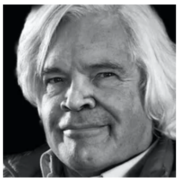
Home / Tech / Security

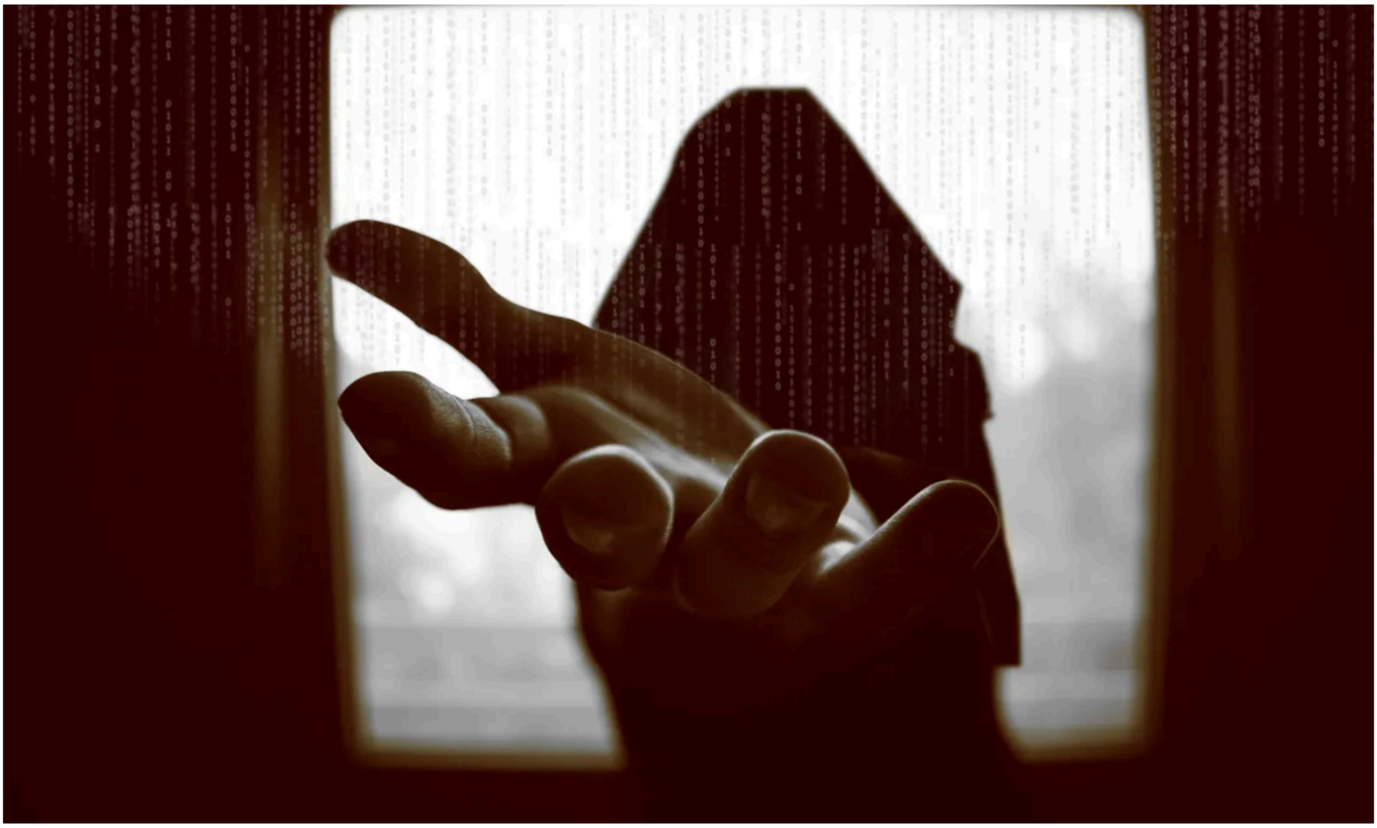
PGP encryption won't protect your data. But PURBs can.

You may think that encrypting your sensitive files with, say, PGP may protect your data - but you'd be wrong. Most encryption formats leak a lot of plaintext metadata, and that's a problem. Here's what you need to know.



Written by **Robin Harris,** Contributor

June 25, 2018 at 5:51 a.m. PT



Getty Images/iStockphoto

Most encrypted data formats have plaintext headers, because, how the heck are you supposed to know anything about the encrypted file - such as which encryption tool protected it - without *some* plaintext info? But this creates a serious security problem.

The plaintext may reveal how many recipients can decrypt the data, and possibly their identities. Info about the encryption software configuration and version level can be used to fingerprint a specific endpoint, facilitating targeted attacks against system weaknesses.

In a network environment - and we're all networked today - a digital fingerprint can facilitate traffic analysis, videos watched, geo-location, social networks, language, password length, and even if you are using TOR.

OK, plaintext metadata can be a security risk. But how far can plaintext metadata be reduced before no one can access it?

PURBs

Pretty far, according to researchers at the Swiss ETF in Lausanne. In a new paper, Reducing Metadata Leakage from Encrypted Files and Communication with PURBs, they propose an encrypted format similar to PGP that minimizes file length and metadata leakage. They call it *Padded Uniform Random Blobs.*

> **A PURB is indistinguishable from a uniform random bit-string to an observer without a decryption key. Legitimate recipients can efficiently decrypt the PURB even when it is encrypted for any number of recipients' public keys and/or passwords, and when those public keys are of different cryptographic schemes.**

How does it work?

A PURB is a file or message whose content and metadata are contained in an encrypted blob that is padded to a standard set of sizes. With a given size, the PURBs are cryptographically indistinguishable from each other, and do not leak the encryption scheme, who or how many recipients can decrypt it, file sizes, or what software created it.

Making it work

There are two main challenges to overcome in designing PURBs. First, there's the problem of allowing any number of recipients to use different cryptographic keys, perhaps from several different cipher suites, to get the info they need to decrypt the PURB.

PURBs solve this by encrypting content with one algorithm, and then adding a variable length encrypted header containing metadata for recipients. The header contains multiple entry points, so users with different decryption tools can read the header and get the data they need to access the content.

/ security

Cyber security 101: Protect your privacy from hackers, spies, and the government

Simple steps can make the difference between losing your online accounts or maintaining what is now a precious commodity: Your privacy.

Read now →

The second challenge is reducing the leakage of information about the length of the file. The proposed padding scheme groups files in sets of logarithmically increasing sizes, and leaks much fewer bits than padding to a fixed block size.

How well does it work?

In their testing, the researchers found that encrypting a PURB for 100 recipients, using 10 different enciphering tools, took less than half a second on a 3.1 Ghz laptop. Decoding performance is comparable to PGP.

Of course, the bigger issue is how well does it hide file lengths, since that single number can easily identify many kinds of objects, from YouTube videos to software packages. They found that, for example, PURBs reduced the percentage of uniquely identifiable videos from 87 to 3 percent, while adding less than 12 percent space overhead.

The Storage Bits take

In a world with billion dollar criminal hacker rings, and massive state-supported hacking cadres, nobody's data is safe. It's easy for civilians to underestimate the ways in which their data can be compromised by clever and determined hackers.

PURB is not a commercial product, but as research it points the way for rearchitecting encryption suites to dramatically improve security. Let's hope that vendors are taking note.

RELATED AND PREVIOUS CONTENT:

Uninstall PGP: EFF warns of exploit that may reveal plaintext of encrypted emails

European researchers claim to have found a vulnerability that could reveal plaintext of encrypted emails, including those in the past.

IBM warns of instant breaking of encryption by quantum computers: 'Move your data today'

Welcome to the future transparency of today as quantum computers reveal all currently encrypted secrets -- a viable scenario within just a few years.

MIT engineers crack IoT encryption problem with ultra-efficient chip

IoT's limited capabilities have caused issues for security, but perhaps, no more.

Courteous comments welcome, of course.