EDITOR HAL BERGHEL
University of Nevada, Las Vegas; hlb@computer.org

911 Swatting, VoIP, and Doxxing

Hal Berghel, University of Nevada, Las Vegas

When it comes to 911 swatting and doxxing, Voice over Internet Protocol (VoIP) takes this digital mischief to a new level.

"Swatting," or "911 swatting," is a malicious act that involves making fraudulent 911 calls to cause emergency response teams, such as law enforcement special weapons and tactics teams, or SWAT teams (that's where the gerund's root comes from), to react forcefully to a nonexistent public threat.[1] Swatting is commonly an act of personal retaliation and/or revenge against targeted victims for offenses and slights real and imagined. 911 swatting has become so widespread that several subclasses have been defined:

1. celebrity swatting directed against public figures[2]
2. gamer swatting directed against adversaries in online game environments[3]
3. ideological swatting directed against ideological adversaries[4]
4. partisan swatting directed against politicians[5,6]
5. hate swatting and mean-spirited attacks motivated by bigotry, racism, homophobia, and personal animosity[7,8]
6. coercion swatting intended to compel others to behave involuntarily; an example is retaliation against the victim of a failed extortion or blackmail attempt[9]
7. coercion swatting that shares objectives with cancel culture.[10]

911 swatting is closely aligned with criminal doxxing, which reveals personally identifiable information to embarrass, traumatize, intimidate, bully, harass, and encourage acts of violence against victims.

In any of its current manifestations, 911 swatting is intuitively an act of primarily domestic terrorism directed against noncombatant targets for personal reasons. Although federal legislation against 911 swatting has been proposed over the past decade, as of this date, none of this legislation has passed through Congress. Domestic terrorism legislation has a similar record. As a consequence, prosecution for 911 swatting and domestic terrorism is subsumed under other statutes dealing with fraud, civil rights, hate crimes, the national defense, and so on.[11] One consequence of this legislative ambivalence is that there is no way to know exactly how widespread 911 swatting is because law enforcement does not track it as a separate category of crime. However,

Digital Object Identifier 10.1109/MC.2023.3239267
Date of current version: 8 March 2023

by everyone's estimate, 911 swatting is on the rise despite the spate of state laws that call for severe punishment.

Who's doing this? A mangy mix of people with low self-esteem and anger management issues? Pranksters? Ill-behaved gamers? Hackers? Lowlife? In short, all of the above and more. With VoIP in their hands, what could possibly go wrong? Since 911 swatting involves computing and network technology, it's worth our attention.

ORIGINS

911 swatting seems to be the latest knot on the thread of mischief that began with telephone pranking and that likely dates back as far as telephony itself. The "Upjohn?—Yes.—Then go back to bed" gag likely dates back to the days of Alexander Graham Bell. And anonymous threats of death and violence by assault, bomb, and other terrorist acts have accompanied humanity throughout history. These two threads converge in bogus threats that are specifically created to alter and disrupt target behavior through fear, intimidation, harassment, and guile. This convergence is the deflection point for 911 swatting, for it is mischievous behavior that can be claimed to be ambiguous with respect to violent intent. While it could be intended as a prank, it could also be intended as a legitimate act of terrorism. As such, 911 swatting seems to enjoy a special place in the anonymous prank–harassment–bullying–doxxing–terrorism spectrum. 911 swatting elevates vitriol, hate, and vengeance to the level of likely violence, with the unique spin that the source of violence is law enforcement. It is, if you will, an individualized form ochlocracy—where every malcontent becomes a dangerous mob unto him/herself.

VoIP is telephony on the cheap, where the digitized messaging is offloaded to the Internet. VoIP is simply an extension of the TCP/IP protocol suite that enables voice communication: the payloads of the packets are audio encodings. As with other practical and useful Internet services/protocols (for example, the World Wide Web/HTTP, HTML, e-mail/Simple Mail Transfer Protocol, Post Office Protocol, Internet Message Access Protocol, multimedia streaming/Rapid Spanning Tree Protocol, and Stream Control Transmission Protocol), the magic takes place at the application layer. VoIP is a conjunction of protocols framed around a core that includes the Session Initiation Protocol (SIP)[12] for connection management and the H.323 family of protocols for managing the multimedia communication.[13] It should be mentioned that as we use the term, VoIP excludes incompatible proprietary standards, such as Skype, that offer similar network-based services.

911 swatting seems to be the latest knot on the thread of mischief that began with telephone pranking and that likely dates back as far as telephony itself.

Since the packet payloads are multimedia encodings, the overall theme of SIP is similar to HTTP but with the notable exception that uniform resource identifiers may also contain phone numbers as user IDs. As with other multimedia delivery-oriented protocols, SIP is ambivalent with regard to transport layer protocols. For our present purposes, we need recognize only that 1) VoIP uses IPv4 and IPv6 packet payloads as the carriers of the audio/video media encodings, 2) that there is a hardware/software connection between a computer or computer system and some media appliances that are compatible with telephony, and 3) that packet addresses will include telephone numbers. After that, VoIP may be thought of as just another packet-based application within the TCP/IP protocol suite.

Dedicated VoIP providers, including Intermedia Unite, RingCentral, and Vonage, work in this space, as do high-tech companies, such as Microsoft. All VoIP businesses offer suites of cloud-based services that can include such things as short message service messaging, call monitoring, voicemail-to-e-mail conversion, video conferencing, and so on. Such suites fall under the rubric of unified communications as a service. When offered by traditional high-tech companies, these suites are integrated with existing products. Microsoft, for example, integrates its VoIP offering in its Teams platform and Microsoft 365 infrastructure. Current cloud-based VoIP offerings are the fulfillment of the National Science Foundation-sponsored Global Schoolhouse Project that interconnected four K–12 classrooms in the United States and England[14,15] and Cornell University's CU-SeeMe videoconferencing platform, both of which date back to the mid-1990s.[16]

HACKING

Since VoIP is built upon TCP/IP, the latter's vulnerabilities carry over to the former and become enhanced. Where traditional Internet denial-of-service attacks might involve packet flooding to overwhelm the network interface cards, VoIP DOS attacks could use similar techniques to overwhelm VoIP routers and circuits with bogus VoIP phone calls. In addition, VoIP hacking has additional attack vectors, such as toll fraud, because, unlike Internet TCP/IP traffic, VoIP is a revenue-based service. In addition to DOS attacks and the theft of services, VoIP is, in principle, vulnerable to the same range of attacks as the Internet itself, including those that result in data theft, impersonation fraud, eavesdropping, call tampering, and all sundry forms of

malware. Needless to say, the remediation is also similar.[17]

Of VoIP vulnerabilities, spoofing is the most directly relevant to 911 swatting. But where packet spoofing in TCP/IP would normally involve the use of inauthentic IP and media access control addresses to achieve stealth, with VoIP, spoofing involves the use and manipulation of inauthentic caller IDs. It should be remembered that the Internet was not built around a robust security model that required authentication. And since packet crafting makes virtually every element of a packet header fungible, there's not much that can be done about it. The packet–fungibility–VoIP ship set sail in the 1960s with the launch of TCP/IP, long before VoIP was conceived. VoIP hacking, for the most part, is just the current manifestation of TCP/IP protocol bending.

In short, VoIP attack tactics follow familiar patterns, including reconnaissance and scanning, topology mapping, active and passive fingerprinting, password detection, and so forth. Those familiar with the principles of network forensics will note the similarities with Enable Security's SIPVicious tool kit.[18]

In short, since VoIP is based upon the TCP/IP protocol suite, it is to be expected that it can be hacked, that users' personal information is vulnerable to misuse, that packets can be corrupted, and that users may find communication metadata unreliable, specifically including caller ID. Armed with spoofed caller IDs and source IP addresses, VoIP swatters are ready for business.

RELEVANT LEGISLATION

The Truth in Caller ID Act of 2009[19] makes it illegal for any person within the United States to "cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information *with the intent to defraud, cause harm, or wrongfully obtain anything of value*" (emphasis added) unless specifically exempted (for example, law enforcement and court actions). In 2020, the Federal Communications Commission (FCC) used this law to fine a telemarketing company for spoofing caller IDs during political robocalls.[20] Unfortunately, the use of spoofed caller IDs to discourage call tracing and avoid call blocking are not specifically addressed in this legislation. Further, there is a logical problem with the structure of this legislation, as it focuses on the intent of the source rather than the activity. One must ask what legitimate lawful uses, if any, society should expect of caller ID spoofing. Crafting criminal law around the predicted intentions of criminals rather than the criminal conduct is a suboptimal strategy. The same mistake of attempting to build in "intent" was made with do-not-call legislation, as exemptions were made for political calls, not-for-profit organizations, pollsters, surveyors, and the like, who collectively proclaim their activity is a public service of indispensable social value. Attempts to frame unacceptable behavior around intent invariably disfavor the general public interest. The motivations behind this approach are driven by political, economic, and parochial interests and not the welfare of society.

Subsequent to the Truth in Caller ID Act, the FCC introduced two rules that bear directly on the ability of law enforcement agencies to identify the source of 911 calls: Kari's Law and the Repack Airwaves Yielding Better Access for Users of Modern Services (RAY BAUM'S) Act that took effect on 6 January 2020.[21] Kari's Law required all new multiline telephone systems (MLTSs) to support 911 direct dialing with appropriate notifications and alerts to the particular branch location (for example, a front desk or security office) along with location and callback information. RAY BAUM'S Act required that every MLTS send a "dispatchable location" with every 911 call along with a call source ID to the public safety answering point (for example, a 911 call center) regardless of the technological platform used. This specifically includes, but is not limited to, the installed MLTS base of legacy private branch exchange, central office exchange service, and key telephone systems along with interconnected VoIP, Internet-based Telecommunications Relay Services, mobile text, and hybrid systems.[22] While the original intent of Kari's Law and RAY BAUM'S Act was to facilitate emergency services response to legitimate threats to public safety, when viewed from the lens of the Truth in Caller ID Act, the laws can also be seen to apply to 911 swatting. Like all anticrime legislation, they also have the unintended effect of motivating tech-savvy 911 swatters to step up their game.

> 911 swatting elevates vitriol, hate, and vengeance to the level of likely violence, with the unique spin that the source of violence is law enforcement.

IS VOIP SWATTING A CRIME?

That depends, and the penalties are a moving target depending on jurisdiction. In California under Senate Bill 333, it is a misdemeanor crime to intentionally and knowingly make a false 911 call. This carries a penalty of one year in county jail and/or a US$1,000 fine. But it is a felony crime to make a false 911 call if one knows, or should know, that the emergency response will likely lead to great bodily injury or death. The penalty for this felony is up to three years in county jail and/or a US$10,000 fine

plus reimbursement of reasonable costs to responding agencies.[23]

In Michigan, under Penal Code Section 750.411a, effective 1 January 2013, it became a misdemeanor crime to intentionally make a false report to a 911 operator or law enforcement, which is punishable for up to 93 days' imprisonment and/or a US$500 fine, but it is a felony crime if personal injury results, which is punishable by up to five years' imprisonment and/or US$20,000. If death results, the punishment increases to up to 15 years' imprisonment and/or a fine up to US$50,000.[24]

Other states (for example, Minnesota and Florida) have followed suit with similar 911 swatting legislation. Connecticut and Nevada have expanded the legislative theme to antidoxing legislation.[25,26] Although federal legislation has been proposed,[27] as of this writing, there is no federal statute that specifically relates to 911 swatting and doxxing. Whatever federal legislative protections are available are currently subsumed under laws relating to interstate threats, conspiracies, endangering public safety, compromising national security, and so on. The state legislative reactions to 911 swatting appear to embrace the general theme that if no one is hurt, such a crime constitutes a misdemeanor; else, a felony. Some states (for example, New York) subsume some swatting under existing laws that penalize a "depraved indifference to human life." Although there are examples of successful federal prosecution of swatters and doxers,[28] for the foreseeable future, any significant statutory relief is likely to be piecemeal, fragmented, and local. States have been more united in legislating the operational side of 911 laws, including VoIP, than the protection of privacy.[29]

We can add 911 swatting, VoIP swatting, and doxxing to our list of antisocial cultural phenomenon at this point, along with social media disinformation campaigns, privacy-abusing apps and websites, the surveillance economy, and so on. Interestingly enough, one of the earliest reports of 911 swatting was actually a hoax.[30] It's not a hoax any longer but, rather, very real, very dangerous, and on the rise. The problem is exacerbated by the fact that the hacking aspects are documented on the Internet.[18,31] There is no question that the current threat deserves continued vigilance by the computing and networking communities.

The state legislative reactions to 911 swatting appear to embrace the general theme that if no one is hurt, such a crime constitutes a misdemeanor; else, a felony.

REFERENCES

1. M. J. Enzweiler, "Swatting political discourse: A domestic terrorism threat," *Notre Dame Law Rev. 2001*, vol. 90, no. 5, Aug. 2015, Art. no. 9. Accessed: Jan. 20, 2023. [Online]. Available: https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=4619&context=ndlr
2. H. Nigam, "Celebrity 'Swatting,' the latest craze for kids," *HuffPost*, Jan. 31, 2013. Accessed: Jan. 20, 2023. [Online]. Available: https://www.huffpost.com/entry/celebrity-swatting_b_2592404
3. B. Gallagher, "What you need to know about swatting, gamers' favorite harassment tactic," *Daily Dot*, Jun. 16, 2018. Accessed: Jan. 20, 2023. [Online]. Available: https://www.dailydot.com/debug/what-is-swatting/
4. G. Lopez, "David Hogg's family was swatted: That's extremely dangerous," *Vox*, Jun. 5, 2018. Accessed: Jan. 20, 2023. [Online]. Available: https://www.vox.com/policy-and-politics/2018/6/5/17429258/david-hogg-swatting-parkland-shooting
5. A. Waller, "Former Neo-Nazi leader sentenced to 3 years in 'Swatting' scheme," *NY Times*, May 4, 2021. Accessed: Jan. 20, 2023. [Online]. Available: https://www.nytimes.com/2021/05/04/us/john-cameron-denton-atomwaffen-division.html
6. S. Machkovech, "NJ legislator who sponsored anti-swatting bill gets swatted," *Ars Technica*, Apr. 14, 2015. Accessed: Jan. 20, 2023. [Online]. Available: https://arstechnica.com/tech-policy/2015/04/nj-legislator-who-sponsored-anti-swatting-bill-gets-swatted/
7. M. Keith, "A drag queen Twitch streamer who was targeted in a recent uptick in swatting says the livestreaming service needs to protect users' privacy," *Bus. Insider*, Nov. 26, 2021. Accessed: Jan. 20, 2023. [Online]. Available: https://www.businessinsider.com/drag-queen-twitch-streamers-swatting-livestreaming-2021-11
8. I. Oluo, "White supremacists 'swatted' my home to silence me. I will not be silent," *Guardian*, Aug. 30, 2019. Accessed: Jan. 20, 2023. [Online]. Available: https://www.theguardian.com/lifeandstyle/2019/aug/30/ijeoma-oluo-essay-swatting-hoax-white-supremacists
9. R. McMillan, "An extortionist has been making life hell for bitcoin's earliest adopters," *Wired*, Dec. 29, 2014. Accessed: Jan. 20, 2023. [Online]. Available: https://www.wired.com/2014/12/finney-swat/
10. H. Berghel, "A collapsing academy, part II: How cancel culture works on the academy," *Computer*, vol. 54, no. 10, pp. 138–144, Oct. 2021. Accessed: Jan. 20, 2023. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9548027, doi: 10.1109/MC.2021.3099048.

11. G. Myre, "Why the government can't bring terrorism charges in Charlottesville," NPR's All Things Considered, Washington, DC, USA, Aug. 14, 2017. Accessed: Jan. 20, 2023. [Online]. Available: https://www.npr.org/2017/08/14/543462676/why-the-govt-cant-bring-terrorism-charges-in-charlottesville
12. M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg, "SIP: Session initiation protocol," Request for Comments, Network Working Group, Internet Engineering Task Force, Fremont, CA, USA, RFC 2543, Mar. 1999. Accessed: Jan. 20, 2023. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2543
13. "Infrastructure of audiovisual services – Systems and terminal equipment for audiovisual services," Telecommunication and Standardization Sector, International Telecommunication Union, Geneva, Switzerland, ITU-T Recommendation H.323, Nov. 1996. Accessed: Jan. 20, 2023. [Online]. Available: https://www.itu.int/rec/T-REC-H.323-199611-S
14. "Global school house phase one: Collaborative uses of internet resources and tools in the classroom," Nat. Sci. Found., Alexandria, VA, USA, Award #9319950, 1993. Accessed: Jan. 20, 2023. [Online]. Available: https://www.nsf.gov/awardsearch/showAward?AWD_ID=9319950
15. J. Tan, "What happened to the global schoolhouse?" *University World News*, Sep. 16, 2016. [Online]. Available: https://www.universityworldnews.com/post.php?story=20160913131137765
16. J. Han and B. Smith, "CU-SeeMe VR immersive desktop teleconferencing," in *Proc. 4th ACM Int. Conf. Multimedia*, Feb. 1997, pp. 199–207, doi: 10.1145/244130.244199.
17. M. Raimondi, "VoIP hacking techniques, *Hakin9*, May 2019. Accessed: Jan. 20, 2023. [Online]. Available: https://hakin9.org/voip-hacking-techniques/
18. "Communication breakdown." Enable Security. Accessed: Jan. 20, 2023. [Online]. Available: https://www.rtcsec.com/article/
19. S. 30 — 111th Congress: Truth in Caller ID Act of 2009. (2009, Nov. 30). www.GovTrack.us. 2009. [Online]. Available: https://www.govtrack.us/congress/bills/111/s30
20. "California telemarketer fined $10M by FCC over political ad," *AP NEWS*, Nov. 19, 2020. Accessed: Jan. 20, 2023. [Online]. Available: https://apnews.com/article/pete-wilson-california-san-diego-a07ed022634a247235c7d18fc3a00419
21. "Public Safety and Homeland Security Bureau announces January 6, 2020, effective date of new rules implementing Kari's law and section 506 of Ray Baum's act," Federal Communications Commission Public Notice, Washington, DC, USA, DA 19-1236, Dec. 5, 2019. Accessed: Jan. 20, 2023. [Online]. Available: https://docs.fcc.gov/public/attachments/DA-19-1236A1.pdf
22. "Who is affected by Kari's law and the Ray Baum's act?" Federal Communications Commission, Washington, DC, USA, FCC Summary Document, Oct. 2020. Accessed: Jan. 20, 2023. [Online]. Available: https://www.911.gov/assets/Karis_Law_And_RAY_BAUMS_Act-Oct_2020.pdf
23. 2013-2014 Regular Session. (2013, Sep. 9). *California Senate Bill 333*. [Online]. Available: https://legiscan.com/CA/text/SB333/2013
24. Michigan Penal Code Section 750.411a. (2013, Jan. 1). *False Report of Crime or Report of Other Emergency..., Effective*. [Online]. Available: https://www.legislature.mi.gov/(S(lfgmzs3kqpttt2czlpjvqoec))/mileg.aspx?page=GetObject&objectname=mcl-750-411a
25. Connecticut General Assembly. (2021, Oct. 1). *Raised Bill No. 989, An Act Concerning Online Harassment, Effective*. [Online]. Available: https://www.cga.ct.gov/2021/TOB/S/PDF/2021SB-00989-R00-SB.PDF
26. Nevada Assembly. (2021, Jun. 4). *Bill No. 296, An Act Relating to Crimes; Defining Certain Terms for the Purposes of the Crime of Doxxing, etc., Enacted*. [Online]. Available: https://legiscan.com/NV/text/AB296/2021
27. H.R. 4057. (2015, Nov. 18). *A Bill to Amend Title 18, United States Code, To Establish a Criminal Violation for Using False Communications with the Intent to Create an Emergency Response*. [Online]. Available: https://www.congress.gov/114/bills/hr4057/BILLS-114hr4057ih.pdf
28. Department of Justice. Press Release Number 16-128. (2016, Jul. 11). *New York Man Sentenced To 24 Months in Prison For Internet Offenses, Including 'Doxing,' 'Swatting,' Making a False Bomb Threat, and Cyber-Stalking*. [Online]. Available: https://www.justice.gov/usao-dc/pr/new-york-man-sentenced-24-months-prison-internet-offenses-including-doxing-swatting
29. "MLTS E911 laws and regulation by state," Millennia Technologies, Grand Rapids, MI, USA, MT Rep., Jun. 13, 2019. Accessed: Jan. 20, 2023. [Online]. Available: https://mtvoip.com/mlts-e911-laws-and-regulation-by-state/
30. S. John, "15-year-old gamer convicted in 'Swatting' hoax: Satirical article creates stir on social media," *Int. Bus. Times*, Jan. 9, 2013. Accessed: Jan. 20, 2023. [Online]. Available: https://www.ibtimes.co.uk/15-year-old-gamer-convicted-swatting-hoax-satirical-article-creates-stir-social-media-1463463
31. L. Thandel, "voIP caller id spoofing – Call hack," *Tech. Navig.*, Jun. 30, 2019. Accessed: Jan. 20, 2023. [Online]. Available: https://technicalnavigator.in/voip-caller-id-spoofing-call-hack/

HAL BERGHEL is a professor of computer science at the University of Nevada, Las Vegas, Las Vegas, NV 89154 USA. Contact him at hlb@computer.org.