Comments on “Protecting the Privacy of Customers of Broadband Other Telecommunications Services”, Docket 16-106

Steven M. Bellovin[*]
smb@cs.columbia.edu
https://www.cs.columbia.edu/~smb

Thank you for the opportunity to submit comments on your NPRM on “Protecting the Privacy of Customers of Broadband Other Telecommunications Services”, and in particular on ¶¶ 192 *et seq.*, “Robust Authentication Requirements”.

By way of introduction, I am the Percy K. and Vida L.W. Hudson Professor of Computer Science at Columbia University, where my research has focused on Internet security and privacy. I am the author or co-author of several books on security.[1] I have served in a high-level technology advisory position at the Federal Trade Commission and am currently in a similar position at another government agency, though I hasten to add that my comments are purely personal opinions and in no way represent the opinions of any government agency or my university.

No authentication mechanism (indeed, no security policy or mechanism) can be selected without consideration of the threat model.[2] In this case, I suspect that there are two primary threats: more or less random attacks by people on the Internet, for the sheer joy of vandalism, and family members, including estranged spouses. The two threats demand different responses.

In neither case is an ordinary password suitable. People rarely change their broadband service; there is little chance that people will either pick suitable passwords or remember them. People will pick something trivially guessable, such as “`123456`”, or they forget their “strong” passwords and resort to secondary authentication mechanisms.[3] These mechanisms, though, are often quite weak.[4] A better design would forgo passwords entirely; they will add little, if any, security, but will result in annoyance.

Family members pose a very serious and difficult-to-cope-with threat. The “attacker” may be a teenager who wants increased bandwidth or the removal of a BIAS-provided (but parent-requested) content filter. Alternatively, it may be an estranged spouse or domestic who wishes to harass the other party to the relationship.[5] I am aware of instances where one spouse, after having moved out, disconnected the utilities to the former marital residence. While the ultimate recourse in such situations is likely the legal system, including restraining orders, BIAS providers should be required to provide account lock capabilities: once an account is locked, no change requests will be accepted except in person with strong identification or via notarized written request. I note that telephone companies and power companies have long had such provisions.

Again, passwords and the usual recovery questions are quite unsuitable against this sort of threat. Spouses often share passwords (and sometimes even email accounts) and know each others’ pasts. Many people write down their

[*] Affiliation listed for identification purposes only.

[1] William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security: Repelling the Wily Hacker*. 1st ed. Reading, MA: Addison-Wesley, 1994. ISBN: 0201633574. URL: `http://www.wilyhacker.com/1e/`, William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin. *Firewalls and Internet Security; Repelling the Wily Hacker*. 2nd ed. Reading, MA: Addison-Wesley, 2003. ISBN: 078-5342634662. URL: `http://www.wilyhacker.com/`, and Steven M. Bellovin. *Thinking Security: Stopping Next Year’s Hackers*. Boston: Addison-Wesley, 2016. ISBN: 978-0-13-427754-7. URL: `http://www.informit.com/store/thinking-security-stopping-next-years-hackers-9780134277547`.

[2] *See* Chapter 3 of *Thinking Security*, foonote 1, *supra*.

[3] *See*, e.g., Dinei Florêncio, Cormac Herley, and Baris Coskun. “Do Strong Web Passwords Accomplish Anything?” In: *Proceedings of HOTSEC ’07*. 2007. URL: `http://www.usenix.org/events/hotsec07/tech/full_papers/florencio/florencio.pdf`.

[4] *See* Chapter 7 of *Thinking Security*, foonote 1, *supra*.

[5] It may not be just harassment. With the rise of the Internet of Things, including Internet-controlled door locks, considerably more may be at stake than peace of mind.

passwords; while this is a reasonable defense against Internet attackers, it is useless against someone with physical access to the computer and surrounding surfaces. For that matter, family computers are often left unlocked, in which case cached authentication credentials may be available in browsers.

What I have described as "random Internet attacks" can be quite vicious and directed, especially towards women and minority group members.[6] Strong security may be necessary to defend against these attackers, too.

The most common means of two-factor authentication involves sending a "text" (SMS) message to the user's phone. While this is a good defense against random attackers, it is of little use against a determined, targeted attack. Even apart from what a spouse with control of the phone account can do, it isn't that hard to steal someone's cell phone service. Dr. Lorrie Cranor, Chief Technologist of the Federal Trade Commission, was victimized in precisely that fashion.[7] Again, someone who has knowledge of the victim—an estranged spouse, an Internet attacker with a grudge, etc.—can easily gather the additional information (such as social security number) needed.[8]

I therefore suggest three different mechanisms. The first is a smartphone app. Most newer smartphones provide some means of biometric authentication, such as a fingerprint reader. While biometrics are by no means perfect,[9] they are more than adequate here: the biometric never leaves the secure device, and the devices is generally in the possession of the user. This provides very strong protection against remote attackers, and while one can certainly imagine physical force being employed by an irate family member, that sort of attack is much better dealt with by law enforcement: the victim of such behavior would have many more serious problems than lack of Internet access. For phone access, such an app could generate a single-use authentication code.

Not everyone has a smart phone, let alone a new-enough model. A second form of authentication relies on commercial data brokers:[10] use their data to ask unusual questions. This technique is already in commercial use by financial services firms that need to grant online access to pre-existing accounts, e.g., pensions. A spouse might know the answers to some of these questions, but if they're biased towards older data, such as childhood street addresses, this risk can be mitigated. This scheme can be used over the phone, too, albeit with some inconvenience. It could certainly be automated via a voice response system.

Finally, requests can be made in writing or in person. Ideally, these would be authenticated via strong identity documents such as drivers' licenses or passports; alternatively, a notarized statement can be used. This does require further inquiry, given reported difficulties in voter registration in some states.[11] Alternatively, some form of "social authentication"[12] can be used, where friends or local businesses with suitable credentials vouch for someone's identity.

Although the schemes I have described are complex, most of the pieces are already in place. Most BIAS providers already have apps; this would simply require adding slightly more functionality. Data broker-based authentication is already in wide use, albeit in specialized environments. Finally, many BIAS providers already have local offices and are accustomed to dealing with in-person requests.

[6] *See* Danielle Keats Citron. *Hate Crimes in Cyberspace*. Cambridge, MA: Harvard University Press, 2014. ISBN: 9780674368293.

[7] *See* Lorrie Cranor. "Your mobile phone account could be hijacked by an identity thief". In: *Tech@FTC Blog* (June 7, 2016). URL: `https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief`.

[8] There is an Internet practice known as "doxxing"—learning the details of someone's life, and using this for malicious purposes, such as threatening them, posting things like home addresses, etc. Doxxers rely on the large amounts of information collected by data brokers; *see*, e.g., Federal Trade Commission. *Data Brokers: A Call for Transparency and Accountability*. May 0, 2014. URL: `https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf`.

[9] *See* Section 7.6 of *Thinking Security*, foonote 1, *supra*.

[10] *See* footnote 8, *supra*.

[11] *See*, e.g., *Fish v. Kobach*, 2016 U.S. Dist. LEXIS 64873 (US Dist. Ct. Kansas, 2016): "18,372 motor voter applications have been held in suspense or cancelled due to the DPOC law", i.e, for lack of suitable identity documenation.

[12] *See* John G. Brainard et al. "Fourth-factor Authentication: Somebody You Know". In: *ACM Conference on Computer and Communications Security*. 2006, pp. 168–178. URL: `http://www.rsasecurity.ca/rsalabs/staff/bios/ajuels/publications/fourth-factor/ccs084-juels.pdf`.