Die Hacking Geschichte

Teil 1: Telefon Phreaking

Bruce Nikkel

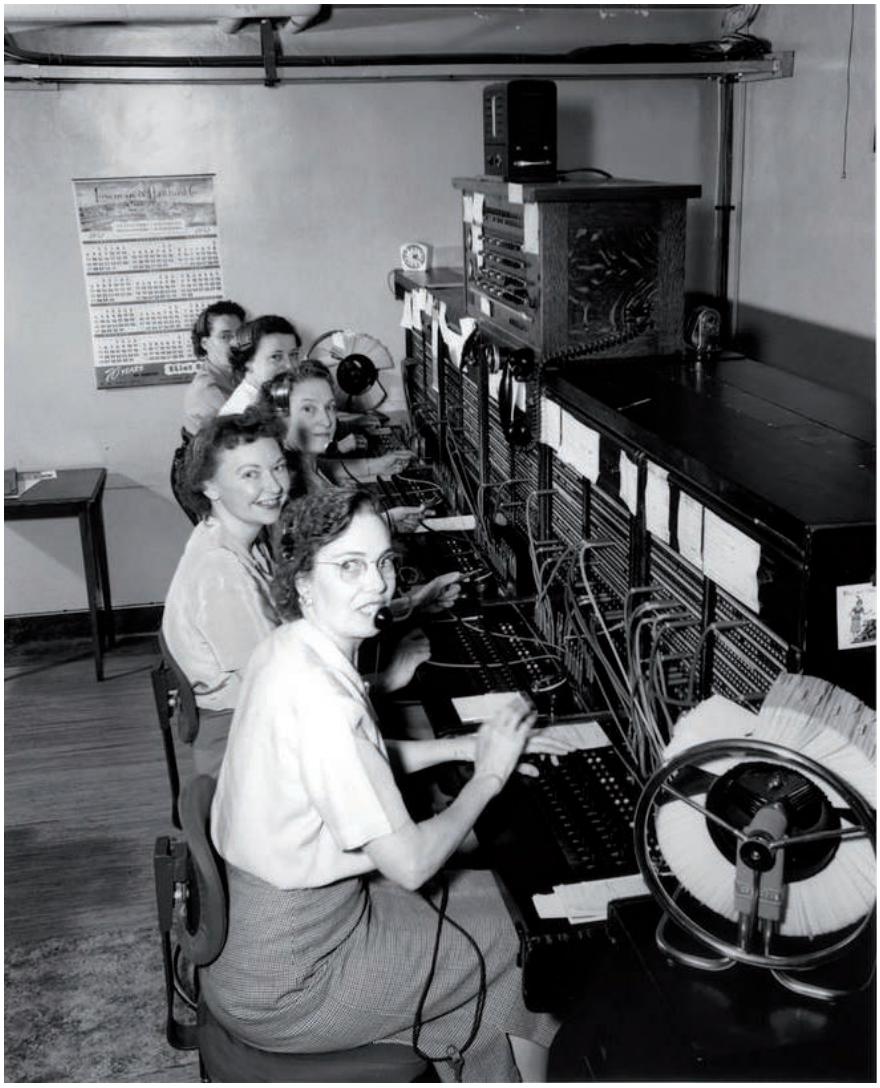
Bruce Nikkel Museumsführer
im Museum ENTER

Dies ist der erste Teil einer vierteiligen Serie zum Thema Computer Hacking.

Das Wort «Hacker» und «Hacken» im Zusammenhang mit Technik wurde zuerst in den 1950ern im **Tech Model Railway Club** des **Massachusetts Institute of Technology (MIT**) benutzt.

Als «Hack» wurde eine clevere technische oder erfinderische Leistung eines Studenten (manchmal in der Art eines Streichs) bezeichnet, aus welcher man lernen konnte oder auch nur daran Spass haben wollte. Das Hacken in der Anfangszeit hatte keinen Zusammenhang mit kriminellen Aktivitäten.

Wir beginnen die Serie mit der Hacking Aktivität auf das erste öffentliche globale Netz, das ursprüngliche Telefonsystem. Wir befassen uns mit den ersten Hackern genannt «phone phreaks» oder «phreakers» und mit ihren technischen Methoden.



Telefonistinnen vor der Zeit der automatischen Schaltzentralen

Bevor der Heimcomputer oder das Internet verbreitet war, wurde die Hackertechnik «phone phreaking» benützt, um die Schwachstellen des globalen Telefonnetzes auszunützen.

Das Wort «phreak» ist eine falsche Schreibweise des Wortes «freak», das «ph» von «phone» wurde absichtlich verwendet. Auch heute gibt es dieses Vorgehen beim Wort «phishing» statt «fishing». (Phishing bezeichnet den Versuch, über gefälschte Emails oder Webseiten sensitive Daten zu stehlen).

Telefon Phreaks lernten, wie das Telefonnetzwerk funktionierte und manipulierten Telefonzentralen, indem sie Töne und Pulse generierten. Phone Phreaking wurde in vielen Ländern, im Gegensatz zu den Aktivitäten der MIT Studenten, oft als kriminelle Handlung angesehen. Es bestehen Gesetze, die den Missbrauch und das Gratis-Benützen der Leitungen verbieten.

Als die Telefongesellschaften von den Schaltzentralen, die von Menschen bedient wurden, auf den automatischen Wählvorgang wechselten, benötigten sie eine

Möglichkeit, um die Signale vom Kundentelefon zur Zentrale zu übermitteln. Sie brauchten zudem ein Signalprotokoll beim lokalen und internationalen Telefonaustausch für Langdistanzanrufe.

Die vom Telefongerät gewählten Nummern benützten eine Sequenz von Pulsen oder Multifrequenztönen, welche direkt von der Fernsprechzentrale interpretiert wurden (In-Band).

Fernsprechämter benützten auch In-Band Signale, um Anrufe an andere Fernsprechämter zu senden. Weil die Signale In-Band auf den gleichen Kanälen übertragen wurden wie Sprache, konnten die Signale unabhängig von irgendjemandem generiert und ins System gebracht werden. Diese Schwachstelle führte zu einem Wildwuchs der phone phreaking community von Hackern, die entdeckten, wie man den benötigten Klang produzierte, um die Schaltzentralen zu kontrollieren. Sie taten dies, indem sie in die Telefonlinie pfiffen oder elektronische Geräte bauten, welche die korrekten Frequenzen generieren konnten.

Informationen über die Infrastruktur der Telefongesellschaften waren meistens nicht publik und schwierig zu finden. Einiges war in akademischen oder industriellen Technikjournalen publiziert. Einiges wurde durch Tests und Experimentieren mit den Systemen adhoc gefunden. Eine Methode, um Informationen zu gewinnen, hiess «trashing» (Mülldurchsuchen) oder «dumpster-diving» (Müllcontainertauchen), wo Hacker den Abfall der Telefongesellschaften nach informativen Druckerzeugnissen durchsuchten. Eine andere Art an Informationen zu gelangen, war das gezielte Ausfragen von Angestellten der Telefongesellschaften. Wenn phone phreaks neue technische Informationen erhalten hatten, teilten sie diese mit der phreaking community.

«blue box» von Steve Wozniak und Steve Jobs

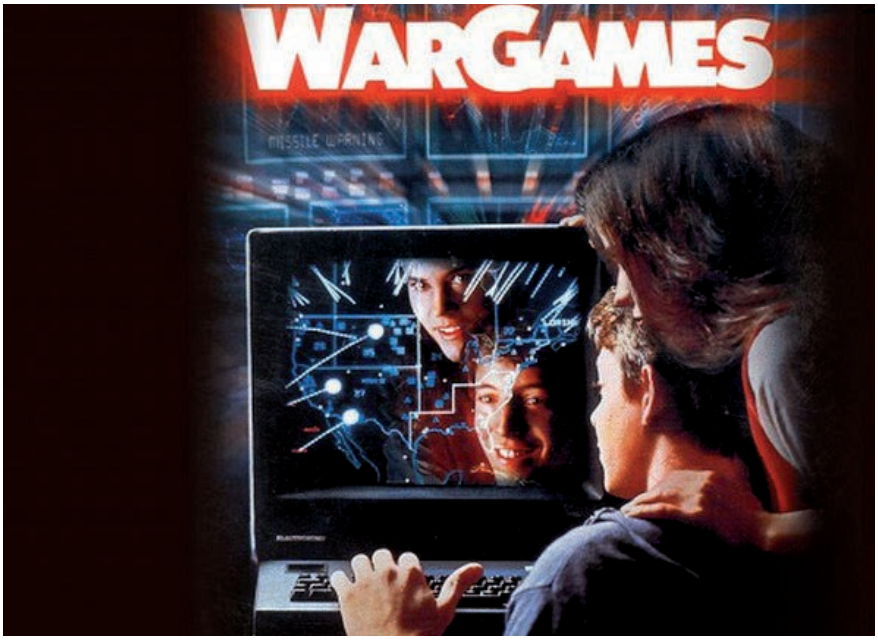
Ein berühmter phone phreak hiess «Captain Crunch» (sein richtiger Name war *John Draper).* Er erfand eine Spielzeugpfeife im Cap'n Crunch Frühstücksmüsli, welche 2600hz erzeugte. Dieser Ton war das Signal des Telefonnetzstamms und veranlasste, dass Verbindungen unterbrochen wurden und akzeptierte, dass ein anderer Ton das System kontrollierte. Das wurde gebraucht um Anrufe von irgendeiner anderen Schaltzentrale der Welt umzuleiten und phreakers konnten damit gratis Ferngespräche führen.

Cap'n Crunch Frühstücksmüsli mit einer Spielzeugpfeife, die 2600hz erzeugte

Phone phreaking wurde oft von blinden Hackern durchgeführt, weil das Sehvermögen nicht nötig war, jedoch ein sensitives Gehör von Vorteil war. Phone phreaking hatte mit Sprechen, Pfeifen, und differenziertem Hören auf Frequenzen und Klicks am Telefon zu tun.

Um den richtigen Ton zu produzieren, musste das In-Band Signal manipuliert werden. Dafür wurde ein elektronisches Gerät genannt «blue box» verwendet. DTMF Töne und andere Töne wurden auf Knopfdruck erzeugt. Bevor *Steve Wozniak* und *Steve Jobs* den Bau des Apple Computers starteten, entwickelten sie eine blue box und verkauften sie der phreaking community. Andere Geräte wurden gebaut, welche Multifrequenztöne für diagnostische und analytische Zwecke fabrizierten. Diese Geräte hatten auch Namen von Farben wie «black box», «red box», «silver box» und andere. Die Farben hatten nichts mit der Aussenfarbe des Gerätes zu tun, sondern mehr mit der Funktion.

Phone phreaking ist bekannt in der Öffentlichkeit, im Hollywood Film «War Games», benützte die Figur «David Lightman» phone



Hollywood Film War Games

phreaking Techniken um Ferngespräche von seinem Computer aus zu tätigen und ebenso von einem Pay phone aus. Im Film «Hackers» wurde phone phreaking benutzt um Ferngespräche zu führen und um das FBI abzuhören.

Telefongesellschaften auf der ganzen Welt sahen das phone phreaking als Bedrohung für ihr Geschäft an. Blue box Geräte begannen auf dem Markt erhältlich zu sein und die Menschen führten vermehrt gratis Ferngespräche. Es ging beim phone phreaking meist um finanzielle Profite und Kriminelle begannen, die Ferngespräche billig anzubieten. In den meisten Ländern wurde phone phreaking als Betrug und Dienstleistungsdiebstahl eingestuft – also eine strafbare Handlung. Die Strafverfolgung und Teams für Betrugsermittlung bei den Telefongesellschaften arbeiteten zusammen, um phreakers zu identifizieren und zu verhaften. Die phone phreaking community startete mit neugierigen Personen, die nur Spass haben wollten und mehr über das Telefonsystem erfahren wollten, aber später ergab sich daraus eine kriminelle Finanzaktivität.

Um dem Missbrauch einen Riegel zu schieben, begannen die Telefongesellschaften Frequenzfilter in die Kundenlinien einzubauen, um dadurch zu verhindern, dass spezielle Töne mit 2600hz verwendet werden können.

Eine Bluebox app vom Apple Appstore

Die grundsätzliche Schwachstelle, die phreaking möglich machte, war das In-Band Signal, welches das Telefonsystem kontrollierte. Die Telefongesellschaften wurden sich dessen bewusst und entwickelten neue Infrastrukturen, welche Out-of-Band Signalisation verwenden, die nicht direkt manipuliert werden konnte und bald Standard wurde.

Phone phreaking funktioniert heute nicht mehr bei modernen Telefonen und ist somit lediglich von geschichtlichem Interesse.

Quellen:

Der berühmte Esquire Artikel, welcher phone phreaking publik machte:
http://www.historyofphonephreaking.org/docs/rosenbaum1971.pdf

Geschichtliche Information über die Telefonschaltung von früher:
https://strowger-net.telefoniemuseum.nl/tel_hist_index.html
https://strowger-net.telefoniemuseum.nl/tel_tech_index.html

Eine Sammlung von aufgenommenen phone phreakings:
http://evan-doorbell
http://elmercat.org/ld-calls/

Verschiedene Arten von phone phreaking Boxen:
https://en.wikipedia.org/wiki/Phreaking_boxes

Von phone phreaks geschriebene HOWTO Artikel:
http://www.textfiles.com/phreak/

Der Artikel wurde von Florence Kunz übersetzt. Der englische Originalartikel befindet sich auf: https://digitalforensics.ch/nikkel20b.pdf

Original English version found here: https://digitalforensics.ch/nikkel20b.pdf