

# **HDFC Security Flaw Part 1**

## **SPF Auth Failure**

Author: Aseem Jakhar  
Email: [null\\_at\\_null.co.in](mailto:null_at_null.co.in)  
null security community ( <http://null.co.in> )

## **Introduction:**

It is wisely said that nothing is perfect. Security issues can creep up anywhere anytime but given that fact one still needs to be fully knowledgeable of the security scheme that is deployed to make the best use of it, failing which can open doors for malicious activities. A customer of a bank depends on its security infrastructure to keep her data secure and most importantly her money intact. HDFC is a well known and a very large banking organization in India. This paper (i.e. Part 1) discusses the security issues with of HDFC bank's DNS SPF records. The next paper will be out when they fix another serious issue which I reported to them (of leaking customer data) or start ignoring my email follow-ups on it (responsible disclosure :-P).

## **March 2008:**

One fine Sunday morning as I was sipping on my Nescafe and browsing through my emails, being the curious person that I am, I opened the headers of an alert mail from HDFC bank. To my surprise what I saw made me go :-O. The mail had soft failed SPF auth. At first I couldn't believe it, but curiosity got the better of me and I put on my engineer hat and opened a shell and started dig'ing deeper.

I queried the DNS TXT records of hdfcbank.com and found that the mail server that had sent the mail indeed was not listed in the DNS TXT records of hdfcbank.com. Holy Cow! What if this mail goes to my spam box, I would not come to know whether there was a transaction done on my account. HDFC sends out alert emails to its users when an online transaction is done through net banking.

## **Sender Policy Framework (SPF) Protocol:**

It's a simple protocol that uses DNS TXT records for a domain to list all the SMTP servers that are authorized to send mail to the internet on that domain's behalf. For the curious people like me you can check out RFC 4408 which describes the "Sender Policy framework" protocol in detail.

Ex:

```
$ dig -t TXT hdfcbank.com
```

```
...
```

```
...
```

```
:: ANSWER SECTION:
```

```
hdfcbank.com.      300  IN   TXT  "v=spf1 ip4:203.124.232.70 a mx ptr  
a:relay1.hdfcbank.com a:relay4.hdfcbank.com a:relay.hdfcbank.com  
a:relay3.hdfcbank.com a:relay2.hdfcbank.com a:relay5.hdfcbank.com  
include:smtp.centurionbop.co.in ~all"
```

```
...
```

```
...
```

## **The Problem:**

The alert emails from HDFC bank generate “Softfail” for SPF records. It means (in terms of SPF standard for SMTP server auth) that the machine that sent this mail out is not authorized to send mail on behalf of hdfcbank.com and can be treated accordingly by spamfilters. In other words it is a phishing email from the antispam engine’s point of view. Though the protocol says that it is not as harmful as a “fail”, spamassassin gives it a good amount of score (1 to 2.5, “5” being the threshold for spam) for softfail’ing as well.

## **A sample HDFC alert email header:**

```
Received: from dl360.air2web.co.in ([210.210.1.31])  
by mx.google.com with ESMTP id 30si5200184wff.18.2008.06.21.06.08.08;  
Sat, 21 Jun 2008 06:08:09 -0700 (PDT)  
Received-SPF: softfail (google.com: domain of transitioning  
alerts@hdfcbank.com does not designate 210.210.1.31 as permitted  
sender) client-ip=210.210.1.31;
```

The mail was sent from dl360.air2web.co.in which is not an authorized outbound SMTP Server for hdfcbank.com based on hdfcbank.com’s SPF record.

## **The Consequences:**

- 1) This can result in mail delivery issues such as being treated as spam and not being delivered to the user’s inbox.
- 2) Online reputation of the machine sending these mails can be at stake and hence may get blacklisted.
- 3) From the user’s point of view, some cracker might have made transaction on the victims account and the alert mail might never reach the victim and he may not come to know about it immediately.
- 4) From HDFC’s point of view. The machine can get blacklisted because of the failing behavior and also it is an embarrassment for such a large banking organization that failed to put its security policies in place.

## **Reporting to HDFC customer care:**

### **March 2008**

I sent 2 reports describing the problem to HDFC through email and web. As expected there was a very cold response.

## **July 2008:**

I attended InfoSec Conference 2008, Mumbai where I reported the issue to HDFC's Chief Information Security officer and gave him a few options on how they could change their policies to solve the issue:

- Adding the alert email sending machine to the SPF record.
- Redirecting their alert emails to another email outbound server which is listed in the SPF records.

## **September 2008:**

I received a couple of mails from HDFC security staff on what problems they are facing to resolve the issue but they still haven't fixed it since that operation is outsourced to some other organization (you could tell that from air2web.co.in SMTP server :-P). I suggested they tell the vendor to add SPF records for their server and change the SMTP "mail from" (return-path) to say "[hdfcalerts@air2web.co.in](mailto:hdfcalerts@air2web.co.in)" instead of [alerts@hdfcbank.com](mailto:alerts@hdfcbank.com) since the actual sender is indeed air2web.co.in and not hdfcbank's mail server.

## **December 2008:**

I was told that they (HDFC) will be adding DKIM support to get around this problem to which I replied that the SPF if not fixed will still remain a problem as it is independent of DKIM protocol (it creates a digital signature for an email, Curious? Google: DKIM rfc ☺)

## **March 2009:**

Finally I get to see some action from HDFC (based on the news in TOI 12<sup>th</sup> Mar 09). Honestly I'm not happy with the response time they took for taking necessary action. It has still not been fixed though.

## **Conclusion:**

- Can we blindly trust any organization to keep our information secure?
- Is it our job also as a user to safeguard ourselves and to keep an open eye on any security issues that may arise out of the blue?
- Better informed is better armed.

To Be Continued....

Disclaimer: I am making this information public only to help people understand the security implications when dealing with different security protocols and only after HDFC publicly announced (in Times of India newspaper dated March 12<sup>th</sup> 2009) that they are using signature technology for sending outbound mails. I am not responsible for any malicious use of the above information.