technology review.es
Published by MIT

Sexta-feira, 08 de agosto de 2014

Black Hat: Google Glass Podem Roubar Suas Senhas

Filmagem de pessoas destravando seus telefones podem ser usadas para roubar suas senhas, mesmo que não dê para vê-las digitando.
Por Tom Simonite

Críticas ao Google Glass, muitas vezes focam na forma como sua câmera torna a gravação de vídeo clandestina fácil demais. Agora, pesquisadores mostraram que as imagens capturadas pela câmera montada na face também poderiam representar uma ameaça à segurança.

Software desenvolvido pelos pesquisadores pode recuperar automaticamente as senhas de pessoas capturadas em vídeo enquanto digitam suas senhas, mesmo quando a tela em si não é visível para a câmera. O ataque funciona, observando o movimento dos dedos para descobrir quais teclas estão tocando. Ele também funciona com videos filmados em câmeras convencionais, webcams e smartphones, mas o Google Glass oferece talvez a maneira mais sutil que criá-los.

O trabalho sugere que "espiar por cima do ombro" - roubando senhas ou outros dados ao ver alguém em um computador - pode se tornar uma ameaça ainda maior à medida que câmeras digitais e software de processamento de imagem poderosos se tornam mais comuns.

Nos testes em que pessoas estavam a três metros de distância da câmera, o software acertou em cerca de 90 por cento dos casos a senha de quatro caracteres digitada no teclado QWERTY do iPhone. Os pesquisadores dizem que o método poderia, teoricamente, reconstruir um e-mail ou SMS curto.

"Com o Glass isso é muito mais sorrateiro", diz Qinggang Yue, um estudante de graduação da Universidade de Massachusetts, em Lowell, que realizou a pesquisa com seus colegas Xinwen Fu e Ling Zhen.

Quando Yue falou com o MIT Technology Review na conferência de segurança Black Hat, onde ele apresentou seus resultados na quarta-feira, olhou ao redor da sala de imprensa ocupada e imediatamente identificou um punhado de pessoas digitando em telas sensíveis ao toque que poderiam estar vulneráveis a esse tipo de ataque.

Yue também mostrou que vídeos podem ser utilizados para recuperar senhas a distância. Em uma série de experimentos, uma câmera de vídeo que alguém segurava da janela do primeiro andar foi usada para capturar com sucesso a senha de alguém que usava um iPad a pouco mais de 43 metros de distância. "Com uma câmera de distância focal longa daria para filmar muito mais longe", diz Yue.

Para capturar uma senha, o software deve identificar a posição e orientação da tela do dispositivo, bem como a posição das pontas dos dedos da pessoa que está digitando. Yue e seus colegas usaram a aprendizagem de máquina para treinar software para resolver ambos os problemas. O software roda em um PC, de modo que as imagens capturadas com o Google Glass precisam ser baixadas para que a senha possa ser extraída.

O software encontra automaticamente um dispositivo capturado em um trecho de filmagem. Em seguida, identifica a posição dos quatro cantos da tela e acompanha a velocidade das pontas dos dedos da pessoa que está digitando.

Os pesquisadores estão testando maneiras de se defender contra esse tipo de espionagem avançada. Uma medida preventiva pode ser trocar aleatoriamente a posição das teclas de um teclado padrão, de modo que o software não consiga traduzir corretamente cada digito. Outra envolve fazer os botões flutuarem ao invés de ficarem fixos em uma grade padrão.