Americans' Access to Strong Encryption Is at Risk, an Open Letter to Congress

May 3rd, 2017 ♦ Written by Frank Rietta ♦ Comments

Dear Honorable Members of the United States Congress:

I work in application security in the cybersecurity field to make software more secure from attack. The cybersecurity threats that face our nation are very important to my wife and me. As Americans, our private data is in great jeopardy because of increased cybersecurity threats. Our infrastructure is prone to being hacked, and major data breaches of both private and government networks are routinely in the news. The best way to prevent these breaches is to increase the use of strong encryption with *no backdoors*.

The track record of data breaches demonstrates an uncomfortable truth: when sophisticated adversaries want to hack a network, they will ultimately win. Among the few tools known to computer science that can prevent a data breach is strong encryption. This means that there is no backdoor and no backup key. Either the original user needs to enter the password, or the data is un-retrievable.

While having the ability to access private information for criminal investigation seems to protect Americans, the technology for this will leave a backdoor open to the general public's private information also. This is because there is not a technologically feasible way to build an encryption backdoor that cannot be compromised by hackers or foreign enemies. This ultimately means that Americans are made less safe with government-mandated backdoors. One example is the hacking of Juniper Networks' firewalls through a backdoor in their software.

As a professional in information security, it is my stance that strong encryption is the best way to protect the privacy and safety of all Americans' information and our cyber infrastructure. If the government starts to require backdoors into encryption, this is equivalent to government-mandated insecurity in our software.

I want to be very clear about my use of the term backdoor. Even today, Wednesday, May 3, 2017, in testimony before the Senate Judiciary Committee, FBI Director James Comey insisted that "none of us want backdoors" in response to a question by Senator Hatch (TechCrunch article (https://techcrunch.com/2017/05/03/fbi-director-comey-backs-new-feinstein-push-for-decrypt-bill/)). Let me be clear. This distinction that the Director makes has no basis in fact or science. Any imaginable key escrow system that would by design provide routine access to encrypted data is a backdoor that will be able to be hacked. Any such system of so-called lawful intercept is an unfixable, mandated security vulnerability that will make Americans less safe both at home and abroad.

The matter of strong encryption versus government-mandated backdoors to accommodate lawful intercept is likely to come before this Congress. Think carefully about your stance because what you do will determine the fate of American's freedom to encrypt so that their data is protected from being stolen.

I am available to discuss this strong encryption topic with you and your staff.

Respectfully,

Frank S. Rietta

CEO of Rietta, Inc., a Web Application Security Firm

About Frank Rietta

 (/about/#frank-rietta)

Frank Rietta (/about/#frank-rietta) is a web application security consultant, software developer, author, and speaker. He is a computer scientist with a Masters in Information Security from the College of Computing at the Georgia Institute of Technology. He teaches about security topics and is a contributor to the security chapter of the 7th edition of the "Fundamentals of Database Systems" textbook published by Addison-Wesley.

Follow @frankrietta Tweet to @riettainc

Written by Frank Rietta May 3rd, 2017

« Breach Prevention for Developers Talk at Kennesaw State University (/blog/2017/02/28/breach-prevention-for-developers-at-kennesaw-state-university/)

Comments

Recent Blog Posts

- Americans' Access to Strong Encryption Is at Risk, an Open Letter to Congress (/blog/2017/05/03/americans-access-to-strong-encryption-is-at-risk/)
- Breach Prevention for Developers Talk at Kennesaw State University (/blog/2017/02/28/breach-prevention-for-developers-at-kennesaw-state-university/)
- Intro to App Sec Podcast Interview (/blog/2017/02/22/intro-to-app-sec-podcast-interview/)
- The MongoDB Hack and the Importance of Secure Defaults (/blog/2017/01/12/the-mongodb-hack-and-the-importance-of-secure-defaults/)
- CPU Benchmark - Raspberry Pi vs AMD Athlon vs Mac Mini (/blog/2016/12/01/cpu-benchmark-raspberry-pi-vs-amd-athlon-vs-mac-mini/)

► Blog Archives (/blog/archives)

As a Developer, You Can Prevent a Data Breach.

(/learning/appsec/)

Rietta's Web Application Security Learning Center (/learning/appsec/)

About Rietta

As an Atlanta-based Ruby on Rails web development consultancy, Rietta builds custom web applications that solve *specific* business needs.

For more, see how our our process focuses on what's most important (/process/).

Call Us Today

(888) 250-6435

About

- Testimonials (/testimonials)
- Services (/services)
- Development Process (/process)
- FAQ (/faq)

- Contact Us (/contact)
- Security Disclosure (/contact/security)

Learn

- Apprenticeship (/apprenticeship)
- Community (/community)
- Craftsmanship (/craftsmanship)

Resources

- Blog (/blog)
- Learn Web Application Security (/learning/appsec)
- Newsletter (/newsletter)
- Legacy Software (/legacy#software)

(https://www.linkedin.com/company/rietta-inc-) (https://www.facebook.com/riettainc) (https://plus.google.com/b/109371973878019519458) (https://twitter.com/RiettaInc/)