

Controle de Acesso Web e Android para Portas e Fechaduras Eletrônicas com Arduino

Guilmour Rossi

¹Curso de Engenharia de Computação – Universidade Tecnológica Federal do Paraná (UTFPR) - Oficinas de Integração I

contato@guilmour.com

Resumo. *O projeto consiste no desenvolvimento e construção de um sistema de automação residencial com Arduino para a abertura e fechamento de portas, portões, trancas ou meios de acesso por meio de dispositivos digitais, tais como: celulares, computadores, cartões ou pulseiras; substituindo assim o uso de chaves físicas convencionais, trazendo um aumento de segurança com o monitoramento remoto sobre o estado da porta (aberta ou fechada) e quem teve acesso por ela.*

Palavras-chave: *tranca-eletrônica, arduino, monitoramento, segurança, automação residencial.*

1. Apresentação

O auxílio de máquinas e métodos automáticos para ajudar o ser humano em seu dia-a-dia é algo que vem sendo buscado à muito tempo, movido por um desejo inerente ao ser humano na tentativa de se obter progresso e melhores condições de vida. Depois da Revolução Industrial no final do século XVII, isso se intensificou, deixando claro a força e a importância da tecnologia e das máquinas automatizadas, e que estas agora fariam parte de nossa sociedade. Assim, perto até das histórias ficções-científicas mais criativas, foram sendo criados cada vez mais equipamentos e máquinas de inúmeros tipos e utilidades, tentando ser os mais independentes possíveis do ser humano afim de servi-lo de forma adequada e reduzir seus esforços.

Tais progressos podem ser percebidos em muitas áreas, mas muitas vezes por serem tecnologias caras ou avançadas, acabam não sendo difundidas em larga escala para todos. Este é o caso da automação industrial, de portas automáticas, trancas eletrônicas e similares. Cujas implementação acaba sendo feita apenas em locais que protegem objetos de valor, em grandes construções comerciais ou em residências das classes com maior poder aquisitivo, deixando a outra parcela da sociedade sem os benefícios práticos e de segurança destas tecnologias.

Segurança esta, que é um fator essencial em qualquer ambiente pré-disposto a ser corrompido, como bancos, lojas, casas e apartamentos que estão vulneráveis tanto fisicamente, por meio de portas, portões ou grades, quanto logicamente, por sistemas que podem ou não utilizar a internet. A maioria dos lares brasileiros ainda estão inseguros por sistemas de “controle de pessoas” ultrapassados, que são facilmente corrompidos, colocando vidas em risco, assim como a perda de um bem material. Dessa forma, aliando sistemas digitais com sistemas físicos poderemos ter um avanço enorme na segurança das residências ou estabelecimentos. Para exemplificar, pensaremos na porta de nossa casa:

o que utilizamos para abri-lá e fecha-lá? Existe chave e maçaneta? Caso esquecermos de fecha-lá será nos avisado? O que acontece caso alguém tente utilizar outra chave? E se perdermos a nossa chave?

Assim, é necessário um sistema que resolva essas questões de insegurança que muitos ainda convivem aliando-se as tecnologias atuais. Um sistema inteligente que não mais utilize uma mera chave, que é uma ferramenta facilmente copiável, mas sim um celular, ou cartão, ou algum *gadget* que possa ser utilizado, elevando o nível de confiabilidade e desinformação das pessoas, proporcionando uma vida mais tecnológica e segura.

Perder a chave não será mais um problema, pois sempre estaremos com um mini-cartão ou alguma pulseira que contem uma ou mais senhas criptografadas para dar acesso a diferentes portões. Também será possível utilizar um celular com *NFC* ou *Bluetooth* como “chave” de acesso como segunda opção, assim como, saber exatamente se a porta esta aberta ou fechada, liberar um “chave” por algum tempo pre estabelecido para um funcionário. A ideia seria que esse funcionário pudesse baixar o aplicativo e digitar a senha de acesso, que será feita avaliada através do celular com o sistema.

Definição do que pode ser feito:

- Abrir e fechar uma porta, portão ou meio de acesso por meio de dispositivos digitais, tais como: celulares, cartões ou pulseiras.
- Liberar uma “Chave” por um tempo determinado.
- Saber se a porta esta aberta ou fechada e efetuar sua troca remotamente, assim como saber quem teve acesso.

2. Análise Mercadológica

Ideias e produtos similares não são novos no mercado, mas como já comentado, possuem valores altos de compra e instalação, além de nem todos terem as praticidades da nova era digital de *smartphones*. Em uma busca rápida no *Google Shopping*, a solução em fechadura digital mais barata, é o produto da empresa brasileira *Intelbrás*, com preços à partir de R\$ 460,00 sem a instalação e possibilitando apenas o uso pelo uso de uma senha numérica. Outros itens de marcas internacionais como *Samsung* e *LG* custas ainda mais caros, à partir de R\$2000,00.

3. Análise Técnica

3.1. Prototipação Simples

Estará baseado no núcleo do projeto com uma simples implementação sem muitos recursos, apenas para um estudo de viabilidade. Conterá com um *Arduino* Uno com USB, um motor, dois LEDs (um verde e um vermelho), uma *protoboard* e um botão.

O sistema será projetado da seguinte forma: o *Arduino* estará conectado ao botão que irá girar o motor, que seria a abertura da porta; o computador estará conectado pela USB, onde será inserido um código e enviado para o *Arduino*, que irá fazer a validação do mesmo. Feito isso, irá girar o motor, acenderá o *LED* verde e um *BIP* será gerado, caso não seja validado o motor não girará, um *LED* vermelho será acesso e dois *BIPs* serão gerados.

3.2. Prototipação Arduino + Android

A segunda parte do projeto tem como função o teste de um celular em vez do computador para enviar o código de validação. Será preciso montar toda uma estrutura de rede favorável a comunicação entre os equipamentos digitais e a tranca com *arduino*. [Igoe, 2011] Será utilizado um celular com o sistema *Android* conectado ao *Arduino*, inicialmente, através de um cabo USB, para posteriormente, ser testado sistemas de comunicação sem fio, como, infravermelho, *bluetooth*, *wireless* ou *NFC*. Também consiste na programação do aplicativo para *Android*, onde será realizada uma pesquisa adequada para efetuar o sistema de comunicação.

3.2.1. Gerenciamento de múltiplos sistemas de acesso:

Para que o sistema possa gerenciar múltiplos equipamentos é necessário implementar uma codificação específica para cada aparelho *Arduino*, que será enviada para o dispositivo celular verificando se existe alguma senha de entrada no seu registro associada a ele e caso seja afirmativo enviará para o equipamento que a validará.

3.2.2. Guardando e gerenciando as senhas no *Arduino*:

Existem três opções possíveis para este caso: a primeira seria um celular com o aplicativo de gerenciamento, onde poderia fazer todo o controle de acesso determinando usuários, seus horários e respectivos dias de acesso; a segunda seria um modulo wifi, como se fosse um servidor WEB, que pudesse ser acessado por qualquer dispositivo da rede, permitindo que fossem feitas as configurações necessárias; a terceira poderia ser um cartão de memória removível onde conteria os dados necessários, caso precisasse alterá-los deveria ser efetuado em um computador.

A primeira opção possui de desvantagens que toda configuração deverá ser efetuada a poucos metros do aparelho e uma programação mais complexa no *Android* será necessária. A segunda, necessitará de um modulo *wireless* para *Arduino* aumentando os custos de manufatura, consumo de energia e programação, no caso do desenvolvimento do servidor *Web*, além de necessitar de um constante acesso a internet. Entretanto, com esse sistema seria possível determinar quase instantaneamente o log de acesso, assim sabendo quem acessou e quando foi acessado, também permitindo fazer configurações remotamente, apenas sendo necessária uma conexão a internet. A terceira, demandaria mais trabalho, pois além de necessitar um software específico para cada sistema ou um conhecimento muito grande do usuário ele terá que retirar o cartão de memória do sistema toda vez que quiser alterar suas configurações, não permitindo um acesso remotamente, e estará preso a um computador. Seria, mais interessante seu uso fixo como um acessório para aumentar a capacidade do LOG ou do gerenciamento de usuários e senhas.

Equipamentos Projeto Inicial:

- Arduino Uno
- Cabo USB
- Motor
- Dois Leds
- Uma Protoboard
- Comunicador Wi-fi para Arduino
- Um botão

- Um computador

Ferramentas Necessárias:

- Alicate
- Cola Quente
- Ferro Solda
- Solda
- Fiação

Referências

Igoe, T. (2011). *Making things talk : Practical methods for connecting physical objects*. Maker Media, Sebastopol, CA.