Eve, Martin Paul. "Notes." *password*. New York: Bloomsbury Academic, 2016. 109–117. Object Lessons. *Bloomsbury Collections*. Web. 26 Apr. 2023. <<http://dx.doi.org/10.5040/9781501314902.0011>>.

Downloaded from Bloomsbury Collections, www.bloomsburycollections.com, 26 April 2023, 15:11 UTC.

Copyright © Martin Paul Eve 2016. Released under a CC BY licence (<https://creativecommons.org/licenses/by/4.0/>). You may share, re-use or adapt this work, provided you give attribution to the copyright holder and the publisher, and provide a link to the Creative Commons licence.

NOTES

Introduction

- 1 Tung-Hui Hu, *A Prehistory of the Cloud* (Boston, MA: MIT Press, 2015), xviii.
- 2 A good number of these are also outlined in more detail in Peter Wisse, ‘Semiotics of Identity Management,’ in *The History of Information Security: A Comprehensive Handbook*, eds. Karl de Leeuw and Jan Bergstra (Amsterdam: Elsevier, 2007), 167–96.
- 3 When we turn to one-way hashing algorithms in Chapter 3, I will show that there is some upset of this timing dilemma.
- 4 M. Atif Qureshi, Arjumand Younus and Arslan Ahmed Khan, ‘Philosophical Survey of Passwords,’ *arXiv Preprint arXiv:0909.2367* (2009), 11, <http://arxiv.org/abs/0909.2367>.
- 5 Aeneas Tacitus, *Aineiou Poliorketika. Aeneas on Sieecraft*, trans. L. W. Hunter and S. A. Handford (Oxford: Clarendon Press, 1927), 61. Two-factor authentication, which will be covered below in more detail, is a form of identification that relies not only upon the respondent knowing the password, but also demonstrating that he or she possesses a specific object. A bank card is a good example of two-factor

authentication: the user must know the Personal Identification Number (PIN) but he or she must also possess the card.

- 6 Robert McMillan, 'The World's First Computer Password? It Was Useless Too,' *WIRED*, 27 January 2012, <http://www.wired.com/2012/01/computer-password/>.
- 7 I am grateful to Jemima Matthews for a conversation on pass-spaces in April 2015.

Chapter 1

- 1 I owe this observation on disparities of scale to Joe Brooker.
- 2 Authentication usually refers to the process of verifying that someone is who they claim, while authorization is used to mean the process of checking that this same person is allowed to perform the action they have attempted.
- 3 Arthur Evans, *The Palace of Minos at Knossos: A Comparative Account of the Successive Stages of Early Cretan Civilization as Illustrated by the Discoveries at Knossos*, vol. 2 (London: Macmillan and Co., 1921), 60–92.
- 4 A. Shand, 'The Occupation of the Chatham Islands by the Maoris in 1835: Part II, The Migration of Ngatiawa to Chatham Island,' *The Journal of the Polynesian Society* 1, no. 3 (1892): 154–63.
- 5 Jonathan Haas, 'Warfare and the Evolution of Culture,' in *Archaeology at the Millennium: A Sourcebook*, ed. G. M. Feinman and T. D. Price (New York: Kluwer Academic/Plenum, 2001), 343.
- 6 Eva Horn, 'Logics of Political Secrecy,' *Theory, Culture & Society* 28, no. 7–8 (1 December 2011): 104, doi:10.1177/0263276411424583.

- 7** I draw heavily here on the work of the afore-cited Eva Horn.
- 8** All of the above from Horn, ‘Logics of Political Secrecy,’ 104–9.
- 9** Tacitus, *Aineiou Poliorketika. Aeneas on Siegemcraft*, 61.
- 10** Ibid., 47, 63.
- 11** For more, see Jason Andress, ‘Chapter 5 – Cryptography,’ in *The Basics of Information Security*, 2nd edn (Boston: Syngress, 2014), 69–88, <http://www.sciencedirect.com/science/article/pii/B9780128007440000051>.
- 12** Recall that the ‘second channel’ refers to the need to pre-communicate a shared secret to a recipient in advance of sending the actual method.
- 13** Tacitus, *Aineiou Poliorketika. Aeneas on Siegemcraft*, 75.
- 14** Ibid., 63.
- 15** Ibid., 77. Underlinings mine.
- 16** Think only of something like *The Hunt for Red October* [1990] to see this.
- 17** Tacitus, *Aineiou Poliorketika. Aeneas on Siegemcraft*, 61.
- 18** Janet Abbate, *Inventing the Internet* (Cambridge, MA: The MIT Press, 2000), 144–5.
- 19** Ibid., 77.
- 20** Jennifer Wilcox, ‘Solving the Enigma: History of the Cryptanalytic Bombe,’ *Center for Cryptologic History, National Security Agency* (2006): 3, https://www.nsa.gov/about/_files/cryptologic_heritage/publications/wwii/solving_enigma.pdf. That’s 3,000 passwords. Much of this section is derived from Wilcox’s excellent account.

- 21 I am thinking, here, primarily of *The Imitation Game* [2014] as a film that slightly overplays the contributions of individuals above team efforts, although it is true that Turing's efforts and intellect were remarkable.
- 22 Only three rotors were actually used at any time but it was impossible for cryptographers to establish which rotors were in use, thus substantially complicating the keyspace.
- 23 Technically, a probable-plaintext attack.
- 24 F. H. Hinsley, *Codebreakers: The Inside Story of Bletchley Park* (Oxford: Oxford University Press, 2001), 121.
- 25 Randall Monroe, 'Xkcd: Security,' *Xkcd*, 2009, <https://xkcd.com/538/>.
- 26 Clark Boyd, 'Profile: Gary McKinnon,' *BBC News*, 30 July 2008, sec. Technology, <http://news.bbc.co.uk/1/hi/technology/4715612.stm>.
- 27 Bruce Schneier, 'All or Nothing,' *CSO*, February 2007, 20.

Chapter 2

- 1 There are potentially Arabic origins for these tales, but they are not from the original *Nights*.
- 2 John Payne, *Alaeddin and the Enchanted Lamp* (London: Villon Society, 1889), chap. Introduction.
- 3 See Richard M. Stallman, 'Did You Say "Intellectual Property"? It's a Seductive Mirage,' *Gnu.org*, 20 April 2015, <https://www.gnu.org/philosophy/not-ipr.en.html>.
- 4 The Aarne-Thompson classification system of folklore traces similarities of plot structure in folk and fairy tales across many cultures then groups stories by these congruences.

- 5 The name of The Doctor has not so far been revealed to viewers of the television show (even though there have been various hints, explored thoroughly on fan websites if one wishes to search).
- 6 I here refer to the title of the first book by its original British name, whereas in the United States it was re-titled *Harry Potter and the Sorcerer's Stone*.
- 7 Passwords to Dumbledore's office include 'acid pops,' 'cockroach cluster,' 'fizzing whizbee,' 'lemon drop,' and 'sherbert lemon,' all types of confection. Passwords to the student common rooms include 'abstinence,' 'balderdash,' 'banana fritters,' 'baubles,' 'caput draconis,' 'dilligrout,' 'fairy lights,' 'flibbertigibbet,' 'fortuna major,' 'Mimulus mimbletonia,' 'oddsbodikins,' 'pig snout,' 'pure-blood' (for the Slytherin common-room), 'quid agis,' 'scurvy cur,' 'tapeworm,' 'toffee éclairs' and 'wattlebird.' The password to the prefects' bathroom is 'pine fresh.'
- 8 Parselmouths mentioned in the series are: Herpo the Foul, Marvolo Gaunt, Morfin Gaunt, Harry Potter, Merope Riddle, Tom Marvolo Riddle (Lord Voldemort) and Salazar Slytherin.
- 9 J. K. Rowling, Open Book Tour, 19 October 2007, <http://www.the-leaky-cauldron.org/2007/10/20/j-k-rowling-at-carnegie-hall-reveals-dumbledore-is-gay-neville-marries-hannah-abbott-and-scores-more>.
- 10 While more advanced wizards in the world of *Harry Potter* can cast non-verbal spells, all students begin by learning incantations.
- 11 As I will go on to discuss, there are, of course, many complications to this such as the category of 'squib' that Rowling uses to denote someone of magical parentage but who has no wizarding aptitude.

- 12 Among the best of these is Walter J. Ong, *The Presence of the Word: Some Prolegomena for Cultural and Religious History* (New Haven, CT: Yale University Press, 1967).
- 13 I owe this last quip/observation to Christos Hadjioannou.
- 14 Scott B. Noegel, “‘Sign, Sign, Everywhere a Sign’: Script, Power, and Interpretation in the Ancient Near East,” in *Divination and Interpretation of Signs in the Ancient World*, ed. Amar Annus, Oriental Institute Seminars 6 (Chicago: Oriental Institute of the University of Chicago, 2010), 149.
- 15 Geraldine Pinch, *Magic in Ancient Egypt*, rev. edn (Austin: University of Texas Press, 2009), 69.

Chapter 3

- 1 See Alan Liu, *The Laws of Cool: Knowledge Work and the Culture of Information* (Chicago: University of Chicago Press, 2004), 76, for more of the ways in which these metaphors are confused.
- 2 There are many sources that can give more information on these metaphors of places. For a legal take, see Mark A. Lemley, ‘Place and Cyberspace,’ *California Law Review* 91, no. 2 (1 March 2003): 521–42, doi:10.2307/3481337.
- 3 Liu, *The Laws of Cool*, 42.
- 4 Those who seek a more mathematical and/or computer-science based approach would do well to consult either Bruce Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C* (New York: John Wiley & Sons, 1995); or Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of Applied Cryptography* (Boca Raton: CRC Press, 1996), from which much material in this chapter is distilled.

- 5 On the basis of being able to try 8,783,000 keys per second, a figure derived from <http://calc.opensecurityresearch.com/>.
- 6 While, for reasons of space, I won't deeply delve into the details of the mitigation against this, the defensive process is called 'salting' and it involves running the algorithm multiple times with a string appended to the end of the first round of hashing, thereby rendering this attack impotent.
- 7 Marc Stevens, 'Single-Block Collision Attack on MD5,' *IACR Cryptology ePrint Archive* (2012): 40, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.400.7023&rep=rep1&type=pdf?>.
- 8 Bart Preneel, 'The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition,' in *Topics in Cryptology – CT-RSA 2010*, ed. Josef Pieprzyk, Lecture Notes in Computer Science 5985 (Berlin, Heidelberg: Springer, 2010): 30, http://link.springer.com/chapter/10.1007/978-3-642-11925-5_1.
- 9 On a strict time limit, he is forced at gunpoint to perform the hack while receiving oral sex from a prostitute.
- 10 There is a convention in descriptions of cryptography to use the character names 'Alice,' 'Bob' and 'Eve.'
- 11 A particularly pernicious version of this rhetoric can be seen in Robert David Steele, *The Open-Source Everything Manifesto: Transparency, Truth, and Trust* (Berkeley, CA: Evolver, 2012).
- 12 'Fake DigiNotar Web Certificate Risk to Iranians,' *BBC News*, 5 September 2011, <http://www.bbc.co.uk/news/technology-14789763>; Bruce Schneier, 'VeriSign Hacked, Successfully and Repeatedly, in 2010,' *Schneier on Security*, 3 February 2012, https://www.schneier.com/blog/archives/2012/02/verisign_hacked.html.
- 13 An aspect that is again interestingly explored in the Harry Potter series through legilimency and occlumency.

- 14 Russell Brandom, 'The Plot to Kill the Password,' *The Verge*, 15 April 2014, <http://www.theverge.com/2014/4/15/5613704/the-plot-to-kill-the-password>.
- 15 Anil K. Jain, Ruud Bolle and Sharath Pankanti, 'Introduction to Biometrics,' in *Biometrics: Personal Identification in Networked Society*, ed. Anil K. Jain, Ruud Bolle and Sharath Pankanti, The Kluwer International Series in Engineering and Computer Science, SECS 479 (Boston: Kluwer, 1999), 1–42.
- 16 'Borrowed Biometric Bypass,' *TV Tropes*, accessed 9 May 2015, <http://tvtropes.org/pmwiki/pmwiki.php/Main/BorrowedBiometricBypass>.
- 17 Yari Lanci, 'Remember Tomorrow: Biopolitics of Time in the Early Works of Philip K. Dick,' in *The World According to Philip K. Dick: Future Matters*, ed. Alexander Dunst and Stefan Schlensag (New York: Palgrave Macmillan, 2015), 111.

Chapter 4

- 1 United Kingdom, *Theft Act 1968*, accessed 23 May 2015, <http://www.legislation.gov.uk/ukpga/1968/60/crossheading/definition-of-theft>.
- 2 Jaron Lanier, *You Are Not a Gadget: A Manifesto* (London: Penguin Books, 2011), 102.
- 3 The Google Books corpus should be taken with a pinch of salt. The black box of its OCR mechanism and proprietary nature do not make it the best source for this type of mining. However, assuming that errors are standardized across the corpus, this nonetheless demonstrates an intriguing parallel rise in these terms.

- 4 United Kingdom, *Fraud Act 2006*, accessed 31 May 2015, <http://www.legislation.gov.uk/ukpga/2006/35/contents>.
- 5 For more on digital hygiene, see Hu, *A Prehistory of the Cloud*.
- 6 Confusingly, 'confessor' refers to the priest receiving the confession while the person confessing is the 'penitent'.
- 7 Foucault also links this form of truth telling back to earlier practices of parrhesia; plain speaking. See also Elizabeth Markovits, *The Politics of Sincerity: Plato, Frank Speech, and Democratic Judgment* (University Park, PA: Penn State University Press, 2008).
- 8 Umberto Eco, *The Role of the Reader: Explorations in the Semiotics of Texts* (Bloomington, IN: Indiana University Press, 1997), 85.
- 9 Theodor W. Adorno, *Negative Dialectics*, trans. E. B. Ashton (London: Routledge, 1973), 5.
- 10 Lanier, *You Are Not a Gadget*, 50.
- 11 Ludwig Wittgenstein, *Preliminary Studies for the 'Philosophical Investigations' (Blue and Brown Books)* (Oxford: Blackwell, 1972), 69.
- 12 Antonia Farzan, 'If You've Recently Done One of These 3 Things, You're at a Higher Risk for Having Your Identity Stolen,' *Business Insider*, 5 July 2015, <http://www.businessinsider.com/highest-risk-of-identity-theft-2015-7>.