

Phone hacking enigmas

Description

News of the World journalists gaining unauthorised access to people's answer phone messages has led to a shut down of the operations of one newspaper, allegations of police bribery, several high-level resignations, and a new found bravado by those who used to fear the Murdoch press.

The apogee of these developments came at about the same time that the Queen unveiled a commemorative sculpture at Bletchley Park, the centre of message hacking in WWII, and now an information-rich visitor attraction. The commemorative sculpture by Charles Gurrey has the words inscribed on it "we also served," referring of course to the influence of those back room hacks who won honours for heroism on the front lines of WWII. Bletchley Park reveals the dangers of listening in to confidential communications.



How were communications kept secret during the war? German

operatives at command stations would be handed messages for encryption. The operative would enter each character of the message into a tabletop machine that looks something like a typewriter, the commercially produced Enigma machine. With each key stroke, a different letter to the one pressed would illuminate on a panel on the top of the machine. Someone would have to write down the new characters as they appeared. The message so encrypted would then be sent in Morse code via conventional telegraph to the recipient, who would then decrypt the message by means of a similar machine, and a similar process. It didn't matter to the sender and recipient that the telegraph service could be tapped, as the interceptor would only pick up an apparently random sequence of characters.

The Enigma didn't map every character in a unique and predictable way, as if every 'A' got encrypted as a 'P'. That would be trivial to decrypt. Each character was translated through several scrambling operations involving a series of disks that rotated with each press of the keyboard. The message recipient could decrypt the message as long as they had the same Enigma machine, with the

same disks in the same position, the same starting conditions and the same circuit. The sender and receiver had the same code book, which listed the required parameters for the machine on any particular day.

Any interceptor with a similar Enigma machine and the code for the day could decrypt any messages they picked up.

The code-breaker challenge for the Allies was to develop a system for deriving the code for the day. This required cunning, experimentation and electromechanical devices that could iterate through very large combinations of parameter configurations. The first such machine was known as the Bombe, a proto-computer of sorts.

The code breakers of Bletchley discovered early on that the Enigma machine had at least one limitation, that no letter could ever be coded to itself. T would never appear as a T in the coded message; an A would never appear as an A, etc. The other flaw in the process was that many messages would often contain the same words, such as WETTERVORHERSAGE (German for weatherforecast). By lining up the known word with part of a message thought likely to contain information about the weather, the decoders would look for a string of characters (a crib) for which there were no such correspondences. This would help the decoders to identify the encrypted form of the word. So the character sequence XPGTFSUYKAVTBEQ could never represent WETTERVORHERSAGE as the 4th character is the same in both cases (T). On the other hand a sequence like YALDRDUWZUYZZSJH could possibly stand for WETTERVORHERSAGE as there are no letters in the same position and in common.

Further steps followed, and many iterations, that might reveal the code for the day. Once the code was known then all messages could be decrypted. The procedures are given extensive treatment on the Wikipedia entry for Enigma Machine and a book by Andrew Hodges about Alan Turing, the mathematician who led on the decryption project and the invention of the Bombe.

Of course, encryption is a key aspect of contemporary communications technologies, with a plethora of techniques now available.

By way of contrast, listening in to private voice mail messages is (or was) a technically simple exercise when placed alongside the challenges dealt with at Bletchley Park. To listen in on messages left on someone's answer phone you just need their phone number and be able to guess their PIN.

For me the most interesting aspect of the Bletchley story and that of so-called phone hacking is the way that error plays into the system. We know that machines can fail through the slightest imperfection. The Bombe, and the attendant decoding practices, was pitted against the Enigma machine and its encryption methods, including miss-practices.

The glitch in the security of automated, PIN-protected voicemail messaging services is that many people do not select a secure PIN, or they default to the PIN number supplied with the device. Human security practices are inevitably error prone.

How did the phone hacking scandal escalate? It seems that the main error by *News of the World* was to deviate from picking on people of power and influence, and attacking the phones of disaster and murder victims, and even deleting messages in order to give potential callers space to leave further

messages. In the case of murder victim Milly Dowler this unwittingly gave relatives and friends the impression that she might still be alive.

The differences between the ethical contexts of the hacking operations of *News of the World* and the Bletchley Park war effort are obvious. The primacy of error is common. In another context, in an essay on cybernetics, Ranulph Glanville observes that “error is, in itself, neither bad nor good, but endemic—it cannot be eliminated. . . . it is error that drives the system!” (p.1181). It is error that makes the hack possible, and error that exposes it.

Hacking the Enigma code started with the comparison of character strings for a sequence where nothing matches, yielding a negative result, a complete negation, “A is not A,” which also has something to do with [metaphor](#).

Reference

- Glanville, Ranulph. 2007. Try again. Fail again. Fail better: the cybernetics in design and the design in cybernetics. *Kybernetes*, (36) 9/10, 1173-1206.
- Hodges, Andrew. 1985. *Alan Turing: The Enigma of Intelligence*. London: Unwin Paperbacks.

Coda

For a simple correlate with architecture think of Vitruvius and the systematic description of the built elements of a city alongside the meticulous description of the machines that would exploit their weaknesses: catapults, balistae and ram tortoises.

- Vitruvius, Pollio. 1960. *Vitruvius: The Ten Books on Architecture*. Trans. M. H. Morgan. New York: Dover Publications. Written c 50 AD.

Category

1. Artificial Intelligence

Tags

1. Alan Turing
2. Bletchley Park
3. Enigma
4. News of the World
5. phone hacking

Date Created

July 23, 2011

Author

rcoyne99