|  |  |
| --- | --- |
| um | **ADMISSÃO A DISSERTAÇÃO / TRABALHO DE PROJETO**  **MESTRADO ENGENHARIA DE SISTEMAS**  **PLANO DE TRABALHOS** |

**Aluno:** Célia Natália Lemos Figueiredo

**Nº** PG 41022

**Orientador(es):** \*Sem orientador, esta proposta serve apenas para avaliação de uma componente da disciplina de Métodos de Investigação, sendo que os nomes da empresa e do projeto utilizados são fictícios. As informações usadas são baseadas num tema de dissertação do Mestrado de Engenharia Informática.

**Tema**: Desenvolvimento de chaves de automóveis inteligentes com utilização de memórias PCM

|  |  |
| --- | --- |
| **Enquadramento**  O projeto SMARTKEY tem como objetivo a utilização das memórias *Phase Change Memory* (PCM) como meio para resolver problemas que outros tipos de memórias não conseguem responder. Um dos tipos de memórias de armazenamento não volátil que apresentam problemas são as memórias *flash.* Este tipo de memória teve origem nas memórias *Electrically Erasable Programmable Read-Only Memory* (EEPROM) que eram usadas em computadores ou outros dispositivos electrónicos para memorizar pequenas quantidades de memória (Ji, Xu, Tian, & Bao, 2018).  A utilização das memórias *flash* tornou-se dominante pois a capacidade de memória armazenada é grande, os tempos de acessos de leitura são elevados, são resistentes a choques, a vibrações, altas pressões e temperaturas, tornando-se muito populares em dispositivos móveis e assumindo-se até como uma alternativa aos discos rígidos. Apesar de toda a sua popularidade as memórias *flash* têm algumas desvantagens, por exemplo, para se efetuar reescrita é necessário aplicar previamente uma limpeza (*erase*) no local onde se pretende escrever e à medida que se vai efetuando este tipo de operação as células vão começando a ficar desgastadas até ao ponto de ficarem danificadas. Outro problema associado às memórias *flash* é conhecido por distúrbio na leitura, este é mais frequente nas memórias do tipo NAND. Esta situação é caracterizada pela alteração das células nas proximidades da célula que é realmente lida e pode ocorrer caso as células circundantes não sejam reescritas periodicamente (Ahn & Lee, 2019).  Por outro lado, as memórias PCM são encaradas com uma alternativa de futuro para as memórias *flash*. A grande vantagem das memórias PCM é que ao contrário das *flash* estas têm melhores performances para escrita, uma vez que os elementos da memória podem ser alterados mais rapidamente e sobretudo porque não é necessário limpar (*erase*) um bloco inteiro para se poder atualizar esse mesmo bloco. Estas têm a particularidade de oferecer alguns mecanismos criptográficos que podem ser usados de forma a garantir que, por exemplo, escritas em memória só possam ocorrer por entidades autorizadas para tal. Desta forma, os dados armazenados estarão protegidos contra adulterações. Para além das características já descritas, as PCM conseguem também armazenar grandes volumes de informação em pouco espaço físico e permitem executar código diretamente da memória, tudo feito a velocidades consideradas elevadas (Bez, 2009). Com estas características, um caso prático interessante a explorar é o de associar as memórias PCM às chaves de automóvel atuais, com o intuito de aumentar as suas funcionalidades. Uma vez que a chave do automóvel é transportada sempre pelo condutor, esta poderia servir como meio de interação entre o condutor e o veículo, permitindo ao condutor usar a chave como mecanismo de transferência de dados (Eisenbarth et al., 2007). O condutor teria então um conjunto de novas funcionalidades como, por exemplo, preparar itinerários, transferir músicas ou *audiobooks* do seu computador pessoal para os usar no seu veículo. Para veículos com mais do que um dono, poder-se-ia também armazenar informação relativa as configurações dos bancos, rádios preferidas, posição de espelhos e temperatura que seriam verificados e aplicados sempre que o dono entrasse no carro. No sentido contrário, do automóvel para o computador pessoal, muita informação poderia ser utilizada, permitindo ao condutor visualizar estatísticas de consumos, quilometragem, velocidades e percursos efetuados, tudo a partir dos dados armazenados na chave (Singh & Singh, 2016).  Dado existirem mecanismos de *authenticated write* e *authenticated read*  (Young & Qureshi, 2015), uma chave inteligente poderia tirar partido desse facto e armazenar chaves simétricas ou chaves assimétricas para as poder utilizar num protocolo alternativo aos mecanismos de fecho atuais nos automóveis. Um dos mecanismos mais utilizado é o *keeloq*, que por esse mesmo motivo já foi alvo de vários estudos (Aerts et al., 2012), estudos esses que conduziram à implementação de vários ataques, demonstrando que este é quebrado com alguma facilidade e deveria portanto ser modificado ou substituído por uma nova solução (Eisenbarth et al., 2007).  A utilização de memória PCM associadas a chaves de automóveis conseguiria assim aumentar o leque da funcionalidade da chave e ao mesmo tempo melhorar os mecanismos de proteção do sistema de fecho centralizado de um veículo. | |
|  | |
| **Objetivos**  Esta dissertação tem como objetivo conceber e implementar componentes de *software* criptográfico que forneçam garantias de segurança adequadas ao desenvolvimento de um protótipo de chaves inteligentes para automóveis.  Para tal, esta dissertação está dividida em duas partes, uma de componente teórica e outra prática. A parte teórica englobará investigação e análise das soluções atualmente existentes na indústria automóvel, análise de segurança do cenário das chaves inteligentes, e especificação dos componentes criptográficos necessários. A componente prática consiste no desenvolvimento, implementação e integração dos referidos componentes no protótipo SMARTKEY através do uso de linguagem de programação.  Por isso, os objetivos definidos são os seguintes:   * Familiarização com o projeto SMARTKEY e com a tecnologia de memórias PCM; * Levantamento e estudo teórico dos métodos e algoritmos usados atualmente na indústria automóvel; * Estudo das metodologias de desenvolvimento de código eficiente e seguro no contexto específico da criptografia; * Análise de segurança em chaves de automóveis e especificação de componentes a desenvolver; * Desenvolvimento e implementação dos referidos componentes, em linguagem C; * Integração e validação no contexto do protótipo da chave do automóvel. | |
|  | |
| **Descrição**  A metodologia seguida na elaboração deste projeto é composta por duas partes sequenciais e uma terceira que irá decorrer em paralelo as duas primeiras, correspondendo à escrita da dissertação. Numa primeira fase, o foco irá ser essencialmente teórico e consistirá na análise e investigação de informação necessária para a fase seguinte, seguido de uma componente prática de conceção, implementação e validação de protocolos criptográficos.  De forma a responder aos objetivos propostos foram definidas 6 fases, que agora se apresentam:  1ª Fase - Familiarização com o projeto SMARTKEY e com a tecnologia das memórias PCM;  2ª Fase - Investigação sobre métodos e algoritmos usados pelas chaves de automóveis atuais;  3ª Fase - Investigação de metodologias de desenvolvimento de código eficiente e seguro no contexto da criptografia;  4ª Fase - Especificação de componentes a desenvolver e análise de segurança para as chaves do automóvel;  5ª Fase - Desenvolvimento e implementação de componentes necessárias para a chave do veículo usando a linguagem C;  6ª Fase - Integração e validação das componentes desenvolvidas no protótipo da chave.  As fases 1, 2 e 3 são relativas à parte teórica. As fases 4, 5 e 6 dizem respeito à parte prática. Todas as fases serão desenvolvidas num contexto de integração com as equipas de investigação e desenvolvimento do projeto SMARTKEY, quer na Universidade do Minho, quer no parceiro industrial MultiProjMinho. | |
|  | |
| **Fases do trabalho e calendarização**  A dissertação terá a duração estimada de 10 meses, com início em Fevereiro de 2020. Prevê-se a seguinte calendarização para a execução dos trabalhos:   |  |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **Fases** | Jan | Fev | Mar | Abr | Mai | Jun | Jul | Ago | Set | Out | Nov | Dez | | 1 - Familiarização com o projeto SMARTKEY |  |  |  |  |  |  |  |  |  |  |  |  | | 2 - Revisão bibliográfica |  |  |  |  |  |  |  |  |  |  |  |  | | 3 - Investigação de metodologias e desenvolvimento de código |  |  |  |  |  |  |  |  |  |  |  |  | | 4 - Especificação de componentes a desenvolver |  |  |  |  |  |  |  |  |  |  |  |  | | 5 - Desenvolvimento e implementação dos componentes |  |  |  |  |  |  |  |  |  |  |  |  | | 6 - Integração e validação das componentes desenvolvidas |  |  |  |  |  |  |  |  |  |  |  |  | | 7 - Escrita da dissertação |  |  |  |  |  |  |  |  |  |  |  |  | | |
|  | |
| **Bibliografia**  Aerts, W., Biham, E., De Moitié, D., De Mulder, E., Dunkelman, O., Indesteege, S., … Verbauwhede, I. (2012). A practical attack on KeeLoq. *Journal of Cryptology*, *25*(1), 136–157. https://doi.org/10.1007/s00145-010-9091-9  Ahn, N., & Lee, D. H. (2019). Schemes for Privacy Data Destruction in a NAND Flash Memory, *XX*, 1–12. Retrieved from http://arxiv.org/abs/2001.00522  Bez, R. (2009). Chalcogenide PCM: A memory technology for next decade. *Technical Digest - International Electron Devices Meeting, IEDM*, 1–4. https://doi.org/10.1109/IEDM.2009.5424415  Eisenbarth, T., Kasper, T., Moradi, A., Paar, C., Salmasizadeh, M., & Shalmani, M. T. M. (2007). Physical Cryptanalysis of KeeLoq Code Hopping Applications, 22.  Ji, F., Xu, Q., Tian, Z. Q., & Bao, J. (2018). A New White Box Test Method Applying to Watt-hour Meter Based on EEPROM Read and Write Data. *2018 Condition Monitoring and Diagnosis, CMD 2018 - Proceedings*, 1–4. https://doi.org/10.1109/CMD.2018.8535828  Singh, S., & Singh, N. (2016). Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce. *Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015*, 1577–1581. https://doi.org/10.1109/ICGCIoT.2015.7380718  Young, V., & Qureshi, M. K. (2015). DEUCE : Write-Efficient Encryption for Non-Volatile Memories. *SIGPLAN Not.*, *50*, 33–44. | |
|  | |
| Braga, 10 de Janeiro de 2020 | |
|  | |
| O(a) Aluno(a),  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | O(s) Orientador(es),  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |