SHAZZLEMAIL, PRIVATE AND SECURE EMAIL APPLICATION

ShazzleMail: August, 2013

For consumers and businesses

ShazzleMail
4835 E. Cactus | Suite 120
Scottsdale, AZ | 85254
(602) 638-5839
Shazzlemail.com

1. The Problem

To date, most email users have traded their privacy for the low cost and simplicity of web mail. While the web's server-based architecture operates as an efficient middleman, to allow great reliability and ease-of-use, it destroys privacy by storing a person's communications on servers outside of their control.

Privacy is an essential element of human freedom, though few consumers think of this as they plow through their email. Some understand that their personal communications are mined for data and sold to marketers for advertising, and now many know that their government is watching as well. Lately, a growing chorus of voices is objecting to the escalating invasion of privacy.

II. Proof the Problem Exists

There are over 1 billion active web email accounts worldwide from the top three providers (in June 2012, Google reported 425 million Gmail users[1], in October 2012, ComScore reported 281 million Yahoo Mail[2] and in May 2013, Microsoft reported 400 million Outlook.com users[3]). These and other web email providers are monetizing what was considered private communications into 'big data.' All three providers have previously stated that their email data mining efforts are used to generate advertising revenue.

> *"Gmail: You weren't really expecting privacy, were you?"*
>
> - - - Molly Wood, CNET, 8/13/13

Web email providers also keep multiple copies of your email and will keep your email long after you have 'deleted' them. Why is that an issue? The Electronic Communications Privacy Act allows the U.S. federal government to access email that is 180 days old or older without a warrant. According to Business Insider[4], "the relevant text of the law (states):

> A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section."

And IRS lawyers stated in recently disclosed documents that Americans enjoy 'generally no privacy' in their email.[5]

Further, Gmail recently stated in a motion to dismiss a class action suit brought forward by Consumer Watchdog that, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[6]

Consumer sentiment regarding privacy and government anti-terrorism efforts are changing as well. "In a massive shift in attitudes, voters say 45% – 40% the government's anti-terrorism efforts go too far restricting civil liberties, a reversal from a January 14, 2010, survey by the independent Quinnipiac University when voters said 63% – 25% that such activities didn't go far enough to adequately protect the country."[7]

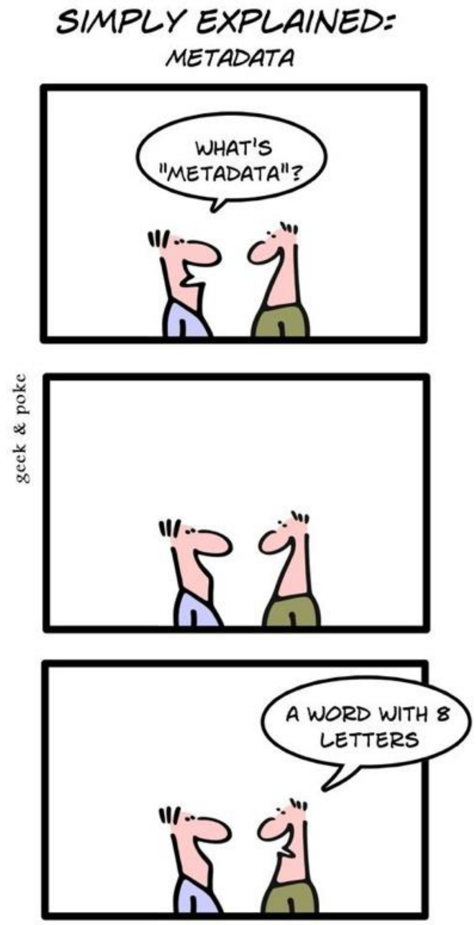
III. Additional Problems

Standard email has been a very powerful communication tool for decades, but its centralized server architecture has helped to erode personal privacy. Major email provides such as Yahoo and Gmail openly declare that a person using their service should not have any expectation of privacy, and strip users of owning even the information exchanged in their personal emails.

Another way central servers destroy privacy is by creating and storing voluminous metadata which exposes the communication patterns of the people that use these services. The value of such data to larger corporations and governments is increasing, and thus so is the erosion of privacy.

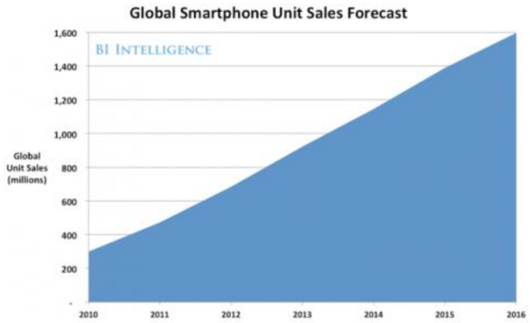
Finally, existing server based secure email solutions have been costly and difficult to use. All that were researched require cumbersome asymmetrical key encryption. Also, these systems must collect and store metadata which can be accessed to the detriment of their users as has been seen with recently shuttered email services from Lavabit and Silent Circle.

In conclusion, the existing suite of privacy focused email solutions are under attack because, with client/server technology, they are not able to effectively guard a user's privacy.



IV. The Basic Solution

Create a simple-to-use and reliable communications architecture that relies on the surging smartphone market (nearing one billion in sales[8]) that is in a user's physical possession and control, so no outside parties have access to the content.



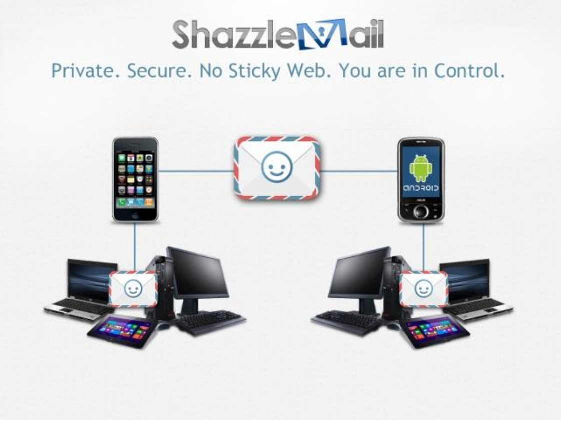
Additionally, a solution should encrypt all communications in transit to prevent hacking with no stored copies en route. In this way, passwords are not required and simplicity is maintained.

Information is less susceptible to abuse if passed between two parties via an encrypted channel.

Modern mobile devices like smartphones and tablets are a solid platform to build a system that will be both private and fully capable of supporting standard email exchange that consumers have been using for many years.

V. Introduction of Solution

ShazzleMail is an email system designed to support direct point-to-point connectivity between smartphones and other computing devices in the physical possession of the people involved in the information exchange. ShazzleMail software, residing on user devices, is able to exchange emails in a very secure and private way providing both a user interface on the mobile device as well as an interface of POP3/IMAP/SMTP server to be used with a standard email client on a PC or Mac computer.



An always-on mobile device that is directly addressable and connected via Wi-Fi to a broadband can serve as a relay to the network members that are on the cellular network and not addressable. Both groups of mobile devices that move between these two states form a network capable of building direct encrypted connections without any significant help from supporting servers, thus keeping the system cost low enough to allow it to be offered free to consumers.

VI. Application of Solution

ShazzleMail makes use of the growing computing power of smartphones and tablets to build a network which allows direct exchange of emails between interested parties without allowing a third party to either eavesdrop, or analyze the communication patterns of the people involved.

The ShazzleMail system employs a centralized registry to support addressing within the network. The sender first requests addressing information for the recipient. If recipient is a member of the ShazzleMail network, the sending software creates an encrypted connection between sender and receiver's devices using recipient's public key and its IP address (if recipient is directly addressable) or an IP of a relay if the recipient is behind a firewall. The email is sent via encrypted connection if recipient is online, otherwise sender must wait until recipient comes online. With this exchange, only the sender and receiver retain possession of the email.

In the case where the recipient is not a member of a network a URL link is sent via non-secure email. When recipient opens the link, an SSL connection is built between recipient's browser and sender's device. The data is then passed in encrypted form without persistence on any device not in sender or receiver's possession.

Mobile devices that are connected to Wi-Fi and are not behind a firewall can serve as relays to support addressability for the members of the network that are not directly addressable at that time.

VI. Application of Solution (continued)

To support standard email clients, ShazzleMail software on the mobile devices can serve as a POP3/IMAP/SMTP server. This connectivity is further facilitated by proxy software called ShazzleMail Connect that is installed on the user's computer. This software tracks the user's mobile device and finds the best connection as the mobile device moves between cellular networks and Wi-Fi. This connectivity is also encrypted.

There are currently two kinds of proxies available, one to support a standard POP3/SMTP account setup on any email client, and ShazzleMail Connect Plug-in for Outlook. The Outlook plug in provides a simplified account setup and supports large file transfers that can otherwise be a problem when sending via Outlook.

VII. Future Direction

Shazzle mail would like to provide secure and private platforms for any data exchange. We have plans to offer an open API and will be introducing an email client with a simplified account setup in Q4 2013. A paid version tailored to facilitate email exchange for a business environment is currently in development and will be available in Q4 2013.

VIII. Conclusion

Recent news has highlighted the lack of privacy in standard email exchange. Despite this issue receiving high profile attention, no significant leader in private and secure email has emerged because all have clung to a server based architecture that is the problem and not the solution. We believe that distributed, easy-to-use, low cost ShazzleMail is the leading candidate to replace the existing outdated email infrastructure.

Thank you for reading this overview. For further information about ShazzleMail or to get started with your own ShazzleMail account, visit our website at www.shazzlemail.com or call us at (602) 638-5839. You can also find us on Facebook, search ShazzleMail.

Appendix

Footnotes

(1) Lardinois, Frederic. “Gmail Now Has 425 Million Users, Google Apps Used By 5 Million Businesses And 66 Of The Top 100 Universities.” TechCrunch. 28 Jun. 2012. 19 Aug. 2013.

(2) Molla, Rani. “Gmail finally beats Hotmail, according to third-party data [chart].” GigaOM. 31 Oct. 2012. 19 Aug. 2013.

(3) Craddock, Dick. “One year since the preview of Outlook.com – thank you for helping us build the world’s fastest growing email.” Microsoft. 31 Jul. 2013. 19 Aug. 2013.

(4) Fuchs, Erin. “No One Is Talking About The Insane Law That Lets Authorities Read Any Email Over 180 Days Old.” Business Insider. 7 Jun. 2013. 8 Jun. 2013.

(5) McCullagh, Declan. “IRS claims it can read your e-mail without a warrant.” CNET. 10 Apr. 2013. 12 Apr. 2013.

(6) Meyer, David. “Oh Google. Of course email users expect privacy – you promised it to them.” GigaOM. 14 Aug. 2013. 19 Aug. 2013.

(7) Brown, Peter. Press Release, Quinnipiac University Poll. 10 Jul. 2013.

(8) “Mobile Phone Sales Expected to hit 1.86 Billion in 2013 on Strong Smartphone Growth.’ Cellular-news. 10 Jun. 2013. 19 Aug. 2013.