The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage

Clifford Stoll

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage

Clifford Stoll

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage Clifford Stoll

Before the Internet became widely known as a global tool for terrorists, one perceptive U.S. citizen recognized its ominous potential. Armed with clear evidence of computer espionage, he began a highly personal quest to expose a hidden network of spies that threatened national security. But would the authorities back him up? Cliff Stoll's dramatic firsthand account is "a computer-age detective story, instantly fascinating [and] astonishingly gripping" (Smithsonian).

Cliff Stoll was an astronomer turned systems manager at Lawrence Berkeley Lab when a 75-cent accounting error alerted him to the presence of an unauthorized user on his system. The hacker's code name was "Hunter" -- a mysterious invader who managed to break into U.S. computer systems and steal sensitive military and security information. Stoll began a one-man hunt of his own: spying on the spy. It was a dangerous game of deception, broken codes, satellites, and missile bases -- a one-man sting operation that finally gained the attention of the CIA...and ultimately trapped an international spy ring fueled by cash, cocaine, and the KGB.

The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage Details

Date : Published September 13th 2005 by Gallery Books (first published 1989)
ISBN : 9781416507789
Author : Clifford Stoll
Format : Paperback 399 pages
Genre : Nonfiction, History, Computer Science, Computers, Science, Technology

⬇ **Download** The Cuckoo's Egg: Tracking a Spy Through the Maze ...pdf

▤ **Read Online** The Cuckoo's Egg: Tracking a Spy Through the Maz ...pdf

Download and Read Free Online The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage Clifford Stoll

From Reader Review The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage for online ebook

Philipp says

Update August 2016: Here's an amazing video of the author showing off his self-built warehouse of Klein bottles including self-built trash warehouse robot

I've seen this book pop up a few times on lists like "recommended reads for programmers" and always wondered why - I didn't know it was such a extremely fascinating read! I tried to read it in one evening but had to stop at 4am.

It's the story of how one US astronomer turned computer programmer ("astroinformatician"?) found a 75 cents bill for computing time he couldn't make sense of, how he traced that bill, found an intruder on his system, and how it took him months to untangle the web of systems the hacker used to disguise himself.

Stoll had a very interesting scientific way in which he approached the problem of an intruder, which resonated with me strongly: he kept neat lab-books of everything that happened, he thought clearly about each step, and all the little details they used to infer more about the hacker are splendid.

For example, on login the hacker kept on using "ps -eafg" to see who was logged in, but "-f" was superfluous under Berkeley Unix, which indicated that the hacker was used to AT&T Unix, which wasn't used on the US West Coast. Therefore it was more likely that the intruder was from the US East Coast, or from abroad.

(Another fun thing about the age of this book - it's clearly written for the layman in 1989, so things that are completely basic today are explained in long terms - "electronic mail", for example)

It becomes a fun cat and mouse game - it's always the same intruder (who turned out to be (view spoiler)), Stoll tried to get the US government involved, but no agency wanted to have anything to do with it - neither the FBI, nor the CIA, nor the NSA had anything to do with computer break-ins, there were no laws yet, nothing (the events in this book happen around 1986-87, I was just a few months old).

It's great fun to read how each step in the plan worked out, how Stoll laid traps, each step in his thinking is detailed (the joys of writing everything down!).

You'll especially love this if you (like me) grew up fascinated with German "hacker culture" of the late 80s, early 90s, back when the Chaos Computer Club started to become a name. I got the biggest smile from this little dialogue:

> "Can you identify who's breaking in?"
> "One guy uses the pseudonym Hagbard. Another, Pengo."

I'm pretty sure every German "computer person" knows who hagbard was. We've all seen the movie "23", and if you haven't, you greatly owe it to yourself, it's one of my favorite German movies (even Robert Anton Wilson, who co-wrote "Illuminatus!", has a small part playing himself). It portrays the KGB hacks from

hagbard alias Karl Koch and his friends, which is closely connected to the story of this book, but the movie focuses on Koch, while the book focuses on the systems Hess broke in. I guess focusing on Koch made for a more interesting story - he had a relatively large cocaine habit, and he was found burned to death, with no suicide note.

Stoll didn't like the CCC at all - in the book he repeatedly calls them vandals, I guess because back then, it was just a couple of kids messing around, not particularly knowing what they were doing. Nowadays the CCC advises the German government on technical security matters. The Chaos Communication Congress is one of the best and biggest technology conferences in Germany (I'm proud that I once held a little talk there at an ungodly hour together with Bastian Greshake/@gedankenstuecke).

Another interesting side-note is that some currently very famous "computer people" appear shortly - such as Paul Graham and Robert T. Morris, who have since then founded several companies and are now known for ycombinator, one of the biggest Internet startup seed funding companies (possible more for ycombinator's social news site, Hacker News)

If you want to read a more technical side of this, Stoll first published a paper: Stalking The Wily Hacker.

I wonder how much the events in this book, and the book itself, made Snowden's revelations possible... Would the NSA ever have started to try and control the entire Internet if the Soviet Union had never started to pay hackers for information?

Recommended for: Computer people, those interested in the history of the Internet, those who enjoyed playing Uplink

Not recommended for: People who want to think that the Internet is Facebook

---

Brian Rosenblat says

I really enjoyed this book. Loved the references to Berkeley, the hacker chase, but most interestingly, it takes you back to an earlier time in computing (in 1989)- which I thought was a fascinating reminder of what things were like. For example, I love the explanation of 'electronic mail.' At this point, I think most people have forgotten what the 'e' in email stands for.

Also, a favorite passage, as he explains what the "Internet" is:

> "At first, DARPA's network [the Internet] was simply a testbed to prove computers could be linked together. Since it was seen as an unreliable experiment, universities and laboratories used it, and main stream military people ignored it. After eight years, only a few hundred computers were connected into the Arpanet, but gradually, others were attracted by the network's reliability and simplicity. By 1985 the network directory listed tens of thousands of computers; today, there must be over one hundred thousand."

100,000 computers! Just for comparison, I did a quick search. Analysts predict there to be more <u>mobile</u> devices connected to the Internet then humans alive in 2016 - that's more than 7.6 billion mobile devices - that doesn't include desktop and laptop computers. (source: Cisco VNI Index). Wonder what it will be like in another 20 years?

The story is also fascinating. Shows how one guy in a computer lab in Berkeley was able to track down a ring of international hackers and awaken some of the US top security agencies to the dawn of a new form of espionage. It was amazing how lax computer security was before this - and how it took an incident like this to awaken these agencies to the threat of cyber espionage.

Only reason it gets 4 instead of 5 starts is that while the beginning and end are very interesting, about mid-book it starts to get pretty repetitive. E.g. (view spoiler)

Overall, really liked it. I think you need to be a bit of a computer geek to enjoy this one. But would definitely recommend to anyone who wants to reminisce a bit who enjoys a good spy chase laden with UNIX commands.

Eric Lin says

Great book. The FBI was incredibly frustrating to read about. Not many people would have been persistent enough to stick with this. I'm impressed with how diligently the author worked to track this guy down.

One small gripe though - the author seemed way too self conscious about his political identity add a result of cooperating with the guys in suits. Was he trying to spin it as an internal struggle between who he was, and who this experience made him become? Not buying it, Cliff.

Mike says

Good old school hacker tale. If you are a techno geek and familiar with the likes of emacs, dot matrix printers and old school bbs boards, this is for you.

Its also a really interesting breakdown of intrusion techniques, much of which holds true today.

Wilson Lanue says

For some years after its 1989 debut, The Cuckoo's Egg was *the* book to read about computer hacking (or, more specifically, counter-hacking). But this superb read is much more than the memoir of an astronomer who followed a 75-cent accounting "error" to a Soviet spy and sudden fame as the world's top computer security expert.

It's the story of a sincere Berkeley liberal who came to see conservative establishment types as fellow human beings, to the confusion of those closest to him. Candid, thoughtful, and funny, perhaps it can help other liberals - and conservatives - to similarly bridge the culture gap.

(An interesting side note: By 1995, Stoll had all but completely sworn off computers, pooh-poohing the idea

of e-commerce and suggesting that computers should not have a place in the classroom. He became a stay-at-home dad and, today, his main concession to computing seems to be the Web 1.0 site where he hawks glass "Klein bottles" he blows in his spare time - including a beautiful mug or "Klein stein.")

Jonathan says

Here is the story of how I came to read The Cuckoo's Egg: I purchased it at a library book sale because it looked interesting, tossed it in a box because I didn't have time to read it, and promptly forgot about it.

Then I got married, and we got real bookshelves instead of boxes, and I put the book on the shelf because it was hardbound and hardbound books show that you are a serious, thoughtful person.

Then my Uncle Steve came over from Florida and started telling me about a book he had read, a true story of a guy tracking down a hacker in the 80s. "Wait a sec," I said, "is it this book?" And I pulled down my dusty copy of The Cuckoo's Egg. It was, in fact, that book, and I decided that it didn't deserve space on the shelf if I hadn't actually read it.

The Cuckoo's Egg is written by an astronomer who had been put in charge of some computers. He'd been trying to track down a 75-cent accounting error–this was back when you had to pay for every cycle of computer time–and, almost entirely by accident, found a hacker in his system, using it as a stepping-stone to attack other computer systems around the country.

That all happens in the first twenty-five pages. Rather than closing the hole the hacker was using to get in, however, Stoll decided he wanted to catch the guy, and that's where the real story begins, because tracking a communications link backwards is not very easy. None of the three-letter government agencies take him seriously, his relationship with his girlfriend is rather strained, and the three weeks his boss gave him to investigate the problem stretch into months. It's tedious work (and, in parts, tedious reading) analyzing every move the hacker makes and trying to piece together enough information to catch him.

This book isn't for everyone. It's a spy story, but it's been pieced together from Stoll's logbook and the man is a scientist–you'll find no melodrama or embellished details here, just the facts. The author doesn't assume a technical audience but if you've ever used Unix (or its successor on PCs, Linux), you will understand a lot more of what's going on inside the systems. There's just enough real-human stuff to break up the technical monotony–Cliff has an active social life, sews his own Pope costume, and at one point microwaves his shoes–but in the end this book is great reading mostly for those interested in computers and security.

I also recommend it if you want to know what the Internet was like in its Wild West days, before the personal computer and the World Wide Web brought it to the masses. Scientists, military networks, and archaic file transfer protocols are all present and accounted for. It's a fascinating how old everything seems even though the book's events happened only a little more than twenty years ago.

In closing, here's a number sequence puzzle that a three-letter-agency spook gave Cliff in the book that–at the time of the book's publishing–Cliff hadn't figured out yet. Can you? Hint: It requires very little math.

1, 11, 21, 1211, 111221, ….

Brian says

(5.0) So much fun! (may need to be a little computer-geeky to really love it)

Crazy cool true story about an astronomer-turned-sysadmin at Berkeley in the 1980s who decides to track down a 75 cent accounting discrepancy in server usage, and turns into a year-long hunt to track down a sneaky computer spy operating for the KGB. Covers several severe holes in Unix security, but emphasizes that the weakest link in security is almost always from human operators.

Very engaging read, tore right through it. It almost reads like a mystery, detective or spy novel, but it's so much more exciting because it's all true. Told by Cliff Stoll, the self-appointed cybersecurity guard who was investigated the discrepancy and eventually tracked the spy/hacker. He got little/no help from many law enforcement agencies who owe him a huge debt of gratitude. Really appreciated hearing his thought process, his approach and reaction to what found.

I recommend this to almost every computer geek I meet or hire (or try to). Strongly recommended and really wish I could read it again for the first time. :)

---

3 no 7 says

The Cuckoo's Egg" by Clifford Stoll was fascinating the first time I read it in 1989, and when I saw it on one of the "books to read" lists on Goodreads, I eagerly reexamined it. It is still compelling today, just in a different manner. The technology has changed, but the crime and the chase have remained the same. The incredibly cat and mouse chase through what was then just the beginnings of the internet still kept me on the edge of my seat, remembering dial-up, dot matrix printers, and long distance phone bills.

In the end, "The Cuckoo's Egg" is computer hacking at its beginning, and it serves to remind us of the benefits and detriments of a cyber-dependent society. Today, internet crime is rampant on so many levels and it still takes skilled and observant people to combat it.

Read and remember, and if you do not remember, read and learn.

Mister E says

This is one of the books that really defined my life.

While in the astrophysics program at Berkalurk, young Clifford Stoll is asked to look into an extra couple cents being charged for their computer use. What follows is the discovery of an East German (Cold War era mind you) hacker using Berkeley's computer network to enter private miliary networks.

This is one of the most realistic novels on hacking you could find. Forget the deck's of Gibson and the 3D, motorcycle racing or Stephenson, this is real hacking. Writing scripts and watching as he enters commands over your network. Waiting for days to see if your logs will say 'user x logged on'.

It also had a fascinating description of the government and how the 3 letter agencies handled computer crime back in the day, as well as an actual description of the NSA.

Rafael says

Por razones laborales he estado revisando temas de seguridad informática, eso me llevó a releer un texto que escribí y publiqué en Revista Red hace como diez años. Los temas de seguridad han evolucionado y hoy estamos inmersos en temas muy interesantes de biometría para autenticación de usuarios, como platicaba hace unos días con mi amigo Enrique Daltabuit, experto nacional en el tema. Sin embargo el texto de hace diez años tiene vigencia en la medida en la que comenta un libro fascinante, uno de esos que se siente inmediata necesidad de compartir.

Se trata del libro de Cliff Stoll, The Cuckoo'segg, es decir El Huevo del Cuclillo, ese pájaro que los suizos han puesto a vivir dentro de sus relojes y que tiene el hábito de parasitar los nidos que construyen otras aves. No se si exista una traducción al español de este libro tan ilustrativo, pero sería una lástima que no fuera accesible a más personas.

Stoll era en 1986, año en el que inicia la historia, un estudiante graduado de astronomía en Berkeley, donde también administraba una de las computadoras del laboratorio Lawrence. A partir de una diferencia de 75 centavos de dólar en la contabilidad de la computadora, cifra que es pequeña, por más fluctuaciones de la moneda que haya, descubre que ha estado ocurriendo un acceso no autorizado a su máquina.

Ahí arranca una obsesiva, desesperada, desesperante y muy ingeniosa persecución del intruso a través del laberinto de conexiones entre las computadoras. La persecución se hará a través de líneas telefónicas locales, cables trasatlánticos, satélites y desde luego varios países en América, Europa y Asia.

El libro, construido con base en la bitácora que Stoll fue escribiendo conforme se desarrollaban los hechos, no es una novela, narra acontecimientos reales, pero su lectura es sumamente adictiva. Uno empieza a pasar página tras página con la angustia de querer saber qué va a ocurrir, en que momento y cómo será descubierto el intruso. Tampoco es un libro de texto pero enseña muchas cosas acerca de la seguridad en cómputo, quizás la más importante es que si bien no existen —y quizás no puedan existir— sistemas de cómputo seguros en 100 por ciento, en muchos casos el principal responsable de la falta de seguridad en una máquina es su administrador.

Muchas veces, quien se dedica a ingresar de manera subrepticia en computadoras a las que no tiene permitido el acceso puede hacerlo si conoce magistralmente las fortalezas y debilidades del software que se utiliza para adminsitrar la máquina, quien quiera evitárselo deberá hacerlo también usando el mismo software. Una especie de guerra de inteligencias se establece entonces, haciendo por eso tan atractivo el asunto. Sumemos a eso que los delitos computacionales pueden ser buen negocio e iremos entendiendo porque el ataque a los sistemas de cómputo se va volviendo un tema de nuestros días.

Esta lucha entre dos cerebros, que emula el placer del juego del ajedrez queda muy clara en el relato de Stoll. El intruso ha descubierto una debilidad en el editor de textos creado por Richard Stallman, Gnu-Emacs. La flaqueza consistía en que el programa permitía llevar archivos a las áreas protegidas de la computadora. Cuando un equipo de cómputo es utilizado por varias personas, cada uno de ellos tiene distintos derechos. Cada uno puede leer y escribir en sus registros, pero no en los de los demás. El administrador del sistema tiene permisos especiales para colocar archivos en áreas protegidas para acceder a los archivos de todos los usuarios.

Valiéndose del Gnu Emacs el hacker de Stoll lograba colocar en un área privilegiada de la computadora un programa que le daba privilegios de super usuario, es decir de administrador del sistema, con posibilidades de crear o destruir cuentas de usuarios y leer archivos confidenciales. En una palabra se volvía dueño de la máquina.

Esta forma de convertirse en superusuario es la que da origen al título del libro: En palabras de Stoll: "El

cuclillo pone sus huevos en los nidos de otros pájaros. Es un parásito de nidos... Nuestro misterioso visitante dejó un programa-huevo en nuestra computadora, permitiendo al sistema empollarlo y alimentarle privilegios".

Pero si el intruso tiene recursos para hacerse con la máquina, Stoll los tiene también para vigilarlo y rastrearlo. Lo observa desde una computadora en la que no puede ser detectado, conecta una impresora a la máquina para registrar cada teclazo que el intruso efectúa cuando está en sesión, construye software para hacer sonar una alarma cada vez que hay una introducción no autorizada. El soft¬ware da incluso, en clave Morse, la inicial de la letra de la clave del acceso no autorizado. Stoll duerme varias noches en la oficina a la espera del hacker, contacta a todas las oficinas de las tres letras, como él llama a la FBI, CIA, DOE, FCI, etc. que pueden intervenir en el caso. Avisa a los administradores de los sistemas, que están siendo vulnerados, de la presencia —muchas veces ignorada por ellos mismos— del hacker.

Algunos administradores reaccionan simplemente cerrando el hueco de sus sistemas, que había permitido el acceso del extraño. Stoll no lo hace; sabe que si eso no resuelve el problema, el fisgón encontraría otra ruta a través de otras máquinas para seguir espiando dentro de los sistemas militares de los Estados Unidos. Stoll decide dejar abierta la puerta de su computadora para que el intruso pase y poder saber que hace.

Cuando en alguna ocasión, el hacker, está obteniendo información indebida, Stoll que lo observa, produce con sus llaves corrientes espurias en las conexiones, para que el espía reciba caracteres ininteligibles en su máquinas. En muchos casos el hacker logra el ingreso a las computadoras mediante un tedioso procedimiento de ensayo y error. Hace la llamada para la conexión y cuando le preguntan nombre y clave en el sistema propone algunos obvios como Quest o Field y Service en las computadoras Vax.

Por increíble que parezca esto le funciona —por descuido de los administradores claro. Algunas veces visita 60 o más máquinas sin éxito y de pronto, ábrete sésamo, ingresa como superusuario. Stoll compara esto con andar deambulando por las calles, moviendo las perillas de las puertas para ver quien olvido echar llave.

Una vez dentro de alguna computadora, el espía coloca su programa-huevo, se vuelve superusuario, lee los archivos y ahí encuentra claves para otras computadoras o copia el archivo donde están las claves de los usuarios o siembra un programa que los lea en el momento en que se conectan.

Stoll que es un estudiante de Berkeley, recordemos que esta universidad es famosa además por la rebeldía de sus estudiantes, encuentra difícil hablar y colaborar con los agentes federales, pero lo hace por un profundo sentimiento de que el hacker está destruyendo lo más importante de las redes de computo: la posibilidad de comunicarse. Los hackers destruyen la confianza de las personas en los sistemas de cómputo y pueden llevarnos a aislar nuestros sistemas en busca de la seguridad.

Stoll logró localizar a su hacker y poner en perspectiva que la irrupción no autorizada en sistemas de cómputo no sólo es como un duelo de inteligencias, no es algo inocuo como el ajedrez, es una actividad que daña la confianza de los usuarios de las redes de cómputo.

Rob says

Executive Summary: A truly excellent and fascinating tale of hacking in the early days of the internet.

Full Review

I'm fascinated with computer crime. I have for as long as I can remember being interested in computers. Somehow I had never managed to read this book.

I'm glad I finally got around to it. It might be my new favorite. Cliff Stoll tells an engaging and personal story of his discovery of computer networks, security exploits and computer crime that reads more like a spy novel than a technical manual.

I think Mr. Stoll does a good job of making things easy to understand for the non-technical person. It has just enough detail to follow the story without being overwhelming. Of course being a computer person myself, I may not be the best to judge how technical this book gets.

This book overlaps with some other stories of computer crime I've read and re-sparked my interest in reading some others I have on my backlog, along with rereading one I read back in high school that seems to overlap with this one a bit.

It's hard for me to judge how non-techies will enjoy this book, but anyone who wants to see what things were like in the early days of the internet should find this fascinating.

The most remarkable thing was how little the various law enforcement agencies seemed to care. It was really the wild-wild west of computer crime. To the FBI, unless they physically stole something, destroyed something or cost your millions of dollars, it wasn't worth pursuing.

How do you quantify computer time? Especially back then when computers weren't affordable and resources were limited. What about the time Cliff Stoll spend tracking the hacker? Time he should have spent doing his job. Everyone wanted him to keep at, and to keep them in the loop, but no one was willing to do anything about it, or cough up funds to support him.

It would take a few more years and some bigger crimes to finally wake them up and change how computer crime ranked in importance. Then again, most people are inundated with malware, spyware, viruses, scams and phishing emails on an almost daily basis. So in some ways it feels like nothing has really changed. You're not going to call the FBI because someone tried to steal your password.

Computer crime is big business these days, and if you want to see how it was in the early days, this is a must read.

Jonathan Leblang says

Interesting book, especially since I worked at MITRE at the time, and had first-hand knowledge of the method the hacker used to go through the systems. Also met him at a security conference -- he gave a nice presentation.

Nick says

I read this book first around sixth grade and again last month. It was wicked good the first time and so-so the second time. I think as I've gotten older and wiser and more discerning, and as technology has progressed, this book hasn't aged well.

Here's the synop: Cliff Stoll is an astrophysicist who knows just a little something about computers (obviously a lot). He's living at UC Berkeley in the early days of the internets. One day he discovers a 75 cent accounting error (this is back before AOL charged you by the minute), and kablammo! he's discovered a hacker. Now all he needs to do is catch him...

When I read this at 12 going on 13, this book seemed like a bleeding edge thrill-a-minute technological game of cat and cuckoo. And now, at 26 going on 27, it's still kinda neat. Cliff is obviously a brilliant guy, and he does really well in 1) explaining his maneuvers to keep the hacker at bay and 2) downplaying how smart he was. What annoyed me was all the personal stuff in this book and how intrusive it is. I don't care about Cliff the person. I want to read about Cliff the cyber-battler, the Cliffinator sent back from 2008 to 1986 to battle the West German hacker Markus Hess. Or simply Cliff the research paper.

Here's the personal shit I don't like: Cliff's a hippie cliche who hates the government, wears tie-dye, likes the Dead, and lives and works in Berkeley. His girlfriend/fiancee is built like a sumo wrestler (this is subtly alluded to). Her old college roommate is a butch lesbian who hates the government. Their present roommate is a violinist who's always brining home a new crazy man.

Cliff's sooo frustrated that no government agency will help him. Why won't they help him?! And what about the future of the internet, and the need for open networks to foster scientific intercourse and shit like that?? Waaaa, waaaa, why don't you cry about it, you big hippie baby?

OK, so I'm being hard on Cliff and his wacky teammates in life. What can I say, though? They're all boring. Cliff and his entire life is boring. Except for the hunt. So Cliff, focus on the hunt.

If you've made it this far through this self-indulgent review, you might wonder why I gave this book 4 stars. I'll tell you why: I loved it the first time, and the second time, last month, was still pretty good. Cliff Stoll - he can keep you up at night past your bedtime. His book's good in bed.

Charlotte says

I really enjoyed this book.
The wild thing is that it's a true story, and that it's still relevant and really interesting 30+ years after it occurred. A definite mark of quality, in my eyes.
Some things have changed a lot; six-letter, all lower-case passwords aren't considered safe anymore, and most people are familiar with the internet. However, it calms my occasional anxiety of the future that nerds basically are unchanged since at least the 80's.
This is a definite recommendation for anyone even slightly interested in computer science.

Rebecca Huston says

This is a compelling, enjoyable read about what is hacking, and how a systems engineer caught and shut down an espionage ring. Told by the engineer himself, Cliff Stoll's story is full of technical details, but also a great deal of wit, and not a little sarcasm. A seventy-five cent discrepancy alerted him that someone was poking about where he shouldn't be, and task of tracking down who it was led him to the Air Force, the Army, the NSA and the FBI, among other entities. For anyone who remembers the early days of the Internet and when computers filled a room, this is a great read. I certainly had a good time with it. Four stars overall.

For the longer review, please go here:
http://personapaper.com/article/26824...

Kaethe says

As well as a gripping techno-thriller, it's also a sweet romance, and includes a great chocolate-chip cookie recipe. Stoll never sets out to be a hero, he's just a problem-solving grad student, who becomes really dedicated to solving one particular problem.

I wonder how dated it seems now?

Otis Chandler says

Super fun book - the story of a sysadmin chasing a hacker during the early internet, but it reads almost like a thriller - fun and fast.

I think I learned more about the early internet from this book than anything I've ever read before. I had heard of the words Arpanet and Milnet, but really didn't know what they were - simple networks of computers. And apparently, with very poor security! Impressive how easy it was for the hacker to get root access back then.

Internet security has come a long ways since those days (and has a very long way to go) - but you can really get a sense of how it started and where it's going by reading this.

Bill says

Engaging chase story in the world of 80s computer networks. He's definitely not a real writer but Stoll does a good job presenting himself as a likable everyman. Lots of Bay Area references. Would've been five stars but the conclusion was a bit anti-climactic after months of methodical build.

Nick Black says

The first "infosec true crime" book I ever read, and thus possibly a major influence on my life's work to this point (although surely not so much as *WarGames*). It's not as good as Sterling's The Hacker Crackdown, but better than most anything else along these lines. Cliff Stoll, astronomer-turned-network-monitor, is still around (last I checked, writing the abominable Silicon Valley Snake Oil), but let's be honest: he was never a computer scientist at heart, ignored decade's-old methods in this hunt for DDR-borne hackers (Bro, widely regarded as the world's first IDS, had been developed and published as early as 1980 by Denning and the InfoSec group at LBNL), and filled this book up with pants-wetting ramblings about "whether to help the Feds". Worth reading for its insights into the early period of academic/industrial internetworking and the fact that it's referenced everywhere.

Robert says

Cliff is an excellent storyteller and has done a great job sharing this true story. Perhaps too good of a job. Although it's consistently well-written, it is frustratingly slow at times. I don't hold that against him because it happens to be appropriate for conveying a hint of what he felt as he went through this. Like him, I kept feeling like there was a breakthrough or resolution just around the corner, only to find myself strung along to a longer road ahead.

As someone who's been through more than a fair share of dealing with hackers, spammers, buggy software, and poorly-designed hardware, I didn't need this story in book-length. Reading it was another chore caused by delinquent computer users (even if indirectly).