E.E Comendador Teixeira Pombo

Análise de Segurança da Informação baseada em cenas de Watch Dogs

3º Serie B NovoTec

Tremembé

2023

Sumário

ESTAÇÃO 1

Watch Dogs é uma renomada série de jogos eletrônicos que mergulha os jogadores em um universo de alta tecnologia e intrigas cibernéticas. Desenvolvida pela Ubisoft, uma das principais produtoras de jogos do mundo, a franquia estreou em 2014 com o lançamento do primeiro título homônimo, introduzindo os jogadores a um cenário distópico e futurista onde a tecnologia se entrelaça com a sociedade de maneiras complexas e, por vezes, ameaçadoras.

A trama central da série Watch Dogs gira em torno do conceito de hacking como uma ferramenta poderosa nas mãos dos protagonistas, permitindo-lhes manipular e controlar diversos elementos da cidade fictícia em que se passam os jogos. A habilidade de invadir sistemas, controlar câmeras de segurança, acessar informações confidenciais e até mesmo manipular semáforos e sistemas de energia elétrica proporciona aos jogadores uma experiência única e envolvente.

O primeiro título, ambientado em Chicago, apresentou Aiden Pearce como protagonista, um habilidoso hacker em busca de vingança após uma tragédia pessoal. O jogo explorou temas como vigilância em massa, privacidade e os perigos de uma sociedade excessivamente conectada. O sucesso do primeiro jogo pavimentou o caminho para continuações e expandiu o universo Watch Dogs. Watch Dogs 2, lançado em 2016, trouxe uma mudança de cenário para San Francisco e uma abordagem mais leve e descontraída em comparação com o tom mais sombrio do antecessor. Os jogadores assumiram o controle de Marcus Holloway, um jovem hacker brilhante que se junta a um grupo de ativistas cibernéticos conhecido como DedSec.

O enredo do segundo jogo mergulhou mais fundo nas implicações éticas da tecnologia e explorou questões sociais contemporâneas, como o papel das grandes corporações na coleta de dados e manipulação da opinião pública. Com uma narrativa rica, personagens cativantes e uma jogabilidade inovadora que

combina ação furtiva, combate e hacking, a série Watch Dogs conquistou uma base de fãs dedicada. Além disso, a Ubisoft continuou a expandir o universo da franquia com o lançamento de Watch Dogs: Legion em 2020, introduzindo uma mecânica única em que os jogadores podiam recrutar e controlar qualquer habitante da cidade de Londres, cada um com suas próprias habilidades e histórias.

Ao longo dos anos, Watch Dogs evoluiu não apenas em termos de jogabilidade e enredo, mas também refletiu a rápida evolução da tecnologia na vida real. A série permanece como uma exploração fascinante e provocativa dos dilemas éticos e sociais associados à interconexão digital e à crescente influência da tecnologia em nossas vidas. Com uma combinação de ação eletrizante, hacking estratégico e uma narrativa envolvente, Watch Dogs continua a ser uma referência no cenário dos jogos eletrônicos contemporâneos.

Já no terceiro, situado dentro de uma representação ficcional de uma futurística e distópica da cidade de Londres, *Watch Dogs: Legion* segue a filial local da DedSec enquanto procuram limpar seus nomes após serem acusados de uma série de atentados terroristas. A DedSec também tenta libertar os cidadãos de Londres do controle de Albion, uma opressora empresa militar privada que transformou a cidade em um estado de vigilância após os bombardeios. O jogo apresenta um sistema de múltiplos personagens jogáveis, permitindo aos jogadores recrutar virtualmente qualquer NPC encontrado no mundo aberto do jogo. Cada personagem jogável tem suas próprias habilidades e experiências únicas, e podem ser perdidos permanentemente se os jogadores habilitarem a opção de morte permanente antes de iniciar um novo jogo. Existem várias maneiras de completar missões, dependendo de qual personagem jogável é selecionado.

O jogo foi lançado para Windows, PlayStation 4, Xbox One e Stadia em 29 de outubro de 2020; As versões PlayStation 5 e Xbox Series X/S também foram disponibilizadas assim que os consoles foram lançados. Ubisoft Toronto liderou o desenvolvimento do jogo, com Clint Hocking servindo como seu diretor criativo.[19] *Legion* recebeu críticas mistas; a maioria das críticas foi direcionada à falta de personalidade dos personagens jogáveis, dublagem pobre e desequilíbrio entre suas habilidades, bem como o mundo do jogo, direção, enredo e dificuldade inconsistente.

Jogabilidade

A série *Watch Dogs* faz parte de um gênero conhecido como sandbox. A série combina elementos de ação, aventura e jogabilidade veicular. O jogador pode vagar livremente pelo mundo virtual a pé ou usando veículos e fazer uso de uma variedade de armas e combates com base em combates. Atividades ilegais, como agressão a civis e policiais
não-jogadores, irão instigar uma resposta proativa e geralmente letal de figuras autorizadas. No caso de morte, o jogador irá reaparecer perto da área onde foi morto.

Em cada jogo, o jogador assume o controle de um hacker, que pode invadir vários dispositivos eletrônicos conectados ao sistema ctOS fictício com seu smartphone no jogo. Enquanto a maioria das habilidades concedidas pelo ctOS são usadas para resolver quebra-cabeças, o jogador também pode usá-lo em mundo livre a qualquer momento para criar o caos e se divertir, como invadir semáforos ou colocar evidências falsas contra NPCs para que a polícia os prenda. Em cada jogo, o jogador pode subir de nível e desbloquear novas habilidades e dispositivos. Os jogos incorporam vários segmentos furtivos, onde o jogador deve tentar evitar ser detectado pelos inimigos e eliminá-los silenciosamente com armas não letais; se o jogador não permanecer sem ser detectado, eles ainda podem tentar matar todos os inimigos restantes, embora na maioria das vezes eles se encontrem encurralados. Em *Watch Dogs 2*, mais armas e gadgets de hacker foram introduzidos, como um taser e um quadricóptero.

Contexto

Os jogos de *Watch Dogs* acontecem em versões fictícias de cidades da vida real que implementaram ctOS. *Watch Dogs* se passa na Região Metropolitana de Chicago, *Watch Dogs 2* na Baía de São Francisco e *Watch Dogs: Legion* em Grande Londres. Enquanto os dois primeiros jogos acontecem durante os tempos modernos, *Legion* se passa em um "futuro próximo" (por volta de 2030), retratando avanços significativos em tecnologia.

ESTAÇAÕ 2

CÂMERAS IP

Câmeras IP s,ão dispositivos de segurança que usam a internet para enviar e receber dados de vídeo. Elas oferecem a capacidade de monitorar locais remotamente, geralmente por meio de um aplicativo ou software. No entanto, como qualquer dispositivo conectado à internet, as câmeras IP também podem ser vulneráveis a ataques de hackers.

Câmeras IP (Câmeras De Rede):

Câmeras IP são dispositivos de vigilância que se conectam à rede, geralmente via Wi-Fi ou cabo Ethernet.

Elas são usadas para monitorar locais, como residências, empresas, escritórios e espaços públicos.

Muitas câmeras IP oferecem recursos avançados, como visão noturna, detecção de movimento e streaming de vídeo em tempo real pela internet.

Como As Câmeras IP Podem Ser Hackeadas:

- **Senhas Fracas:** Se as câmeras têm senhas fracas ou padrões de senha previsíveis, os hackers podem tentar adivinhá-las.
- **Vulnerabilidades de Software:** Falhas de segurança no software da câmera podem ser exploradas por hackers para obter acesso não autorizado.
- **Ataques de Força Bruta:** Os hackers podem usar ataques de força bruta para testar diversas combinações de senhas até encontrarem a correta.
- **Ataques de Injeção de Comandos**: Se a câmera não está protegida contra injeção de comandos, os hackers podem enviar comandos maliciosos para controlar a câmera.

- **Ataques de Roteador:** Se o roteador que conecta a câmera à internet for comprometido, isso pode permitir o acesso à câmera.
- **Firmware Desatualizado:** Versões antigas de firmware podem ter vulnerabilidades conhecidas que os hackers podem explorar.

Para Proteger As Câmeras IP Contra Hackers, É Importante Tomar As Seguintes Medidas:

- Alterar senhas padrão para senhas fortes e exclusivas.
- Manter o firmware da câmera atualizado com as últimas atualizações de segurança.
- Configurar a câmera e o roteador com configurações de segurança adequadas.
- Monitorar o tráfego de rede em busca de atividades suspeitas.
- Isolar a câmera em uma rede separada para limitar seu acesso.

Em resumo, as câmeras IP são dispositivos de vigilância úteis, mas é vital protegê-las contra ataques de hackers, uma vez que a falta de segurança pode permitir o acesso não autorizado e a invasão da privacidade.

Hackear câmeras é uma ação fundamental para o protagonista. Ao hackear câmeras, ele pode:

- obter acesso a informações valiosas
- dados de localização
- imagens de vigilância
- controlar dispositivos conectados à rede
- obter uma visão privilegiada do ambiente ao redor e acessar locais perigosos para ir fisicamente
- identificar alvos
- planejar estratégias
- obter informações para avançar na história do jogo.

ATAQUE DDOS

Um Ataque DDoS (Distributed Denial of Service) é um tipo de ataque cibernético em que uma grande quantidade de tráfego malicioso é direcionada a um alvo, como um site, servidor ou serviço online, a partir de vários dispositivos ou computadores comprometidos. O objetivo desse ataque é sobrecarregar o alvo com um volume excessivo de tráfego, tornando-o lento ou indisponível para usuários legítimos.

Aqui estão os principais pontos a serem lembrados sobre ataques DDoS:

- **Distribuído:** O "D" em DDoS significa "distribuído". Isso significa que o ataque é realizado por uma rede de computadores ou dispositivos comprometidos em vez de um único local.
- **Negação de Serviço:** O objetivo principal de um ataque DDoS é negar o serviço ou torná-lo inacessível para usuários legítimos, impedindo que eles acessem um site ou serviço online.
- **Tráfego Malicioso:** Os atacantes usam tráfego malicioso para sobrecarregar a largura de banda, recursos do servidor ou aplicativos, causando interrupções no serviço.
- **Motivação:** Os motivos por trás de ataques DDoS podem variar, desde motivos financeiros, concorrência desleal, ideológicos ou simplesmente o desejo de causar interrupções na internet.

Para combater ataques DDoS, as organizações implementam medidas de segurança, como filtros de tráfego, serviços de mitigação em nuvem e configurações de rede resistentes a ataques, a fim de manter seus serviços online disponíveis e seguros.

Mecanismos De Ataque Ddos:

- **Ataques Volumétricos:** São os mais comuns e buscam sobrecarregar a largura de banda da vítima com tráfego excessivo. Exemplos incluem ataques de amplificação, onde os atacantes usam servidores mal configurados para enviar grandes volumes de dados à vítima.

- **Ataques de Esgotamento de Recursos:** Esses ataques visam esgotar os recursos do servidor, como CPU, memória e conexões. O ataque SYN Flood, por exemplo, gera uma grande quantidade de conexões incompletas para sobrecarregar o servidor.

- **Ataques de Camada de Aplicação:** Diferentemente dos ataques de camada de rede ou transporte, esses ataques miram a camada de aplicação do servidor, explorando vulnerabilidades nos aplicativos web. Exemplos incluem ataques HTTP Flood, que tentam sobrecarregar um servidor web enviando um grande número de solicitações HTTP.

Tipos De Ataque Ddos:

- **Ataques DoS (Denial of Service):** Envolvem um único dispositivo para sobrecarregar um serviço. Os ataques DDoS, por outro lado, são distribuídos e geralmente mais poderosos.

- **Ataques Amplificados:** Os atacantes exploram serviços mal configurados para amplificar o tráfego direcionado à vítima. Isso pode incluir servidores DNS, NTP ou servidores de reflexão SNMP.

Defesa Contra Ataques Ddos:

- **Filtros de Tráfego:** Empresas e provedores de serviços de internet usam filtros para bloquear tráfego malicioso antes que ele atinja a vítima.
- **CDNs (Redes de Distribuição de Conteúdo):** CDNs distribuem o tráfego globalmente, minimizando o impacto de ataques DDoS.
- **Monitoramento de Tráfego:** O monitoramento em tempo real ajuda a identificar picos de tráfego anormais que podem sinalizar um ataque DDoS.
- **Mitigação em Nuvem:** Algumas empresas oferecem soluções de mitigação DDoS baseadas em nuvem que filtram o tráfego antes que ele alcance o servidor.
- **Configuração de Redes Resistentes a DDoS:** Projetar redes com redundância e capacidade de escalonamento ajuda a resistir a ataques.

ATAQUE MAN IN THE MIDDLE

Um ataque de negação de serviço distribuído (DDoS - Distributed Denial of Service) é uma tentativa maliciosa de tornar um serviço online inacessível ao sobrecarregar o servidor ou a infraestrutura de rede com uma quantidade excessiva de tráfego. Nesse tipo de ataque, diversos dispositivos infectados, conhecidos como "zumbis" ou "bots", são controlados remotamente por um invasor para enviar uma grande quantidade de solicitações ao servidor alvo simultaneamente.

Os ataques DDoS são capazes de sobrecarregar os recursos do servidor, como largura de banda, processamento de dados e memória, impedindo que os usuários legítimos acessem o serviço. Esses ataques podem ser realizados por motivos diversos, como extorsão, sabotagem ou simplesmente por diversão, causando prejuízos financeiros e danos à reputação da organização ou indivíduo alvo.

Principais Aspectos Do Ataque Man-In-The-Middle:

- **Interceptação:** O atacante consegue interceptar as comunicações entre duas partes sem que elas percebam. Isso pode ocorrer em uma variedade de cenários, como em uma conexão Wi-Fi não segura ou por meio da manipulação de roteadores ou servidores.
- **Escuta Ativa:** O atacante pode escutar ativamente as conversas, coletando informações confidenciais, como senhas, números de cartão de crédito ou mensagens pessoais.
- **Alteração de Dados:** Além da interceptação, o atacante também pode modificar os dados em trânsito, o que pode ser particularmente perigoso. Por exemplo, ele pode injetar malware em arquivos sendo transferidos ou redirecionar um usuário para um site falso que se parece com o legítimo.

- **Ataques de Homem no Meio de Rede:** Em redes Wi-Fi públicas, por exemplo, um atacante pode criar uma rede falsa que se parece com a rede legítima. Quando as pessoas se conectam a essa rede falsa, o atacante pode interceptar todo o tráfego que passa por ela.
- **Uso de Certificados Falsos:** Em conexões seguras (HTTPS), o atacante pode usar certificados falsos para criar uma falsa "camada segura" e enganar os usuários. Isso é conhecido como ataque SSL/MITM.

Proteção contra o Man-In-The-Middle

- Usar conexões seguras, como HTTPS, ao acessar sites e serviços online.
- Não se conectar a redes Wi-Fi públicas não confiáveis.
- Manter o software e os dispositivos atualizados para evitar vulnerabilidades conhecidas.
- Verificar certificados SSL para garantir a autenticidade de sites.
- Usar uma VPN (Rede Virtual Privada) para criptografar o tráfego e proteger a comunicação.

BOTNET

Uma botnet é uma rede de computadores infectados e controlados remotamente por um invasor, conhecido como botmaster. Esses computadores infectados, também chamados de "bots" ou "zumbis", são geralmente comprometidos sem o conhecimento dos usuários legítimos.

O botmaster utiliza a botnet para realizar atividades maliciosas, como ataques DDoS, envio de spam, roubo de informações pessoais e bancárias, mineração de criptomoedas e propagação de malware. Os bots são comandados a partir de um servidor de controle centralizado, permitindo que o botmaster envie instruções para todos os computadores infectados simultaneamente.

Os computadores que fazem parte de uma botnet são frequentemente comprometidos por meio de malware, como cavalos de Troia, worms ou botnets auto-propagáveis. Esses malwares exploram vulnerabilidades em sistemas operacionais, aplicativos ou até mesmo técnicas de engenharia social para infectar os computadores.

A criação e operação de uma botnet é ilegal e pode resultar em consequências legais graves para o botmaster. Para proteger-se contra infecções por botnet, é importante adotar boas práticas de segurança cibernética, como manter o sistema e os aplicativos atualizados, utilizar soluções antivírus e firewall confiáveis e evitar clicar em links ou abrir anexos de fontes desconhecidas.

Além disso, conscientização e educação sobre segurança cibernética são essenciais para que os usuários possam identificar sinais de infecção por botnet e adotar medidas adequadas para proteger seus dispositivos e informações pessoais.

Características Principais De Uma Botnet:

- **Controle Remoto:** Os dispositivos infectados em uma botnet são controlados remotamente por meio de um servidor central ou uma infraestrutura de comando e controle (C&C) que permite aos operadores enviar comandos e receber informações dos bots.
- **Invasão Silenciosa:** Os dispositivos que fazem parte de uma botnet são frequentemente infectados sem o conhecimento de seus proprietários. Isso pode ocorrer por meio de malware, como cavalos de Troia ou vírus, que exploram vulnerabilidades de segurança.
- **Diversidade de Dispositivos:** Uma botnet pode consistir em uma variedade de dispositivos, incluindo computadores, servidores, smartphones, roteadores, dispositivos de IoT (Internet das Coisas) e até mesmo câmeras de segurança.
- **Atividades Maliciosas:** As botnets podem ser usadas para realizar uma série de atividades maliciosas, como ataques DDoS (Distributed Denial of Service), envio de spam, roubo de informações, mineração de criptomoedas, disseminação de malware e muito mais.
- **Anonimato:** Os operadores de botnets muitas vezes usam técnicas para esconder sua identidade e localização, dificultando a identificação e responsabilização.

As botnets são uma ameaça significativa à segurança cibernética, pois podem ser usadas para realizar ataques em larga escala, comprometer informações confidenciais e prejudicar a infraestrutura de internet. A detecção e a mitigação de botnets são desafios constantes na segurança cibernética e envolvem o uso de antivírus, firewalls, atualizações de segurança e práticas seguras na internet.

Proteger-se contra botnets envolve práticas de segurança cibernética sólidas e medidas preventivas. Aqui estão algumas etapas que você pode seguir para se

Proteger Contra Botnets E Manter Seus Dispositivos Seguros:

- **Mantenha Software e Dispositivos Atualizados:**

Mantenha seu sistema operacional, aplicativos e dispositivos atualizados com as últimas correções de segurança. Isso ajuda a corrigir vulnerabilidades conhecidas.

- **Use Antivírus e Antimalware:**

Instale um software antivírus e antimalware confiável e mantenha-o atualizado. Isso pode ajudar a detectar e remover ameaças.

- **Firewalls:**

Ative um firewall em seu computador ou roteador para bloquear tráfego indesejado e não autorizado.

- **Senhas Fortes:**

Use senhas fortes e exclusivas para suas contas online e dispositivos. Considere o uso de um gerenciador de senhas para facilitar a criação e gerenciamento de senhas.

- **Autenticação de Dois Fatores (2FA):**

Ative a autenticação de dois fatores sempre que possível. Isso adiciona uma camada extra de segurança às suas contas online.

- **Desconfie de Emails e Anexos Suspeitos:**

Evite abrir emails de remetentes desconhecidos e não clique em links ou faça o download de anexos de fontes não confiáveis. Muitas botnets se espalham por meio de malware enviado por email.

- **Evite Redes Wi-Fi Não Seguras:**

Evite conectar-se a redes Wi-Fi públicas ou não seguras sempre que possível. Se você precisar usar uma rede pública, use uma VPN para criptografar seu tráfego.

- **Atualizações de Firmware do Roteador:**

Mantenha o firmware do seu roteador atualizado para corrigir vulnerabilidades e proteger a rede local.

- **Monitoramento de Tráfego de Rede:**

Monitore o tráfego de rede em busca de atividades suspeitas. Isso pode ajudar a identificar possíveis infecções por botnets.

- **Educação Cibernética:**

Esteja ciente dos riscos de segurança cibernética e eduque-se sobre as últimas ameaças. A conscientização é fundamental para evitar armadilhas.

- **Atualização de Dispositivos de IoT:**

Mantenha dispositivos de Internet das Coisas (IoT), como câmeras de segurança ou termostatos, atualizados com os patches de segurança mais recentes. Eles são frequentemente alvos de botnets.

- **Bloqueio de Portas e Serviços Não Utilizados:**

Desative ou bloqueie portas e serviços que não são necessários em seu roteador ou firewall para reduzir a superfície de ataque.

O ATAQUE À DYN EM 2016

O segundo maior ataque de DDoS foi dirigido à Dyn, um grande provedor de DNS, em outubro de 2016. Foi um ataque devastador e provocou disrupção em muitos sites importantes, incluindo o AirBnB, a Netflix, o PayPal, a Visa, a Amazon, o jornal The New York Times, o Reddit e o GitHub. O ataque foi efetuado usando um malware chamado Mirai. O Mirai cria uma botnet composta de dispositivos comprometidos da Internet das Coisas (IoT), como câmeras, TVs inteligentes, rádios, impressoras e até monitores de bebês. Para criar o tráfego de ataque, todos esses dispositivos comprometidos são programados para enviar solicitações a uma única vítima.

Felizmente, a Dyn conseguiu debelar o ataque em um único dia, mas o motivo do ataque nunca foi descoberto. Grupos de hacktivistas reivindicaram a responsabilidade pelo ataque como resposta ao fato de o acesso à internet ter sido negado ao fundador do WikiLeaks Julian Assange no Equador, mas nenhuma prova corroborou essa reivindicação. Também há suspeitas de que o ataque tenha sido realizado por um gamer insatisfeito.

ESTAÇÃO 3

CONTROLE DE ACESSO EM PORTAS

Em watch dogs, o protagonista Aiden Pearce frequentemente precisa invadir algum lugar para realizar alguma ação na sua luta por vingança, mas acaba se deparando com portas trancadas com fechaduras eletrônicas no seu caminho, mesmo assim ele consegue acesso ao local desejado ao hackear algum outro equipamento que contenha a senha da fechadura.

Na vida real, existem várias opções de sistemas digitais para controle de acesso, um muito comum é o rfid - que é utilizado pelas portas do jogo - e vem se tornando cada vez mais comum na vida real. A tecnologia rfid (sigla em inglês para “Radio Frequency Identification”, significa “identificação por radiofrequência”) consiste em utilizar sinais de rádio emitidos por tags rfid para identificar ou rastrear o portador da tag. Uma fechadura rfid é simplesmente um mecanismo que abre a porta ao identificar a etiqueta do dono, quando o mesmo a aproxima de um painel de controle.

A atividade de hackear portas em Watch Dogs evidencia uma das principais vulnerabilidades das fechaduras rfid: Clonagem. Depois de hackear uma máquina com acesso à senha, Aiden apenas copia a senha em uma tag a qual ele tem acesso, ou seja, faz uma clonagem. Na vida real, criminosos podem fazer isso também hackeando computadores, mas também com outros métodos, o que leva riscos seríssimos à segurança da pessoa que teve seu cartão clonado, já que o mesmo fica muito suscetível a invasões.

RFID

Leitor RFID é o elemento transceptor da comunicação em um sistema RFID, ou seja, ele recebe os sinais emitidos pela tag.O dispositivo de leitura é composto por uma antena que é responsável por emitir as ondas de rádio que formam o raio de leitura e também por receber os sinais enviados pela tag. Quando a antena recebe um sinal ela o envia para um segundo elemento que compõe o dispositivo de leitura que é um sistema responsável por validar a tag,

mas vale ressaltar que a depender das configurações o sistema pode apenas traduzir o sinal para linguagem de máquina e enviá-lo a um computador para que esse faça a avaliação da tag.

TAGS RFID

A tag é o elemento transponder da comunicação em sistema RFID, ou seja, é ela que envia o sinal para o dispositivo de leitura. A tag é composta por um chip que armazena um conjunto de dados com a identidade da tag e por uma antena responsável por emitir o conteúdo do chip para o dispositivo de leitura.

No mercado, as tags estão disponíveis nos mais diversos tipos de radiofrequência, tamanho e encapsulamento. Entretanto a melhor forma de classificá-las é por tipo de alimentação, existindo três tipos:

TAGS ATIVAS: Esse tipo de tag possui uma fonte de energia própria, uma bateria, dessa forma ela emite seu sinal mesmo se estiver fora do raio de ação do dispositivo de leitura.

TAGS PASSIVAS: As tags passivas são aquelas que não possuem uma fonte de energia própria, elas são alimentadas pela energia eletromagnética do leitor.

TAGS SEMI PASSIVA: Esse tipo de tag uni características dos dois outros tipos, ela possui uma fonte de energia própria, porém só emite seus dados quando está no raio de ação de um leitor.

ESTAÇÃO 4

Portas de garagem

A clonagem de controles de portão de garagem é um tópico que envolve a replicação não autorizada de dispositivos de controle remoto usados para operar portões automáticos em garagens e entradas de propriedades. Embora a clonagem de controles remotos de portões de garagem seja um assunto frequentemente discutido em relação à segurança residencial e a possíveis vulnerabilidades nos sistemas de controle de acesso, também é uma prática que suscita questões éticas e legais.

Neste contexto, é fundamental entender o funcionamento dos sistemas de controle de portão de garagem, as técnicas de clonagem utilizadas, os riscos associados a essa atividade e as medidas de segurança que podem ser adotadas para proteger a integridade dos sistemas de acesso. A clonagem de controles de portão de garagem é um exemplo de como avanços tecnológicos podem ser usados tanto para fins legítimos quanto para atividades ilícitas, destacando a importância da conscientização e proteção adequada para garantir a segurança das propriedades e seus ocupantes.

Cuidados com o portão da garagem

Portões automáticos podem ser mais práticos e seguros, desde que a empresa fornecedora ofereça alguns recursos. Além disso, os moradores também devem adotar medidas de segurança.

- **Certifique-se que seu controle remoto é anti-clonagem**

Nossa recomendação é que você converse com o seu fornecedor do portão para se certificar que o seu portão da garagem possui um sistema de placa e controle remoto anti clonagem.

Muitos portões eletrônicos, especialmente mais antigos, utilizam sistemas que são acionados sempre pelo mesmo código de frequência ou com uma variação

pequena de códigos, o que viabiliza a clonagem. Nesses casos, a recomendação é substituir por novos controles com sistema que mudam continuamente o código.

Ou seja, o investimento em um controle de portão automático mais moderno, com um controle remoto anti clonagem, é uma forma de reforçar a segurança do seu imóvel e evitar que criminosos obtenham o código de acesso.

- **Não empreste o controle**

Evite emprestar o controle remoto da sua garagem a terceiros, pois isso pode facilitar o risco de clonagem. Ainda que seja recomendado manter um controle reserva com uma pessoa de confiança, certifique-se de que ela manterá o item em segredo.

- **Instale travas de segurança**

Avalie, com apoio do seu fornecedor, a viabilidade de instalação de travas de segurança nos portões da sua residência. Essa nova camada de proteção pode ser o diferencial para impedir a entrada dos bandidos na sua garagem.

- **Invista em um motor veloz**

Como dito antes, os portões automáticos podem ser mais seguros desde que contenham alguns recursos e um deles é o motor com acionamento rápido. Com isso, você reduz o tempo de exposição da residência evitando a entrada de criminosos enquanto o portão está abrindo ou fechando.

Além dos cuidados com o portão da garagem, você pode adotar uma série de equipamentos e medidas para diminuir o risco de invasão. Se tratando de infraestrutura, aposta em:

- Cercas
- sensores perimetrais
- alarmes residenciais
- Câmeras na fachada da sua casa e nos muros adjacentes.

Além disso, também é interessante instalar um gavetão no muro da fachada da residência, se possível, para receber encomendas com segurança e evitar o contato com os entregadores. Com o aumento das compras feitas pela internet, houve o crescimento no número de golpes aplicados por entregadores.

ESQUEMA DE TRANSMISSÃO DE UM PORTÃO DE GARAGEM

O esquema de transmissão de um portão de garagem automático envolve a comunicação entre o controle remoto (transmissor) e o receptor no motor do portão. Aqui está uma explicação simples de como esse processo ocorre:

1. **Controle Remoto (Transmissor):** O controle remoto é um dispositivo portátil que o proprietário do portão utiliza para abrir ou fechar o portão da garagem de forma remota. Geralmente, ele funciona com uma bateria que alimenta o transmissor.

2. **Botão de Comando:** O controle remoto possui um botão ou um conjunto de botões que o usuário pressiona para ativar o comando de abrir ou fechar o portão.

3. **Codificação do Sinal:** Quando o botão é pressionado, o controle remoto gera um sinal de rádio frequência (RF) codificado. Essa codificação é uma medida de segurança que evita que terceiros interceptem o sinal e acessem a garagem de forma não autorizada. O sinal pode ser codificado de várias maneiras, como utilizando códigos de rolagem ou chaves de segurança exclusivas.

4. **Transmissão do Sinal:** O controle remoto envia o sinal codificado em forma de ondas de rádio para o receptor no motor do portão.

5. **Receptor no Motor do Portão:** O motor do portão de garagem contém um receptor que é configurado para reconhecer e decodificar o sinal enviado pelo controle remoto. O receptor é programado para aceitar apenas sinais que correspondem à codificação correta.

6. **Ação no Portão:** Quando o receptor no motor do portão reconhece o sinal como válido, ele aciona o mecanismo do portão, fazendo com que ele se abra ou feche, dependendo do comando emitido pelo controle remoto.

7. **Retorno de Feedback (Opcional):** Alguns sistemas de portão de garagem oferecem um feedback visual ou sonoro para confirmar que o comando foi executado com sucesso. Isso pode incluir luzes piscando ou um som de beep no controle remoto.

Este é o esquema básico de transmissão em um sistema de portão de garagem. É importante notar que a segurança desse sistema depende da codificação do sinal, que deve ser difícil de ser decifrada por terceiros, a fim de evitar a clonagem não autorizada dos controles de portão. Portanto, a proteção da codificação e a manutenção adequada do sistema são essenciais para garantir a segurança de sua garagem.

SAMY KAMKAR

Samy Kamkar é um pesquisador de segurança cibernética e um hacker ético conhecido por suas contribuições significativas para a comunidade de segurança. Ele ganhou destaque por uma série de projetos e pesquisas inovadoras.

Samy Kamkar é um hacker e pesquisador em segurança cibernética, conhecido por suas descobertas no campo da segurança de dispositivos sem fio, incluindo controles remotos de automóveis. O "RollJam" é um dos projetos que demonstra como as vulnerabilidades podem ser exploradas e como as empresas podem melhorar a segurança de seus produtos.

Objetivos:

- Identificar e explorar vulnerabilidades em sistemas de controle remoto sem fio.
- Demonstrar a importância de adotar medidas de segurança robustas para proteger dispositivos contra ataques de clonagem.

Metodologia:

Samy Kamkar desenvolveu o "RollJam," um pequeno dispositivo que intercepta os sinais de rádio frequência (RF) de controles remotos sem fio usados em automóveis, portões de garagem e sistemas de segurança. O dispositivo foi projetado para operar em frequências comuns de controles remotos.

Funcionamento RollJam:

1. Quando um usuário pressiona o botão de um controle remoto alvo para abrir um veículo, o RollJam intercepta o sinal RF.
2. Em vez de encaminhar imediatamente o sinal para o veículo, o RollJam armazena o código de desbloqueio.
3. Enquanto o usuário acredita que o carro foi desbloqueado, o RollJam bloqueia o sinal original de chegada ao veículo.

4. Posteriormente, quando o usuário tenta trancar o veículo, o RollJam faz o mesmo processo de interceptação.
5. Agora, o invasor tem em sua posse os códigos de desbloqueio e bloqueio, o que pode ser usado para acessar o veículo posteriormente.

Resultados e Impacto:

O projeto RollJam de Samy Kamkar teve um impacto significativo, demonstrando as vulnerabilidades comuns em sistemas de controle remoto sem fio e o risco de clonagem. Isso levou a uma conscientização mais ampla sobre a necessidade de melhorar a segurança em dispositivos RF, como controles remotos de automóveis e portões de garagem.

Como resultado do RollJam e outras pesquisas semelhantes, muitas empresas começaram a adotar medidas de segurança mais robustas em seus produtos, como a implementação de códigos de rolagem e criptografia nos sinais de RF.

O projeto RollJam de Samy Kamkar é um estudo de caso importante que ilustra como a pesquisa em segurança cibernética pode identificar vulnerabilidades em tecnologias do dia a dia. Kamkar demonstrou as fragilidades em sistemas de controle remoto sem fio e incentivou melhorias na segurança desses dispositivos. Essa pesquisa destaca a importância da constante inovação em segurança cibernética e da conscientização sobre as ameaças em constante evolução.

ROLLING CODE

"Rolling code," em português "código de rolagem," é uma tecnologia de segurança comumente usada em sistemas de controle remoto, como controles remotos de automóveis, portões de garagem, sistemas de segurança residencial e outros dispositivos que usam comunicação sem fio para acesso. O objetivo do "rolling code" é tornar mais difícil a clonagem ou a reprodução não autorizada dos códigos de transmissão, aumentando a segurança desses sistemas.

Geração de Códigos Dinâmicos: Em vez de usar um único código de transmissão fixo, os sistemas que utilizam o "rolling code" geram uma sequência de códigos únicos e dinâmicos. Esses códigos mudam a cada vez que um comando é enviado.

Armazenamento de Códigos: Tanto o controle remoto quanto o receptor no dispositivo (por exemplo, o receptor no automóvel ou no portão de garagem) mantêm uma lista dos códigos recentemente gerados. Essa lista é sincronizada entre o controle remoto e o receptor.

Transmissão e Verificação: Quando um comando é enviado, o código atual é transmitido. O receptor verifica se o código recebido corresponde ao próximo código na sequência armazenada.

Uso Único: Uma vez que um código é usado, ele é descartado e não pode ser reutilizado. O próximo código na sequência é então programado para ser usado na próxima transmissão.

Isso significa que, mesmo que um invasor intercepte um código de transmissão, ele será inútil para futuros acessos, uma vez que o sistema já passou para um novo código. Essa abordagem torna muito mais desafiador clonar o controle

remoto ou realizar ataques de repetição, pois o código capturado não tem utilidade fora do contexto imediato.

O "rolling code" é uma camada adicional de segurança importante para proteger contra a clonagem não autorizada de dispositivos de controle remoto e é amplamente usado em sistemas de segurança para veículos e residências. No entanto, é importante que os fabricantes implementem o "rolling code" de forma adequada, pois falhas na implementação podem comprometer a segurança do sistema.

MAN IN THE MIDDLE (QUEBRANDO O ROLING CODE)

realizar um ataque "Man-in-the-Middle" (MitM) em um sistema "rolling code" é altamente desafiador e, em muitos casos, inviável devido às características de segurança do "rolling code", é importante entender como esse tipo de ataque funcionaria em teoria.

Aqui está uma descrição teórica de como um ataque MitM poderia ser tentado em um sistema "rolling code":

Interceptação do Sinal: O atacante precisaria interceptar um sinal de controle remoto enquanto ele está sendo transmitido do controle remoto ao dispositivo receptor, como o receptor do portão de garagem ou do veículo.

Repetição do Sinal Original: O atacante gravaria o sinal de controle remoto interceptado e, em seguida, tentaria repeti-lo na tentativa de enganar o receptor. Isso poderia ser feito com um equipamento especializado de transmissão de RF.

Problema da Sincronização: A principal dificuldade aqui é que o atacante precisaria interceptar e repetir o sinal em um momento específico. Isso ocorre porque os códigos "rolling code" são gerados sequencialmente, e a sincronização entre o controle remoto e o receptor é crucial. Se o atacante não repetir o sinal no momento certo, ele será inútil.

Prevenção de Ataques MitM: Para prevenir esse tipo de ataque, muitos sistemas "rolling code" possuem mecanismos de prevenção contra repetição. Isso significa que o receptor só aceitará o código uma vez, e não funcionará em transmissões subsequentes do mesmo código. Além disso, a sincronização entre o controle remoto e o receptor normalmente é estabelecida durante o emparelhamento inicial e, portanto, é difícil para um atacante acompanhar.

Em resumo, embora seja teoricamente possível tentar um ataque MitM em um sistema "rolling code," as medidas de segurança implementadas, como a sequencialidade dos códigos e a sincronização, tornam esse tipo de ataque extremamente difícil na prática. Os fabricantes de sistemas "rolling code" projetam suas tecnologias com foco na segurança e na prevenção de ataques MitM. Além disso, tentar realizar esse tipo de ataque é ilegal e antiético. A segurança cibernética deve ser usada para proteger e defender, não para prejudicar.

,

ESTAÇÃO 5

Carros

O carro inteligente é uma fusão entre o carro independente e o carro conectado, oferecendo uma série de recursos avançados. Ele é capaz de dirigir de forma independente, com níveis de automação altos (nível 4) ou completos (nível 5), o que significa que o veículo pode realizar a maioria das funções de condução com segurança, com ou sem intervenção do condutor. Além disso, o carro inteligente está conectado à Internet, fazendo parte da Internet das Coisas (IoT), permitindo que os passageiros acessem informações sobre o veículo, sua localização e dados técnicos. Você também pode notificar os serviços de emergência em caso de acidente e entrar em contato com uma oficina ou revendedor em caso de problemas mecânicos.

No entanto, o desenvolvimento de carros autônomos enfrenta desafios, incluindo a habilidade dos passageiros em se adaptarem a apenas passageiros e não motoristas. Além disso, há questões técnicas a serem resolvidas, como o aprimoramento do desempenho e do software, mapas mais avançados, sensores mais precisos e eficientes, e melhor comunicação entre veículos e infraestrutura.

Vários países, incluindo os Estados Unidos, o Reino Unido e os Países Baixos, estão investindo em tecnologias de carros inteligentes, mas o verdadeiro avanço deve ser liderado pelos fabricantes de automóveis. Muitos deles planejam testar veículos autônomos de nível 3 ou 4 em torno de 2021, que ainda terão a opção de condução manual em estradas específicas. Os veículos de nível 5, totalmente independentes, podem demorar mais para se tornarem disponíveis.

Um carro inteligente é capaz de dirigir autonomamente e ter conexão à Internet para compartilhar acesso à rede com passageiros. Além disso, ele permite o acesso a configurações específicas do carro por meio de dispositivos localizados no interior e remotamente. Pode se comunicar com sistemas de navegação por satélite para compartilhar dados de tráfego e sugerir desvios para evitar congestionamentos. Também oferece recursos como ligar o ar condicionado antes da chegada do motorista, acender as luzes externas e reservar hotéis, vagas de estacionamento ou restaurantes.

Além disso, você pode programar revisões ou manobras mecânicas e reportar variações tanto ao proprietário quanto às oficinas parceiras.

Existem várias soluções para tornar um carro inteligente. Uma delas é o Echo Auto, uma inteligência artificial da Alexa da Amazon projetada para motoristas. Ele se conecta ao carro via Bluetooth ou cabo de áudio e pode funcionar como assistente de voz e sistema de navegação, integrando-se com aplicativos como Apple Maps, Google Maps e Waze.

Outras soluções incluem dispositivos de hardware que utilizam a tecnologia head-up display (HUD) para projetar informações no para-brisa, semelhantes às usadas em aeronaves militares. Alguns desses dispositivos são conectados a smartphones e podem exibir dados de navegação, velocidade, previsão do tempo e entretenimento durante viagens. Além disso, existem aplicativos que se conectam a adaptadores inseridos na porta de diagnóstico de bordo (ODB) do carro, permitindo a visualização de informações como distância percorrida, velocidade, consumo de combustível e status do motor, funcionando como um sistema de diagnóstico.

Carros Inteligentes

No futuro dos carros, a revolução está em andamento, com avanços tecnológicos como carros conectados, autônomos, elétricos e sistemas de inteligência artificial. Até 2025, espera-se um foco na ecologia, conveniência, segurança e acessibilidade, impulsionado pela pressão por redução de emissões e crescimento urbano. A indústria automobilística deve se tornar mais inteligente e funcional, com motores eficientes e materiais leves, graças ao 5G e sistemas autônomos avançados.

Até 2030, megatendências incluem conectividade total, carros adaptados para idosos, veículos elétricos ecológicos, experiências de direção aprimoradas e personalização com base em sinais biológicos e emocionais dos motoristas. Em 2040, prevê-se que os carros de combustão sejam substituídos por veículos elétricos. Carros particulares podem se tornar símbolos de status luxuosos, com a economia compartilhada predominante.

Os carros terão espaços de trabalho, sistemas avançados de infoentretenimento, comandos por voz e gestos, e serão controlados principalmente pelo computador de bordo. Os carros poderão se comunicar com as estradas, outros carros e infraestruturas, oferecendo viagens eficientes e serviços de mobilidade.

Sistemas Avançados de Assistência ao Motorista (ADAS):

Desenvolvimentos recentes na segurança veicular estão concentrados em sistemas de segurança ativa, conhecidos como ADAS. Esses sistemas incluem sensores e dispositivos eletrônicos que auxiliam os motoristas em situações de direção, como sensores de chuva, controle de cruzeiro adaptativo, frenagem autônoma de emergência, assistência de estacionamento, assistência de faixa e reconhecimento de sinais de trânsito. A introdução de tais sistemas visa melhorar a segurança rodoviária, reduzir acidentes e proteger os ocupantes dos veículos. A União Europeia busca melhorar a segurança rodoviária por meio da automação e inovação tecnológica, com o objetivo de reduzir pela metade o número de acidentes nas estradas da Europa.

Fornecimento de Energia e Carregamento de Carros Elétricos:

A transição dos veículos movidos a combustíveis fósseis para veículos elétricos traz desafios relacionados à infraestrutura de recarga e ao fornecimento de energia. O aumento da demanda por energia elétrica requer melhorias na produção de energia a partir de fontes renováveis e infraestrutura de recarga expandida. O conceito de "Veículo para a Rede" (V2G) é proposto para equilibrar a carga na rede elétrica. No entanto, essa solução também apresenta desafios, como o desgaste das baterias dos veículos. A autonomia dos carros elétricos e o tempo de recarga também são preocupações importantes.

Estudo de caso Jeep Cherokee (Charlie Miller e Chris Valasek)

Em 2015, Chris Valasek e eu demonstramos a invasão remota do meu Jeep Cherokee 2014. Exploramos uma vulnerabilidade na unidade principal produzida pelo fornecedor Harmon Kardon (Figura 1). Após essa exploração inicial, reprogramamos um chip de gateway na unidade principal para permitir o envio de mensagens CAN (Controller Area Network) arbitrárias. Após uma pesquisa

adicional, conseguimos controlar aspectos físicos do carro, como direção e freios em alta velocidade.

De muitas maneiras, esse foi o pior cenário imaginável. Da minha sala de estar, poderíamos comprometer qualquer um dos 1,4 milhões de veículos localizados em qualquer lugar dos Estados Unidos. Isso não exigia interação do usuário ou configuração especial nos veículos; o único requisito para o ataque era que o veículo estivesse ligado.

O ataque era quase invisível para o motorista e deixava quase nenhuma evidência forense. Foi uma excelente demonstração de por que a cibersegurança automotiva é um tópico tão importante. Agora, depois de mais de três anos, tive tempo para refletir sobre essa experiência e tirar conclusões. Uma das percepções é a importância da assinatura de código para verificar o software nos sistemas eletrônicos. unidades de controle (ECUs) no veículo. Tanto em nosso ataque quanto em uma exploração demonstrada posteriormente em um Tesla Model S, havia um gateway que impedia a unidade principal comprometida de enviar mensagens CAN diretamente.

Em ambos os casos, os atacantes conseguiram simplesmente reprogramar o gateway, uma vez que ele não realizava nenhuma verificação do código usado para reprogramá-lo. Se o gateway estivesse realizando verificação do código, teria tornado um ataque de ponta a ponta significativamente mais difícil de ser realizado. Na verdade, teria sido muito mais difícil, e duvido que Chris e eu teríamos continuado a pesquisa além desse ponto, e teríamos mostrado apenas a invasão da unidade principal sem demonstrar como afetar fisicamente o veículo ao enviar mensagens CAN.

Outro ponto que fica claro com a reflexão é que, não importa o quanto tentemos e quão complexas sejam as soluções de segurança nos veículos, é impossível tornar algo perfeitamente seguro e à prova de invasão. Portanto, a segurança de um veículo não deve depender apenas da prevenção de ataques, mas também deve projetar sistemas que possam detectar ataques e tomar medidas apropriadas. Durante a pesquisa no Jeep, atacamos com sucesso o Jeep centenas de vezes, reprogramamos as ECUs dezenas de vezes e desativamos várias funcionalidades dos veículos mais vezes do que consigo me lembrar.

Apesar de todo esse comportamento anômalo, o Jeep nunca entrou em contato com a Chrysler para relatar um problema ou tomar qualquer ação defensiva significativa. Idealmente, se um ataque fosse detectado, o motorista poderia ser notificado e ações poderiam ser tomadas pelo veículo, como automaticamente desativando algumas funcionalidades avançadas especialmente suscetíveis à manipulação. Isso leva ao próximo ponto sobre a cibersegurança de automóveis.

Eu adoraria ver mais comunicação entre os fabricantes de automóveis e pesquisadores externos na academia e na indústria. Por exemplo, após a exploração do Tesla Model S por um grupo de pesquisadores do Keen Security Lab, a Tesla adicionou a assinatura de código à sua gateway. Seria ótimo saber quantos outros fabricantes também adicionaram a assinatura de código às suas unidades de controle eletrônico (ECUs), e além disso, quantas de suas diferentes ECUs exigem que o código seja assinado antes de ser reprogramado. Da mesma forma, quantos fabricantes de automóveis possuem gateways entre suas unidades principais e a direção, quantos têm gateways entre a porta OBDII e a direção e quantos têm algum tipo de detecção de anomalias em sua rede CAN? Estes são dados que não estão disponíveis para nós e provavelmente nem mesmo são compartilhados entre os fabricantes. A divulgação dessa informação poderia incentivar os fabricantes a adicionar segurança, ao mesmo tempo em que forneceria lições aprendidas com o sucesso e o fracasso dessas tecnologias. Também forneceria informações aos consumidores que tentam comprar o veículo mais resistente a ciberataques.

Embora a demonstração da vulnerabilidade do Jeep tenha suscitado muita discussão sobre a cibersegurança automotiva, de certa forma, não foi um completo sucesso. A maior decepção desde que começamos a fazer pesquisa automotiva é a falta de pesquisas semelhantes realizadas por outros grupos. Chris e eu lançamos diversos artigos, totalizando mais de 300 páginas, bem como todas as nossas ferramentas que utilizamos. Esperávamos que isso iniciasse um grande número de pesquisadores nesse importante espaço.

Esperávamos ver vários artigos sobre como controlar fisicamente outros veículos usando mensagens CAN, bem como outras maneiras de explorar veículos remotamente. Infelizmente, o único grupo que produziu trabalhos semelhantes parece ser o Keen Security Lab da China, que explorou o Tesla discutido acima em 2016. O campo da pesquisa de segurança automotiva ofensiva não avançou significativamente nos últimos anos. Até entendermos melhor os ataques, será difícil projetar defesas eficazes.

Entendo que a pesquisa em segurança automotiva tem uma grande barreira de entrada, mas ainda tenho esperança de que no futuro mais pessoas continuem a pesquisar neste campo. No final, a boa notícia é que não precisamos de novas ideias ou tecnologias fundamentais para proteger automóveis. Podemos tratar os veículos como pequenas redes de computadores e aplicar as tecnologias e técnicas do mundo da segurança empresarial para proteger veículos com conceitos bem estabelecidos, incluindo minimização da superfície de ataque, verificação de código em execução em sistemas, segregação de redes e detecção de anomalias. Não precisamos de novas ideias, em vez disso, precisamos nos concentrar e aplicar mecanismos de segurança que já conhecemos, mas de maneira completa e cuidadosa. Afinal, se não conseguirmos proteger veículos, o resultado não será limitado ao roubo de informações de cartões de crédito."

Firmware Infectado

Os veículos modernos passaram de sistemas mecânicos tradicionais para sistemas de controle eletrônico, executando uma grande quantidade de software e hardware. Em alguns veículos de alta qualidade, mais de 100 unidades de controle eletrônico (ECUs) são usadas para funções complexas de segurança e conforto. Com o avanço dos veículos autônomos, é esperado que o número de componentes eletrônicos nos veículos continue a crescer. No entanto, o aumento no uso de tecnologia da informação e comunicação (TIC) introduz novas questões de segurança. Ameaças de segurança de dentro e fora do veículo podem afetar a privacidade do sistema e, em casos extremos, a segurança da vida, como quando um invasor assume o controle do sistema de controle dinâmico do veículo.

A operação estável dos sistemas de segurança automotiva é fundamental para garantir a segurança de motoristas e passageiros. Com a crescente conectividade dos veículos, alguns sistemas não essenciais para a segurança tornam-se críticos em veículos conectados. Por exemplo, se o banco do motorista recuar inesperadamente, o motorista pode não conseguir frear em caso de emergência.

No passado, os engenheiros automotivos concentravam-se na pesquisa de sistemas críticos de segurança para evitar falhas, mas a segurança desses sistemas não recebia a mesma atenção. O sistema de segurança do veículo é composto por diversos componentes eletrônicos, como controladores, sensores e atuadores, interconectados por várias redes internas, como redes de área de controle (CANs) e redes de interconexão local (LINs). Essas redes, originalmente projetadas para ambientes fechados, tornaram-se vulneráveis a ataques maliciosos à medida que a conectividade aumentou.

O texto enfatiza a necessidade urgente de estudar métodos abrangentes de defesa de segurança para esses sistemas críticos de veículos. As funções implementadas pelo software nos veículos estão aumentando a uma taxa de cerca de 30% ao ano, o que torna o gerenciamento das funções do veículo um grande desafio em termos de tempo real, segurança e segurança.

Com o desenvolvimento de sistemas avançados de assistência à direção, tecnologia de direção automática e tecnologia V2X, os cenários de ameaças à segurança enfrentados pelos veículos se tornaram mais complexos e impactantes. Portanto, é necessário um método sistemático para avaliar as ameaças de cibersegurança dos sistemas críticos de segurança em veículos conectados. Embora o J3061 tenha recomendado muitos métodos orientadores para análise de segurança de veículos, esses métodos são subjetivos e carecem de resultados de análise quantitativa. Na fase inicial do desenvolvimento automotivo, ainda é necessário um método de análise de ameaças de segurança quantitativa em nível de sistema.

O artigo fornece uma visão geral dos carros inteligentes, abordando o estado atual da tecnologia e suas perspectivas futuras. Ele também explora a relação entre carros inteligentes e redes 5G, bem como as evoluções esperadas nos sistemas avançados de assistência ao motorista (ADAS) e nos motores.

Estação 6

As redes PLC (Power Line Communication), ou Comunicação por Rede Elétrica, representam uma alternativa notável no campo das telecomunicações e da conectividade. Essa tecnologia possui uma vantagem significativa: a capacidade de transmitir dados através da infraestrutura elétrica preexistente, eliminando a necessidade de instalar novos cabos ou linhas de comunicação. Esta abordagem inovadora utiliza os cabos elétricos que já percorrem residências, edifícios e infraestruturas elétricas para transmitir informações, como internet, voz e dados.

Uma das vantagens mais notáveis das redes PLC é a disponibilidade de uma grande quantidade de tomadas elétricas em ambientes residenciais e comerciais. Isso significa que a infraestrutura necessária para a implementação de uma rede PLC já está amplamente disseminada, tornando-a uma opção atraente para ampliar a conectividade e a cobertura de redes de comunicação.

Estudo de caso (Ucrânia)

Empresas de segurança estão divulgando os primeiros detalhes sobre um ataque cibernético que teria causado um apagão e cortado parte do abastecimento de energia de Kiev, capital da Ucrânia, no dia 17 de dezembro.

Este é o segundo apagão elétrico causado por hackers. O primeiro ocorreu também na Ucrânia em 23 de dezembro de 2015. A ISSP, uma empresa de segurança ucraniana que conduz a investigação para a companhia de energia Ukrenergo, vê uma ligação entre este ataque e seu antecessor.

O vírus responsável pelo ataque é chamado de "BlackEnergy". Segundo uma reportagem do site "Motherboard", o novo ataque foi menos agressivo que o realizado em 2015. Na época, os invasores utilizaram ferramentas para destruir completamente os terminais dos operadores e a possibilidade de restauração remota do sistema, o que exigiu a presença física de técnicos nas subestações para religar a energia. Desta vez, a destruição não ocorreu.

De acordo com a "BBC", o apagão durou pouco mais de uma hora. Por causa do volume de dados que precisa ser analisado, porém, a investigação do incidente pode levar meses até ser concluída.

Há um temor de a Ucrânia esteja sendo usada como "campo de testes" para ataques em outros países, já que a tecnologia usada para gerenciar a rede elétrica é bastante semelhante em outros lugares. Reconhecendo a semelhança com o ataque de 2015, a ISSP também afirmou que o novo foi "mais organizado", segundo a "BBC".

Especialistas e investigadores não apontam claramente a origem do ataque, mas autoridades ucranianas culpam a Rússia por diversos ataques e incidentes cibernéticos no país.

O próprio presidente da Ucrânia, Petro Poroshenko, acusou a Rússia de estar em uma "guerra cibernética" contra o seu país, de acordo com um comunicado

do governo em dezembro. As ações também foram classificadas como "atos de terrorismo". Instituições no país teriam sofrido um total de 6,5 mil ataques nos dois +últimos meses de 2016, segundo o governo.

Ataque Phishing

O ataque phishing consiste em tentativas de fraude para obter ilegalmente informações como número da identidade, senhas bancárias, número de cartão de crédito, entre outras, por meio de e-mail com conteúdo duvidoso.

O phishing começa, geralmente, com um e-mail fraudulento ou outra comunicação destinada a atrair a vítima. A mensagem parece ter vindo de um remetente confiável. Se isso engana a vítima, ela é persuadida a fornecer informações confidenciais geralmente em um site fraudulento.

Assim como a grande maioria dos golpes cibernéticos, o phishing apresenta certa complexidade, e por isso, os ataques acontecem em etapas. Nesse caso são seis: planejamento, preparação, ataque, coleta e fraude.

Um ataque de phishing bem-sucedido pode ter sérias consequências. Entre elas roubo de dinheiro, cobranças fraudulentas em cartões de crédito, perda de acesso a fotos, vídeos e arquivos, e até mesmo os cibercriminosos podem se passar por você e colocar outras pessoas em risco.

Como identificar um e-mail phishing

Sites ou e-mails de phising pedem nome de usuário, senha ou alteração de senha, CPF ou CNPJ, número de conta bancária, número de cartão de crédito, nome completo de pai e mãe, data de aniversário ou outra informação pessoal. Na dúvida, não forneça nenhuma informação.

Se você receber um email de phishing:

- Nunca clique em links ou anexos em emails suspeitos. ...
- Se a mensagem suspeita parece vir de uma pessoa que você conhece, entre em contato com essa pessoa por outros meios, como mensagem de texto ou chamada telefônica, para confirmar.
- Denuncie a mensagem (veja abaixo).
- Exclua.

Ataque malware

Malware significa "malicious software" (software mal-intencionado), incluindo qualquer software que aja contra os interesses do usuário. Um malware pode afetar não apenas o computador ou dispositivo infectado, mas qualquer outro aparelho que se conecte a ele. Embora malware não possa danificar o hardware físico dos sistemas e equipamentos de rede (com uma exceção conhecida, ele pode roubar, criptografar ou excluir seus dados, alterar ou sequestrar funções essenciais do computador e espionar a atividade de seu computador.Os sinais mais comuns de que você pode estar infectado é quando o seu computador passa a ficar lento de forma inexplicável ou apresentar comportamento fora do padrão esperado.

Entre os sintomas comuns de infecção por malware no site estão: redirecionamentos de URL indesejados, anúncios pop-up, alteração nos resultados de pesquisa, adição de barras de pesquisa laterais ou barras de ferramentas indesejadas em navegadores e baixa velocidade do computador.

Como remover o malware como vírus, spyware ou software de segurança invasor:

- Instalar as atualizações mais recentes do Microsoft Update. ...
- Usar o Verificador de Segurança da Microsoft. ...
- Usar a Ferramenta de Remoção de Software Mal-Intencionado do Windows.
- Remover manualmente o software de segurança não autorizado.

Ataque de negação de serviço

Os ataques de negação de serviço distribuídos, conhecidos como DDoS (Distributed Denial of Service, em inglês), são uma forma de ataque cibernético que tem como objetivo sobrecarregar um servidor, rede ou serviço com um grande volume de tráfego de dados, tornando-os inacessíveis para usuários legítimos.

Ao saturar um servidor visado com uma enorme quantidade de pacotes, um ator malicioso pode saturar demais a capacidade do servidor, resultando em negação de serviço. Para que a maioria dos ataques de inundação DoS tenha sucesso, o ator malicioso deve ter mais largura de banda disponível do que o alvo.

Um dos ataques mais comuns e capazes de gerar altos prejuízos para os gestores de TI desavisados é o DDoS - um crime bastante antigo.

ESTAÇÃO 7

A ascensão da era digital trouxe consigo desafios significativos em relação à proteção de dados pessoais, impulsionando a criação de leis robustas em diferentes partes do mundo. Duas dessas legislações proeminentes são a Lei Geral de Proteção de Dados (LGPD), em vigor no Brasil desde 2020, e a Regulação Geral de Proteção de Dados (GDPR), implementada na Europa em 2018. Este texto busca explorar as semelhanças, diferenças e a importância dessas leis no contexto contemporâneo. Dados pessoais, no contexto da LGPD, nada mais são do que informações. Quando damos uma informação a uma pessoa, permitimos que ela, com esse dado, forme sua própria ideia sobre aquele assunto.

Logo, os dados pessoais são as informações relativas à pessoa, que permitem sua identificação, ou, como consta da LGPD, “informação relacionada à pessoa natural identificada ou identificável”. São considerados dados pessoais aqueles que comumente fornecemos em um cadastro, como nome, RG, CPF, gênero, data e local de nascimento, filiação, telefone, endereço residencial, cartão ou dados bancários. Mas também são dados pessoais algumas informações que nem sempre fornecemos de forma consciente, como localização via GPS, retrato em fotografia, prontuário de saúde, hábitos de consumo, endereço de IP (Protocolo da Internet) e cookies.

Ao explorar o conceito de "Cidades Inteligentes," o texto amplia o escopo, evidenciando a aplicação dessas leis em ambientes urbanos planejados, inovadores e sustentáveis. O avanço tecnológico, especialmente no reconhecimento facial, é discutido como uma ferramenta cada vez mais utilizada, embora apresente desafios significativos, como a possibilidade de discriminação e vulnerabilidades à segurança. Dois estudos de caso, um sobre a startup Clearview AI e outro sobre a multa aplicada ao Facebook, ilustram desafios reais na implementação dessas leis. O vazamento de dados da Clearview AI destaca as preocupações sobre a segurança e proteção das informações, enquanto a multa aplicada ao Facebook destaca os desafios enfrentados por empresas na transferência internacional de dados, conforme exigido pelo GDPR.

LGPD E OUTRAS LEIS

A LGPD (Lei Geral de Proteção de Dados) e a GDPR (General Data Protection Regulation) são leis muito similares. Mas isto não acontece à toa, já que a GDPR, na Europa, foi a base de inspiração para a criação da LGPD, no Brasil. Inclusive, há quem diga que a GDPR é a irmã mais velha da LGPD.

Tanto a LGPD quanto a GDPR são leis de proteção de dados. De maneira geral, as duas leis procuram determinar a maneira como empresas e organizações devem tratar dados pessoais. Isto é, como elas devem coletar, processar, compartilhar e fazer uso das informações de terceiros.

Por falar nisso, o tratamento de dados, de acordo com a LGPD e a GDPR, deve sempre respeitar alguns princípios básicos, como a segurança dos dados, o uso ético das informações e a garantia dos direitos dos titulares dos dados. Portanto, como se pode perceber, os propósitos da LGPD e da GDPR são praticamente os mesmos. Mas há alguns pontos e diferenças que são interessantes de serem analisados e destacados, até pelo contexto em que as leis estão inseridas.

A GDPR foi implementada em 2018, enquanto a LGPD entrou em vigor apenas em 2020. As empresas que não estiverem em cumprimento com a LGPD podem sofrer ações, sanções e multas de até 2% da receita da empresa no ano anterior, limitada a R$ 50 milhões por incidente (Artigo 52).

Por que essa lei é importante para você?

Os dados pertencem ao seu titular e não às empresas que os coletam, armazenam ou tratam, por isso a lei coloca em destaque a proteção da sua privacidade e a necessidade de transparência e uso adequado no tratamento do dado.A LGPD inaugura no Brasil um novo olhar sobre um direito fundamental do indivíduo, que é a proteção de seus dados pessoais. A evolução tecnológica ampliou o uso de dados, para as mais diversas finalidades, por pessoas, empresas e governos. Os modelos de negócios estão cada vez mais dependentes de dados, em especial de dados pessoais.O objetivo da Lei é

regular a utilização dos seus dados pelas empresas, estabelecendo princípios gerais de proteção, privacidade, transparência e tratamento adequado dos seus dados.

O que são dados pessoais e dados pessoais sensíveis?

De acordo com a LGPD, dado pessoal é a informação relacionada à pessoa natural identificada – tais como nome, sobrenome, RG e CPF – ou identificável, como no caso dos dados de geolocalização (GPS), endereço IP, identificação de dispositivo etc. Adicionalmente, a Lei traz o conceito de dado pessoal sensível, que diz respeito à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

CIDADES INTELIGENTES

"CIDADES INTELIGENTES" são cidades comprometidas com o desenvolvimento urbano e a transformação digital sustentáveis, em seus aspectos econômico, ambiental e sociocultural, que atuam de forma planejada, inovadora, inclusiva e em rede, promovem o letramento digital, a governança e a gestão colaborativas e utilizam tecnologias para solucionar problemas concretos, criar oportunidades, oferecer serviços com eficiência, reduzir desigualdades, aumentar a resiliência e melhorar a qualidade de vida de todas as pessoas, garantindo o uso seguro e responsável de dados e das tecnologias da informação e comunicação".

Segundo a União Européia, Smart Cities são sistemas de pessoas interagindo e usando energia, materiais, serviços e financiamento para catalisar o desenvolvimento econômico e a melhoria da qualidade de vida. Esses fluxos de interação são considerados inteligentes por fazer uso estratégico de infraestrutura e serviços e de informação e comunicação com planejamento e gestão urbana para dar resposta às necessidades sociais e econômicas da sociedade. De acordo com o Cities in Motion Index, do IESE Business School na Espanha, 10 dimensões indicam o nível de inteligência de uma cidade: governança, administração pública, planejamento urbano, tecnologia, o meio-

ambiente, conexões internacionais, coesão social, capital humano e a economia. Apesar de ser um conceito relativamente recente, o conceito de Smart City já se consolidou como assunto fundamental na discussão global sobre o desenvolvimento sustentável e movimenta um mercado global de soluções tecnológicas, que é estimado a chegar em US$ 408 bilhões até 2020.

Atualmente, cidades de países emergentes estão investindo bilhões de dólares em produtos e serviços inteligentes para sustentar o crescimento econômico e as demandas materiais da nova classe média. Ao mesmo tempo, países desenvolvidos precisam aprimorar a infraestrutura urbana existente para permanecer competitivos. Na busca por soluções para esse desafio, mais da metade das cidades europeias acima de 100.000 habitantes já possuem ou estão implementando iniciativas para se tornarem de fato Smart Cities.

RECONHECIMENTO DE IDENTIDADE POR IMAGENS

A biometria facial é uma tecnologia feita por inteligência artificial que tem por objetivo verificar os aspectos faciais de uma pessoa. Sua categoria de software realiza esse armazenamento como uma impressão digital facial por meio de algoritmos que comparam a imagem digital com a real armazenada, possibilitando validar a identidade e o reconhecimento do usuário. Essa tecnologia é construída em diversas camadas de segurança, respeitando os requisitos da Lei Geral de Proteção de Dados (LGPD), garantindo o sigilo feito por meio de um dispositivo eletrônico. Os dados do usuário precisam ser preservados e navegar por um local seguro. O sistema é tão eficaz que consegue acompanhar as mudanças do ser humano mesmo com o passar dos anos, o que é muito seguro. Falaremos mais adiante sobre isso. Validar identidade é um recurso que tem sido cada vez mais utilizado pelas empresas, sendo uma ferramenta que está totalmente ligada aos protocolos de segurança digitais das plataformas de uma instituição. Quando o usuário realiza a sua biometria facial, instantaneamente no momento do cadastro, a organização pode solicitar futuramente autenticações que não exijam senhas. Diante de um mundo repleto de informações por conta da tecnologia, a proteção de dados tem sido cada vez

mais pauta das empresas que buscam por recursos confiáveis para se protegerem e preservarem seus usuários. A substituição de senhas tradicionais tem crescido no mercado e é uma das grandes tendências para os próximos anos, o que facilita processos, traz agilidade e muito mais segurança.

Como funciona a validação de identidade por selfie

A validação de identidade por selfie é uma fórmula que conecta comodidade e segurança. É utilizada para checar e validar transações onlines de diversas fontes. Por exemplo, pagamentos feitos com cartão de crédito, solicitação de aplicativos de transporte de passageiros ou mesmo check-in para um voo. Muitas empresas já têm utilizado esse serviço para assegurar que as solicitações foram de fato realizadas pelos seus clientes ou usuários.

Quando uma pessoa opta pela sua autenticação por selfie para a realização de uma compra ou serviço online, basicamente ele envia um registro automático das suas feições para uma instituição, como uma operadora de crédito ou um banco. Se a identificação for positiva, a compra ou serviço poderá ser realizado.

Validar identidade por foto é seguro?

A autenticação por selfie é considerada muito mais segura do que os procedimentos tradicionais que consistem em senhas ou códigos de solicitação. Afinal de contas, tanto o rosto como a impressão digital são únicos e exclusivos de uma pessoa, o que não acontece com senhas e tokens de segurança. Esse procedimento auxilia na prevenção de fraudes. É importante destacar que as fotos das pessoas não são armazenadas, mas sim as representações matemáticas criptografadas de seus rostos. Os algoritmos dividem as imagens em pixels mapeando os pontos nodais, que são informações que diferem uma pessoa da outra. Todo esse processo realizado por inteligência artificial garante toda a segurança e tranquilidade dos usuários e das empresas.

Desafios e limitações do uso de reconhecimento facial na verificação de identidade.

Apesar de suas vantagens, o uso de reconhecimento facial na verificação de identidade também apresenta alguns desafios e limitações. Um dos principais problemas é a possibilidade de discriminação. Alguns algoritmos de reconhecimento facial podem ter dificuldade em reconhecer características faciais de pessoas de certas raças, o que pode levar a erros de autenticação e a discriminação.

Além disso, a tecnologia de reconhecimento facial pode ser vulnerável a ataques de hackers e a fraudes por meio de fotos ou vídeos manipulados. Por isso, é importante que as empresas implementem medidas de segurança para garantir a integridade do sistema.

A verificação de identidade é um tema cada vez mais relevante no mundo digital e o reconhecimento facial se mostra uma tecnologia promissora para auxiliar na autenticação de documentos. Apesar de seus desafios e limitações, o uso de reconhecimento facial pode trazer diversos benefícios para a segurança das empresas e dos consumidores. Por isso, é importante que as empresas invistam em tecnologias de verificação de identidade mais robustas e seguras para proteger seus usuários e evitar prejuízos financeiros e de imagem.

ESTUDO DE CASOS (STARTUP CLEARVIEW AI)

A empresa norte-americana Clearview, especializada no desenvolvimento de tecnologia de reconhecimento facial para autoridades policiais, está informando aos seus clientes sobre um vazamento de dados. Este incidente expôs a lista de clientes da startup, detalhes sobre suas atividades no banco de dados e a quantidade de contas de acesso associadas a cada um. Embora a empresa tenha confirmado o ocorrido, ressaltou que seus servidores não foram comprometidos e que a vulnerabilidade foi prontamente corrigida. O advogado da Clearview, Tor Ekeland, comentou que, infelizmente, vazamentos de dados são comuns na era atual, em um comunicado ao site "CNET". A Clearview fornece uma solução de reconhecimento facial para autoridades policiais, apresentando-a como uma ferramenta para facilitar a identificação de suspeitos. O fundador, Hoan Ton-That, a descreveu como "uma ferramenta de busca para rostos", com a tecnologia baseada em um extenso banco de dados contendo três bilhões de imagens provenientes de sites como Facebook, YouTube, Venmo e outros milhões de páginas, conforme reportagem do "The New York Times".

A prática de coletar informações de redes sociais e sites públicos, conhecida como "raspagem" (scrapping), é geralmente proibida pelos termos de serviço, inclusive no Facebook, que anunciou estar investigando o incidente. Embora o banco de dados em si não tenha sido comprometido, a exposição da lista de clientes suscita dúvidas sobre a capacidade da empresa de proteger outras informações, especialmente ao prestar serviços ao governo. Já havia questionamentos nos Estados Unidos por parte de políticos e autoridades sobre o uso do produto devido aos métodos de coleta de dados e aos riscos para a privacidade. A divulgação do vazamento foi realizada pelo site "The Daily Beast", que teve acesso a uma notificação enviada pela empresa aos clientes. Conforme a legislação nos Estados Unidos, as vítimas de vazamentos de dados devem receber notificação do incidente. Embora a imprensa não tenha obtido acesso à lista de clientes vazada, sabe-se que o produto é utilizado por departamentos policiais em Atlanta e na Flórida (ambos nos EUA) e em Toronto (Canadá). Segundo a "Reuters", o aplicativo também é oferecido a instituições financeiras.

ESTUDO DE CASOS (MULTA FACEBOOK)

A empresa controladora do Facebook, a Meta, foi penalizada em 1,2 bilhão de euros (aproximadamente R$ 6,5 bilhões) devido à má utilização de dados de usuários durante sua transferência entre a Europa e os Estados Unidos. A decisão foi proferida pela Comissão de Proteção de Dados (DPC, em inglês) da Irlanda, marcando a imposição da maior multa até o momento sob as disposições de privacidade do Regulamento Geral de Proteção de Dados (GDPR, em inglês) da União Europeia. O cerne dessa determinação reside na utilização de cláusulas contratuais padrão (SCCs, em inglês) para a transferência de dados da União Europeia para os Estados Unidos. Estes contratos legais, desenvolvidos pela Comissão Europeia, incorporam medidas de proteção destinadas a garantir a contínua segurança dos dados pessoais quando são movidos para fora da Europa. Embora essas cláusulas contratuais ofereçam salvaguardas, persiste uma apreensão em relação à possibilidade de que os fluxos de dados ainda exponham os cidadãos europeus a leis de privacidade consideradas 9mais permissivas nos Estados Unidos. Este receio sublinha os desafios associados à transferência internacional de dados e destaca a necessidade de equilibrar as práticas de transmissão com a garantia da privacidade dos usuários, em conformidade com as regulamentações vigentes.