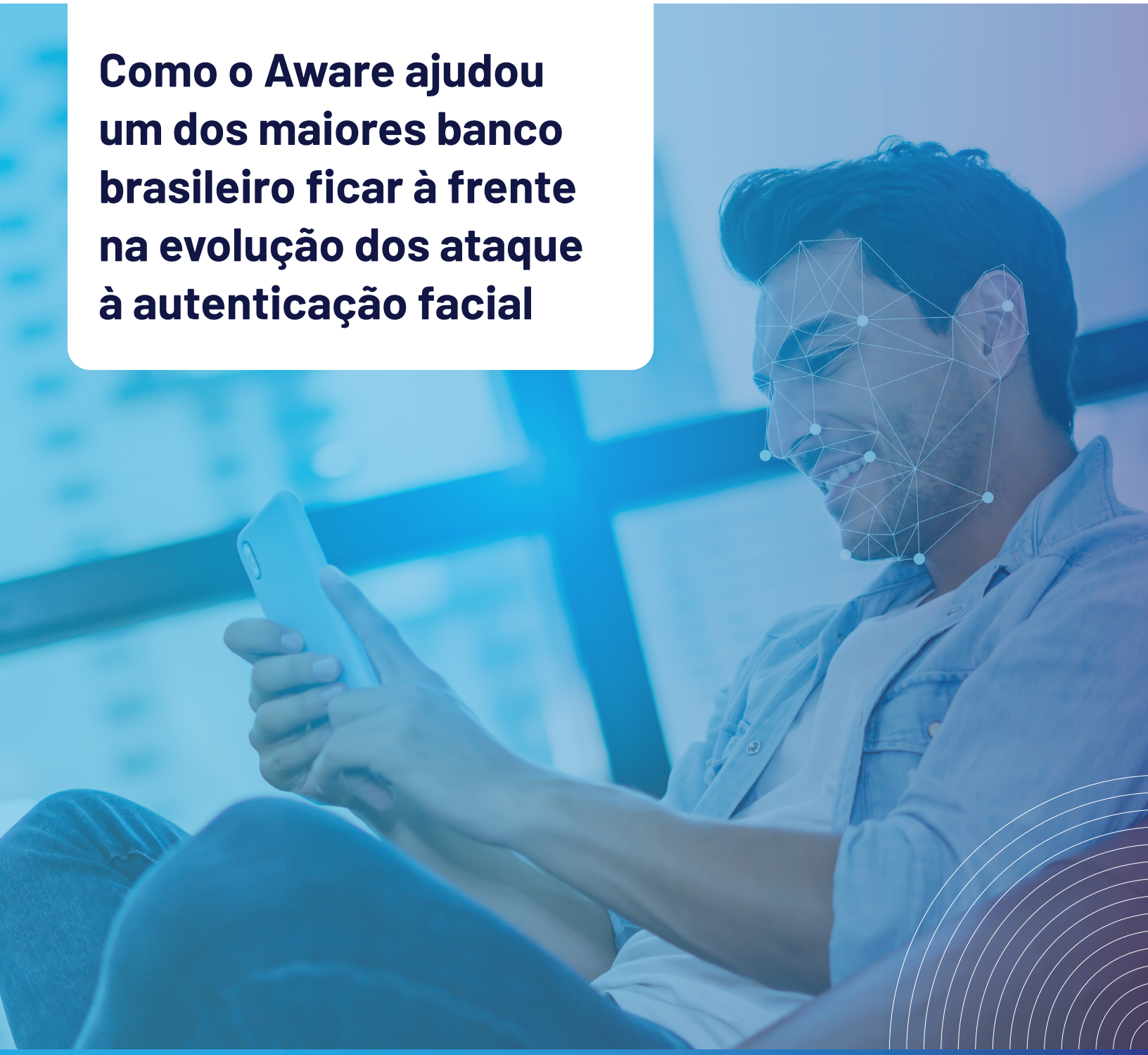
White Paper

Como o Aware ajudou um dos maiores banco brasileiro ficar à frente na evolução dos ataque à autenticação facial



AWARE

781.687.0300 | sales@aware.com | www.aware.com

A Aware é uma empresa líder global de produtos de software e soluções para identificação e autenticação biométrica. Os mesmos são utilizados em uma variedade de aplicações, incluindo serviços financeiros, segurança empresarial, gestão de fronteiras e segurança pública. A Aware é uma empresa de capital aberto (NASDAQ: AWRE) com sede em Burlington, Massachusetts.

Embora as senhas ainda sejam o método de autenticação mais comum para aplicativos de banco online e serviços financeiros móveis, elas também são altamente propensas ao uso indevido. Além disso, o atrito criado pelo processo de redefinição de senha continua sendo um problema real para os usuários.

O uso de uma a autenticação facial, é mais segura e eficaz na prevenção de fraudadores configurar contas falsas para lavagem e roubo de dinheiro de outras pessoas, com o benefício de melhorar a experiência do usuário.

Nos últimos anos, o uso da autenticação biométrica facial tornou-se dramaticamente mais preciso, rápido e resiliente às variáveis ambientais e do usuário. No entanto, a realidade é que os bancos ainda podem ser atacados e subvertidos se não houver tecnologia e serviços de suporte adequados. O tipo mais comum de ataque, muitas vezes chamado de "spoof" ou ataque de apresentação, pode enganar os sistemas de autenticação facial apresentando uma "máscara de rosto" de um usuário legítimo, que pode ser gerado prontamente através da fácil disponibilidade de imagens e vídeos de pessoas nas redes sociais.

Com mais de 60% das violações de dados devido a casos de senhas fracas ou roubadas, as organizações estão procurando alternativas mais seguras, como a biometria. No entanto, com a mudança da autenticação baseada em senha para a autenticação biométrica, muitas vezes ocorrem escaladas nas tentativas de violação.

Um exemplo é o trabalho da Aware com o sistema de autenticação de biometria facial de um grande banco brasileiro, muito popular entre seus usuários devido à sua alta eficiência e precisão. No entanto, este banco começou a perceber casos de ataques de apresentação ataques de injeção, que estavam penetrando o componente de autenticação facial de seu sistema de registro.

Neste white paper, exploraremos como a resposta rápida da Aware para implementar um sistema de várias camadas de aprimoramentos de segurança biométricos e não biométricos forneceu várias linhas de defesa contra esses ataques.

O problema do banco

Como muitas empresas de serviços financeiros líderes do setor, esse banco r estava usando autenticação facial para fornecer a seus clientes alta segurança e facilidade de uso.

Na verdade, esse banco tinha um sistema de autenticação de biometria facial antes de iniciar seu trabalho com o Aware e já havia sido alvo de fraudes usando fotografias de outras pessoas para falsificar o sistema. Em alguns casos, os titulares de contas tiveram suas fotos ou carteiras de identificação roubados e usados por invasores para criar contas fraudulentas. Como primeiro passo, a Aware trabalhou com o banco para implementar o Knomi Liveness Detection para garantir que apenas pessoas vivas pudessem configurar contas.

Os ataques de apresentação geralmente envolvem um fac-símile de um usuário autorizado – como uma imagem tirada do carteira de identificação de alguém ou mesmo um perfil de mídia social – sendo apresentado a uma câmera. O objetivo do hacker ou usuário não autorizado é induzir o dispositivo a pensar que está lendo o rosto da pessoa autorizada para que eles possam obter acesso fraudulento.

No entanto, com o passar do tempo, a sofisticação desses ataques de apresentação continuou aumentando. Em vez de usar fotos para configurar contas fraudulentas, os fraudadores começaram a produzir ataques de apresentação com imagens de alta qualidade, bem como deepfakes e morphs.

Ataques de apresentação mais sofisticados envolvem máscaras em vez de uma foto. Um invasor pode cortar os olhos de uma fotografia e apresentar seu rosto ao dispositivo de imagem ou até mesmo ter uma máscara 3D produzida especificamente para esse fim. O objetivo aqui é garantir que a vivacidade dos olhos e/ou a qualidade das máscaras dêem uma vantagem para ultrapassar a verificação biométrico.

E então, cerca de nove meses atrás, o banco começou a ver um tipo diferente de ataque: ataques de injeção destinados a frraudar o sistema de cadastro de clientes. Os ataques de injeção representavam um vetor de ataque totalmente diferente dos ataques de apresentação do mundo real que o banco havia experimentado inicialmente. Em vez de atacar a apresentação do usuário e os algoritmos que analisam essa apresentação, eles atacaram o software que realiza a captura em si.

As vulnerabilidades de injeção permitem que os invasores insiram entradas maliciosas ou relacionem códigos mal-intencionados por meio de um aplicativo em outro sistema. Durante um ataque de injeção, entradas não confiáveis ou código não autorizado são injetados em um programa, onde são interpretados como parte de uma consulta ou comando. O programa é então alterado, e essa alteração redireciona o programa para um propósito nefasto.

Os ataques de injeção são particularmente assustadores. O ataque pode atingir um sistema inteiro. Os ataques de injeção também são uma classe de vulnerabilidade incrivelmente bem difundida, o que significa que existem muitos recursos e ferramentas facilmente acessíveis que permitem que até invasores inexperientes explorem essas vulnerabilidades.

Solução da Aware

A Aware implementou três camadas de proteção adicional para impedir tentativas de burlar o componente de autenticação facial do sistema de cadastro do banco. A primeira camada foi proteger o aplicativo para que a integridade do processo de captura biométrica seja preservada. A segunda camada foi a análise dos dados biométricos para ataques de apresentação.

A terceira camada contou com as melhores práticas não biométricas para verificar a segurança dos dados biométricos dos usuários em cada uma das etapas a seguir. A Aware abordou os aspectos de segurança para todas essas diferentes partes da integração i:

- **Aquisição de dados:**
  No momento em que o dispositivo aceita dados de um usuário.
- **Segurança na transferência de dados:**
  Garantir que os dados do usuário sejam codificados e transferidos para onde serão processados.
- **Processamento de dados:**
  manter os dados codificados e seguros até que sejam devolvidos com a resposta.

Como resultado das medidas implementadas pela Aware, o banco viu imediatamente uma diminuição significativa no vetor de ataque de injeção.

Práticas recomendadas e lições

Existem várias lições do trabalho da Aware com este banco que outros devem considerar quando confrontados com a evolução dos vetores de ataque de autenticação biométrica:

Abordando a autenticação biométrica de forma holística:

A detecção de ataque de apresentação (PAD) é um componente crítico, mas apenas um elemento em um sistema de autenticação biométrica complexo que precisa fornecer um equilíbrio cuidadoso entre segurança e usabilidade. Uma solução bem-sucedida deve fornecer um conjunto abrangente de defesas que minimize o atrito, mas maximize a probabilidade de um resultado preciso e que possa se adaptar às ameaças em evolução.

Isso inclui:

1. Um método eficaz para controle de qualidade que motiva os usuários a otimizar sua apresentação para uma análise mais precisa, conforme fornecido pelo excelente recurso de captura automática do Aware
2. Um conjunto primário de algoritmos PAD sofisticados para detectar ataques de apresentação antes mesmo que eles entrem no subsistema biométrico, fornecido como parte da soluçãode vivacidade Knomi da Aware
3. Um conjunto secundário de algoritmos sofisticados de detecção de ataques de hackers para proteger o sistema contra ataques de emulador, injeção e funções que podem incluir deep fakes, morphs ou entradas de replay
4. Um método seguro de ponta a ponta que verifica a integridade de toda a transação
5. Por fim, uma infraestrutura de design de solução que permite uma abordagem altamente responsiva e adaptável a ameaças em constante evolução, cujo sucesso se reflete na posição de liderança da Aware em autenticação biométrica hoje

Proteções institucionais adicionais, como monitoramento de IDs de dispositivos (ou endereços IP) associados a transações frequentemente rejeitadas, manutenção de uma memória do número de contas diferentes acessadas pelo mesmo ID de dispositivo (ou endereços IP) e/ou uso de correspondentes para verificar identidades de todos os titulares de contas podem contribuir para garantir transações financeiras que desejam aproveitar ao máximo a tecnologia de autenticação biométrica.

A esse respeito, a importância de colaborar ativamente com as instituições participantes não

pode ser exagerada, pois o objetivo comum de autenticação facial altamente precisa e segura pode fornecer oportunidades de sinergia para o avanço ao estado da arte. A Aware se destaca em desenvolver e nutrir relacionamentos mutuamente benéficos, necessários para ter sucesso no ambiente complexo e dinâmico da autenticação biométrica.

Aprendendo com as realidades operacionais:

é fácil delinear o que pode ser feito no caso de um ataque de autenticação biométrica, mas isso é muito diferente de aplicar soluções no mundo real e em tempo real. Ao trabalhar com esse banco, a Aware conseguiu acessar esses vetores de ataque e aplicar medidas de proteção de forma direta e extremamente rápida.

Além disso, a Aware conseguiu aprimorar a eficácia e a precisão de seus algoritmos com base nos dados dos vetores de ataque fornecidos pelo banco. Essa relação sinérgica beneficiou os esforços da Aware e o trabalho de segurança do banco à medida que os vetores de ataque evoluíram.

Equilíbrio entre segurança e usabilidade:

Resolver problemas de segurança complexos e maximizar a usabilidade pode ser um equilíbrio difícil de atingir. A maioria dos bancos reconhece a necessidade de fazer trade-offs entre conveniência e segurança do cliente, na verdade, muitos veem isso apenas como o custo de fazer negócios. Como exemplo, a VISA ignora cerca de US$ 6 bilhões em fraudes por ano para manter seus sistemas de autenticação fáceis de usar.

Em outro exemplo, muitos bancos implantam mecanismos de proteção adicionais, como recursos de correspondência: Quando, depois que um indivíduo acessa uma conta, um mecanismo de correspondência compara continuamente a imagem facial do usuário com a imagem do titular da conta no arquivo. O limite de correspondência em muitos bancos é muito brando, tanto que, mesmo que um spoofer passe pelo ponto de verificação de autenticação inicial, o mecanismo de correspondência ainda não consegue determinar que o spoofer não é o titular da conta. Isso é feito especificamente para garantir uma experiência fácil para usuários legítimos.

A conclusão é que, ao implementar proteções de segurança, a usabilidade precisa ser valorizada tanto quanto o aspecto de segurança. Felizmente, a Aware forneceu ao banco o recurso de captura automática para a interação, o que proporcionou oportunidades para impactar diretamente a usabilidade de forma positiva.

Garantindo uma Parceria de Qualidade:

A Aware prioriza parcerias verdadeiras com seus clientes, principalmente nesta era digital, com ataques cibernéticos cada vez mais frequentes e mal-intencionados. Isso é particularmente verdadeiro no Brasil, que experimentou um enorme aumento nas interações móveis após o COVID-19 e, por sua vez, um grande aumento de vetores de ataque mais agressivos.

A estreita parceria da Aware com este banco—que envolveu cooperação nos níveis de segurança técnica e empresarial e compartilhamento de dados transacionais—foi um dos principais componentes para uma colaboração bem-sucedida e permitiu que o banco ficasse à frente dos vetores de ataque em evolução, a fim de perceber todos os benefícios de seu investimento em autenticação biométrica.

Resumo

As senhas ainda são o método de autenticação mais comum para a maioria dos aplicativos bancários on-line e de serviços financeiros móveis, mas são propensas ao uso indevido e o processo de redefinição de senha continua sendo um grande ponto de frustração para os usuários. À medida que os bancos aumentam sua receptividade às novas tecnologias de autenticação biométrica, eles precisam colaborar com seus parceiros de tecnologia para ficar um passo à frente das ameaças emergentes.

Aware forneceu a esse banco orientação dentro e fora do domínio da segurança biométrica e obteve um alto grau de sucesso. A Aware fará o que for preciso para ajudar, pois nada é mais importante para a empresa do que proteger os ativos confidenciais e valiosos de seus clientes corporativos e seus usuários contra ameaças insidiosas.

Esse tipo de parceria é essencial para o futuro da segurança biométrica, especialmente no mundo dos bancos e das fintechs. À medida que essas organizações continuam avaliando a autenticação biométrica, é vital que considerem fortemente a escolha do parceiro, e a maioria se beneficiará de um investimento em comunicação consistente e resposta proativa a ameaças em tempo real. Trabalhando juntos, o parceiro de tecnologia certo pode ajudar as organizações a obter o máximo de benefícios da autenticação biométrica - segurança superior combinada com a máxima conveniência que mantém os usuários fiéis à marca.

Quer saber mais? www.aware.com

AWARE

781.687.0300 | sales@aware.com | www.aware.com