Most used passwords: IEEE accidentally exposed 100,000 unencrypted user credentials

By Matthew DeCarlo
On September 26, 2012, 6:30 PM EST

A Romanian researcher who recently found plaintext usernames and passwords on an IEEE (Institute of Electrical and Electronics Engineers) server has published his analysis of the data. Radu Dragusin, a computer scientist who works for search engine FindZebra, discovered the unsecure data on an IEEE FTP server last week.

Dragusin reports that 100GB of log files were open to anyone who visited a specific URL (now closed) for at least one month and contained unencrypted account credentials of nearly 100,000 IEEE members, which includes employees of Apple, Google, IBM, Oracle, Samsung, NASA, Stanford and many other organizations.

Dragusin reported the issue to the IEEE this Monday. The electronics association has since responded with what Dragusin calls a "partial" fix. He noted that the publicly accessible logs could have been a simple mistake with permissions, but storing sensitive information such as user credentials in plaintext is less forgivable.

Dragusin doesn’t plan to share the data with anyone, there’s no telling who else may have wiped it off the server. Instead of deleting his copy, he has decided to use it for analysis including the location of affected users (above), the most used passwords, a chart of email domains and a graph of browser preferences.

Compromised IEEE members span practically every continent, with particularly high concentrations in the US, the UK, India and China. Of the 99,979 unique accounts exposed, 271 of them were "secured" with the password "123456," the second most used password was "ieee2012," while the third was "12345678."

The word "password" itself was one of the most used passwords, while other accounts used "admin," "student," "library," and "ADMIN123." We’ve seen the same types of weak passwords in previous breaches, but you’d think members of a technology organization like the IEEE would be a little more security conscious.

Unsurprisingly, Gmail was the most popular email with 38% of the pie, while Yahoo held second place with 7.6%. Hotmail ranked third with 4.7% and IEEE.org was fourth at 3.5%. The three major browsers had a similar share, though Chrome was consistently the most used, followed by Firefox and then Internet Explorer.

Data breach at IEEE.org: 100k plaintext passwords.

Using the data to gain insights into the engineering and scientific community

IEEE suffered a data breach which I discovered on September 18 (UPDATE: the breach is now confirmed). For a few days I was uncertain what to do with the information and the data. On September 24, I let them know, and they fixed (at least partially) the problem. The usernames and passwords kept in plaintext were publicly available on their FTP server for at least one month prior to my discovery. Among the almost 100,000 compromised users are Apple, Google, IBM, Oracle and Samsung employees, as well as researchers from NASA, Stanford and many other places. I did not and will not make the raw data available to anyone else.

IEEE and the log story

IEEE (Institute of Electrical and Electronics Engineers) is renowned as one of the world-leading organizations in standard development and the promotion of scientific and educational development within the Electrical, Electronics, Communications, Computer Engineering, Computer Science and related fields. The organization has more than 415,000 members all over the world, almost half of them in the United States [1].

By the nature of the organization, IEEE members are highly specialised individuals, many of them working in critical industry, governmental and military projects. Furthermore, it would be reasonable to assume, that an organization publishing leading security-focused publications [2], would value the privacy of its members, and be proactive in keeping their data secure.

Due to several undoubtedly grave mistakes, the ieee.org account username and plaintext password of around 100,000 IEEE members were publicly available on the IEEE FTP server for at least one month. Furthermore, all the actions these users performed on the ieee.org website were also available. Separately, spectrum.ieee.org visitor activity is also publicly available.

The simplest and most important mistake on the part of the IEEE web administrators was that they failed to restrict access to their webserver logs for both ieee.org and spectrum.ieee.org allowing these to be viewed by anyone going to the address ftp://ftp.ieee.org/uploads/akamai/ (closed on September 24 around 13:00 UTC, after I reported it). On these logs, as is the norm, every web request was recorded (more than 376 million HTTP requests in total). Web server logs should never be publicly available, since they usually contain information that can be used to identify users (sometimes even after the log was anonymized as in the "AOL incident" [3]). However, this case is much worse, since 411.308 of the log entries contain both usernames and passwords. Out of these, there seem to be 99,979 unique usernames.

If leaving an FTP directory containing 100GB of logs publicly open could be a simple mistake in setting access permissions, keeping both usernames and passwords in plaintext is much more troublesome. Keeping a salted cryptographic hash of the password is considered best practice, since it would mitigate exactly such an access permission mistake. Also, keeping passwords in logs is inherently insecure, especially plaintext passwords, since any employee with access to logs (for the purpose of analysis, monitoring or intrusion detection) could pose a threat to the privacy of users.

Log analysis

It is certainly unfortunate this information was leaked out, and who knows who got it before it got fixed. Maybe there are access logs for the FTP so the damage can be assessed. Anyway, the affected users will probably have to be informed, since it is my understanding that the law requires it (UPDATE: IEEE informs members). In Europe there is Article 4 of the Directive on privacy and electronic communications ([Directive 2002/58/EC] and its amendment [@directive 2009/116/EC]). In the US, 46 states seem to have similar requirements [4].
While the cause of the data breach has been solved, one must point out the value of this dataset from a research perspective. It is rare that researchers gain access to such rich datasets. Various ethical and privacy-related considerations must be evaluated before such datasets can be publicly released. Deciding on how to anonymize the data is no easy challenge. Simply excluding any information making users directly identifiable is not enough, as past dataset releases have shown that some users can still be pinpointed. This resulted in lawsuits in the case of Netflix [5] and AOL [6], or the withdrawal of the data, like in the recent Wikipedia case [7]. For this reason, companies such as Google prefer to keep such data for study by internal researchers and do not release it to the public [3]. Furthermore, some companies release data to a trusted researcher with the condition to remain anonymous, like an unnamed European mobile phone operator did for Albert-László Barabási [8]. This means academic researchers working in such fields as Information Retrieval have limited access to fresh real-world data, being at a disadvantage to their industrial counterparts.

For these reasons, I cannot give in to the urge to perform a basic analysis of this serendipitously acquired data, although I acknowledge this might be ethically dubious. However, I did not, and plan not to release the raw log data to anyone else.

**Data overview**

- Log data time span: 01/Aug/2012:20:46:28 +0000 to 18/Sep/2012:08:47:17 +0000
- Total number of log entries: 376,021,496
- Log entries for ieee.org: 301,319,566
- Log entries for spectrum.ieee.org: 74,701,930
- Log entries with password details: 411,308 (of which 17,157 are password reset requests and have no username field)

The following analysis is only based on the 411,308 log entries with password details, accounting for 99,979 distinct username values.

All compromised IEEE members plotted on the World map. (IP geolocation)

Compromised IEEE members in Europe.
Compromised IEEE members in USA.

Japan

United Kingdom

Germany

Most used passwords
123456
ieee
201212345678
123456789
password
library
123456789012312345123
ADMIN123
IEEE2012student.ieee2011SUNIV358Passwordabcd1234admin209160230300usersusers

Email domain name pie
cart@gmail.com
com.yahoo.com
iee.org
yaho.co.in
163.com
rediff.com
mail.com
qq.com
yahoo.in
ymail.com
126.com
comcast.net
ups.edu
ecaol.com
live.com
commail.runsn.com
yahoo

Web browsers line chart
Internet Explorer:322
Firefox:402
Opera:21
Chrome:369
Android:15
Safari:12
Safari - mobile:3

Citations