Data: 13-01-2020

Título: Governo avança com reconhecimento facial, apesar de riscos. AMA não revela participantes do concurso

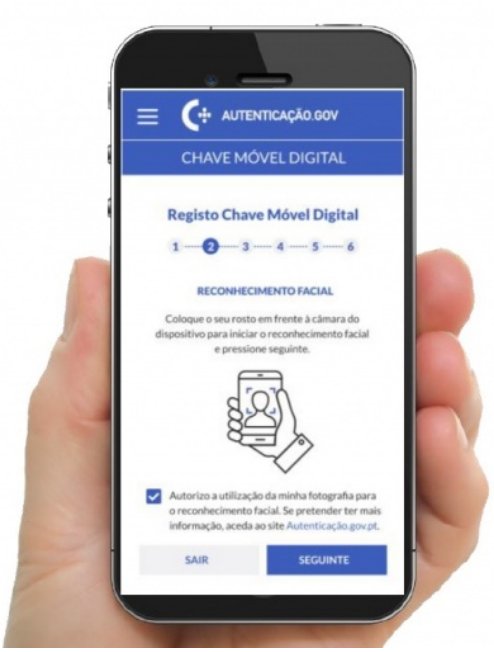
Pub: VISÃO

Tipo: Internet Secção: Nacional

Mercados
13.01.2020 às 10h21


Hugo Séneca

Governo avança com reconhecimento facial, apesar de riscos. AMA não revela participantes do concurso



Especialistas apontam vulnerabilidades na tecnologia de reconhecimento facial que a AMA pretende implementar para a autenticação da Chave Móvel Digital. AMA recorda que vão ser seguidas as normas de segurança mais avançadas e não revela propostas recebidas num concurso público que terminou na noite de consoada

A Agência para a Modernização Administrativa (AMA) vai avançar com um sistema de autenticação para a Chave Móvel Digital (CMD) que funciona com base no reconhecimento facial remoto, que pode ser efetuado através de câmaras de telemóvel do utilizador. Apesar dos alertas de segurança relativamente a estes sistemas que, na gíria, são conhecidos como liveness, a AMA lançou um concurso público no dia 10 de dezembro, para a escolha de fornecedores de uma solução com um teto máximo de 150 mil euros, mediante um contrato de três anos. O concurso terminou à meia-noite de 24 de dezembro, quando a maioria dos portugueses possivelmente estaria a festejar a consoada de Natal. O júri do concurso está atualmente a analisar propostas – mas não se sabe quantas foram rececionadas e que marcas concorreram. Apesar de se tratar de um concurso público anunciado no Diário da República, a AMA recusa fornecer qualquer dado sobre a matéria, invocando o enquadramento jurídico em vigor, sem especificar cláusulas ou as leis que justificam esta posição.

O "Concurso Público Nº235/19/DCP/GACD/Software de Reconhecimento Facial e Deteção de Vida" foi lançado pela AMA com o propósito de desenvolver uma ferramenta de autenticação facial através do telemóvel de cada internauta para fins de ativação e uso da CMD, que hoje é usada nos vários serviços da Administração Pública e até em alguns serviços bancários como o da Caixa Geral de Depósitos (CGD) ou do Millenium BCP. Segundo o caderno de encargos, a solução selecionada deverá permitir criar uma ferramenta de autenticação digital para cada cidadão, com base na captação de imagens do cartão do cidadão e também do rosto do utilizador na própria hora, a partir do telemóvel. Além de garantir a autenticação através de dados biométricos, a solução escolhida deverá estar apta a confirmar que as imagens dizem respeito a uma pessoa "ao vivo" (e não são fotos de "terceiros").

Apesar de acompanhar as tendências de mercado (a banca de nova geração já usa ferramentas similares para a abertura de contas), o concurso não se livrou da polémica – a começar pela fiabilidade da tecnologia de reconhecimento facial através dos telemóveis dos utilizadores.

«Estranhámos o lançamento de um concurso para um sistema de autenticação da CMD através de tecnologia de reconhecimento facial, apesar de se saber da possibilidade de falsificação. E estranhamos também que esta solução esteja associada ao cartão do cidadão», frisa Fernando Moreira, proprietário e administrador da DigitalSign, empresa que desenvolve e comercializa ferramentas para certificações e assinaturas eletrónicas.

Uma pessoa com conhecimento técnico conseguiria fazer este tipo de ataque. Não é trivial, mas também não é especialmente difícil

Ricardo Chaves

A DigitalSign não se apresentou a concurso – mas fora do circuito das empresas que operam nas certificações eletrónicas, há outras vozes que põem em causa a fiabilidade das tecnologias de liveness: depois de uma análise ao caderno de encargos do concurso, Ricardo Chaves, especialista em segurança eletrónica e professor no Departamento de Informática do Instituto Superior Técnico (IST), aponta aquela que, na sua opinião, será a principal vulnerabilidade técnica dos requisitos de segurança exigidos pela AMA: «O caderno de encargos não exige qualquer garantia de que os sistemas usados pelos telemóveis dos utilizadores não foram adulterados».

O próprio investigador do Técnico admite que os fornecedores que participam no concurso público não estão em condições de garantir que os telemóveis dos portugueses não foram adulterados – mas é essa incapacidade que, pelo menos em teoria, torna também impossível garantir que a nova ferramenta não será usada para o roubo de identidade e dados biométricos que funcionam como método de autenticação dos vários serviços públicos disponíveis na Internet: «O telemóvel pode ter sido adulterado por um "atacante" para enviar um filme do rosto de outra pessoa, em vez das imagens que a câmara capta nesse momento; e também é possível usar uma câmara de alta resolução que permite filmar outra pessoa à distância de alguns metros (sem que a potencial vítima

que é filmada se aperceba)», refere o especialista em cibersegurança, aludindo a alguns métodos possíveis para a exploração daquela que será a principal vulnerabilidade presente no caderno de encargos.

O software proposto tem de assegurar uma taxa de falsos positivos (False accept rate – FAR) inferior ou igual a 1 em 10 milhões. Tal assegura a qualidade da solução a adotar nunca será inferior à verificação efetuada no registo de CMD efetuada atualmente

Agência Para a Modernização Administrativa

As desconfianças quanto à ativação da autenticação facial remota não são exclusivas de Portugal: Em França, o sistema Alicem, que o governo gaulês pretendia implementar com o objetivo de criar uma nova ferramenta de reconhecimento facial para todos os cidadãos, motivou um parecer negativo da Comissão Nacional de Informática e Liberdades (CNIL, na sigla em francês), que supervisiona a proteção de dados no país, por não permitir que os cidadãos expressem o consentimento ou a recusa no tratamento de dados. Por estas e outras razões, um grupo ativista de defesa da privacidade iniciou um processo nos tribunais para tentar travar a implementação do sistema Alicem. A este dado junta-se outro, que não chega para confirmar que uma tecnologia é insegura, mas serve para lançar o alerta: não terá sido necessária mais de uma hora para um hacker alegar que conseguiu quebrar a tecnologia proposta pelo governo gaulês, recorda a Bloomberg.

A AMA reage à desconfiança de especialistas e marcas de certificação digital, lembrando que o recurso às tecnologias de liveness já havia sido determinado como uma medida do programa Simplex, que estipulava o uso de um sistema de biometria que opera remotamente com imagens captadas, na própria hora, por câmaras de telemóveis. A AMA também recorda que o concurso exige a «certificação ISO/IEC 30107 (Anti-Spoofing technology, também conhecido como Presentation Attack Detection) nível 1 e nível 2, ou equivalente – assegurando resistência a ataques com fotos, vídeos de alta resolução, máscaras de papel, máscaras 3D de resina, látex e silicone usadas por humanos».

«Adicionalmente, (…) o software proposto tem de assegurar uma taxa de falsos positivos (False accept rate – FAR) inferior ou igual a 1 em 10 milhões. Tal assegura a qualidade da solução a adotar nunca será inferior à verificação efetuada no registo de CMD efetuada atualmente. Finalmente, considerando a inovação da medida, a AMA prevê iniciar em regime de piloto a disponibilização desta funcionalidade de forma a permitir aferir e otimizar a segurança e experiência do utilizador e, em função destes resultados, aferir o ritmo da sua disseminação», acrescenta a AMA, por e-mail.

A confiança que a AMA deposita no sistema não chega para acabar com os receios de Ricardo Chaves: «Há uma grande exigência em relação à taxa de falsos positivos, mas isso não impede que alguém tire partido da principal falha que se encontra no caderno de encargos (e que diz respeito à inexistência de garantias de que os dispositivos usados na autenticação não foram adulterados)».

Contactado pela *Exame Informática*, o Centro Nacional de Cibersegurança (CNCS) informa que os sistemas de autenticação eletrónica usados pelos serviços públicos são geridos por entidades nacionais em consonância com o que prevê o regulamento europeu eIDAS (sigla de Electronic Identification, Authentication and Trust Services), que está em vigor em Portugal desde 2016. Este regulamento prevê que as diferentes entidades que gerem sistemas de identidade e autenticação eletrónica (eID) respeitem um conjunto de requisitos técnicos. O CNCS confirma que a AMA «é a entidade nacional designada para gerir e operar o nó-eIDAS nacional, bem como para efetuar a notificação dos meios nacionais de eID».

O caderno de encargos prevê um contrato com duração máxima de três anos, que exige um sistema que capaz de garantir a verificação básica de segurança e a leitura de carateres do Cartão do Cidadão sem qualquer limite. Em contrapartida, o fornecedor escolhido apenas está obrigado a garantir 220 mil verificações de liveness; 210 mil comparações da foto visível no Cartão do Cidadão (CC) com foto obtida da verificação de liveness; 200 mil comparações da foto na base de dados com foto obtida da verificação de liveness; e ainda 20 mil verificações de segurança avançada do Cartão do Cidadão. A AMA fixa ainda os valores máximos que podem ser cobrados pelo fornecedor em cada um destes processos: cada verificação de liveness tem um custo máximo de 0,25 €; cada comparação da foto visível no Cartão do Cidadão com foto obtida da verificação de liveness tem um custo máximo de 0,15 €; a comparação da foto na base de dados com a foto obtida da verificação de liveness tem um custo máximo de 0,15 €; e verificação de segurança avançada Cartão de Cidadão não pode custar mais de 1,50 €.

«Para a componente de “Recolha de informação constante de Cartão de Cidadão e verificação básica de segurança” é definido um preço base de 3 500 € para uma utilização ilimitada durante o período do contrato», refere o Caderno de Encargos.

Segundo o site Autenticação.gov há, atualmente, mais de 800 mil CMD ativas.

Seguro ou talvez não

O tema está longe de ser consensual, mesmo entre peritos de segurança eletrónica. O facto de um hacker ter conseguido vencer a ferramenta proposta para a população francesa é ilustrativo: é um sinal de alerta a ter em conta como algumas outras notícias que indicam que é possível enganar sistemas de liveness, mas importa não esquecer que poderá ser uma vulnerabilidade exclusiva de uma ferramenta e não de toda a família de tecnologias.

Nos últimos dois anos, tem havido uma evolução muito significativa na tecnologia de deepfakes, e não podemos pôr de parte que, num futuro próximo, poderá comprometer as defesas implementadas para este tipo de autenticação

Pedro Fortuna

Além de ver no liveness uma forma de «contribuir para uma maior utilização do CMD» e «uma maior digitalização da nossa sociedade», Fortuna enaltece o facto de a AMA ter fixado como requisito a certificação ISO/IEC 30107, que é «a norma de verificação biométrica que obriga, entre outras técnicas, à deteção de vida (liveness) como forma de mitigação da maioria dos atuais ataques».

«Contudo, nos últimos dois anos, tem havido uma evolução muito significativa na tecnologia de deepfakes, e não podemos pôr de parte que, num futuro próximo, poderá comprometer as defesas implementadas para este tipo de autenticação», lembra, por e-mail, Pedro Fortuna, para depois apontar o dedo a outro tipo de vulnerabilidade: «A AMA pede o desenvolvimento de um SDK (um kit de ferramentas de programação e desenvolvimento de software) para iOS e para Android. Não é indicado se o SDK deve ser fornecido com tecnologia de proteção da integridade do código. Estas tecnologias, que incluem entre outras coisas, deteção de adulteração maliciosa de código, deteção de ferramentas de análise e inspeção da memória, etc. – são consideradas standard para aplicações críticas por instituições como a OWASP (a principal comunidade de profissionais de segurança aplicacional, que recomenda as melhores práticas de segurança aplicacional)».

Pedro Fortuna lembra que o facto de não ser exigida proteção contra a adulteração de códigos facilita ataques que podem levar à fuga de dados biométricos que poderão ser aproveitados por cibercriminosos. «Esta potencial fuga de dados é independente do requisito de remoção obrigatória dos dados biométricos dos servidores, aspeto que foi salvaguardado no caderno de encargos», acrescenta.

A falta de consensualidade em torno do liveness e do caderno de encargos apresentado pela AMA está também patente nas análises de vários especialistas contactados pela *Exame Informática* e que solicitaram anonimato: há quem considere que as vulnerabilidades do liveness não serão muito mais graves que aquelas a que se sujeita quem perde a carteira nos dias que correm, mas também há quem admita o aparecimento de uma nova "janela" de oportunidade para potenciais ataques. Um terceiro caso ilustrativo, proveniente de uma fonte bem colocada no segmento dos fornecedores de tecnologias, contrasta com as duas análises anteriores apontando as exigências técnicas como a principal falha do sistema que a AMA pretende montar nos próximos tempos: «Duvido que haja empresas que consigam cumprir as exigências técnicas e os limites de custo previstos pelo concurso público. A menos que seja uma empresa que precise de apresentar este projeto como bandeira para ganhar clientes noutros mercados».

Consoada com fornecedores não revelados

Coincidência ou não, o prazo do concurso também mereceu surpresa entre quem costuma acompanhar o setor, pelo facto de terminar às 00h00 de 24 de dezembro. A AMA responde sem fazer qualquer alusão à consoada de Natal e recorda apenas que os 14 dias do prazo de entrega de propostas excedem o mínimo exigido por lei para os concursos públicos nacionais, que está fixado em seis dias. «Este prazo considera-se suficiente e adequado para os interessados elaborarem as suas propostas, principalmente

se forem diligentes para o efeito. Contudo, salienta-se que é sempre possível solicitar a prorrogação do prazo, o que não foi feito por nenhum interessado até ao momento», conclui a Agência.

Através do gabinete de Alexandra Leitão, Ministra da Modernização do Estado e da Administração Pública, a AMA também fez saber que, depois de uma primeira análise ao «enquadramento jurídico», decidiu não fornecer informação sobre as marcas que se apresentaram a concurso ou o número de propostas recebidas nesse mesmo concurso.

A *Exame Informática* tentou verificar o fundamento legal desta recusa da AMA – e apurou que a Agência poderá estar a desrespeitar a lei ao recusar indicar o número de propostas recebidas no concurso. Catarina Limpo Serra, advogada coordenadora do Departamento de Contencioso da sociedade de advogados CCA, recorda que a Constituição da República Portuguesa (CRP) prevê o direito dos cidadãos a serem informados sobre diferentes processos em curso e aponta para os artigos do Estatuto do Jornalista que obrigam os diferentes órgãos da Administração Pública a fornecerem informação, desde que não envolva processos considerados classificados, em segredo de justiça ou implique a violação de dados pessoais.

Catarina Limpo Serra também faz alusão à Lei nº 26/2016, que regula o acesso a diferentes repositórios de dados da Administração Pública. Esta lei pretende facilitar o acesso aos dados na posse do Estado a todos os cidadãos, e apenas permite que um organismo estatal possa recusar fornecer «documentos administrativos» (o que a *Exame Informática* não solicitou), no caso de envolver um processo ainda em curso, cuja decisão final ainda está em preparação.

«O meu entendimento é que a AMA deve facultar, pelo menos, a informação sobre o número de concorrentes. Poderá também facultar a identificação das empresas que concorreram. De todo o modo, a recusa no fornecimento da informação deve ser legítima e terá sempre de ser fundamentada, podendo ter por base, por exemplo, o artigo 6º, nº 3 da Lei nº 26/2016», conclui a advogada da CCA .