Radio-Frequency Identification (RFID)

Luis F. de Deus*
Centro de tecnologia, Universidade Federal de Santa Maria.
(Dated: 2 de dezembro de 2019)

RFID is a technology that enables the communication of identification data using electromagnetic waves. This data is stored in a tag. However the security of this data is not consolidated, and may suffer from the most varied types of attacks, this report seeks to elucidate these concepts, as well as to test the vulnerabilities of these systems in a practical way, followed by an implementation of an additional layer of security using the DES algorithm.

Keywords: RFID, Tag, Security.

I. INTRODUÇÃO

RFID (*Radio-Frequency IDentication)*, é uma tecnologia que permite a comunicação de dados de identificação usando ondas eletromagnéticas. Estes dados, são armazenados em uma etiqueta, ou tag.

A origem do conceito da tecnologia RFID é de meados da Segunda Guerra Mundial, nos sistemas de radares utilizados por várias nações (Alemanha, Japão, Inglaterra e EUA). Estes radares notificavam a aproximação de aviões, mesmo eles ainda estando distantes, facilitando a preparação das defesas contra ataques inimigos. Proposto pelo físico escocês Sir Robert Alexander Watson-Watt, em conjunto com o exército britânico, foram implantados transmissores em aviões ingleses que davam respostas diferentes ao radar, diferenciando os aviões ingleses dos inimigos no radar. Deste modo, foi concebido o primeiro sistema de identificação por rádio frequência.

O *hardware* do RFID é composto pelos seguintes comonentes:

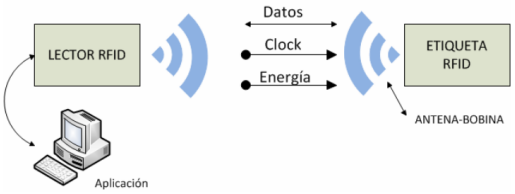
- Antena;
- Transceptor;
- Leitor;
- Transponder.

O transceptor faz a leitura do sinal e transfere a informação para um dispositivo leitor, o transponder ou etiqueta de RF (rádio frequência) por sua vez, contem a informação a ser transmitida. Estas etiquetas podem estar presentes em uma gama de objetos como pessoas, animais, produtos, embalagens, entre outros.

A antena transmite a informação, emitindo o sinal do circuito integrado para transmitir suas informações para o leitor, que por sua vez converte as ondas de rádio do RFID para informações digitais. Depois de convertidas, elas poderão ser lidas e compreendidas por um computador para então ter seus dados analisados, a Fig.1 descrita na implementação de [1] aborda este conceito.

As *tags* podem ser divididas em dois grupos, as Ativas e as Passivas.

Figura 1. Exemplo de comunicação RFID.



Fonte: [1]

A. Tag Passiva

As etiquetas RFID passivas são as mais comuns devido à sua simplicidade. Elas não possuem bateria e alimentam seus circuitos através das ondas eletromagnéticas emitidas pela antena do leitor. Sendo assim, não podem iniciar nenhuma comunicação por conta própria e funcionam a curta distância, características essas que as tornam mais baratas e com maior vida útil.

B. Tag Ativa

A etiqueta ativa possui uma fonte de energia própria tanto para alimentar seu circuito quanto para fornecer a troca de informações. Esse tipo de funcionamento permite a realização de tarefas mais complexas, tem maior capacidade de armazenamento de dados (até 32 KB em memória RAM). Devido a essa maior complexidade, possui tamanho e custo mais elevados.

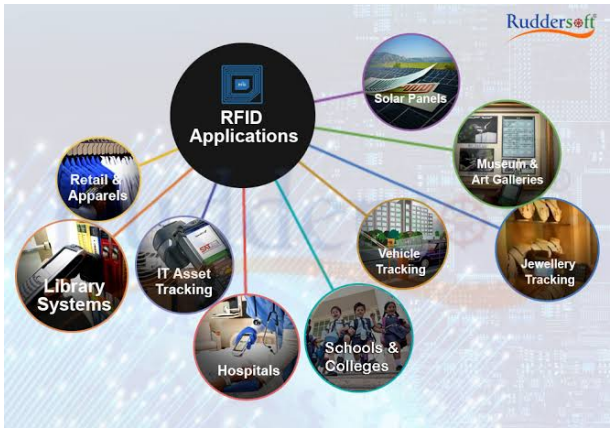
Com o emprego do RFID em empresas e produtos, o seu custo tem diminuindo, e tem se tornado mais popular. Sistemas como pedágios automatizados, identificação de pacientes, rastreamento de animais e registro de produtos, são utilizações recentes desta tecnologia.

A principal motivação para a utilização do RFID, vem da necessidade de obter informações de coisas em movimento, situados em locais de difícil acesso, ou em qualquer tipo de processo que impeça a utilização de código de identificação. O RFID tem uma ampla aplicabilidade em inúmeros setores industriais, de distribuição, identificação e controle de acesso, agregando eficácia e eficiência a estes processos, um exemplo de case de sucesso é a empresa Ruddersoft, expecializada em desenvol-

* felipe.deus@ecomp.ufsm.br

ver aplicações usando esta tecnologia, como demonstra a Fig.2.

Figura 2. Aplicações da tecnologia RFID.



Fonte: [2]

II. VANTAGENS X DESVANTAGENS

Como todo sistema possui suas vatangens e desvantagens, no caso do RFID, não é diferente, mesmo que sua aplicabilidade siga aumentando ano após ano, sempre existem desvatagens e riscos que o usuário deve estar ciente.

A. Vantagens

- **Confiabilidade**: Sistemas com RFID são capazes de manter seu funcionamento em ambientes hostis e com climas extremos;
- **Facilidade de leitura**: As etiquetas não dependem do campo visual para serem lidas.
- **Capacidade de armazenamento**: Uma etiqueta é capaz de armazenar dados coletados referentes ao objeto ou ao processo a que está relacionada.
- **Otimização dos processos**: Ocorre em decorrência da redução de erros humanos e da alta velocidade de processamento.

B. Desvantagens

- **Interferência por metais**: Os campos magnéticos gerados por materiais metálicos podem causar uma interferência no sistema e causar problemas em seu desempenho.
- **Custo**: Custo total maior considerando a infraestrutura necessária para que a solução funcione: antenas, leitoras, software para tratamento da informação capturada, desenvolvimento de aplicativos, sistema de comunicação, etc;
- **Distância de leitura**: Em geral as tags de menor custo não tem um alcance muito longo, para assegurar grande distância de leitura é preciso mais investimento.
- **Segurança**: Dependendo da aplicação necessita-se um esquema de segurança para garantir a confiabilidade e integridade dos dados que estão suscetíveis a diversas formas de ataques.

III. AMEAÇAS E REQUISITOS DE SEGURANÇA

Como qualquer tecnologia que envolve troca de dados entre usuário e sistema, a implantação deve passar por diversas análises e testes de segurança. Deve se garantir os requisitos básicos de segurança para o sistema, como autenticidade, confidencialidade, integridade às informações, devem ser fortemente levados em consideração, independente do tipo de modelo de negócio envolvido. Como todos os sistemas, o RFID é suscetível a diversos tipos de ataques de segurança, onde pode-se citar alguns como:

- ***Sniffing*** - O objetivo das tags é que sejam lidas por qualquer dispositivo compatível e da melhor forma possível. Entretanto, a leitura se faz independe da vontade do portador. Qualquer dispositivo a uma certa distância por recolher informações da tag;
- ***Tracking*** - Esta técnica é similar ao *sniffing*, porém é feita de maneira contínua. Uma sequência de leitores poderia, por exemplo, revelar o trajeto realizado por um portador de uma tag RFID, violando direitos de privacidade;
- ***Spoofing*** - O atacante poderia simular uma identidade, ganhando as mesmas permissões do identificador original, possibilitando o acesso a áreas ou itens que teoricamente não deveriam ser acessados por outro usuário gerando uma informação falsa para o leitor;
- ***Replay Attacks*** - Caracteriza-se na interceptação e manipulação dos sinais trocados entre leitor e receptor, o clássico MITM (*Man In The Middle)*;
- ***Denial of Services*** - Negação de serviço, ou DOS. Pode ser feito de diversas maneiras. Por exemplo, criando uma "gaiola de Faraday" ao redor de uma tag, impendindo que possa ser lido por um leitor;
- ***Buffer Overflow*** - Quando um programa é copiado para a memória, ele é dividido em segmentos específicos para dados, variáveis e controle do executável. Nesta técnica sobrecarregasse a área referente a dados, invadindo a área de controle.

- ***Code Insertion*** - Tags escritas em linguagem de *script* podem permitir ataques em sistemas finais se as aplicações do RFID utilizam protocolos web para se conectar ao banco de dados. O script pode ter um conteúdo malicioso e se aproveitar de falhas de segurança do servidor.
- ***SQL Injection*** - Parecido com o Code insertion, porém específica para a SQL. Caso não haja métodos de tratamento de entrada de dados, uma simples consulta pode expor totalmente o banco de dados.

IV. IMPLEMENTAÇÃO DE SEGURANÇA

Como visto no capítulo anterior, existem uma gama de possíveis ataques que violam os conceitos de segurança, e dependendo da aplicação, uma falha de segurança pode ser catastrófica, logo, faz-se necessário implementações que visam bloquear ou dificultar as ações dos atacantes.

A. Criptografia

A primeira abordagem que deve vir atona, seria o uso de criptografia, o que provavelmente resolve muitos problemas, entretanto as etiquetas em geral possuem um bloco muito pequeno de bits. No âmbito dos sistemas embarados, responsáveis por ler e manipular os dados, até a decada passada, não tinham capacidade coputacional suficiente para criptografar e descriptografar dados, no entando essa premissa já não é mais verdade, visto que a evolução dos sitemas embarcados, como microcontroladores, já permite esta demanda.

B. Chaves de acesso

Uma das abordagens mais usadas atualmente é o uso de chaves de acesso, normalmente existem duas ou três chaves que permitem manipular os dados da tag, onde que cada chave possui diferentes permissões de manipulação de dados, e também em quais blocos de dados estas permissões são válidas, um exemplo deste tipo de implementação será aborado na seção sobre o Chip da empresa Mifare.

C. Redução de dados

Outra proposta de proteção, não tão ortodoxa é a redução de dados sigilosos nas etiquetas, já que por exemplo, em um cartão de transporte o saldo do usuário, se encontra no próprio cartão, e não no *middleware* (Sistema Embarcado), a usabilidade da tag seria apenas de autorizador para que o dado possa ser modificado, evitando que o usuário carregue a informação consigo.

D. Blindagem

Outro meio é a proteção com blindagem eletromagnética, existe uma camada metálica que envolve a etiqueta quando ela não estiver em uso, o que causa interferências em caso de algum atacante esteja tentando um ataque de *Sniffing/Tracking*.

E. Modulação

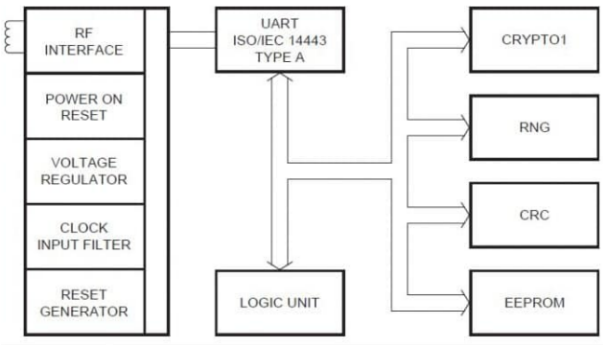
Outra medida adotada é a modulação pseudoaleatória, que é uma técnica que visa criar um canal modulado de comunicação entre leitor e receptor, pois se somente os dois conhecerem o esquema de modulação para a transmissão correspondente, o invasor terá uma dificuldade expressiva em demodula-los, entretanto na era de informação dos dias atuais, esquemas de modulação já não são secretos.

V. RFID: MIFARE CHIPS

A linha de chips da empresa Mifare é uma das mais uitlizadas no mercado, ela utiliza a faixa de comunicação na frequência de 13.56 MHz.

Internamente o chip é divido em blocos, cada um com sua função específica, como demonstra a Fig.3

Figura 3. Diagrama de Blocos chip Mifare



Fonte: [3]

- **Bloco de RF**: Composto por sistemas de modulação e demodulação do sinal, regulador de tensão, Power On Reset (POR) e gerador de clock.
- **Anticolisão**: Atendendo a ISO-14443, esse sistema permite fazer a seleção de um único cartão, mesmo que vários estejam dentro do campo do leitor.
- **Unidade Lógica**: Responsável por controlar os processos lógicos dentro do chip, como solicitar autenticação, leitura e escrita na memória, controlar acesso aos dados, gerenciar os comandos, etc.

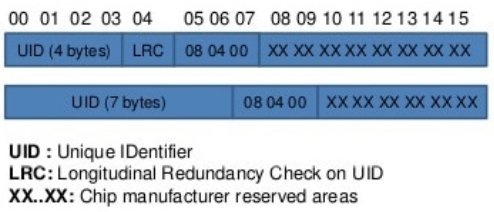
- **Unidade de criptografia**: Responsável pela autenticação da comunicação através do sistema CRYPTO1, desenvolvido pela NXP para utilização nos chips Mifare.
- **EEPROM**: Memória interna do chip onde os dados são gravados e lidos.

A. Estrutura de Memória

O chips contemplam uma memória EEPROM interna, as capacidades mais comuns são de 1KB, 2KB e 4KB. Internamente as memórias são divididas em setores, os setores divididos em blocos, e cada bloco tem 16 bytes.

O primeiro bloco do primeiro setor é chamado *manufacturer block* Fig.4, reservado para armazenar algumas informações do fabricante. Cada chip tem um número de série próprio, podendo ser de 4 ou 7 bytes.

Figura 4. Bloco de identificação do fabricante



Fonte: [3]

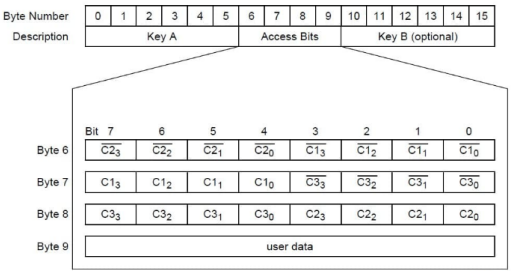
Os 3 primeiros blocos de cada setor (0 a 2) são para armazenamento de dados, podendo ser configurados como *value blocks* ou *read/write blocks*. Os *read/write blocks*, como o nome sugere, são blocos para leitura e escrita de dados. Já os *value blocks* foram pensados para serem utilizados em sistemas que envolvem contagem de crédito, pois também oferecem as funções de incremento e decremento de valores, além de restauração e transferência.

O último bloco de cada setor é chamado *sector trailer*, e é crucial para a segurança do chip. Esse bloco armazena as chaves de acesso aos demais blocos daquele setor e também as condições de acesso de cada bloco daquele setor.

Para acessar os blocos dos setores é necessário fazer a autenticação. O setor trailer armazena duas chaves, KEY A e KEY B, onde a chave B é opcional. Uma dessas chaves deve ser usada para fazer a autenticação, após isso, os dados dos blocos daquele setor podem ser acessados de acordo com o que está gravado no campo *Access Condition*.

O campo *Access Condition* é composto 4 bytes, armazenando as condições de acesso e o modo de funcionamento de cada bloco do seu setor. De acordo com a configuração deste campo, sabe-se qual chave se usa para autenticação, qual o modo de funcionamento dos blocos de dados, e se os dados poderão ser acessados. A Fig.5 mostra o bloco *sector trailer*.

Figura 5. Estrutura do *Sector trailer*: chip Mifare



Fonte: [3]

A estrutura do *access condition* utiliza 3 bits para definir o funcionamento de cada bloco do seu setor (C1, C2 e C3). As funções possíveis para cada *data block* são configuradas no *access condition*, assim ele será um *value block* ou *read/write block* como demonstra a Fig.6.

Figura 6. Configuração do chip Mifare

Access bits			Access condition for				Application
C1	C2	C3	read	write	increment	decrement, transfer, restore	
0	0	0	key A|B	key A|B	key A|B	key A|B	transport configuration[1]
0	1	0	key A|B	never	never	never	read/write block[1]
1	0	0	key A|B	key B	never	never	read/write block[1]
1	1	0	key A|B	key B	key B	key A|B	value block[1]
0	0	1	key A|B	never	never	key A|B	value block[1]
0	1	1	key B	key B	never	never	read/write block[1]
1	0	1	key B	never	never	never	read/write block[1]
1	1	1	never	never	never	never	read/write block

Fonte: [3]

B. Estrutura de Comunicação

A comunicação entre o leitor e os dispositivos Mifare é realizada do seguinte modo: De início o leitor gera o campo que alimenta os chips (POR), e envia um *request*. Todos os chips que estiverem no alcance do campo do leitor irão tentar responder, o sistema de anticolisão impede que mais de um dispositivo responda simultaneamente. Os dispositivos respondem com seu número identificador.

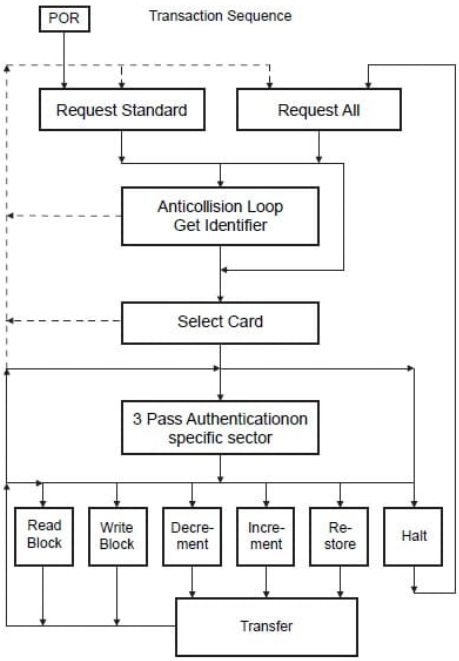
O leitor seleciona o chip com quem quer trocar informações. Nesse momento os demais dispositivos entram em modo *stand by* aguardando por um novo *request*. Com o módulo selecionado o leitor especifica o local que quer acessar na memória e usa a chave configurada para fazer a autenticação do bloco de memória.

Depois da autenticação, todas as informações trocadas são encriptadas pela CRYPTO1, uma criptografia criada pela NXP para os dispositivos Mifare. Nos dias atuais a criptografia já foi quebrada, e não é recomendável a utilização apenas deste meio de segurança para as informações trocadas.

Após a autenticação, o leitor deve enviar o comando referente à ação desejada, este poder ser leitura, escrita,

incremento, decremento, restaurar e parar. A Fig.7 mostra o fluxograma que corresponde ao processo de comunicação.

Figura 7. Fluxograma de execução: Chip Mifare



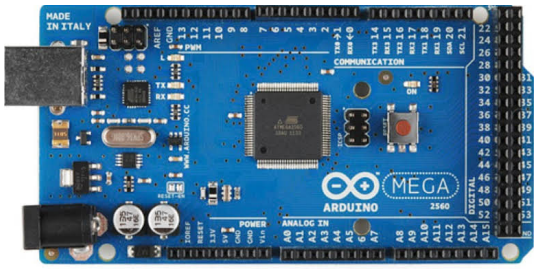
Fonte: [3]

VI. IMPLEMENTAÇÃO PRÁTICA

Com o objetivo de explorar de forma prática as vulnerabilidades dos sistemas RFID, adquirir conhecimentos relevantes, bem como por em prática conceitos desenvolvidos sobre segurança de rede, foi efetuado uma implementação prática usando plataforma Arduino, e o kit leitor de RFID MFRC da empresa Mifare que conta com duas tags Fig.9.

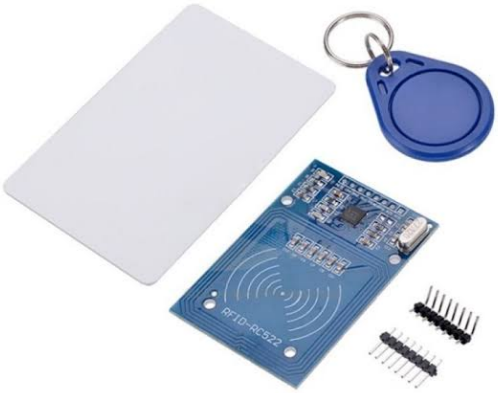
Foi escolhido a plataforma Arduino, mais precisamente o Arduino Mega Fig.8, devido a facilidade e rapidez com que se consegue uma implementação de protótipo, bem como a gama de implementações disponíveis na internet.

Figura 8. Arduino Mega



Fonte: [4]

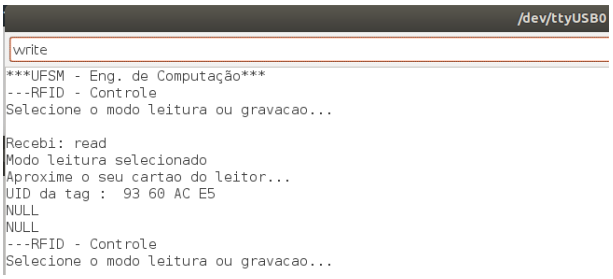
Figura 9. Kit RFID MFRC



Fonte: [5]

Primeiramente explorando o módulo foi efetuada a leitura das informações dentro da tag, como é possível ver na Fig.10 se tem acesso ao UID e a informação que neste caso é NULL.

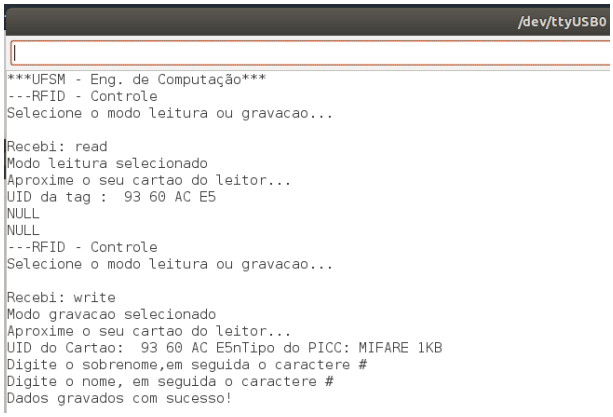
Figura 10. Leitura de Informações



Fonte: Autor

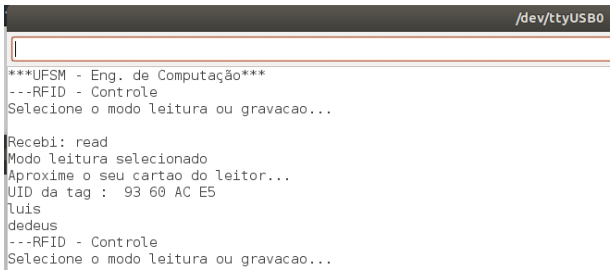
Da mesma forma, pode-se gravar dados em um determinado bloco da memória da tag, como mostra a Fig.11 foi gravado o nome e o sobrenome na tag, efetuando novamente a leitura a informação estará la como mostra a Fig.12.

Figura 11. Gravando informações



Fonte: Autor

Figura 12. Novo processo de aquisição de informações

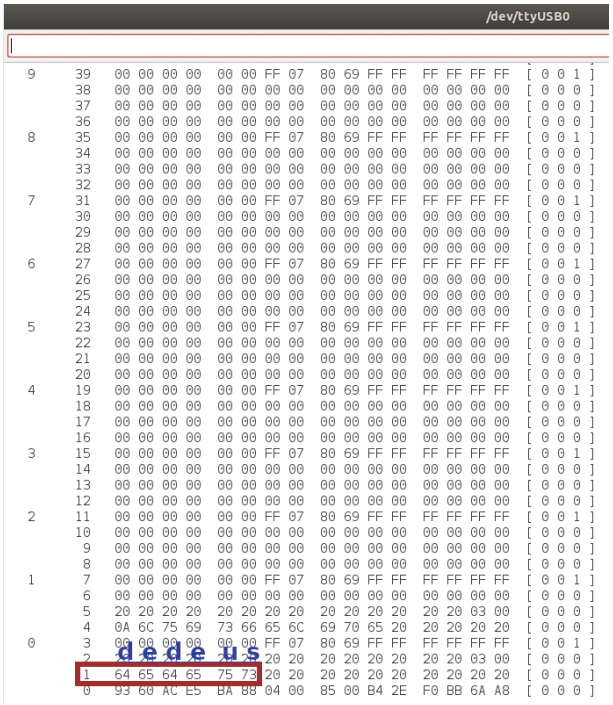


Fonte: Autor

No caso deste Kit, segue o padrão que foi exemplificado no capítulo anterior, tendo o controle de acesso aos blocos de informação por meio de chaves de acesso, nas implementações sempre é necessário enviar a chave de controle de acesso para a tag enviar a informação, o que ajuda no quesito de segurança, como também foi descrito a função criptográfica CRYPTO1 que é usada nestes módulos para a troca de informação já não é mais tão segura.

É possível também a leitura de toda a memória da tag, como demonstra a Fig.13, onde se tem em evidência o bloco 1, onde se tem os seguintes bytes em hexadecimal 64, 65, 64, 65, 75, 73, com o auxílio de uma tabela ASCII é possível interpretar estes dados como caracteres, resultando no nome “dedeus”.

Figura 13. Leitura de toda a memória



Fonte: Autor

Como visto até agora, o processo de obtenção de informação é simples, qualquer atacante que souber a chave de acesso poderia descobrir dados privados do portador da tag. Pensando nisso, foi proposto a utilização de outra camada de criptografia, para isso foi implementado o algoritmo de criptografia simétrica DES (*Data Encryption Standard*), baseado na implementação de [6], a implementação completa pode ser adquirida no repositório descrito por [7].

O exemplo abordado nesta implementação é, antes da informação ser salva na tag, passar pela encriptação do DES, e posteriormente ser salva na memória da tag os bytes criptografados, tendo em vista que a chave é apenas conhecida pelo sistema embarcado em questão, dificulta consideravelmente a implementação de um ataque.

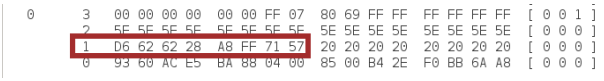
A Fig.14 demonstra o fluxo de execução, onde, neste caso o sistema recebeu o nome “luis”, transformou os caracteres em valores inteiros, seguindo a tabela ASCII, e com estes valores, aplicou a criptografia, resultando em 8 bytes de dados, onde a informação esta escondida e será gravada na tag, a chave usada para criptografar foi: 3b 38 98 37 15 20 f7 5e.

Efetuando a leitura do bloco de memória, como mostra a Fig.15 onde havia os bytes da informação explicita, agora estão os bytes criptografados, dificultando possíveis ataques, para comprovar o sucesso da aplicação, a Fig.16 mostra um site de criptografia da internet, onde estão os bytes descriptografados, e a informação do nome em evidência.

Figura 14. Criptografia DES

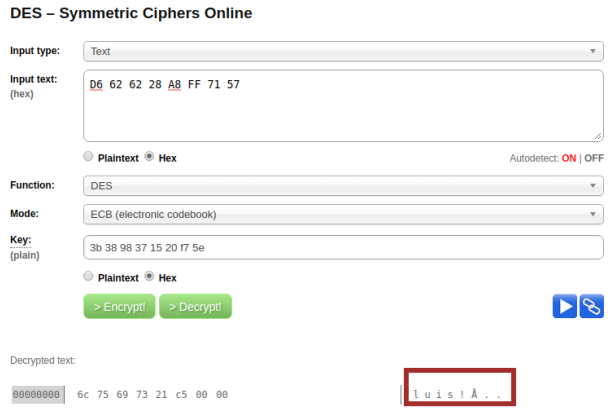
Fonte: Autor

Figura 15. Bloco de memória criptografado



Fonte: Autor

Figura 16. Comprovação da cifra correta



Fonte: Autor

VII. DISCUSSÃO CRÍTICA

Como descreve a empresa de consultoria Gartner Group, toda tecnologia emergente segue o modelo do *Hype Cycle*, onde começa no crescente, onde se pensa que a mesma irá revolucionar o mundo, tempo depois começam a aparecer os problemas e desvantagens, tais como segurança, custos, entre outros, período característico de um declive, e por fim, tende-se a estabilizar.

Com o RFID não foi diferente, pode-se dizer que hoje é uma tecnologia consolidada, tanto no sentido de suas vantagens onde pode-se citar o custo/benefício, a praticidade e aplicabilidade, como em suas fraquezas e problemas, como na parte de segurança e interferência por materiais magnéticos.

Porém toda tecnologia é baseada em seus pontos fortes e fracos, bem como toda tecnologia evolui, no caso do RFID, pode-se citar o surgimento do NFC, que está presente nos cartões de credito *contactless*, e hoje é presente tanto em cartões quanto em smartphones.

VIII. CONCLUSÕES

A utilização da radiofrequência ja é consolidada e está tomando conta de uma enorme gama de áreas, se tornando comum no cotidiano das pessoas. A contínua busca pela otimização de processos e redução de erros de origem humana faz com que tecnologias eficientes como o RFID sejam cada vez mais estudadas, e aprimoradas, principalmente para suprir seus problemas de segurança, privacidade e padronização.

Contudo é possível concluir que o uso de tags em áreas onde a tecnologia não é presente com tanta ênfase vem sendo aprimorada, como na pecuária, supermercados e shoopings, bem como áreas médicas e transporte, tornando-se uma tecnologia de senso comum onde mesmo as pessoas leigas, tem ou tiveram contato com a tecnologia de RFID.

[1] P. González, K. Rohoden, C. Palacios, and M. Rohoden, "Yanapay: sistema de evacuación basado en tecnología RFID y dispositivos Android," *Ingenius*, 2016.

[2] "Applications of rfid," Ruddersoft LTD. [Online]. Available: https://www.ruddersoft.com

[3] "Rfid - introdução aos cartões mifare," Embarcados. [Online]. Available: https://www.embarcados.com.br/rfid-cartoes-mifare/

[4] "Arduino," Github. [Online]. Available: https://www.arduino.cc

[5] "Mifare," Mifare. [Online]. Available: https://www.mifare.net/pt/

[6] "Github, implmenetação des," Github. [Online]. Available: https://github.com/Octoate/ArduinoDES

[7] "Implementação," Github. [Online]. Available: https://github.com/dedeus10/embeddedProjects/tree/master/RFID_DES/RFID_DES