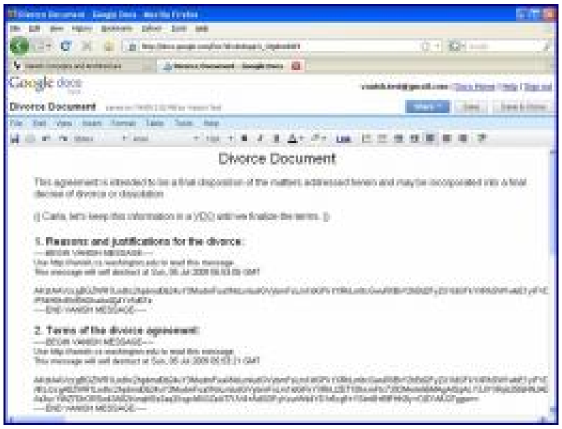
This article will self-destruct: A tool to make online personal data vanish (w/ Video)

July 21 2009



Divorce Document

This agreement is intended to be a final disposition of the matters addressed herein and may be incorporated into a final decree of divorce or dissolution.

{{ Carla, let's keep this information in a VDO until we finalize the terms. }}

1. Reasons and justifications for the divorce:

-----BEGIN VANISH MESSAGE-----
Use http://vanish.cs.washington.edu to read this message.
This message will self destruct at Sun, 05 Jul 2009 05:03:05 GMT

[illegible]
-----END VANISH MESSAGE-----

2. Terms of the divorce agreement:

-----BEGIN VANISH MESSAGE-----
Use http://vanish.cs.washington.edu to read this message.
This message will self destruct at Sun, 05 Jul 2009 05:03:21 GMT

[illegible]
-----END VANISH MESSAGE-----

Vanish + Google Docs

Computers have made it virtually impossible to leave the past behind. College Facebook posts or pictures can resurface during a job interview. A lost cell phone can expose personal photos or text messages. A legal investigation can subpoena the entire contents of a home or work computer, uncovering incriminating, inconvenient or just embarrassing details from the past.

The University of Washington has developed a way to make such information expire. After a set time period, electronic communications such as e-mail, Facebook posts and chat messages would automatically self-destruct, becoming irretrievable from all Web sites, inboxes, outboxes, backup sites and home computers. Not even the sender could retrieve them.

"If you care about privacy, the Internet today is a very scary place," said Tadayoshi Kohno, a UW assistant professor of computer science. "If people understood the implications of where and how their e-mail is stored, they might be more careful or not use it as often."

The team of UW computer scientists developed a prototype system called Vanish that can place a time limit on text uploaded to any Web service through a Web browser. After a set time text written using Vanish will, in essence, self-destruct. A paper about the project went public today and will be presented at the Usenix Security Symposium Aug. 10-14 in Montreal.

Co-authors on the paper are doctoral student Roxana Geambasu, Kohno, professor Hank Levy, and undergraduate student Amit Levy, all with the UW's department of computer science and engineering. The research was funded by the National Science Foundation, the Alfred P. Sloan Foundation and Intel Corp.

"When you send out a sensitive e-mail to a few friends you have no idea where that e-mail is going to end up," Geambasu said. "For instance, your friend could lose her laptop or cell phone, her data could be exposed by malware or a hacker, or a subpoena could require your e-mail service to reveal your messages. If you want to ensure that your message never gets out, how do you do that?"

Many people believe that pressing the "delete" button will make their data go away.

"The reality is that many Web services archive data indefinitely, well after you've pressed delete," Geambasu said.

Simply encrypting the data can be risky in the long term, the researchers say. The data can be exposed years later, for example, by legal actions that force an individual or company to reveal the encryption key. Current trends in the computing and legal landscapes are making the problem more widespread.

"In today's world, private information is scattered all over the Internet, and we can't control the lifetime of that data," said Hank Levy. "And as we transition to a future based on cloud computing, where enormous, anonymous datacenters run the vast majority of our applications and store nearly all of our data, we will lose even more control."

The Vanish prototype washes away data using the natural turnover, called "churn," on large file-sharing systems known as peer-to-peer networks. For each message that it sends, Vanish creates a secret key, which it never reveals to the user, and then encrypts the message with that key. It then divides the key into dozens of pieces and sprinkles those pieces on random computers that belong to worldwide file-sharing networks, the same ones often used to share music or movie files. The file-sharing system constantly changes as computers join or leave the network, meaning that over time parts of the key become permanently inaccessible. Once enough key parts are lost, the original message can no longer be deciphered.

In the current Vanish prototype, the network's computers purge their memories every eight hours. (An option on Vanish lets users keep their data for any multiple of eight hours.)

Unlike existing commercial encryption services, a message sent using Vanish is kept private by an inherent property of the decentralized file-sharing networks it uses.

"A major advantage of Vanish is that users don't need to trust us, or any service that we provide, to protect or delete the data," Geambasu says.

Researchers liken using Vanish to writing a message in the sand at low tide, where it can be read for only a few hours before the tide comes in and permanently washes it away. Erasing the data doesn't require any special action by the sender, the recipient or any third party service.

"Our goal was really to come up with a system where, through a property of nature, the message, or the data, disappears," Levy says.

Vanish was released today as a free, open-source tool that works with the Firefox browser. To work, both the sender and the recipient must have installed the tool. The sender then highlights any sensitive text entered into the browser and presses the "Vanish" button. The tool encrypts the information with a key unknown even to the sender.

That text can be read, for a limited time only, when the recipient highlights the text and presses the "Vanish" button to unscramble it. After eight hours the message will be impossible to unscramble and will remain gibberish forever.

Vanish works with any text entered into a Web browser: Web-based e-mail such as Hotmail, Yahoo and Gmail, Web chat, or the social networking sites MySpace and Facebook. The Vanish prototype now works only for text, but researchers said the same technique could work for any type of data, such as digital photos.

It is technically possible to save information sent with Vanish. A recipient could print e-mail and save it, or cut and paste unencrypted text into a word-processing document, or photograph an unscrambled message. Vanish is meant to protect communication between two trusted parties, researchers say.

"Today many people pick up the phone when they want to talk with a lawyer or have a private conversation," Kohno said. "But more and more communication is happening online. Vanish is designed to give people the same privacy for e-mail and the Web that they expect for a phone conversation."

The paper and research prototype are available online at http://vanish.cs.washington.edu.

Source: University of Washington (news : web)

Citation: This article will self-destruct: A tool to make online personal data vanish (w/ Video) (2009, July 21) retrieved 17 April 2024 from https://phys.org/news/2009-07-article-self-destruct-tool-online-personal.html