Thomas von Randow, Btx System (1984)

Abstract

In November 1984, two members of the "Chaos Computer Club" (CCC), Herwart ("Wau") Holland and Steffen Wernéry, hacked into the Btx system of the Hamburger Sparkasse (Haspa). The hackers seized 135,000 DM, which they then transferred back to the bank. The CCC's data hack aimed to point out security deficiencies in the German Federal Post Office's Btx system.

Source

"Whoever signs up for the Btx system in the next two to three years should be punished for stupidity." This scathing verdict on the Federal Post Office's new service, *Bildschirmtext* [or Btx, a so-called videotex system], was uttered last week at the Eighth Data Protection Conference in Cologne – and came from the mouth of an expert. Professor Reinhard Vossbein, head of the Society for Data Protection (GDD), the conference organizer, arrived at this opinion after hearing an account by a computer freak. Using wit and playful language, Herwart ("Wau") Holland of the Hamburg-based "Chaos Computer Club" (CCC) had described how his 23-year-old club mate Steffen Wernéry managed to outsmart the videotex service.

Videotex experts at the Post Office had boasted that it was easier to guess the six winning numbers in the national lottery than to illegally obtain the password of a Btx subscriber. But the Hamburg hackers succeeded straightaway in doing just that. An error – actually called a *bug* – in the system's program made it child's play for hackers. Many videotex providers had already noticed that something was wrong with the program.

Providers create full-screen pictures with information about what they have to offer: goods from mail-order catalogs, vacation packages, account statements for bank customers, or simple messages to friends. These "pages" can then be called up by authorized Btx subscribers, and the questions they contain, for example, about a plane reservation or a money transfer, can be answered on the keyboard of their home Btx add-on device.

But space on a television screen is limited, and a Btx page can only hold 1,626 characters. This figure is displayed at the bottom of the screen, so that the designer knows, when editing, how many characters he can still fit into his work. Until recently, however, this figure was not accurate – programmers are notoriously bad at mental calculations. The page was already full before the number of the available characters had reached zero. For this reason, many providers experienced a chaotic character overrun, which was not supposed to happen.

Suddenly, all sorts of words, numbers, or indecipherable letter sequences wandered, ghostlike, on the page. The reason for this salad of characters: the creator of the Btx program had apparently forgotten to attend to "garbage collection," that is, to make sure that surplus text is ignored or somehow cast aside by the program. That's why an excess of typed characters ended up pushing parts of the program writer onto the screen; and as the Hamburg hackers found out, they were sometimes revealing. They can reveal the very secret that a Btx user wants to guard: his identifier. This password is the key to accessing the system. You can't plunder someone else's bank account with it, but you can still cause a lot of trouble. You can order goods, book vacations, and subscribe to magazines. According to the contract, the rightful owner of the security code is liable for any damages.

Steffen Wernéry and his comrades – the club is a registered videotex page provider – massively overloaded Btx pages and then studied the ghost characters on the screen. There, they discovered the password, "usd 70 000," of the Hamburg Savings Bank (Haspa). With it, they were able to demonstrate the utter inadequacy of the videotex,

something the hackers had long planned. They set up a "donation page." Providers can charge a nominal or donation fee when their pages are accessed, but this may not exceed 9.99 marks. Anyone who accesses such a page is automatically charged this fee. Using the savings bank password, the hackers accessed their own paid page – and earned 9.97 marks.

This was process was supposed to happen as often as possible, so they programmed a home computer to call up the page automatically on a continuous basis. The computer did a good job – while club members were busy doing other things, the cash register rang every three seconds. From 6:00 pm on Saturday to 1:00 pm on Sunday, the Club's account collected a total of 135,000 marks. Of course, they transferred this back to the savings bank.

Long before computers were popular, American students dubbed the kind of trick that could outwit technology a *hack*. One hack became legendary. It was by Captain Crunch, a student who took his name from a brand of breakfast cereal. Packages of Captain Crunch cereal contained a small plastic musical pipe, which, by coincidence, was tuned to exactly 2600 hertz. Captain Crunch figured out that when this frequency was piped into a telephone receiver in the American long-distance telephone system, it disconnected the meter.

News of the trick – and its promise of free long-distance phone calls – spread quickly; it made the cereal company rich and the telephone company poor. Anyway, the telephone company found itself in real trouble. It needed to weigh a difficult-to-detect loss against an expensive technical change to its continental network. Bell decided on the latter.

Such a strike against a computer system delivers an exquisite sense of triumph that far outweighs the financial advantages that are sometimes associated with it; it is a liberating strike that momentarily frees us from the rule of machines. In the 1930s, Hamburg allotment gardeners managed to illuminate their huts for free. The power source was the nearby antennae of a powerful radio broadcaster, whose energy was redirected into the gardeners' lamps via a simple blocking circuit. For years, this hack went undiscovered – and when it finally became known, it prompted a discussion of fundamental legal principles: Are radio waves moveable property in the eyes of the law?

Almost ten years ago, one tinkerer discovered a way to hack SEL's first long-distance touchtone payphone; that person remained anonymous. A piezo ignition lighter was used in this hack. Whoever wanted to make a free call stepped into a telephone booth with SEL's coin-operated model, inserted a five-mark coin, and placed the call. Before the money ran out, the caller had to click a lighter next to the telephone's keypad. The spark interfered with the electronics to such an extent that the phone had to suppose that the conversation had never taken place, and therefore – *in dubio pro comparticipte* – the five-mark coin was returned. The logic board had to be replaced in all payphone models of that type.

For the victim, the hack is not merely troublesome but also generally serves as a lesson that reveals a technical design flaw. Of course, the possible damage that can be inflicted during an initial hack increases with the system's degree of complexity. Thus, it is somewhat miraculous that up to now the Btx hackers' little games have played out harmlessly. Whatever the case, they completely exposed the pitiful quality of the videotex design.

In Btx's country of origin, Great Britain, hackers have enjoyed breaking into Prince Philip's electronic mailbox. These Btx mailboxes are strangely constructed anyway. Videotex mail that has already been deposited there can still be rewritten by the sender after the fact. Each mailbox can even be made fully unusable. To do this – and the Hamburg hackers figured this out too – there needs to be a command at the end of a published page to repeat the entire request. A page prepared in this way appears again and again. It does the same in the mailboxes to which it is sent, with the result be that nothing else can be retrieved. Only the Post Office is able to break this vicious cycle.

The videotex system even allows a microcomputer to be connected to it. But woe to anyone who accesses the crash program specifically designed for his type of device. It crashes the computer and erases the programs stored on it. Only one thing helps: turning the computer off and on again. The destructive program presents as a harmless screen page. Clever hackers have even fashioned it into a time bomb. Only after a while, when the page (which is usually filled with absurd sayings) is long forgotten, does the device break down, so that the cause can most likely no longer be determined.

All of this should have been a lesson to the Federal Post Office long before its favorite pet project videotex was given a resounding slap in the face by the savings bank trick at the beginning of last week. Clearly, the little bit of patchwork they did after every known Btx hack was not enough. A program that needs so much cleaning up is hopelessly compromised.

They know this at the Post Office, of course, and it is particularly painful because Btx had just overcome the final political hurdles on its way to general introduction. It also hurts because interest in the new communication medium is meager anyway. According to the ministry's optimistic predictions, Btx should now have around 150,000 subscribers. In truth, there are only 19,000, of whom 3,000 are page providers.

It is doubtful whether the Post Office will be able to hold itself harmless against the company that set up the system, IBM. The “blue giant” will hardly be able to avoid delivering a new computer program. And until that is ready, two to three years will likely pass, which is probably what data protection strategist Reinhard Vossbein was referring to when he declared anyone who subscribed to videotex before the end of this period to be criminally stupid.

Source: Thomas von Randow, “Ein Schlag gegen das System: Ein Computerclub deckt Sicherheitslücken im Btx-Programm der Post auf,” *Die Zeit*, no. 49, November 30, 1984. © Die Zeit.

Translation: David Haney and GHI staff

Recommended Citation: Thomas von Randow, Btx System (1984), published in: German History Intersections, <https://germanhistory-intersections.org/en/knowledge-and-education/ghis:document-22> [January 29, 2023].