Método de criptografia usado mundialmente apresenta falha, segundo pesquisa

Matemática

Enviado por: skura@seed.pr.gov.br

Postado em:17/02/2012

Método é usado em sites de compras, de bancos, e-mails e outros serviços. Falha está na maneira como números aleatórios são gerados.

Método é usado em sites de compras, de bancos, e-mails e outros serviços. Falha está na maneira como números aleatórios são gerados. Examinando bancos de dados de cerca de 7,1 milhões de chaves de segurança, matemáticos e criptógrafos americanos e europeus descobriram uma grande falha em um sistema de criptografia usado no mundo todo em sites de compras, bancos, e-mails e diversos outros serviços, e que deveria ser extremamente seguro e privado. O problema é que o sistema pede para os usuários inserirem o resultado de uma conta matemática envolvendo 2 grandes números, usados para gerar a chave e mantidos em segredo. Porém, é essencial que esses 2 grandes números sejam aleatórios. E foi aí que os pesquisadores descobriram a falha: uma pequena, mas significante porcentagem desses números não é gerada aleatoriamente, comprometendo a segurança. Ao todo, os pesquisadores acharam 27 mil chaves que não oferecem segurança, segundo o jornal americano The New York Times. "Isso traz um aviso indesejável que mostra a dificuldade da geração de chaves no mundo real. Algumas pessoas acham que 99,8% de segurança é algo bom", diz James P. Hughes, um analista de criptopgrafia do Vale do Silício e que trabalho na pesquisa, explicando que os 0,2% podem representar grandes riscos. Embora as falhas possam afetar as transições individuais dos usuários, não há nada a ser feito por eles. A mudança tem que vir dos próprios sites, que devem mudar as medidas de segurança em seus sistemas. Para resolverem o problema, as empresas têm de coletar as chaves públicas e remover as informações da internet, tomando atitudes para que não haja vazamento ou roubo desses dados. Esta notícia foi publicada em 15/02/2012 no Olhar Digital. Todas as informações nela contida são de responsabilidade do autor.