Executive Summary:

This six page letter to Google's CEO, Eric Schmidt, is signed by 38 researchers and academics in the fields of computer science, information security and privacy law. Together, they ask Google to honor the important privacy promises it has made to its customers and protect users' communications from theft and snooping by enabling industry standard transport encryption technology (HTTPS) for Google Mail, Docs, and Calendar.

Google already uses industry-standard Hypertext Transfer Protocol Secure (HTTPS) encryption technology to protect customers' login information. However, encryption is *not* enabled by default to protect other information transmitted by users of Google Mail, Docs or Calendar. As a result, Google customers who compose email, documents, spreadsheets, presentations and calendar plans from a public connection (such as open wireless networks in coffee shops, libraries, and schools) face a very real risk of data theft and snooping, even by unsophisticated attackers. Tools to steal information are widely available on the Internet.

Google supports HTTPS encryption for the entire Gmail, Docs or Calendar session. However, this is disabled by default, and the configuration option controlling this security mechanism is not easy to discover. Few users know the risks they face when logging into Google's Web applications from an unsecured network, and Google's existing efforts are little help.

Support for HTTPS is built into every Web browser and is widely used in the finance and health industries to protect consumers' sensitive information. Google even uses HTTPS encryption, enabled by default, to protect customers using Google Voice, Health, AdSense and Adwords. Google should now extend this degree of protection to users of Gmail, Docs and Calendar.

Rather than forcing its customers to "opt-in" to adequate security, Google should make security and privacy the default.

Eric Schmidt, PhD
CEO, Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
USA

June 16, 2009

Re: Ensuring adequate security in Google's cloud based services

Dear Dr. Schmidt,

The signatories of this letter are researchers and academics in the fields of computer science, information security and privacy law. We write to you today to express our concern that many users of Google's cloud-based services are needlessly exposed to an array of privacy and security risks. We ask you to increase users' security and privacy protection by enabling by default transport-level encryption (HTTPS) for Google Mail, Docs and Calendar, a technology already enabled by default for Google Voice, Health, AdWords and AdSense.

As a market leader in providing cloud services, Google has an opportunity to engage in genuine privacy and security leadership, and to set a standard for the industry.

Google's services are not secure by default

Google's default settings put customers at risk unnecessarily. Google's services protect customers' usernames and passwords from interception and theft. However, when a user composes email, documents, spreadsheets, presentations and calendar plans, this potentially sensitive content is transferred to Google's servers *in the clear*,[1] allowing anyone with the right tools to steal that information.

Google uses industry-standard Hypertext Transfer Protocol Secure (HTTPS) encryption technology[2] to protect customers' login information. However, encryption is *not* enabled by default to protect other information transmitted by users of Google Mail, Docs or Calendar. As a result, anyone who uses these Google services from a public connection (such as open wireless networks in coffee shops, libraries, and schools) faces a very real risk of data theft and snooping, even by unsophisticated attackers. Tools to steal information are widely available on the Internet.

As the massive data breach suffered by T.J. Maxx clearly demonstrated, valuable information that is transmitted without sufficient protection can and will be exploited by criminals.[3] Widely available tools known as *packet sniffers*[4] make it easy for even amateur hackers to intercept users' confidential files and communications as they are transmitted between a user's laptop or handheld device and Google's servers-- attackers can steal data without being detected. These sniffing tools are available for free, and even come pre-installed with some operating systems.[5]

Authentication cookies and the risks of account hijacking

Google's implementation of cookies makes it easy for attackers to effectively impersonate users. Google, like many other companies, uses *authentication cookies*, which are transmitted by the user's browser to Google's servers for all requests after the initial login. These cookies are, by default, sent without encryption, and can thus be intercepted by hackers. By using one of these intercepted authentication cookies, a hacker can access a user's account, read their documents, delete their files, and even send new email messages in their name.[6]

This risk is real, and Google's response to date has been inadequate. In 2007, two researchers highlighted this cookie theft vulnerability in talks at the DefCon security conference.[7] A year later, one of them released a tool to automate cookie theft and account hijacking.[8] A year after first being notified of the flaw, and just a few days before the security researcher planned to release his tool, Google announced the release of a new configuration option in Gmail to protect these authentication cookies and to force the use of HTTPS for Gmail sessions.[9] However, to this day, this option is *off* by default, and is not widely known or publicized.

A large body of scientific research shows that users overwhelmingly retain default options; thus, unless the security issue is well known and salient to consumers, they will not take steps to protect themselves by enabling HTTPS.[10] To deliver on Google's promises about privacy and security, the company should shift the default option to the more protective HTTPS setting.

Data interception vulnerabilities are not new

The technology industry has long known about the risks of transmitting private information in the clear. Web browsers have supported HTTPS since 1994, and many companies have made this switch. Today, all financial companies in the United States use the industry standard HTTPS technology to protect their customers' communications and transactions. Companies including Bank of America and American Express have gone even further, by using HTTPS to encrypt every single page served from their Web sites, even promotional information and non-confidential data.

Google itself has long known about these risks, and as a result, has supported HTTPS since the first day that the Gmail service launched. HTTPS support for Docs and Calendar is similarly long-standing, although as with Gmail, it is not enabled by default.

Google is not the only Web 2.0 firm which leaves its customers vulnerable to data theft and account hijacking. Users of Microsoft Hotmail, Yahoo Mail, Facebook and MySpace are also vulnerable to these attacks. Worst of all – these firms do not offer their customers any form of protection. Google at least offers its tech savvy customers a strong degree of protection from snooping attacks. However, due to the fact that HTTPS protection is disabled by default and only enabled via an obscure configuration option, most regular users are likely to remain vulnerable.

Performance impact is minimal while security impact is large

Enabling HTTPS for Google services by default will have a small impact in performance for the user, but will yield considerable security gains. In a 2008 blog post describing a new Gmail feature to force the use of HTTPS, Google engineer Ariel Rideout defended the company's decision to not enable HTTPS by default:

> "We use https to protect your password every time you log into Gmail, but we don't use https once you're in your mail unless you ask for it (by visiting https://mail.google.com rather than http://mail.google.com). Why not? Because the downside is that https can make your mail slower. Your computer has to do extra work to decrypt all that data, and encrypted data doesn't travel across the internet as efficiently as unencrypted data. That's why we leave the choice up to you."[11]

Once a user has loaded Google Mail or Docs in their browser, performance does not depend upon a low latency Internet connection. The user's interactions with Google's applications typically do not depend on an immediate response from Google's servers. This separation of the application from the Internet connection enables Google to offer 'offline' versions of its most popular Web applications.[12]

Even when low latency is important, financial firms such as Bank of America and American Express have demonstrated how to provide users with a pleasant, low-latency browsing experience, while still implementing strong encryption by default. Likewise, Adobe's cloud-based Photoshop Express lets users interactively edit images via a Web application that is 100% encrypted by default.

Other Google applications demonstrate that security need not come at the cost of performance. Google's Health service enables users to browse through and manage their private health information online. Google's Voice service lets customers initiate VOIP phone calls, send text messages, and manage voicemail inboxes. However, unlike with its Gmail, Docs, and Calendar products, Google only provides access to Health and Voice via HTTPS encrypted communications sessions, recognizing the highly sensitive health and call record information users entrust to Google. Likewise, Google's AdWords and AdSense products, which are the backbone of Google's advertising business, can only be managed by customers using a secure HTTPS connection.

Google's engineers have created a low-latency, enjoyable experience for users of Health, Voice, AdWords and AdSense – we are confident that these same skilled engineers can make any necessary tweaks to make Gmail, Docs, and Calendar work equally well in order to enable encryption by default.

Google does not inform users adequately of the risks of unencrypted sessions

Users do not adequately appreciate the risks of failing to use encryption and need protective defaults. Researchers have shown that most users have no idea of the data interception risks that they face when using public wireless networks.[13] Other researchers have demonstrated that few users notice the presence or absence of HTTPS encryption and fail to take appropriate precautions when HTTPS is not used.[14] Furthermore, Google employee Alma Whitten wrote one of the foremost studies documenting the human factors which lead to the many problems faced by users who wish to employ encryption.[15]

If Google believes that encryption and protection from hackers is a choice that should be left up to users, the company must do a better job of informing them of the risks so that they are equipped to make this choice. The company currently does very little to educate its users, and the sparse information describing encryption options is hidden, and presented in terms that few members of the general public will understand.

Indeed, Google's disclosures may mislead users about how secure their activities are. When users create a new Google account, or login to Google Mail, Docs, or Calendar, they are not told about the risks they face if they use these services from a public network. However, each time a user logs in to Google Docs, they see promotional text on the login page stating that "Files are stored **securely** online" (bold in original).[16]

Likewise, a *Privacy and Security* page on Google's help site advises customers:

> "Many Google Docs users add personal information to their documents, spreadsheets and presentations, and this information is safely stored on Google's secure servers ... That means by default, your data is private, unless you grant access to others and/or publish your information."[17]

These statements have significant potential to mislead users, who understandably may not know the difference between storage security, access control, and network-transport security. As a result, many users may be lulled into a false sense of safety.

Google's interface design discourages users from enabling encryption

Not only is it hard for users to learn about enabling encryption for Google Mail, Google's interface design discourages them from doing so. Google Mail users can automatically enable HTTPS encryption for all future connections. This preference also protects users from the session cookie theft attacks mentioned earlier in this letter. However, the only way to learn how to do so is to take the time to explore the "Settings" configuration menu, something that few users are likely to do.

Design, as Google knows, is important to shaping users' behavior and expectations. Unfortunately, the design for the HTTPS option nudges users away from good security decisions. This critical security preference is the *last* of thirteen configuration options on the "General" screen of Gmail's "Settings" page, placed below the preferences for the automatic vacation responder, keyboard shortcuts, and outgoing message encoding. The options are not arranged alphabetically, and so the placement creates a strong implied message that this security setting is the least important of all the options listed.

In addition, users can easily be confused by how the setting is presented. The HTTPS preference is labeled "Browser connection", with two options: "Always use https" and "Don't always use https." This text serves users poorly.

Many users are unlikely to know what https means, or understand that enabling this option is critical to protect them from data theft, account hijacking, and snooping. Google's interface fails to explain either the risk or the solutions adequately explained. While there is a "learn more" link to another page with more information on this option, Google does not convey the importance of this setting, and few users are likely to click the link.

Google does have a help page that accurately explains the risks faced by Google users who connect from public wireless networks. The page states:

> "If you sign in to Gmail via a non-secure Internet connection, like a public wireless or non-encrypted network, your Google account may be more vulnerable to hijacking. Non-secure networks make it easier for someone to impersonate you and gain full access to your Google account, including any sensitive data it may contain like bank statements or online log-in credentials. We recommend selecting the 'Always use https' option in Gmail any time your network may be non-secure. HTTPS, or Hypertext Transfer Protocol Secure, is a secure protocol that provides authenticated and encrypted communication." [18]

This page offers users important information, but it is buried five layers deep in Google's help Web site (Google Help › Gmail Help › Your Account › Privacy & Security › Enabling the HTTPS setting). If Google does not enable HTTPS by default – the best strategy -- it is vitally important that information about risk be presented to all users, so that their use of HTTPS is an informed choice, and not merely the result of sticking with a poor default option.

Existing security options fail to adequately protect users

People who use multiple Google services are at particular risk – and Google does not offer them a way to protect themselves adequately. The "always use https" preference in Gmail helps Gmail users (at least those who locate it) safeguard their information. However, this preference *only applies to Gmail sessions*. When those users login to Docs and Calendar, their information again flows over the public Internet *without* the protection offered by HTTPS encryption.

There is no encryption setting available for Docs or Calendar. The only way for users of these other Google services to protect themselves is to remember to type https://docs.google.com and https://www.google.com/calendar into their browser's location bar every time they employ those applications. Google does not explain this difference between applications, and users may incorrectly believe that setting the Gmail preference will protect *all* of their Google sessions.

Google's authentication design puts users at risk. Google uses a single authentication cookie. This means that once users have logged into Google Docs, they do not need to enter their usernames and passwords again when they switch to Google Mail during the same session. This design choice means that an authentication cookie captured from a Google Docs or Calendar session can later be used by criminals to gain access to a Google Mail account – even if the victim attempted to protect herself by setting the "always use https" preference in Gmail. This makes Docs and Calendar sessions the weakest link in the chain of security, and attackers can use this cookie information to steal far more important data that would otherwise have been protected.

Our recommendations

We strongly urge you to follow the lead of the financial industry and enable HTTPS encryption by default for the users of Google Mail, Docs, and Calendar. As Google's own help page notes, mail inboxes often contain "sensitive data … like bank statements or online log-in credentials."[19] Given the huge threat posed by identity theft, it is vital that Google take proactive steps to protect its users from these risks.

Google has long argued that the reason it does not enable HTTPS encryption by default is because of latency-related issues – that is, encrypted data may load more slowly, causing noticeable delays for the user. The company states that it wants users to have the "choice" to enable encryption, so they can weigh the security benefits against possible reductions in interface responsiveness.

We support empowering users. However, rather than forcing users to "opt-in" to adequate security, we strongly urge you to make security and privacy the default setting, and allow informed users to "opt-out" of the encryption if they feel it is an unnecessary burden.

If Google insists on not enabling these encryption-based protective measures by default, the company should at least make the consequences of this decision more prominent, so that users make a fully informed choice. Few users know the risks they face when logging into Google's Web applications from an unsecured network, and Google's existing efforts are little help. We suggest that, at minimum, Google do four things:

1. Place a link or checkbox on the login page for Gmail, Docs, and Calendar, that causes that session to be conducted entirely over HTTPS. This is similar to the "remember me on this computer" option already listed on various Google login pages. As an example, the text next to the option could read "protect all my data using encryption."
2. Increase visibility of the "always use https" configuration option in Gmail. It should not be the last option on the Settings page, and users should not need to scroll down to see it.
3. Rename this option to increase clarity, and expand the accompanying description so that its importance and functionality is understandable to the average user.
4. Make the "always use https" option universal, so that it applies to all of Google's products. Gmail users who set this option should have their Docs and Calendar sessions equally protected.

Google has made important privacy promises to users, and users naturally and reasonably expect Google to follow through on those promises. We therefore urge Google to put the privacy and security of its customers first by making the changes described here.

Thank you.

Affiliations are for identification purposes only, and imply no institutional endorsements.

Jacob Appelbaum
Researcher
The Tor Project

Derek E. Bambauer
Assistant Professor of Law
Brooklyn Law School

Jay Beale
Senior Security Analyst and Co-Founder
InGuardians, Inc.

Thomas A. Berson, PhD, FIACR
President, Anagram Laboratories
Past-Chair, IEEE Technical Committee on Security and Privacy

Ian Brown, PhD
Senior Research Fellow
Oxford Internet Institute
University of Oxford

Steven M. Bellovin, PhD
Professor of Computer Science
Columbia University

Jon Callas
CTO, CSO
PGP Corporation

William R. Cheswick
Lead Member of Technical Staff
AT&T Research

Richard Clayton, PhD
Visiting Industrial Fellow
Computer Laboratory
University of Cambridge

Lorrie Faith Cranor, DSc
Associate Professor, Computer Science and Engineering & Public Policy
Director, CyLab Usable Privacy and Security Laboratory
Carnegie Mellon University

Roger Dingledine
Project Leader and Director
The Tor Project

Benjamin Edelman, PhD
Assistant Professor
Harvard Business School

Nico A.N.M. van Eijk
Professor
Institute for Information Law (IViR)
University of Amsterdam

Allan Friedman, PhD
Post-Doctoral Fellow
Center for Research in Computation and Society
Computer Science Department
Harvard University

Joe Grand
President
Grand Idea Studio

Matthew D. Green, PhD
CTO
Independent Security Evaluators

Robert "RSnake" Hansen
CEO
SecTheory

Chris Hoofnagle
Director - Information Privacy Programs
Berkeley Center for Law & Technology
University of California, Berkeley School of Law

Bart Jacobs, PhD
Professor of Computer Security
Radboud University
Nijmegen, The Netherlands

Markus Jakobsson, PhD
Principal Scientist
Palo Alto Research Center

3ric Johanson
Security Researcher
The Shmoo Group

Jerry Kang
Professor of Law
UCLA School of Law

Ian Kerr, PhD
Canada Research Chair in Ethics, Law & Technology
Faculty of Law, University of Ottawa

Harry R. Lewis, PhD
Gordon McKay Professor of Computer Science
Harvard University

Michael Lynn
Security Researcher

Rob Miller, PhD
Associate Professor, Department of Electrical Engineering and Computer Science
The Massachusetts Institute of Technology

Jeff Moss
Founder and Director
Black Hat and DEFCON
Member, U.S. Department of Homeland Security Advisory Council

Steven Myers, PhD
Assistant Professor of Informatics
Indiana University Bloomington

Peter G. Neumann, PhD
Principal Scientist
SRI International Computer Science Lab,
Moderator of the ACM Risks Forum

Paul Ohm
Associate Professor of Law
University of Colorado School of Law

Ronald L. Rivest, PhD
Andrew and Erna Viterbi Professor of Electrical Engineering and Computer Science
The Massachusetts Institute of Technology

Bruce Schneier
Chief Security Technology Officer
BT Group

Christopher Soghoian
Student Fellow
Berkman Center for Internet & Society
Harvard University
PhD Candidate
School of Informatics, Indiana University

Eugene H. Spafford, PhD
Professor of Computer Science
Executive Director,
Center for Education and Research in Information and Security (CERIAS)
Purdue University

Frank Stajano, PhD
Senior Lecturer
Computer Laboratory
University of Cambridge

Matthew Wright, PhD
Assistant Professor
Computer Science & Engineering
University of Texas at Arlington

Michael Zimmer, PhD
Assistant Professor
School of Information Studies
University of Wisconsin-Milwaukee

Alessandro Acquisti, PhD
Associate Professor of Information Technology and Public Policy
H. John Heinz III School of Public Policy and Management
Carnegie Mellon University

[1] "'In the clear' is a term of art which means without encryption." See: Paul Ohm, Good Enough Privacy, 2008 University of Chicago Legal Forum. (citing Neil Daswani, Christoph Kern, and Anita Kesavan, Foundations of Security: What Every Programmer Needs to Know 204 (Apress 2007)).

[2] See: Eric Rescorla, "HTTP Over TLS (RFC 2818)," Internet Engineering Task Force, May 2000, http://tools.ietf.org/html/rfc2818.

[3] See generally: Mark Jewell, "Encryption Faulted in TJX Hacking," Associated Press, September 25, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/25/AR2007092500836.html

[4] See generally: http://en.wikipedia.org/wiki/Packet_sniffer. Common packet sniffers include Wireshark (http://www.wireshark.org/) and Ettercap (http://ettercap.sourceforge.net/).

[5] See generally: tcpdump, http://www.tcpdump.org/ which is typically included with Linux operating systems

[6] See generally: Nicholas Weaver, "Sidejacking, Forced Sidejacking and Gmail", February 1, 2008, http://blog.icir.org/2008/02/sidejacking-forced-sidejacking-and.html

[7] See generally: Robert Graham, "More SideJacking", January 14, 2008, http://erratasec.blogspot.com/2008/01/more-sidejacking.html. See also: Mike Perry, "Active Gmail 'SideJacking' – https is NOT ENOUGH', Post to Bugtraq, August 06, 2007, http://www.securityfocus.com/archive/1/475658. See also: Kim Zetter, "SSL Gmail Not As Safe As You Thought – UPDATED", January 31, 2008, http://www.wired.com/threatlevel/2008/01/ssl-gmail-not-a

[8] See generally: Mike Perry, "CookieMonster: Cookie Hijacking", http://fscked.org/projects/cookiemonster. Source code available at: http://code.google.com/p/cookiemonster/.

[9] See generally: Ryan Singel, "Gmail HTTPS Doesn't Protect Account, New Setting Does," Wired News Threat Level Blog, August 19, 2008, http://www.wired.com/threatlevel/2008/08/gmail-https-doe/.

[10] "A Pew Internet & American Life Project study from August 2000 found that 84% of Internet users in the United States were concerned about businesses and strangers getting their personal data online. However, 56% did not know about cookies. More notably, 10% said they took steps to block cookies from their PCs. However, a study by Web Side Story found the cookie rejection rate was less than 1%. These data show that while people were concerned about their online privacy, they were unaware of the most significant technology that affects online privacy. While a small proportion of these people claimed to have changed the default setting, the data actually show that a very small percentage, less than 1%, actually change the default setting. In sum, despite the overwhelming concern for privacy, almost everyone deferred to the default setting and accepted cookies." See: Kesan, Jay P. and Shah, Rajiv C., "Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics," Notre Dame Law Review, Vol. 82, pp. 583-634, 2006. See also: Richard Thaler and Cass Sunstein, Nudge: Improving Decisions About Health, Wealth, and Happiness (Yale University Press, 2008). See also: Carroll, Gabriel D, Choi, James J., Laibson, David I., Madrian, Brigitte C. and Metrick, Andrew, Optimal Defaults and Active Decisions, NBER Working Paper Series, 2005, Available at SSRN: http://ssrn.com/abstract=653021

[11] See: Ariel Rideout, "'Making Security Easier," The Official Gmail Blog, July 24, 2008, http://gmailblog.blogspot.com/2008/07/making-security-easier.html.

[12] See: Andy Palay, "New in Labs: Offline Gmail," The Official Gmail Blog, January 27, 2009, http://gmailblog.blogspot.com/2009/01/new-in-labs-offline-gmail.html.

[13] "[T]he broadcast nature of Wi-Fi means that anyone within range of the network can receive and potentially read transmissions intended for any other device on the network… Despite living in a technologically sophisticated area of the U.S., the participants were not aware that information sent over Wi-Fi could be seen by others." See: Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., and Wetherall, D., "When I am on Wi-Fi, I am fearless": privacy concerns & practices in everyday Wi-Fi use. In *Proceedings of the 27th international Conference on Human Factors in Computing Systems,* 2009. http://www2.seattle.intel-research.net/~jjung/FormativeUserStudy4CHI.pdf

[14] "Prior studies have reported that few users notice the presence of HTTPS indicators such as the browser lock icon. Our results corroborate these findings and extend them by showing that even participants whose passwords are at risk fail to react as recommended when HTTPS indicators are absent." See: S Schechter, R Dhamija, A Ozment, I Fischer , "The Emperor's New Security Indicators: An evaluation of website authentication and the effect of role playing on usability studies," IEEE Symposium on Security and Privacy, 2007. http://www.usablesecurity.org/emperor/

[15] See generally: Alma Whitten and J. D. Tygar, “Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0,” Proceedings of the 8th USENIX Security Symposium, 1999, http://www.gaudior.net/alma/johnny.pdf

[16] See: http://docs.google.com

[17] See: “Privacy and Security: Keeping Data Private,” http://docs.google.com/support/bin/answer.py?hl=en&answer=87149

[18] See: “Enabling the HTTPS Setting,” http://mail.google.com/support/bin/answer.py?answer=74765&cbid=1weqt2sh3wpti&src=cb&lev=answer

[19] See: “Enabling the HTTPS Setting,” http://mail.google.com/support/bin/answer.py?answer=74765&cbid=1weqt2sh3wpti&src=cb&lev=answer