The hack that never happened

Pranesh Prakash

2016-12-05

The Ken

Abstract

The NaMo app left 7 million people's personal information at risk, despite having been told about the flaw more than a year ago.

Data security shouldn't be political. It applies to all of us. Each one of us. Which is why this story is important.

The morning of December 2, news portal YourStory published an unsigned story titled "22-year-old hacker from Mumbai hacks Narendra Modi app, exposes threat to 7 million user data". In it Javed Khatri, a 22-year old mobile developer from Mumbai, makes the following claim:

> *"I am able to access private data of any user on the app. The data includes phone number, email, name, location, interests, last seen etc. I successfully managed to extract the personal phone numbers and email ids of ministers like Smriti Irani (screenshot at the end of the article). Please find attached the screenshot.*
>
> *"Not only that, I can make any user on the platform follow any other user on the platform. This is just the summary of this huge security loophole which I want to report. The privacy of more than seven million users is at stake if this gets ignored."*

The app Khatri was referring to was the official Android app of Indian Prime Minister Narendra Modi (NaMo app, for short), with over 7 million users.

Yet within hours, the story had vanished entirely from YourStory's site, with the site implementing an HTTP 302 to redirect visitors to its home page instead. After radio silence from the site all through the day as social media users pilloried it for having deleted the article without any explanation, it put out a clarification later that evening.

Khatri's website went down as well (and still was, at the time of writing this article), though it isn't clear whether that was intentional or not.

Except for a handful of smaller players, none of the leading Indian newspapers, TV channels or online news portals covered the news. It was as if this never happened.

That's not even the shocking part. It is this: this flaw was reported more than a year ago and even now hasn't been properly fixed.

This "non-hack" — since it exploits some very basic flaws, making it like picking a lock made of paper — is a significant one because it sits at the intersection of various trends like digital citizen-government interactions, exploding mobile usage especially by first-time technology users, data security, and legal protection. Understanding this will require some patience, so with sleeves rolled up, let's dive in.

Technology enables, technology exposes

How does the Narendra Modi app work? It has a great many features, including a newsfeed, a social network, a survey component, etc., and also has gamification in the form of badges. People are encouraged to provide personal details, being told that registration will enable them to: "join the conversation and be heard", "contribute with special tasks", "earn special credit points for every activity on the app", and "receive personalised birthday greetings directly from PM Modi". Given the gamified nature of the app, this can be quite persuasive. The personal information they are asked to provide include their date of birth, phone number, e-mail address, state and district, profession, interests (yes, this is mandatory), and voter ID (non-mandatory, but it is easy to miss that fact), and access to their contact list (for automated discovery of friends who also use the app). They are also required to provide a password. The app also has permissions to "read the contents of your USB storage" and "modify or delete the contents of your USB storage".

All this stands in stark contradiction to what Amit Malviya, the Bharatiya Janata Party's (BJP) National Convener — Information & Technology wrote in a statement to YourStory:

> "The App doesn't capture any private or sensitive data."

This clearly doesn't comport with what has been described above. He went on to say:

> "App user's information is stored in an encrypted mode. We take data security very seriously, and adequate measures are in place to avoid any possible security breach or threat."

As we will see, this is simply not true.

The NaMo app used to communicate with its servers using an "API", a way to standardize data transmission to and from a server, located at http://api.narendramodi.in/api/. Do note the "http" at the beginning of that address instead of "https". This means that information communicated between the app and the server can take place without any encryption. This also meant that an attacker could "sniff" the traffic flow between the app and the server and find out people's passwords. This was finally fixed in September 2015, after a report by Bhavyanshu Parasher. However, the BJP (the app is operated by the Bharatiya Janata Party rather than the government) did not ask people to change their passwords even though they realised that this flaw left passwords vulnerable.

Parasher's vulnerability reports to the BJP in September and October 2016 (which I have a copy of since I helped facilitate that dialogue as Parasher on his own wasn't able to get the developer's attention despite e-mailing them) also noted that the API was not authenticating the requester or poster of information. That meant that Parasher could request anyone's information simply by changing the "user id" field in his requests to the API. Given that these User IDs are sequential numbers, he noted that anyone could download everyone's details. He also showed that he could post comments pretending to be someone else, as the API simply wasn't checking who was doing the posting.

While in October 2015, the developers did fix the problems that Parasher identified, they did not do so in the way that he had suggested. They simply applied band-aids on the immediate problems, whereas the problem was in the very design of the API and the app. As Parasher writes, " The only solution to this problem is to rewrite the API from scratch and add standard auth[entication] methods for API. That should take care of most of the vulnerabilities."

Hence, more than a year later, Javed Khatri rediscovered these flaws and informed YourStory about it before waiting for the developers to (again) fix the issues. Apparently, at some point the band-aids had fallen off, leaving all this information public. This was a simple flaw, not something that it took great ingenuity to discover. The article in YourStory provided sufficient detail to allow others to replicate it with ease since exploiting the flaw wasn't difficult at all. (A separate article is waiting to be written on the ethics of responsible disclosure of security vulnerabilities by journalists and security researchers.) Srinivas Kodali, a researcher, noted (with screenshots) that it took him "less than 5 minutes" to gain access to more than 7 million people's data after he read about the flaw.

> 2 Dec
>
> ![]Srinivas kodali @iotakodali3
>
> Anyone want some expert review of the #PM app hack. Get in touch#cybersecurity
>
> ![]Srinivas kodali @iotakodali3
>
> Once the hack is out, anyone can replicate it. Here it took me less than 5 minutes. #cybersecurity #privacy #modi @PMOIndia
>
> 6:54 PM - 2 Dec 2016

What have the NaMo app developers done? They've replaced everyone's e-mail addresses to xyz@xyz.com (sidenote: the domains "example.com", "example.net", and "example.org" have been reserved by the IETF for precisely such dummy-value purposes). They've also replaced everyone's phone numbers with "+91 0000000000". Other details, including organization, profession, their photo, and district/city are still available. And they are transmitted in standard JSON format to whoever asks. "Encryption" of the data on the narendramodi.in servers (if it is indeed happening) is pointless since they seem to have the decryption key on the same server and make the data available in unencrypted fashion to everyone. Thus, every part of Mr. Malviya's statement is seen to be simply untrue.

An important question remains: why haven't the developers fixed this properly, as was suggested by Parasher more than a year ago? Because doing so would have entailed redesigning the API and that would require them getting everyone to update their app. Should they have preferred backward compatibility over security and privacy? It is clear that given the personal details of millions of Indians, they should have forced people to upgrade their apps. For a party that is okay with the hardships caused by the removal of 86.4% of the currency in circulation, it is odd that the idea of forcing people to upgrade their apps seems a step too far.

When it comes to data security, the law is an ass

India lacks a proper legal framework for data protection and data security. The closest we come to such a law is the horrendously drafted section 43A of the Information Technology Act, which has the semblance of being a provision that allows for compensation (under limited circumstances) upon instances of "wrongful loss or wrongful gain" arising from the lack of reasonable security practices.

While the narendramodi.in website has no internal link to its privacy policy, on the Google Play Store, the NaMo app provides a link to a privacy policy that clearly states that: "Your personal information and contact details shall remain confidential..." Perhaps, "personal information" includes other information that the app collects, like your contact list as well, but that isn't clear.

I have already described their lax security practices. So the core issues for the legal analysis of this situation are:

1. Is the app a government app or is it by a "body corporate"
2. Were "reasonable security practices" followed?
3. Was there a "wrongful loss" or "wrongful gain"?

It seems the BJP seeks to have it both ways when it comes to this app. They have clearly used government (DAVP) funds to advertise the NaMo app, yet the details on the Google Play Store and the narendramodi.in website seem to suggest that this is wholly run by the BJP political party and not the NDA government. Given that it is the BJP that responded to the data breach rather than the central government, it seems clear that it is the BJP that is responsible for the NaMo app. The BJP, quite clearly, is a "body corporate", so section 43A is applicable to this case.

On the question of reasonable security practices, it seems rather clear from what I have shown earlier that there has been a rather reckless attitude taken towards security by the developers who still haven't really fixed the issue and only taken stop-gap actions that prevent the immediate damage, despite having been told more than a year ago of the glaring holes in their API's security.

On the third question, given glaring nature of the problem, it is unimaginable that people other than Parasher, Javed Khatri, and those who admitted to gaining access to the data like Sriniva Kodali, were the only ones who noticed it. In the aftermath of the YourStory article, I had tweeted that narendramodi.in ought to immediately cut access to the API. They did not do so. So clearly, a wrongful loss has almost certainly happened, and a careful perusal of the server logs of narendramodi.in should be able to prove that.

In short, even under India's astoundingly shoddy data breach law, this seems to be as clear a case as can be that the NaMo app developers should have to compensate their users.

Users are the weakest link in the chain

There is a developer called "Government of India" on the Google Play store, with e-mail addresses like "govtjobs@gmail.com", "info@bjpup.xyz", and "info@narendramodi.press". Two of the apps made by this developer called "Narendra Modi" and "MyGov" each have between 100,000 and 500,000 downloads. I traced back the creator of those apps by looking at the registration details of "bjpup.xyz" and "narendramodi.press". They were registered using a privacy proxy, but they were both hosted on a server belonging to a Bangladeshi resident named "Surid Halder Shayan" (who might have let someone else use it, though that looks improbable). So up to a million people have been duped by a developer called "Government of India". These apps even requested permissions to access photos and other media stored on the device, and to be able to use the phone's camera, so surreptitious photos and videos could have been clicked by the app (with precise location information, since GPS permissions were also requested).

Being shocked by this, I used Google's reporting mechanism to complain about both the apps on December 3, yet I haven't received even an acknowledgement from Google, leave alone an update. Needless to say, both these apps are still online as of this writing.

There are more than a dozen apps on the Google Play Store that have "Narendra Modi" or "Namo" in their name. Clearly that is a problem, and going by the high ratings of many of these apps, it is clear that regular users cannot tell the difference. How could casual users tell the difference when even the developer of the genuine NaMo app uses the e-mail address "narendramodi1234@gmail.com"?

This is clearly not a problem limited to the NaMo app. While browsing throught the Google Play Store, I found an app ostensibly made by "State Bank of India UK" which is developed by "rosie@goliveuk.com".

Surprisingly, or by now, unsurprisingly, even the genuine "MyGov" app by the Indian government has the contact e-mail as "mygov.mobile@gmail.com", which is an email address that could have be registered by anyone. (The only way I know it is genuine is because it is linked to from the MyGov website.)

Fixing time

Firstly, we need the BJP to take responsibility for what has happened and to fix things properly (yes, by redesigning the API and using standard security techniques), rather than to mendaciously claim that there is no personal data stored by narendramodi.in. They should update the developer information on all app stores to make it clear that "narendramodi1234@gmail.com" is, in fact, a genuine developer. They should also explain to users why they need each of the permissions they seek while the app is installed. On older versions of Android, users do not have an option to individually reject permissions. (And as I noted, even if one denies the permissions the app requests to gain access to one's photos and other media, that request pops up every few seconds.) They also ought to inform all their users and ask them to change their passwords, especially if they registered before October 3, 2015.

Secondly, Google, Apple, and Microsoft should ensure that there is some way of verifying the authenticity of certain developers' names, the way Twitter and Facebook do. People expecting to download an app from a bank or from a government shouldn't be defrauded. The central and state governments should immediately search these app stores for such deceptive apps, and notify the app stores, and initiate legal action for passing off.

Thirdly, we need laws on data protection and safeguard citizens' privacy. I'm aware of no movement on the Privacy Bill over the last three years. Importantly, the government cannot be exempt from such a law, the way the government is exempt from section 43A of the IT Act. A strong data protection law would necessarily include data breach notifications to all consumers and potentially affected persons.

Lastly, we need the government to take information security seriously. There are knowledgeable and talented people in India who can help it. Some of them work at National Technical Research Organisation. More of them need to be hired by MEIT and MEIT should have a data security (as well as an accessibility) checklist when it outsources app development. These apps should request the minimum permissions needed and should explain clearly why those are required. Those apps should also be registered using a .GOV.IN e-mail address. As Kodali argues, the NaMo app scandal is just the tip of the data security nightmare that researchers have furiously trying to get the government to fix.