Tamanho do bloco de texto claro	128 bits		
Número de rodadas de criptografia	10	12	14
Tamanho da chave expandida	176 bits	208 bits	240 bits

Fundamentos de segurança cibernética
Confiabilidade: Criptografia Simétrica

Compartilhamento seguro de chaves secretas

- Existem várias formas de distribuir chaves secretas de maneira segura. Normalmente, as formas mais usadas são baseadas no uso da criptografia de chave pública para distribuição das chaves secretas.

- Distribuição de chaves secretas com criptografia de chave pública. (Usada no SSL/TLS)

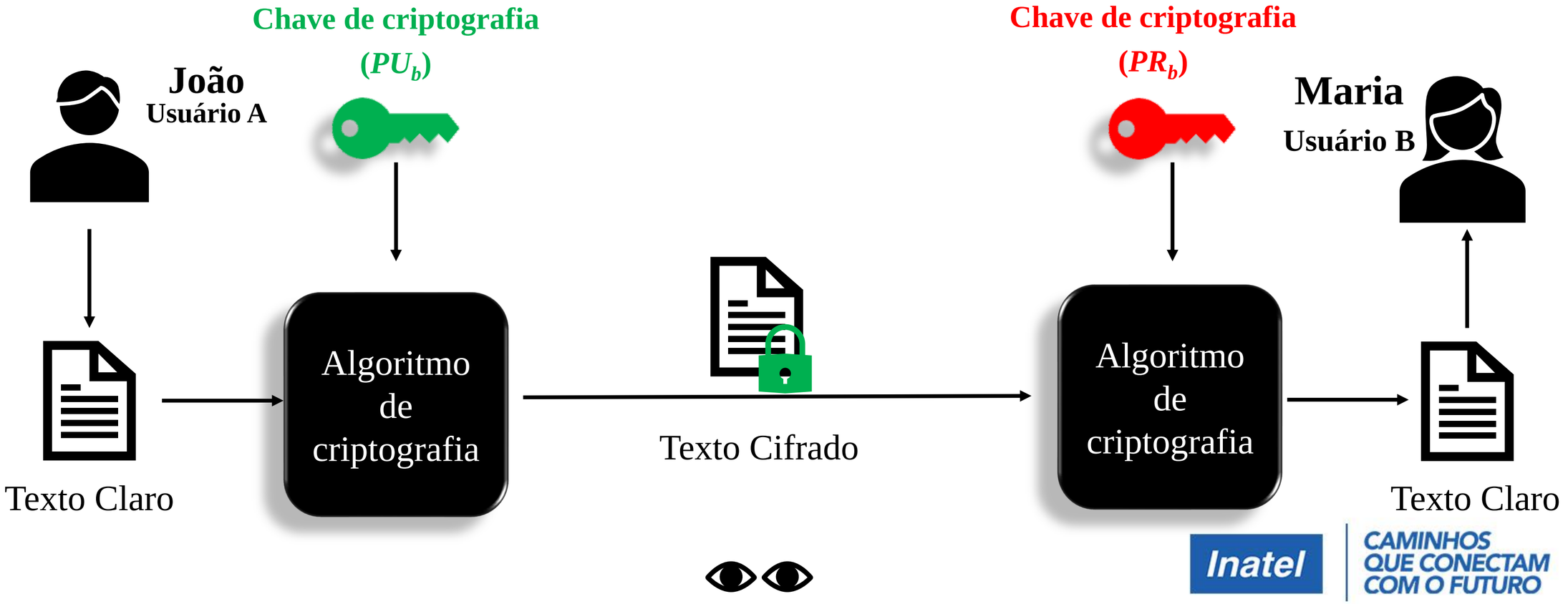
- Acordo de chaves Diffie-Hellman. (Usada no IP-Sec)

- Criptografia quântica. (Usada em sistemas QKD, *Quantum Key Distribution*)

Fundamentos de segurança cibernética

Confiabilidade: Criptografia Assimétrica

A criptografia assimétrica é uma forma de criptossistema em que a criptografia e a decriptografia são realizadas usando diferentes chaves: uma chave pública (PU_b) e uma chave privada (PR_b). É conhecida também como criptografia de chave pública.



Fundamentos de segurança cibernética
Confiabilidade: Criptografia Assimétrica

***Rivest Shamir Adlleman* - RSA**

Publicado em 1978 por 3 professores do MIT. É desde então a técnica de uso geral mais aceita e implementada para criptografia de chave pública. Trata-se de um esquema de cifra por bloco.

- Criptografia: $C = M^e mod(n)$
- Decriptografia: $M = C^d mod(n)$

M é o valor do texto claro
C é o valor do texto cifrado
e é o valor de chave pública
d é o valor de chave privada
n é um parâmetro que deriva da operação entre dois números
mod(*x*) é a função módulo congruente (devolve o resto da divisão de um número por *x*)

Fundamentos de segurança cibernética
Confiabilidade: Criptografia Assimétrica

***Rivest Shamir Adlleman* - RSA**

Para entender o algoritmo de criptografia RSA é necessário definir alguns termos matemáticos:

- Fatores: números que multiplicados resultam em um número original inicialmente escolhido

Fatores do número 10: 1, 2, 5, 10

- Número Primo: Número divisível por 1 e por ele mesmo ou aquele em que os fatores possíveis é 1 e ele mesmo

Números Primos: 2, 3, 5, 7...

- Número Semi-primo: Número cujos fatores são 1, ele mesmo e outros dois números primos

Número Semi-Primo: 35 → 5 x 7

Inatel CAMINHOS QUE CONECTAM COM O FUTURO

Fundamentos de segurança cibernética
Confiabilidade: Criptografia Assimétrica

***Rivest Shamir Adlleman* - RSA**

Processo de geração do par de chaves pública e privada:

- Selecionar dois números primos: p e q

$p = 7 \quad e \quad q = 19$

- Calcular o produto entre os números primos escolhidos: $n = p \times q$

$n = 7 \times 19 = 133$

- Calcular o tociente: $t = (p - 1) \times (q - 1)$

$t = (7 - 1) \times (19 - 1) = (6) \times (18) = 108$

Fundamentos de segurança cibernética
Confiabilidade: Criptografia Assimétrica

***Rivest Shamir Adlleman* - RSA**

Processo de geração do par de chaves pública e privada:

- Selecionar a chave pública, seguindo as condições:
  - Deve ser um número primo
  - Deve ser menor que o tociente
  - Não pode ser um fator do tociente

$e = 29$

- Selecionar a chave privada, seguindo a condição:
  - Produto da chave privada e da pública, dividido pelo tociente tem que ter resto 1 (d*e) mod(t) = 1

$d = 41$

Fundamentos de segurança cibernética
Confiabilidade: Criptografia Assimétrica

***Rivest Shamir Adlleman* - RSA**

Aplicando o par de chaves gerado para encriptar e decriptar uma mensagem:

$$PU = \{29, 133\}$$

$$PR = \{41, 133\}$$

Considerando $M = 80$

$$80^{29} mod(133) = 54$$

O valor 54 representa o valor do texto cifrado ($C = 54$), aplicando a chave privada:

$$54^{41} mod(133) = 80$$

Fundamentos de segurança cibernética
Integridade

Definição:

Integridade de mensagens é um mecanismo ou serviço usado para verificar a integridade de uma mensagem. A integridade garante que os dados recebidos sejam exatamente iguais aos enviados.

Técnicas de criptografia para autenticação de mensagens:

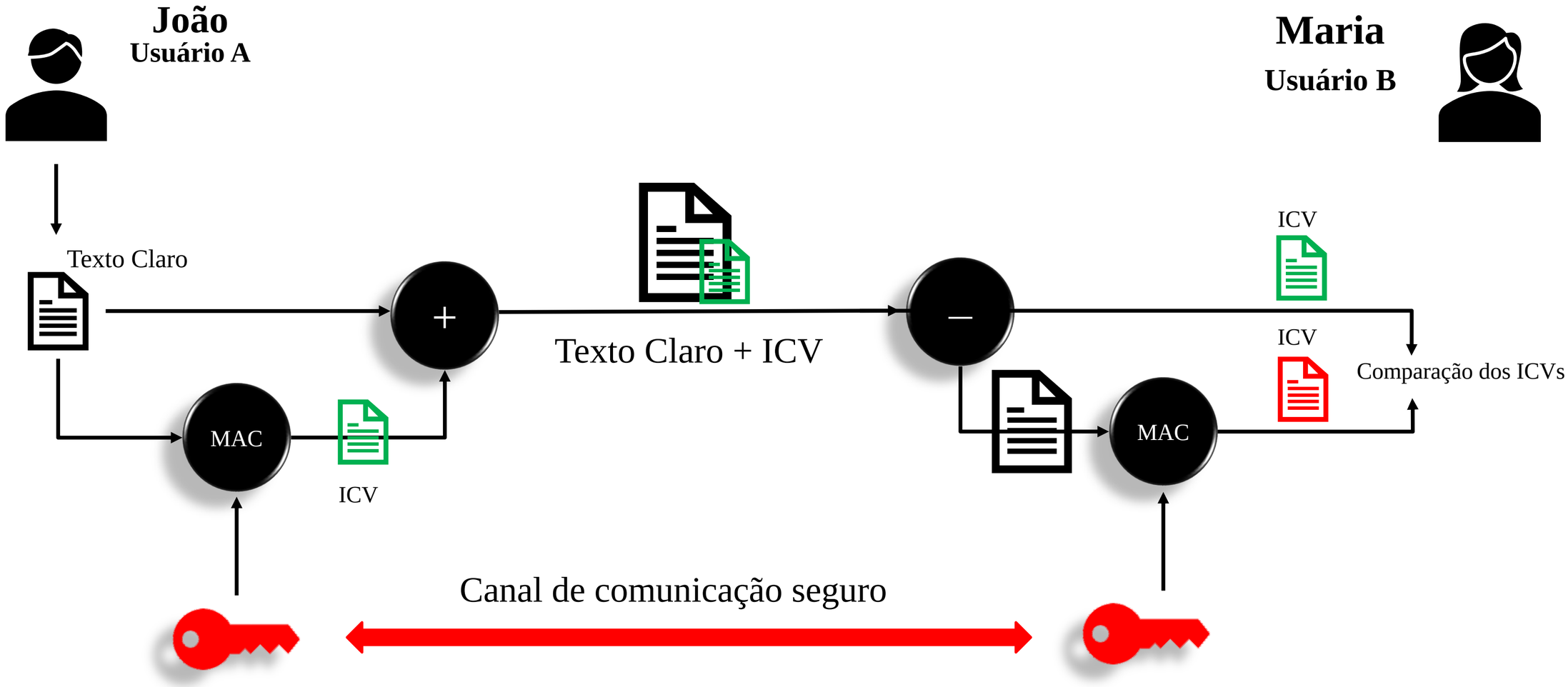
Código de autenticação de mensagem – MAC, *Message Authentication Code*: é uma função da mensagem e de uma chave secreta que produz um valor de tamanho fixo, que serve como autenticador.

Função de Hash: é uma função que relaciona uma mensagem de qualquer tamanho a um valor de hash de tamanho fixo, que serve como autenticador.

Fundamentos de segurança cibernética

Integridade: Código de Autenticação de Mensagem, MAC

É o uso de uma chave secreta de tamanho *K* para gerar um pequeno bloco de dados de tamanho fixo, conhecido como MAC, que é anexado à mensagem *M*.



Fundamentos de segurança cibernética
Integridade: Código de Autenticação de Mensagem, MAC

- Um algoritmo MAC é também denominado de função de dispersão chaveada (*keyed hash function*)

- Esse algoritmo recebe como entrada uma chave secreta e uma mensagem de tamanho arbitrário para ser autenticado, e tem como saída o Código de Verificação de Integridade (*Integrity Check Value*, ICV)

- O valor de saída do MAC protege tanto a integridade dos dados da mensagem, como sua própria autenticidade, permitindo aos verificadores detectar quaisquer mudança no conteúdo da mensagem.

- O comprimento do ICV é sempre fixo, independente do tamanho da entrada

- A chave secreta deve ser compartilhada por um canal seguro

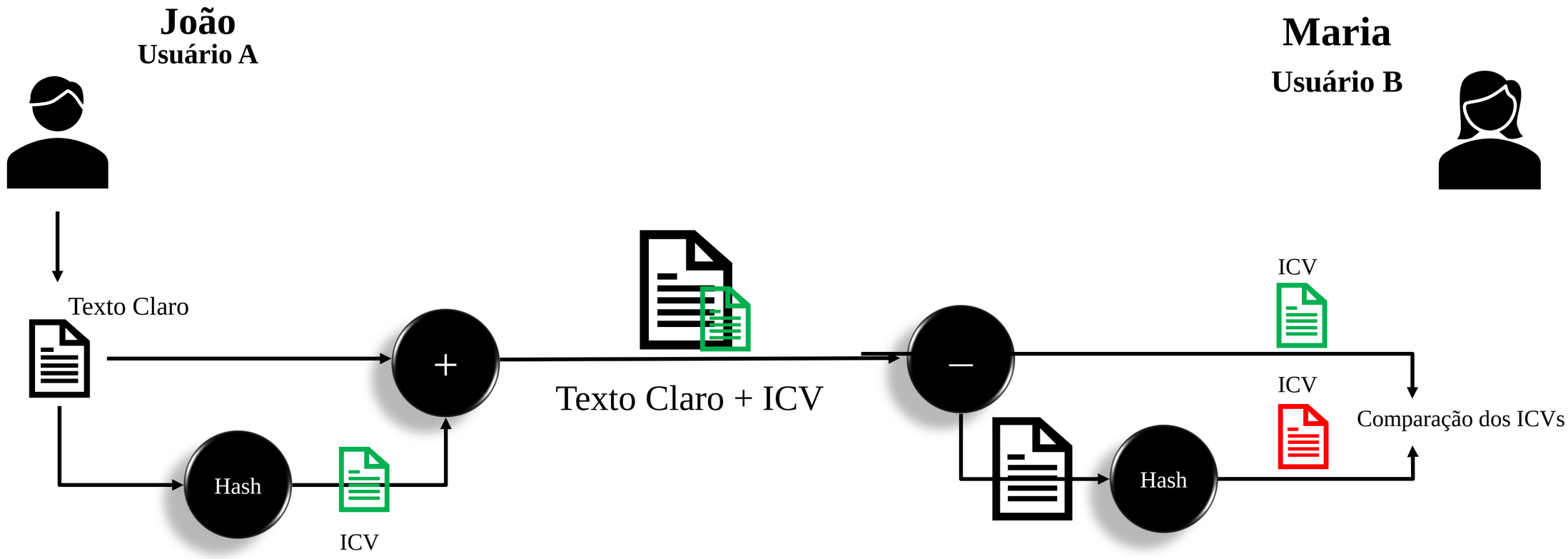
Fundamentos de segurança cibernética
Integridade: Código de Autenticação de Mensagem, MAC

- O MAC é considerado um algoritmo de criptografia, a função de transferência empregada pelo algoritmo não tem a finalidade de gerar um texto cifrado.
- Portanto, o MAC é considerado um algoritmo de criptografia irreversível.
- Exemplo: Um arquivo de tamanho de 1GByte é inserido no MAC, que gera um ICV de 128 bits em sua saída e não um arquivo cifrado.
- Note que é impossível reverter os 128 bits do ICV em um arquivo em texto claro de 1GByte.
- Portanto, o processo de verificação de integridade deve ser feito por comparação

Fundamentos de segurança cibernética

Integridade: Função de Hash

Função de Hash ou apenas Hash é diferente de um algoritimo MAC, um código de Hash não usa uma chave *K*, sendo uma função apenas de mensagem de entrada.



Fundamentos de segurança cibernética
Integridade: Função de Hash

- A função de Hash possui a mesma finalidade que um algoritmo MAC, ou seja, a partir da informação do texto claro gera o ICV.

- Essa função não emprega uma chave secreta no processo de geração do ICV, eliminando a necessidade de um canal seguro para compartilhamento de chave secreta.

- Vulnerabilidade em algoritmos Hash: Colisão de Hash

- Considerações ao se construir uma função Hash:
  - Uma pequena modificação no texto deve resultar em uma grande modificação no ICV
  - A função de Hash deve ter baixíssima probabilidade de colisão de Hash

- Exemplos de funções de Hash: MD4, MD5, SHA-1, WHIRLPOOL

Fundamentos de segurança cibernética

Autenticidade

Definição:

Autenticidade é a propriedade da capacidade de verificação da identidade de uma fonte e sua confiabilidade. Logo, a autenticidade é um mecanismo ou serviço de confirmação de identidade de outro participante em uma troca de mensagens.

Quebra de autenticidade:

Um ataque que envolva o atacante ou agente malicioso de disfarçando e se passando por uma terceira pessoa configura a quebra de autenticidade.

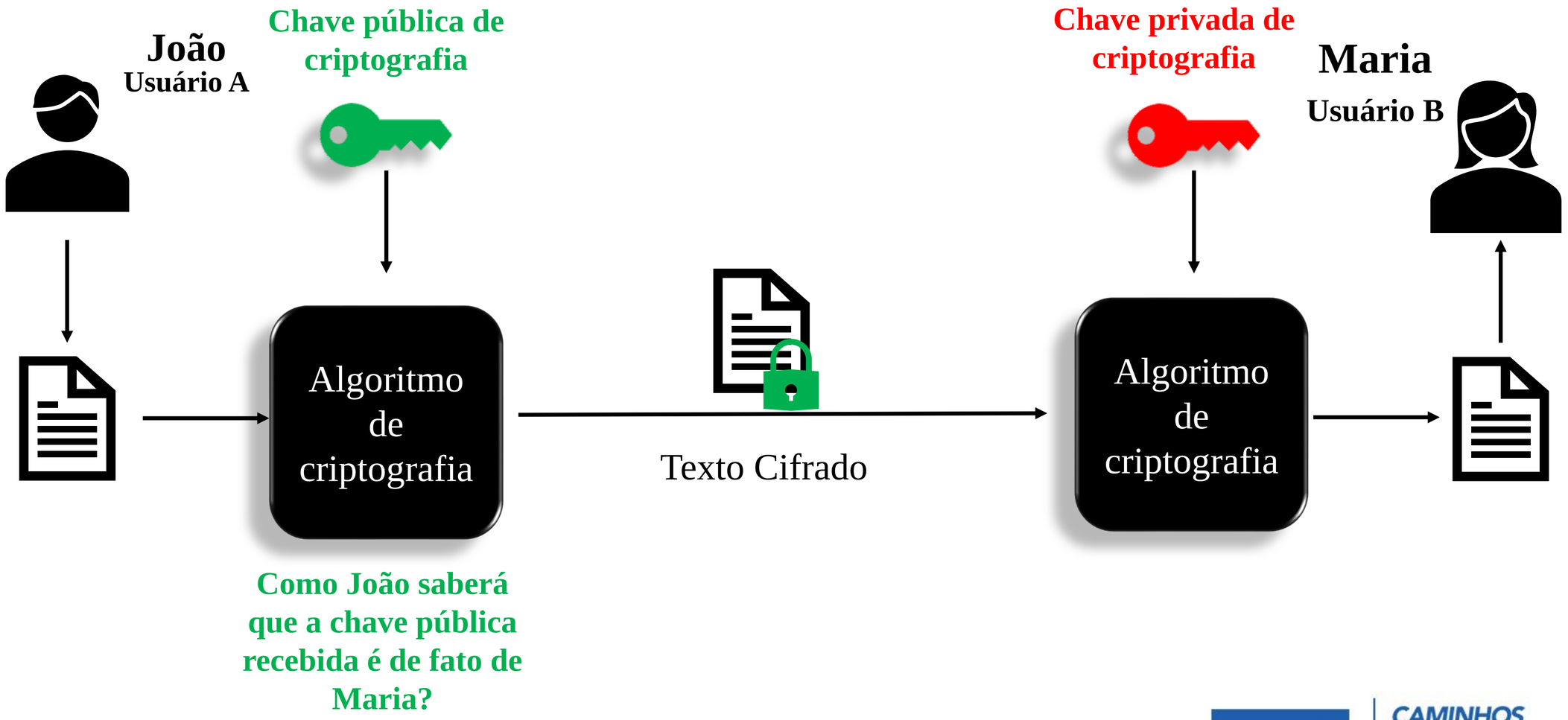
Ex.: Golpes aplicados no Whatsapp

Fundamentos de segurança cibernética
Autenticidade: Mecanismos de autenticação

Alguns mecanismos de autenticação são:

- Biometria
- Login e senha
- Autenticação em duas vias(*tokens*)
- Certificado e Infraestrutura de chave pública
- Assinatura digital

Fundamentos de segurança cibernética
Autenticidade: Certificado digital



Fundamentos de segurança cibernética
Autenticidade: Certificado digital

- A certificação digital é uma assinatura eletrônica com todos os dados do titular, seja pessoa física ou empresa.

- A tecnologia utiliza chaves criptográficas – em arquivo digital ou *token* – para gerar essa identidade exclusiva e segura

- Na prática, o certificado digital funciona como uma identidade virtual que permite a identificação segura do autor de uma mensagem ou transação em meios eletrônicos.

Fundamentos de segurança cibernética
Autenticidade: Infraestrutura de chave pública

Várias técnicas têm sido propostas para a distribuição de chaves públicas. Praticamente todas essas propostas podem ser agrupadas nos seguintes esquemas:

- Anúncio Público
- Diretório disponível publicamente
- Autoridade de chave pública
- Certificado de chave pública

Fundamentos de segurança cibernética
Autenticidade: Infraestrutura de chave pública

Anúncio público de chaves públicas

Envio da chave publica para qualquer outro participante ou transmissão broadcast para a comunidade em geral.

Diretório disponível publicamente

Trata-se de um diretório dinâmico disponível publicamente com chaves públicas. A manutenção e a distribuição do diretório público teria de ser de responsabilidade de alguma entidade ou organização confiável.

Fundamentos de segurança cibernética
Autenticidade: Infraestrutura de chave pública

Autoridades Certificadoras

Trata-se de um órgão confiável. Normalmente uma agência do governo ou uma instituição financeira.

Um usuário pode apresentar sua chave pública à autoridade certificadora e obter o seu certificado

Exemplos de autoridades certificadoras

ICP Brasil

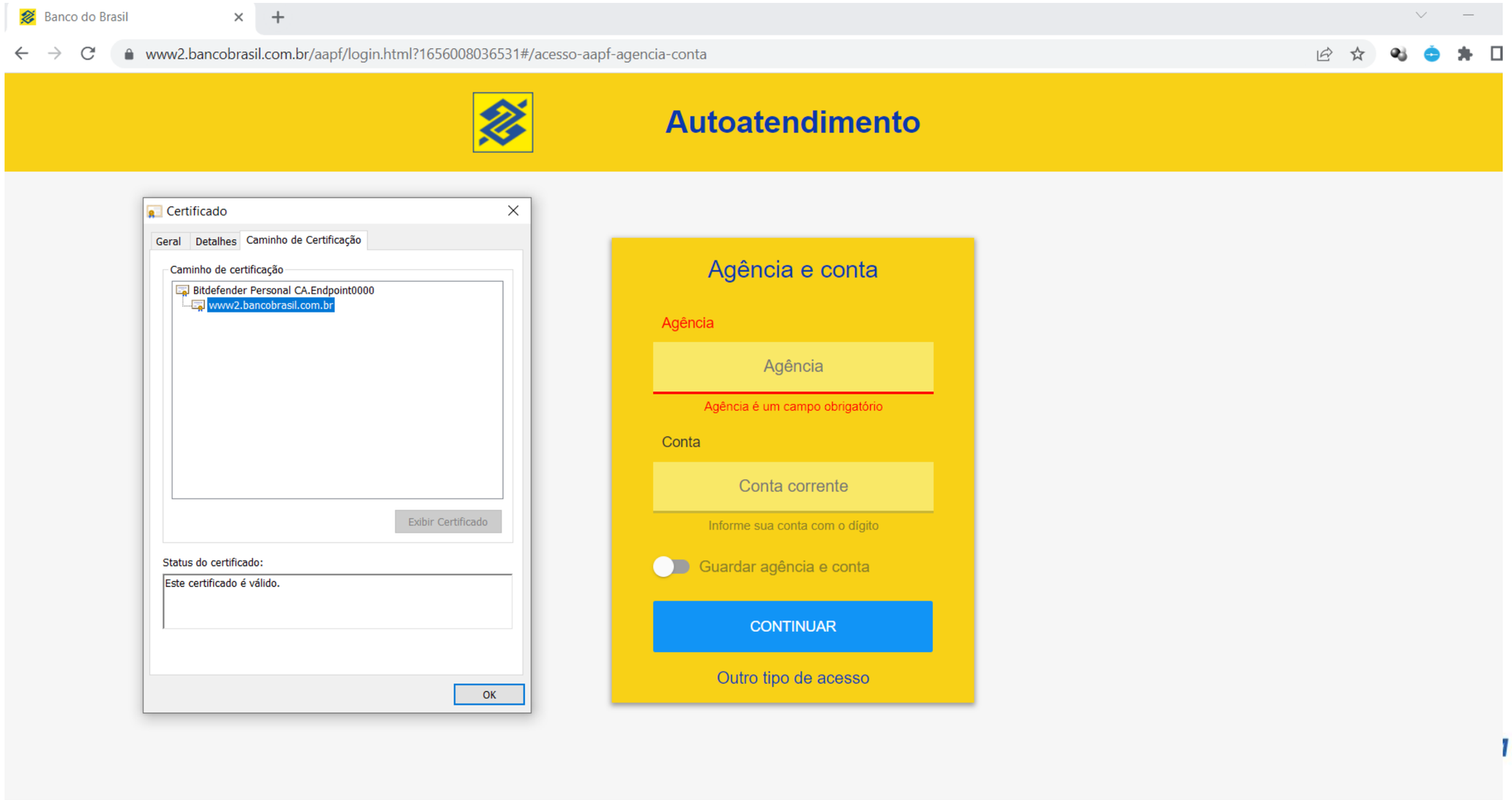
digicert®

CERTISIGN
A sua identidade na rede

Inatel
CAMINHOS QUE CONECTAM COM O FUTURO

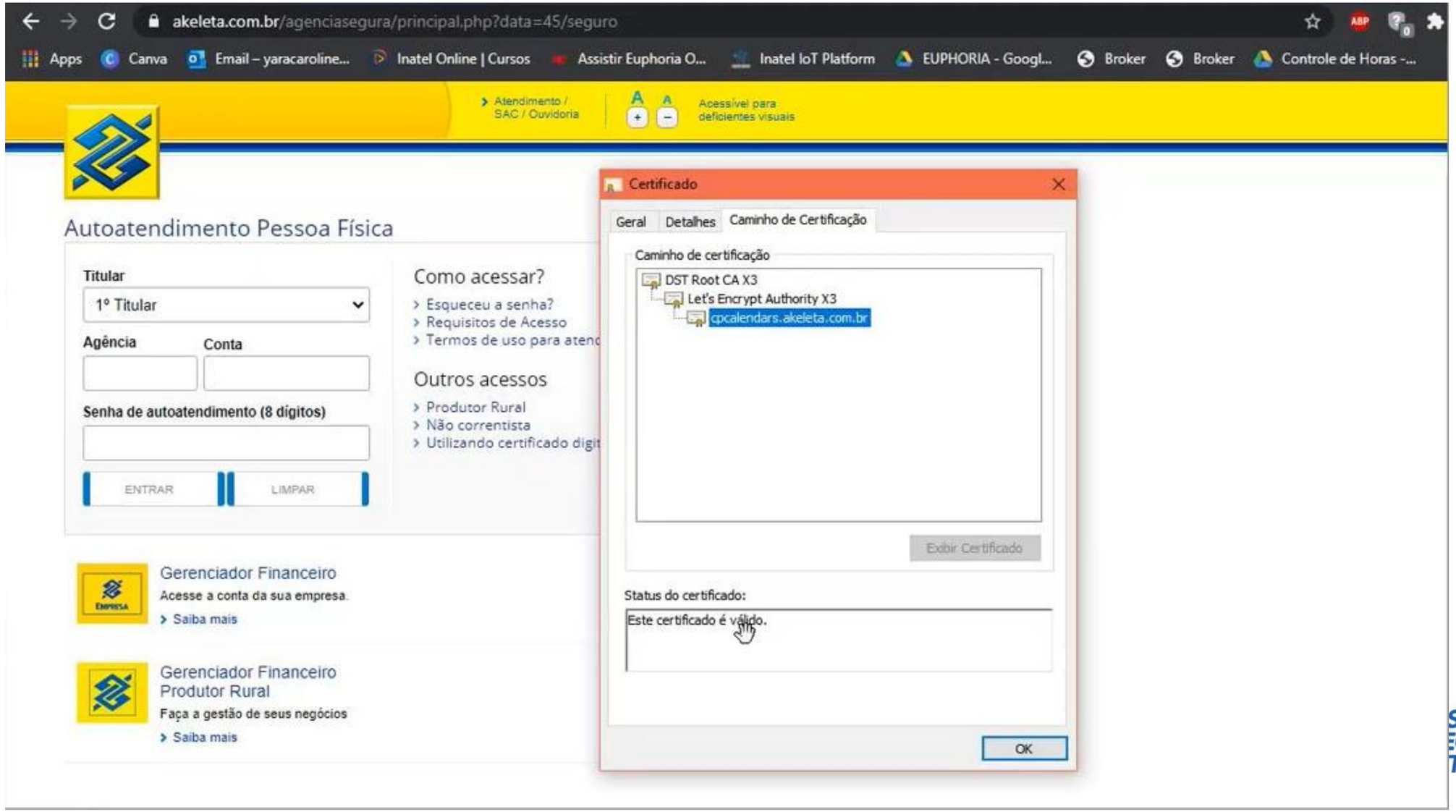
Fundamentos de segurança cibernética

Autenticidade: Verificação de certificado digital



Fundamentos de segurança cibernética

Autenticidade: Verificação de certificado digital



Fundamentos de segurança cibernética
Irretratabilidade

Definição:

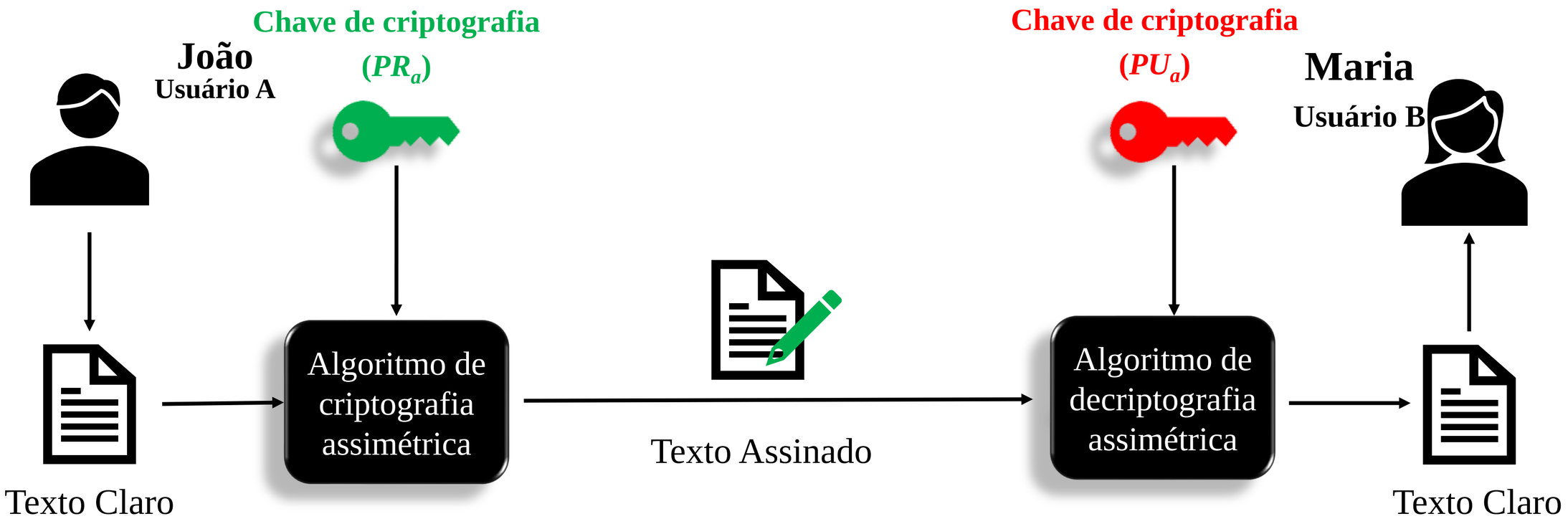
A irretratabilidade (ou não-repúdio) é caracterizada pela impossibilidade de um ator negar uma ação que tenha feito. Em outras palavras, a irretratabilidade permite que ações de um ator sejam imputadas exclusivamente a ele, sem possibilidades de retratação.

Quebra de irretratabilidade:

A falta de registros de atividades que permitam rastrear violações caracteriza a quebra da irretratabilidade.

Fundamentos de segurança cibernética
Irretratabilidade: Assinatura digital

A autenticação de mensagens protege duas pessoas contra uma terceira. Porém, ela não protege as duas partes uma da outra. Abaixo, tem-se o mecanismo de assinatura digital, que deve sempre empregar um algoritmo de criptografia assimétrico.



Fundamentos de segurança cibernética
Modelo Geral da comunicação Segura

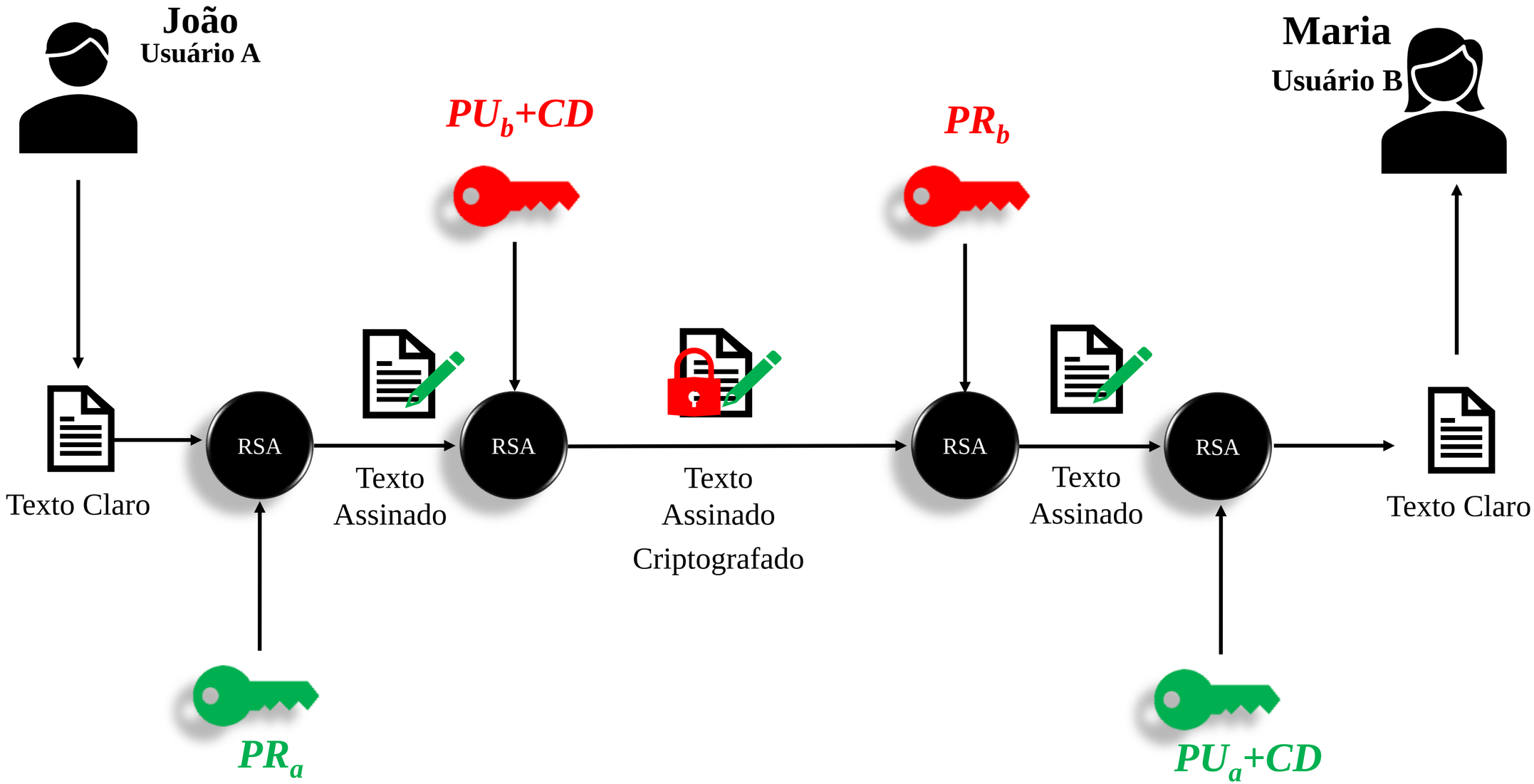
Estudamos os pilares da segurança cibernética de forma independente para entendê-los. Agora, vamos construir um modelo geral que garanta a existência de todos os pilares e a comunicação segura de fato.

Para o estudo, retomamos ao caso da comunicação entre João e Maria. Essa comunicação deve garantir:

- Informação confidencial
- Informação íntegra
- Capacidade de checar/confirmar a autenticidade
- Garantir a irretratabilidade das partes

Fundamentos de segurança cibernética

Modelo Geral da comunicação Segura: Criptografia Dupla



Fundamentos de segurança cibernética

Modelo Geral da comunicação Segura: Criptografia Dupla

O modelo de criptografia dupla garante os pilares da comunicação segura:

Confidencialidade: Processo de criptografia (transmissor) com a chave pública de B e de decriptografia (recepção) com a chave privada de B

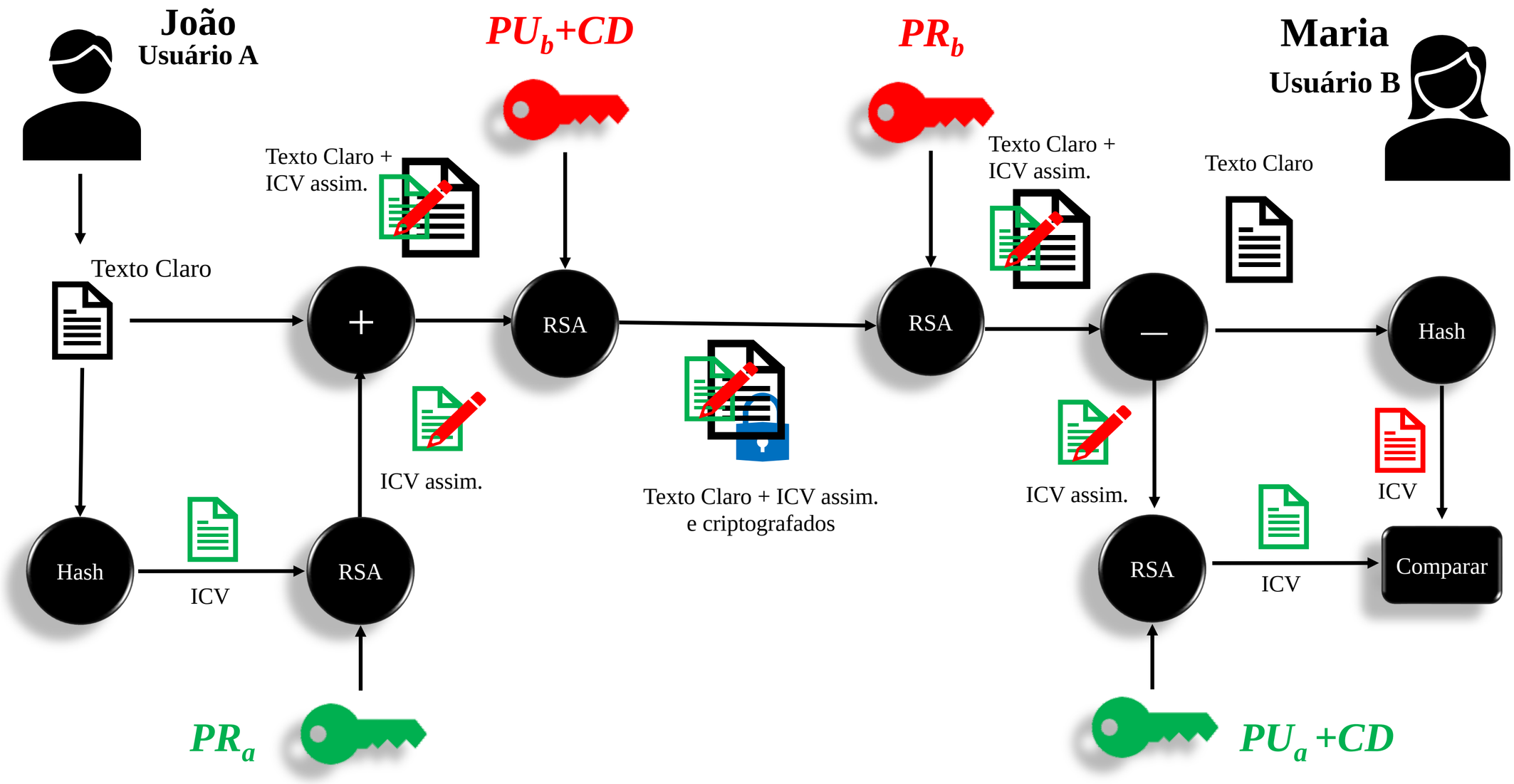
Irretratabilidade: Processo de criptografia (transmissor) com a chave privada de A e de decriptografia (recepção) com a chave pública de A

Integridade: Ocorre de forma indireta. Se algum terceiro malicioso alterar a informação pertencente ao texto claro durante a transmissão, as saídas dos algoritmos serão distintas às entradas.

Autenticidade: é garantida pelo compartilhamento das chaves públicas em conjunto com a certificação digital

Fundamentos de segurança cibernética

Modelo Geral da comunicação Segura



Fundamentos de segurança cibernética
Modelo Geral da comunicação Segura

O modelo anterior garante a comunicação segura por meio da seguinte abordagem:

Confidencialidade: O ICV e o texto claro são criptografados (transmissor) com a chave pública de B e decriptografado (receptor) com a chave privada de B

Irretratabilidade: O ICV é criptografado (transmissor) com a chave privada de A e de decriptografado (recepção) com a chave pública de A

Integridade: A integridade envolve a comparação do ICV transmitido com aquele extraído do texto claro transmitido

Autenticidade: é garantida pelo compartilhamento das chaves públicas em conjunto com a certificação digital

Fundamentos de segurança cibernética
Importância, exemplos de ataque e técnicas de mitigação

- Atualmente, os dispositivos IoT são um dos maiores alvos de ataques para a realização de ataques DoS (*Denial of Service*). Estes dispositivos estão sendo amplamente difundidos pelo mundo, em casas, hospitais, escolas, indústrias, entre outros, e se tornaram um atrativo para os atacantes que dispõem dos recursos operacionais e expertise necessária para indisponibilizar estes dispositivos.

- Primeiramente, define-se **resiliência**, no âmbito da segurança, como a capacidade do dispositivo de suportar diversas mensagens simultâneas, ou, de que caso se torne momentaneamente indisponível, seja capaz de reestabelecer suas operações o mais rápido possível e sem necessidade de intervenção humana.

- A **disponibilidade** é o pilar da segurança cibernética que discorre sobre a necessidade dos dispositivos estarem disponíveis sempre que necessário, para o pessoal autorizado.

Fundamentos de segurança cibernética
Importância, exemplos de ataque e técnicas de mitigação

- Cenários reais de ataque:

IOT

Ataques cibernéticos a dispositivos de IoT crescem cinco vezes em um ano

EDUARDO VASCONCELOS 7 DE JUNHO DE 2023 | 12:48

Relatório indica que número de aparelhos de Internet das Coisas invadidos por botnets passou de 200 mil para aproximadamente 1 milhão; alta foi sentida com mais força após a invasão da Ucrânia pela Rússia

NOTÍCIAS

Mais de 1 milhão de dispositivos IoT foram usados para ataques DDoS

Por: Da Redação da Abranet - 09/06/2023

A Internet das Coisas está sob ataque, adverte o último Relatório de Inteligência de Ameaças da Nokia. O levantamento informa que cerca de 1 milhão de dispositivos IoT foram usados para ataques de negação de serviços (DDoS) nos primeiros três meses deste ano como forma de interromper as redes de telecomunicações. No mesmpo período do ano passado, foram cerca de 200 mil.

Ciberataques a dispositivos IoT têm salto em janeiro e fevereiro

Da Redação

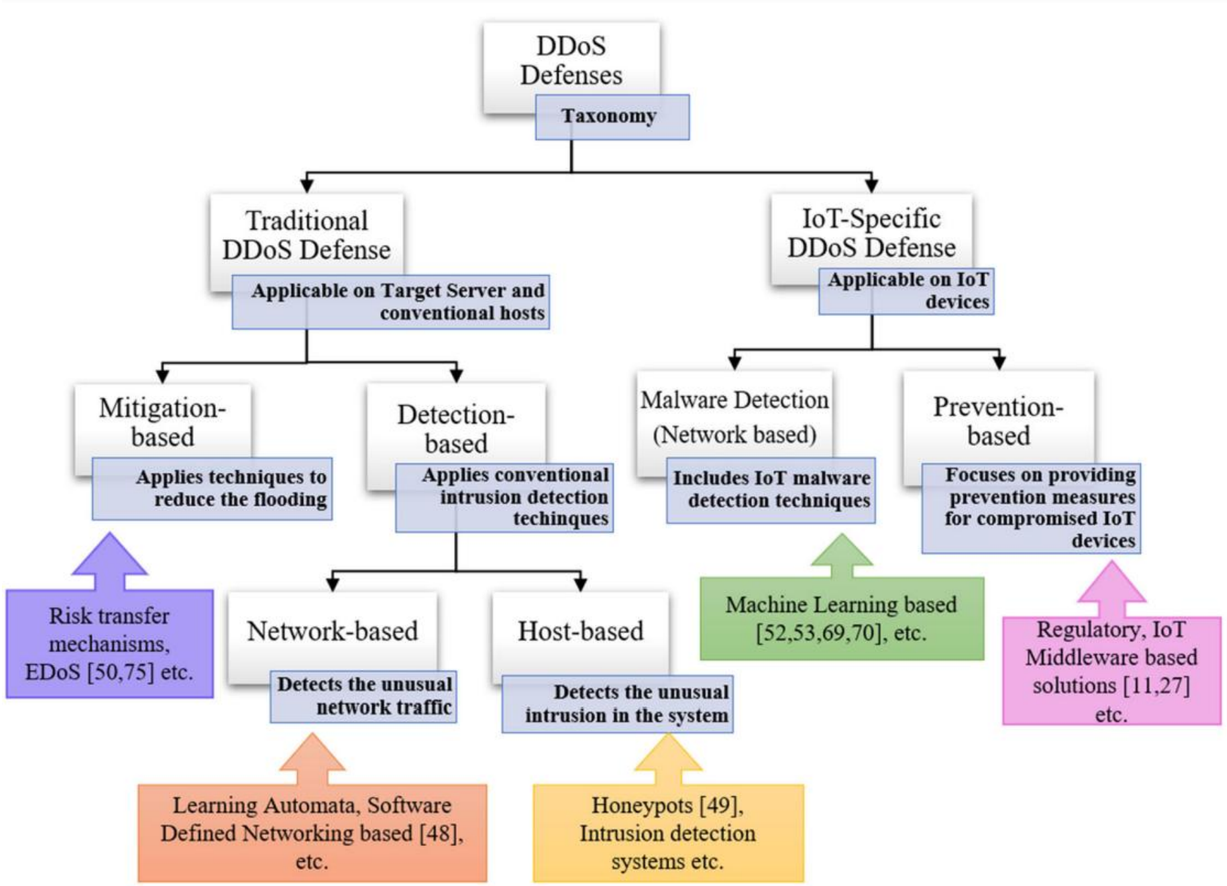
20/04/2023

O número de ciberataques semanais a dispositivos IoT (internet das coisas) teve aumento de 41% somente nos meses de janeiro e fevereiro, de acordo com levantamento da Check Point Research (CPR). Um dos fatores apontados pelo laboratório de inteligência em ameaças da fornecedora de soluções de cibersegurança para esse crescimento é a rápida transformação digital que ocorreu em vários setores, tais como a educação e saúde, durante a pandemia da Covid-19. Essa transformação, impulsionada pela necessidade de continuidade dos negócios, ocorreu frequentemente sem a devida consideração das medidas de segurança, deixando as vulnerabilidades ativas.

Inatel | CAMINHOS QUE CONECTAM COM O FUTURO

Fundamentos de segurança cibernética
Importância, exemplos de ataque e técnicas de mitigação

Técnicas de mitigação:



Inatel | CAMINHOS QUE CONECTAM COM O FUTURO

Fundamentos de segurança cibernética
Importância, exemplos de ataque e técnicas de mitigação

- Técnicas de mitigação:
  - Para garantir a resiliência do dispositivo, pode-se implementar rotinas de detecção de congestionamento de tráfego. Por exemplo: o dispositivo pode ter uma rotina em que ele reinicia quando os níveis de tráfego atingem valores alarmantes, ou o mesmo se desconecta da rede em que está, se isolando.
  - Outras técnicas incluem a implementação de sistemas de filas, de forma que o dispositivo lide com um número previamente estabelecido de solicitações que condizem com sua capacidade operacional, e caso as requisições sobreponham o limite, estas esperam em uma fila ou são descartadas.
  - Além disso, caso possível, a redundância é uma forma de prover disponibilidade, de forma a se ter mais de um equipamento disponível, que se torna ativo caso necessário.

Agenda

1. Fundamentos de segurança cibernética.
2. **Introdução ao Bluetooth Low Energy**
3. Modelos de segurança e vulnerabilidades do Bluetooth Low Energy
4. Modelo de segurança proposto para Bluetooth Low Energy
5. Demonstração prática das vulnerabilidades do Bluetooth Low Energy

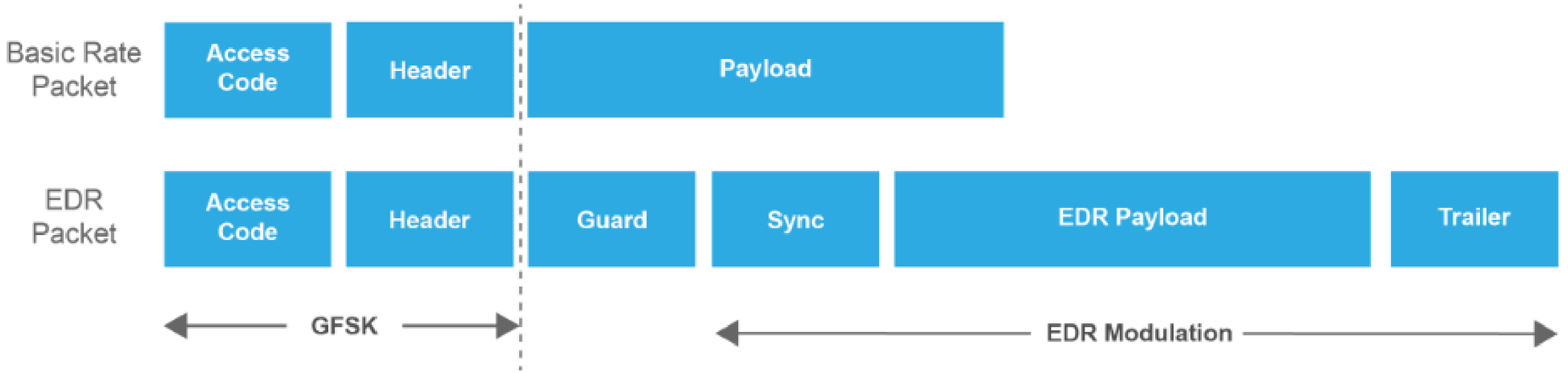
Introdução ao Bluetooth Low Energy

Bluetooth Classic

- O Bluetooth surgiu como um protocolo para transmitir diferentes tipos de dado entre dispositivos.
- O Bluetooth Classic é usado por dispositivos que precisam de conexões com altas taxas de dados, como fones de ouvido ou caixas de som.
- O Bluetooth Classic opera na faixa de 2.4 GHz e requer mais energia que outras versões do Bluetooth para transmitir pacotes de dados maiores.
- Possui 79 canais e opera com *frequency hopping*.
- As especificações Bluetooth 1.0, 1.0b, 1.1 e 1.2 continham vários bugs e limitações que fizeram com que o protocolo se solidificasse apenas na versão 2.0.
- O Bluetooth 2.0 não tinha nenhuma funcionalidade de segurança real, e o 2.1 trouxe o Secure Simple Pairing.

Introdução ao Bluetooth Low Energy
Bluetooth Classic

- Formato do pacote Bluetooth para o Basic Rate e Enhanced Data Rate.



Introdução ao Bluetooth Low Energy
Bluetooth Classic

- Os rádios Bluetooth podem usar 79 canais para transmissão de dados utilizando um algoritmo de salto de frequência pseudoaleatório, com até 1600 saltos por segundo pelo *frequency hopping*. Cada canal é dividido em intervalos de tempo de 625 μs.
- O mestre e o escravo alternam o envio de dados. O mestre envia dados nos intervalos de tempo pares, enquanto o escravo envia dados nos intervalos de tempo ímpares.

- Emparelhamento e vínculo: o processo de emparelhamento consiste da troca de dados para criar uma chave de segurança que será utilizada na criptografia dos dados da comunicação. Vinculação significa armazenar essas informações para uso posterior.

Introdução ao Bluetooth Low Energy
Bluetooth Classic

- Antes que o processo de pareamento seja concluído, há um processo de autenticação por meio de um dos quatro métodos a seguir:
  - **Just Works -** para dispositivos que não têm entrada ou saída de interface do usuário. Utiliza um dígito fixo.
  - **Comparação numérica** – comparação de dois números e verificação da correspondência.
  - **Entrada de senha -** inserção do número exibido em um dispositivo na interface de teclado do outro dispositivo.
  - **Fora de Banda (OOB) -** a chave de segurança é fornecida por um protocolo que não seja o Bluetooth. NFC é uma abordagem popular.

Introdução ao Bluetooth Low Energy

Bluetooth Low Energy

- O Bluetooth Low Energy é uma extensão do protocolo Bluetooth criada com o propósito de fornecer uma solução de baixo consumo de energia para aplicações de controle e monitoramento e também para aplicações de IoT.
- Especificado com foco na eficiência e no baixo consumo de energia dos dispositivos, sendo os mecanismos de segurança introduzidos de forma opcional.
  - **Consumo de bateria**: operação em níveis de energia mais baixos, permitindo que as baterias dos dispositivos possuam uma vida útil mais longa. Oferece a capacidade de operar em modo de espera (*idlestate/sleepmode*) ate que seja necessário conduzir uma transferência de dados. No Bluetooth Classic, o dispositivo está sempre ligado ou desligado.
  - **Transferência de dados**: O BLE opera com uma taxa de 1Mbps, enquanto o BT trabalha com taxas maiores de transmissão. Esse item foi despriorizado no BLE devido aos objetivos dessa tecnologia.

Agenda

1. Fundamentos de segurança cibernética
2. Introdução ao Bluetooth Low Energy
3. **Modelos de segurança e vulnerabilidades do Bluetooth Low Energy**
4. Modelo de segurança proposto para Bluetooth Low Energy
5. Demonstração prática das vulnerabilidades do Bluetooth Low Energy

Modelos de segurança e vulnerabilidades do BLE

Funcionalidades de segurança do Bluetooth Low Energy

- O BLE possui dois modos de segurança, com seus respectivos níveis:

1. **Modo de segurança 1 (associado com criptografia):**
    - Nível 1: não utiliza autenticação nem criptografia.
    - Nível 2: utiliza criptografia com pareamento não autenticado.
    - Nível 3: utiliza criptografia com pareamento autenticado.
    - Nível 4: utiliza pareamento do Secure Connections com criptografia.
2. **Modo de segurança 2 (associado com integridade dos dados)**
    - Nível 1: utiliza pareamento não autenticado com integridade dos dados.
    - Nível 2: utiliza pareamento autenticado com integridade dos dados.

Modelos de segurança e vulnerabilidades do BLE

Funcionalidades de segurança do Bluetooth Low Energy

- O emparelhamento envolve a primeira fase para o estabelecimento de uma conexão usando o BLE. O processo é dividido em três fases:

  1. Os dispositivos trocam mensagens de requisição e resposta de emparelhamento, comunicando suas capacidades.
  2. Troca de parâmetros que resulta na derivação de uma chave de criptografia para a conexão.
  3. Distribuição de chaves específicas de transporte.

Modelos de segurança e vulnerabilidades do BLE

Funcionalidades de segurança do Bluetooth Low Energy

- Os métodos de emparelhamento da segunda etapa são definidos de acordo com a versão de especificação do protocolo Bluetooth em *legacy pairing* e *secure connections*.
  - ***Legacy pairing*:** os dispositivos trocam uma chave temporária (TK) através de métodos de emparelhamento definidos como Just Works, Passkey Entry ou Out Of Band. Em seguida, empregam a chave TK para derivar uma chave de curto prazo, que é utilizada para criptografia da conexão.
  - **LE *secure connections:*** considera o uso do protocolo ECDH (*Elliptic-curve Diffie–Hellman*) para derivar chaves públicas e privadas, que são trocadas para implementar o acordo de Diffie–Hellman. Posteriormente, utiliza-se um método de emparelhamento para autenticação da conexão e gera-se a chave de longo prazo (LTK, long-term key) para criptografar a conexão.

Modelos de segurança e vulnerabilidades do BLE

Funcionalidades de segurança do Bluetooth Low Energy

- Métodos do *legacy pairing*:
  - ***Just Works*:** configura a chave TK com valor nulo ou fixo, comprometendo a confidencialidade da comunicação e sendo suscetível a ataques de força bruta, espionagem e MITM (*Man-in-the-Middle)*.
  - ***Passkey Entry*:** um dos dispositivos gera e exibe uma TK numérica de seis dígitos que deve ser inserida no segundo dispositivo. Embora ofereça um nível básico de segurança, a quebra desse código por meio de força bruta é relativamente fácil, permitindo que um atacante use a TK para derivar a STK correspondente ao enlace Bluetooth.
  - ***Out of Band*:** permite o emparelhamento por meio de um canal externo, utilizando uma tecnologia sem fio diferente do Bluetooth (ex.: NFC, *Near Field Communication*). No entanto, ambos os dispositivos devem ter capacidades de hardware compatíveis para usar este método.

Modelos de segurança e vulnerabilidades do BLE

Funcionalidades de segurança do Bluetooth Low Energy

- Métodos do *secure connections*:
    - Os métodos de emparelhamento citados anteriormente são adotados pelo LE *secure connections*, incluindo uma quarta variação denominada *Numerical Comparison*.

- Nesse tipo de conexão, há também a possibilidade de utilizar a comparação numérica para o pareamento. Nesse caso, um número de seis dígitos é exibido em ambos os dispositivos, e o usuário deve confirmar se os dois números são idênticos.

Modelos de segurança e vulnerabilidades do BLE

Funcionalidades de segurança do Bluetooth Low Energy

***Legacy pairing*:**

- Em conexões legadas, a maioria dos dispositivos utiliza o método ***PassKey Entry***, já que o *Just Works* não oferece mecanismos de segurança adequados e o *Out of Band* requer um canal alternativo.

LE *secure connections:*

- Em conexões seguras, o ***PassKey Entry*** também prevalece, visto que o *Numerical Comparison* demanda a intervenção humana na etapa final. Além disso, a implementação do ECDH implica em um custo de processamento mais elevado para uma aplicação BLE.

Modelos de segurança e vulnerabilidades do BLE

Funcionalidades de segurança do Bluetooth Low Energy

- No que diz respeito à privacidade, o BLE emprega endereços privados temporários que impedem a identificação de um dispositivo por meio de seu endereço MAC.

- Logo, dispositivos confiáveis têm a capacidade de resolver esses endereços por meio de uma chave de resolução de identidade. Isso permite que o dispositivo central resolva os endereços privados dos dispositivos periféricos, evitando identificá-los.

- Em suma, o protocolo Bluetooth Low Energy se concentra na **confidencialidade** dos dados e na **privacidade** dos dispositivos, sendo que as soluções apresentadas possuem vulnerabilidades referentes aos pilares de segurança e oportunidades para outras soluções.

Modelos de segurança e vulnerabilidades do BLE

Vulnerabilidades de segurança do Bluetooth Low Energy

- O Bluetooth Low Energy, mesmo implementando alguns métodos para emparelhamento seguro, está vulnerável a ataques de:
  - Espionagem passiva/ativa.
  - Ataque de personificação.
  - Ataque de *replay*.
  - Força Bruta nos métodos de pareamento.
  - Ataques de negação de serviço.

Modelos de segurança e vulnerabilidades do BLE

Modelos de segurança do Bluetooth Low Energy

- Propostas de implementações de segurança na literatura I:

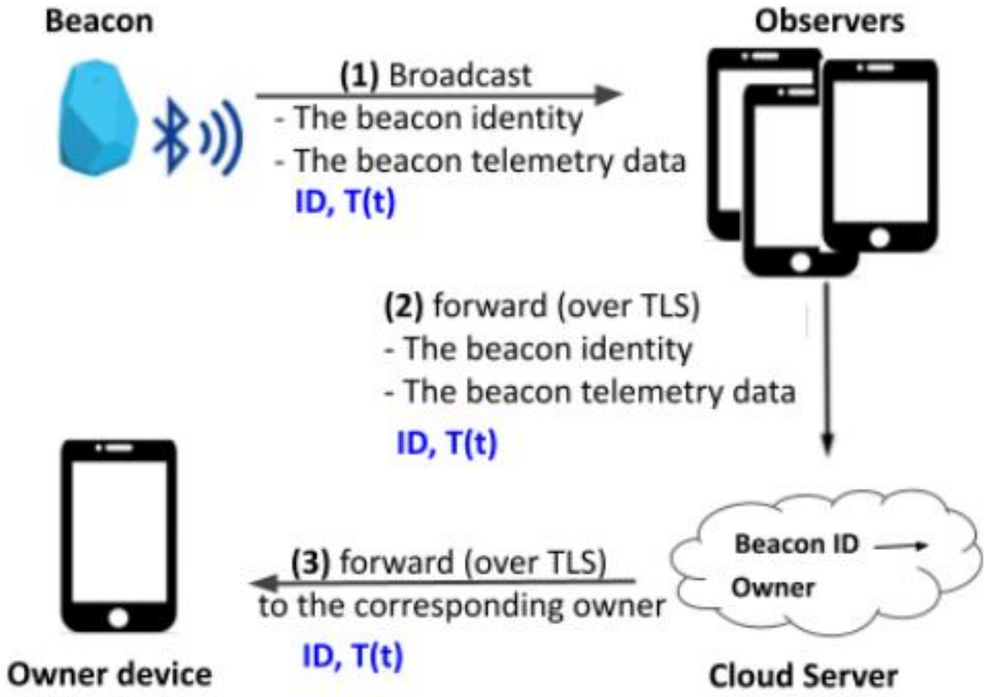


Fig. 1. The original Eddystone protocol.

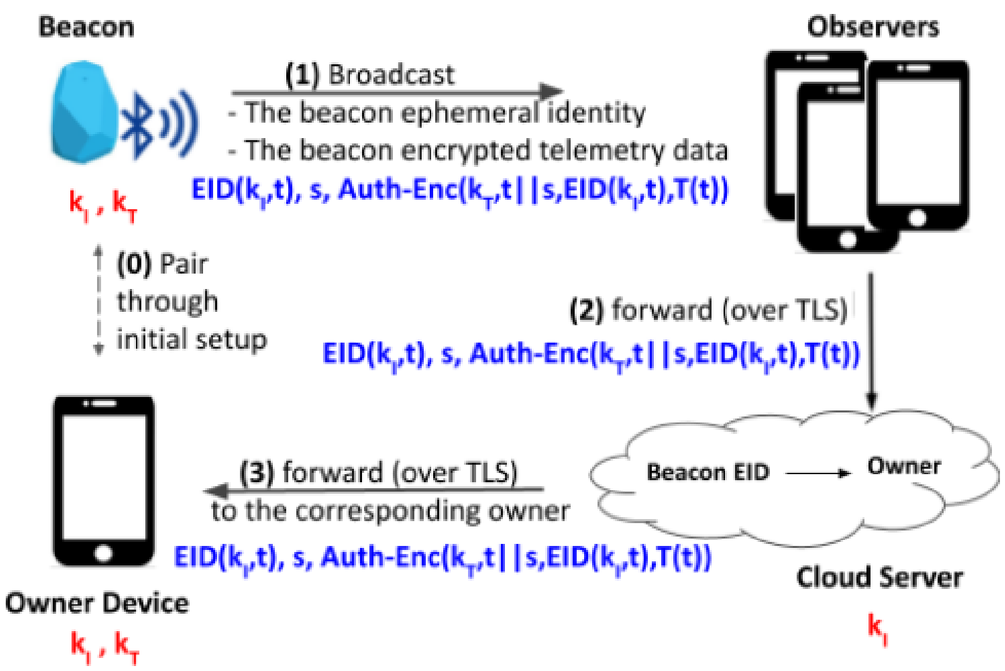


Fig. 3. The private and secure Eddystone-EID protocol.

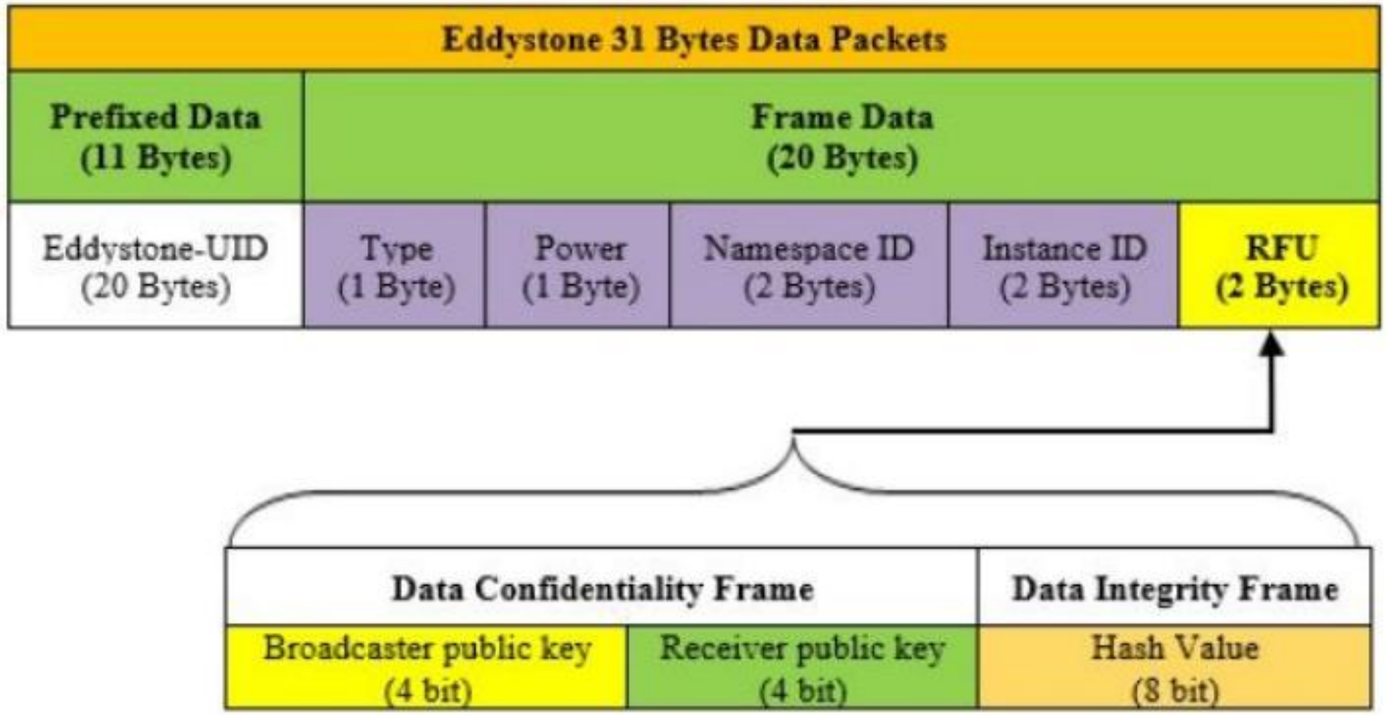
L. David, A. Hassidim, Y. Matias, M. Yung, and A. Ziv, “Eddystoneeid: Secure and private infrastructural protocol for ble beacons,” IEEE Transactions on Information Forensics and Security, vol. 17, pp. 3877– 3889, 2022.

Modelos de segurança e vulnerabilidades do BLE

Modelos de segurança do Bluetooth Low Energy

- Propostas de implementações de segurança na literatura II:

Extended Eddystone-UID Frame (Proposed)

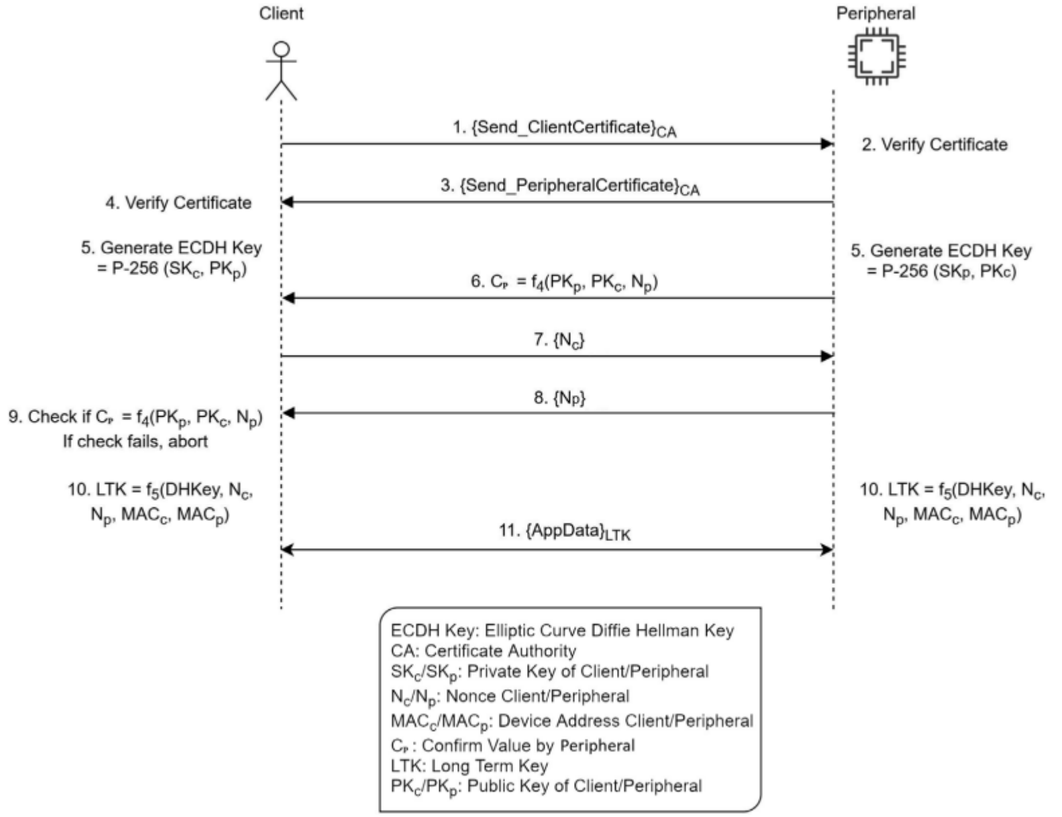


V. S. Gulhane and S. D. Padiya, “Eddystone-uid frame with data confidentiality and integrity for secured data broadcasting by ble beacons,” Research Square, Sep. 2022, pREPRINT (Version 1). [Online]. Available: https://doi.org/10.21203/rs.3.rs-2095668/v1

Modelos de segurança e vulnerabilidades do BLE

Modelos de segurança do Bluetooth Low Energy

- Propostas de implementações de segurança na literatura III:

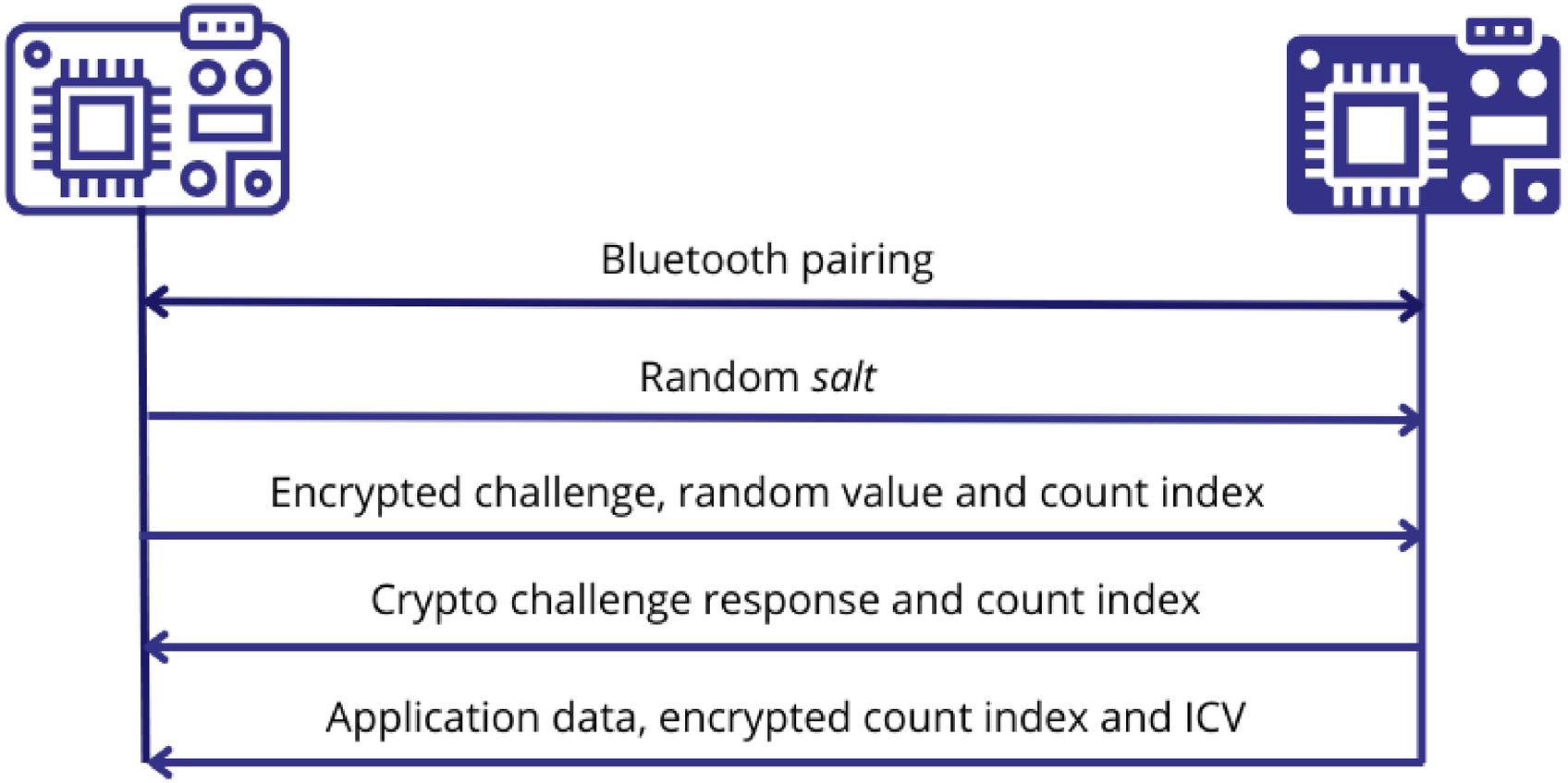


C. Gupta and G. Varshney, “An improved authentication scheme for ble devices with no i/o capabilities,” Computer Communications, vol. 200, pp. 42–53, 2023. [Online]. Available: https://www.sciencedirect. com/science/article/pii/S0140366423000014

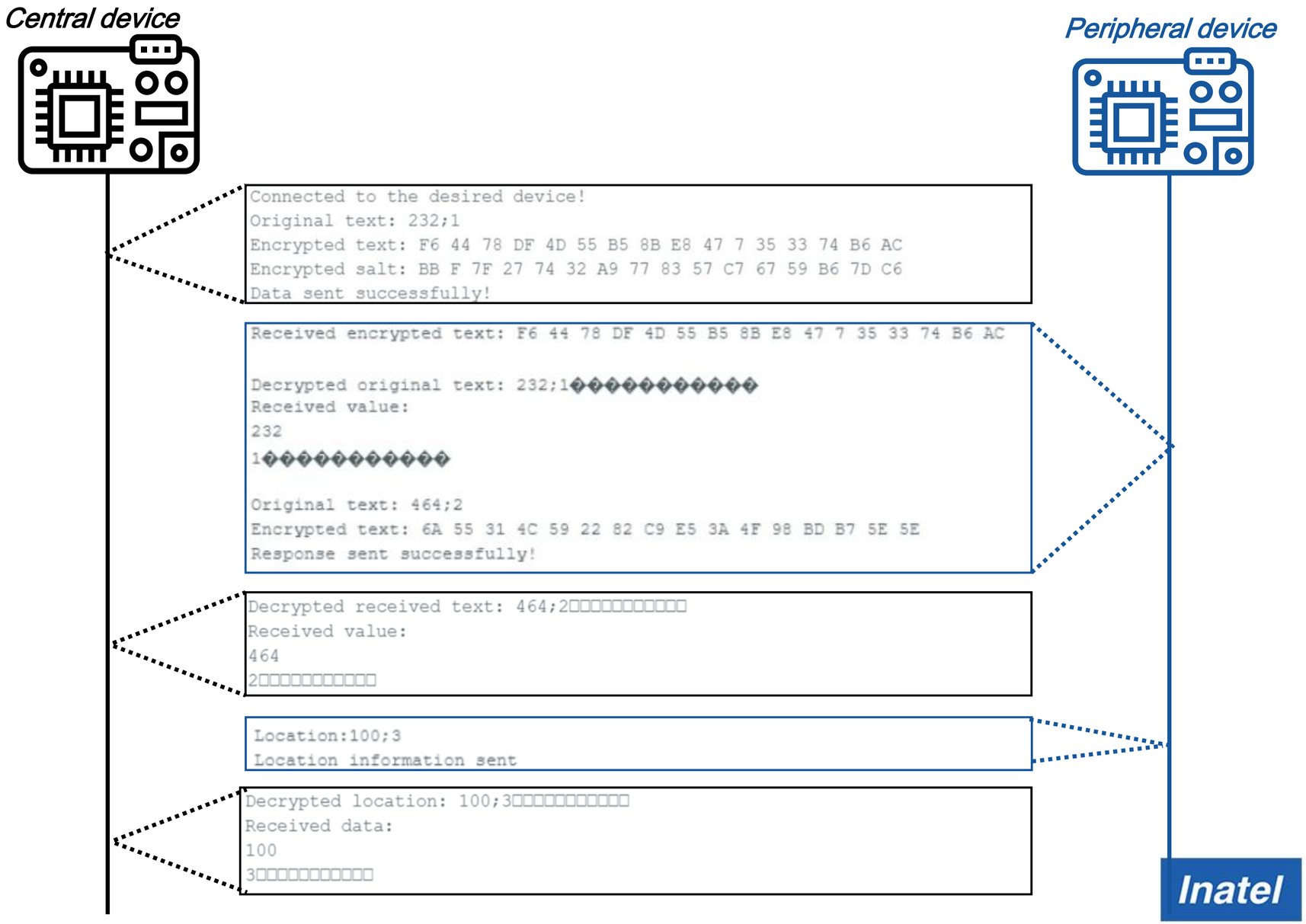
Agenda

1. Fundamentos de segurança cibernética.
2. Introdução ao Bluetooth Low Energy.
3. Modelos de segurança e vulnerabilidades do Bluetooth Low Energy.
4. **Modelo de segurança proposto para Bluetooth Low Energy**
5. Demonstração prática das vulnerabilidades do Bluetooth Low Energy.

Modelo de segurança proposto para BLE



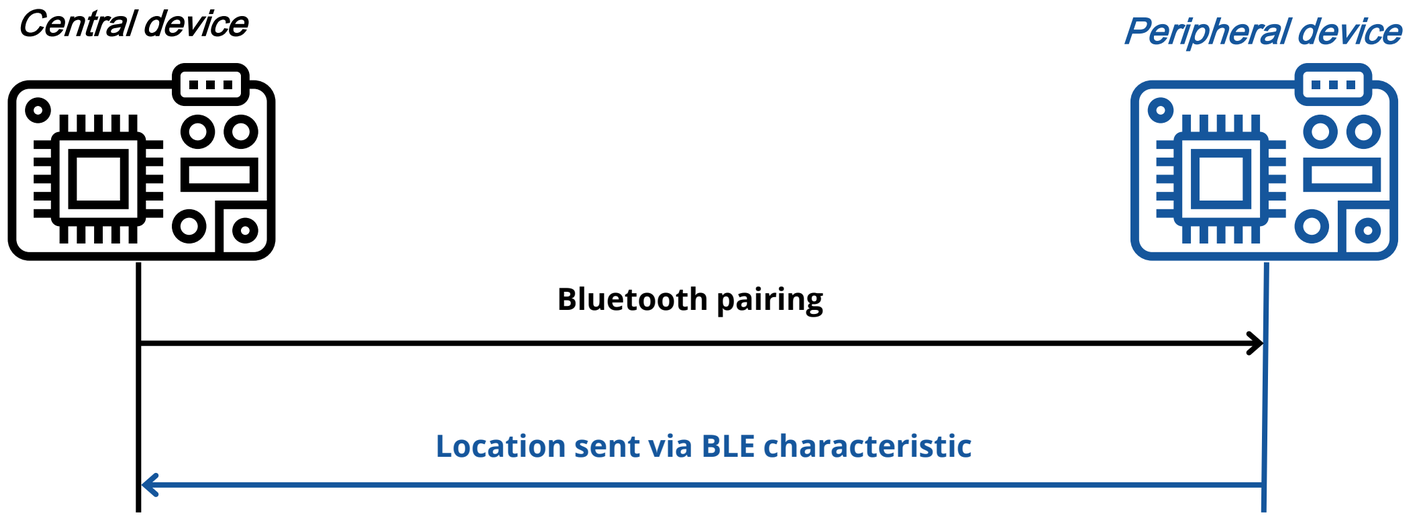
Esquema da comunicação



Inatel

CAMINHOS QUE CONECTAM COM O FUTURO

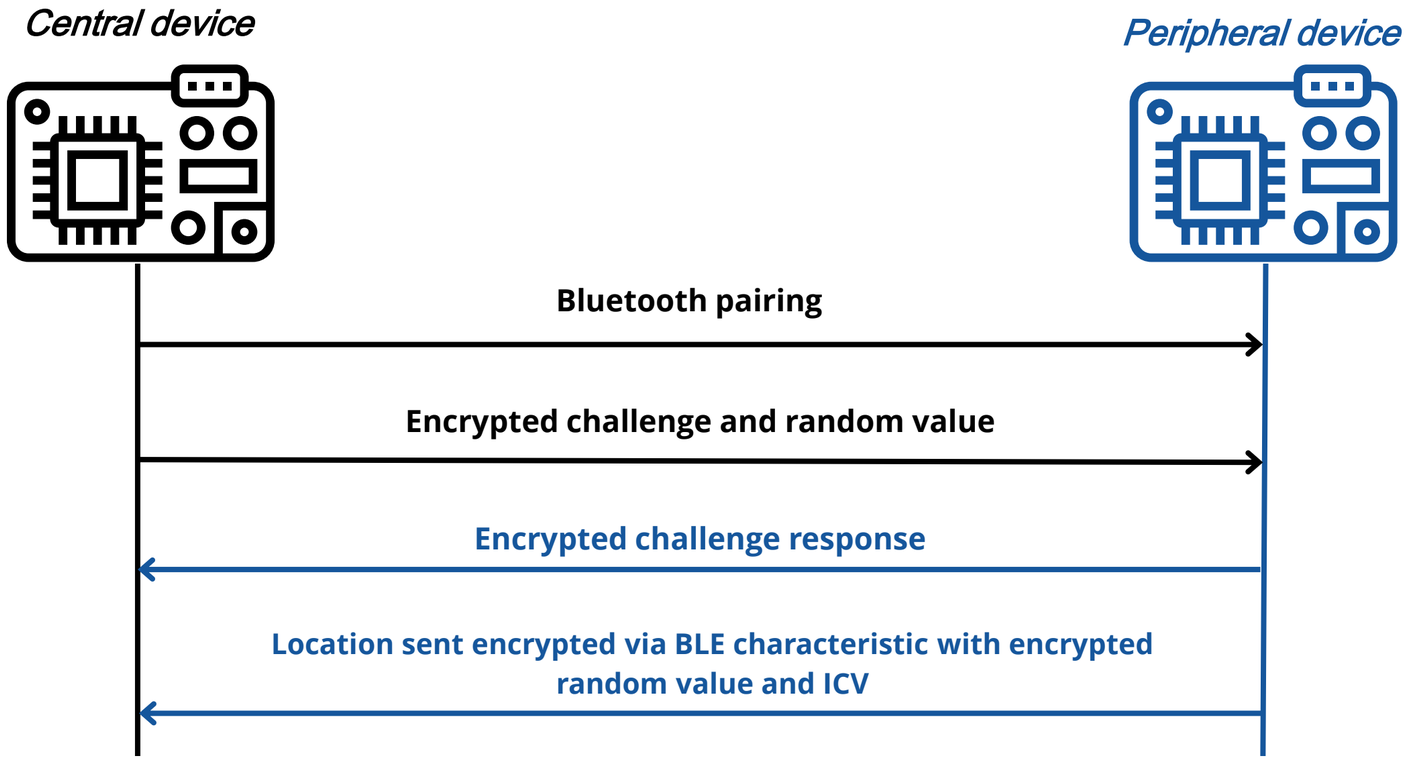
Implementação padrão



Executions	1º	2º	3º	4º	5º
Time (µs)	1352479	1327327	1392893	1260067	1432319

Executions	1º	2º	3º	4º	5º
Time (µs)	691043	676044	684043	668043	683041

Implementação proposta



Executions	1º	2º	3º	4º	5º
Time (µs)	1496181	1797547	1705289	1596344	1507277

Executions	1º	2º	3º	4º	5º
Time (µs)	1391560	1616677	1571800	1430325	1358007

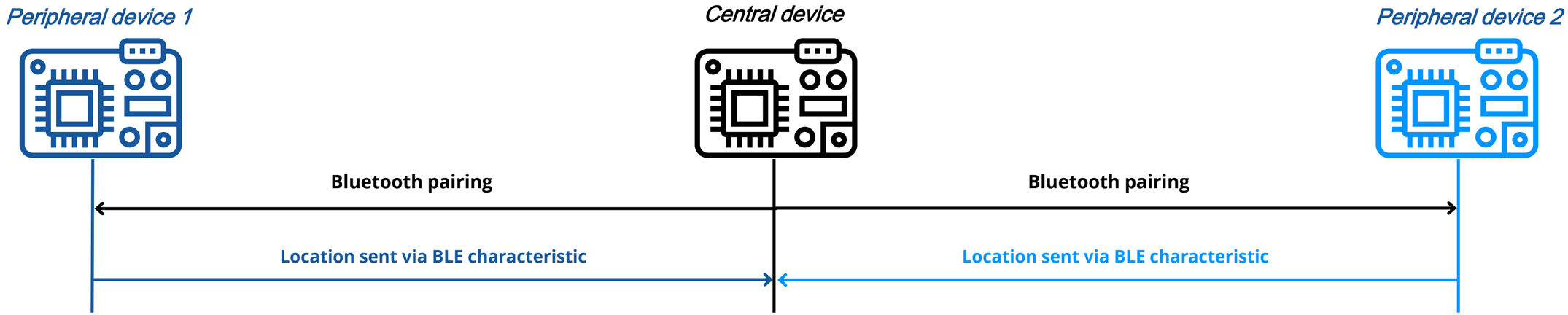
Inatel

CAMINHOS QUE CONECTAM COM O FUTURO

Comparativo

Implementations	Average Execution Time (µs)	
	Central	Peripheral
Standard Implementation	1353017	680442,8
Proposed security Implementation	1620527,6	1473673,8
Final Difference (µs)	267510,6	793231

Implementação padrão para rede BLE



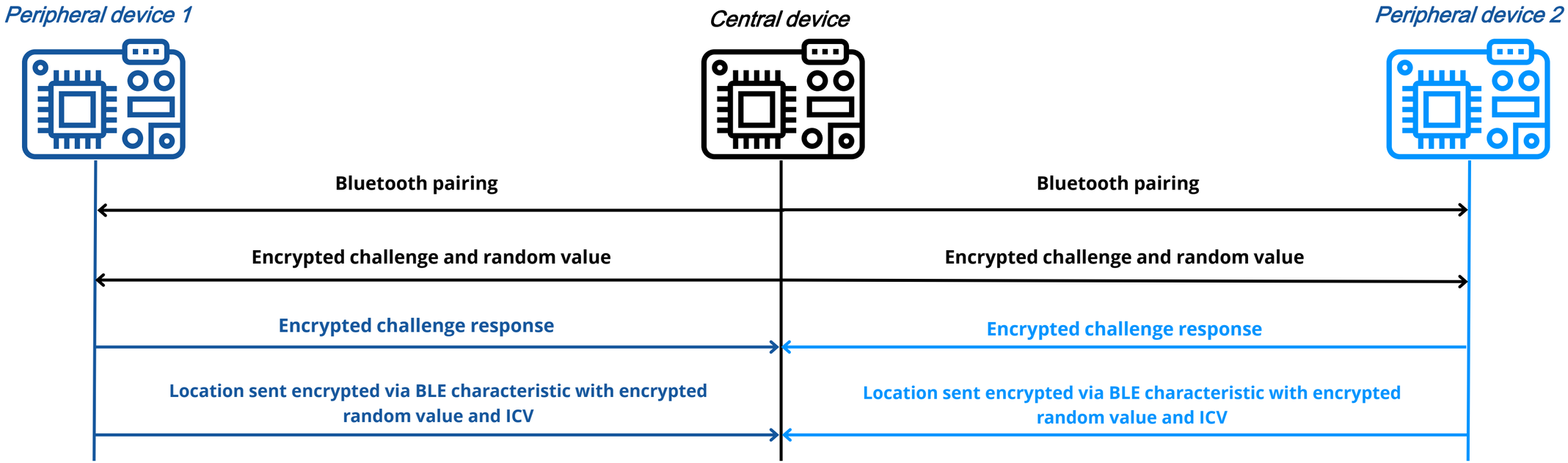
Executions	1º	2º	3º	4º	5º
Time (µs)	1395340	1520874	1381887	1374065	1387921

Executions	1º	2º	3º	4º	5º
Time (µs)	672044	672043	672045	676045	678046

Executions	1º	2º	3º	4º	5º
Time (µs)	677049	700044	701057	692051	668045

Inatel | CAMINHOS QUE CONECTAM COM O FUTURO

Implementação proposta para rede BLE



Executions	1º	2º	3º	4º	5º
Time (µs)	1320806	1378980	1380038	1506763	1364155

Executions	1º	2º	3º	4º	5º
Time (µs)	1585035	1576250	1727875	1697458	1570019

Executions	1º	2º	3º	4º	5º
Time (µs)	1657505	1682542	1753376	1901334	1714249

Inatel
CAMINHOS QUE CONECTAM COM O FUTURO

Comparativo

Implementations	Average Execution Time (µs)	
	Central	Peripheral
Proposed security Implementation (P2P)	1620527,6	1473673,8
Proposed security Implementation (BLE Network)	1741801,2	1510737,9
Final Difference (µs)	121273,6	37064,1

Implementations	Average Execution Time (µs)	
	Central	Peripheral
Standard Implementation (BLE Network)	136169,38	680846,9
Proposed security Implementation (BLE Network)	302147,58	1510737,9
Final Difference (µs)	165978,2	829891

Agenda

1. Fundamentos de segurança cibernética
2. Introdução ao Bluetooth Low Energy
3. Modelos de segurança e vulnerabilidades do Bluetooth Low Energy.
4. Modelo de segurança proposto para Bluetooth Low Energy
5. **Demonstração prática das vulnerabilidades do Bluetooth Low Energy**

Nome: Guilherme Pedro Aquino

E-mail: guilhermeaquino@inatel.br

Nome: Evandro César Vilas Boas

E-mail: evandro.cesar@inatel.br

Nome: Isabela Ferreira de Vito

E-mail: i.ferreira@inatel.br

CxSC Telecom
Centro de Segurança Cibernética

Inatel