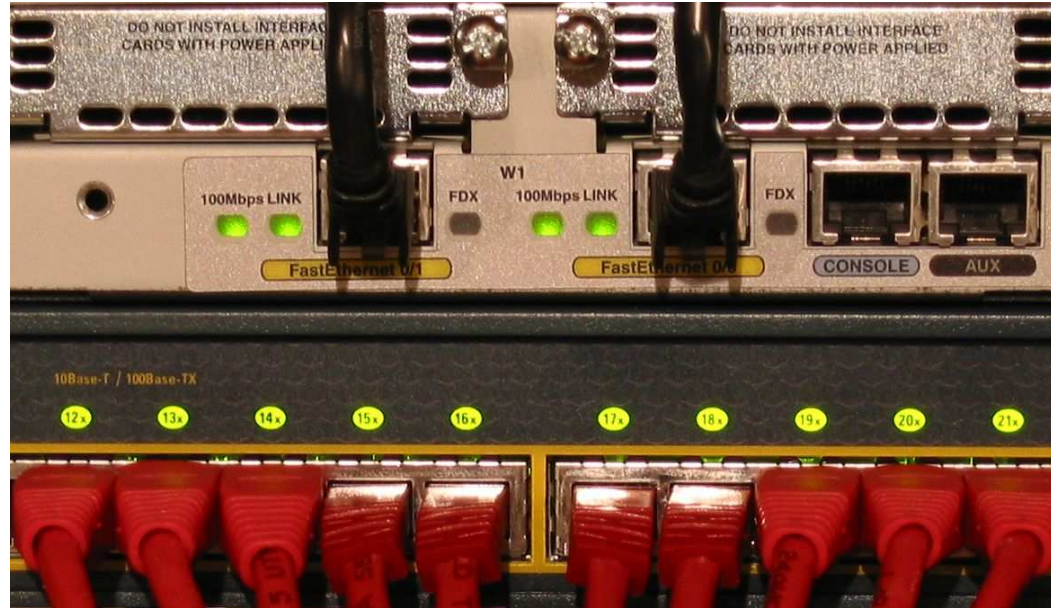


# Cooking the Cucko's Egg v1.0



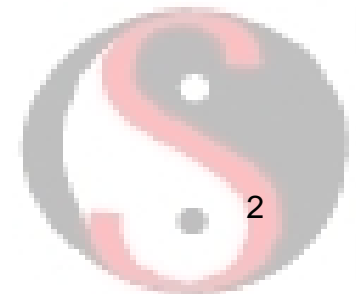
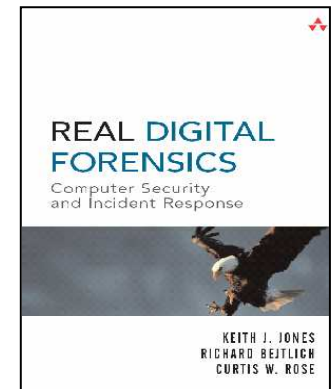
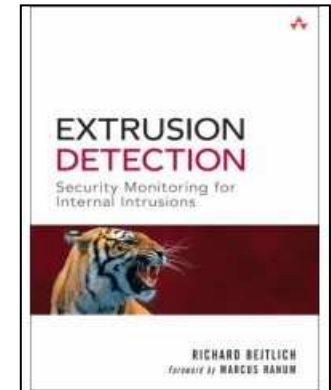
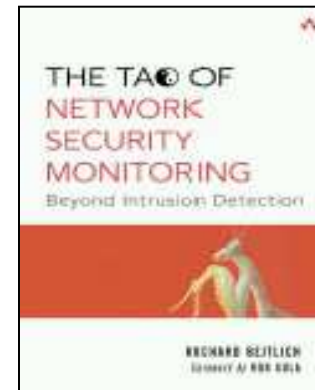
**TAOS**SECURITY  
THE WAY OF DIGITAL SECURITY

Richard Bejtlich  
richard@taosecurity.com  
www.taosecurity.com / taosecurity.blogspot.com

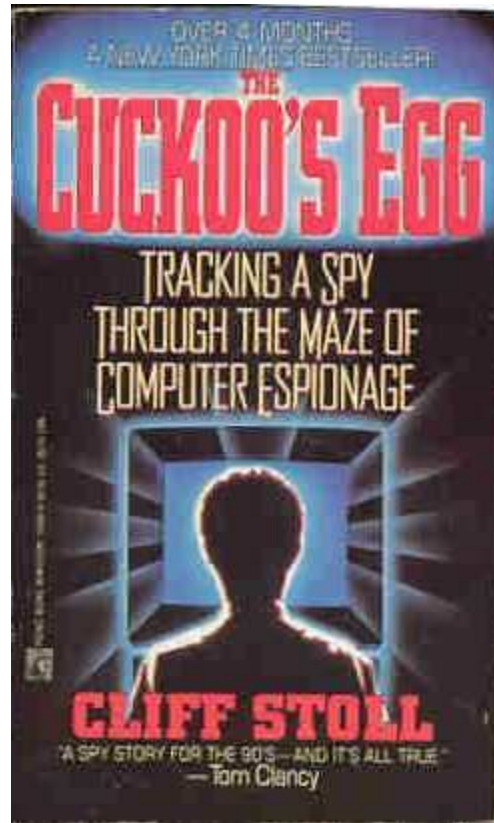


# Introduction

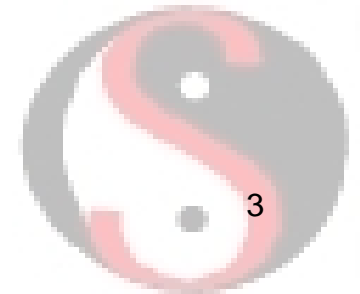
- Bejtlich ("bate-lik") biography
  - General Electric, (07-present)
  - TaoSecurity (05-07)
  - ManTech (04-05)
  - Foundstone (02-04)
  - Ball Aerospace (01-02)
  - Captain at US Air Force CERT (98-01)
  - Lt at Air Intelligence Agency (97-98)
- Author
  - Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
  - Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
  - Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
  - Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed
  - TaoSecurity Blog (<http://taosecurity.blogspot.com>)



# Lessons from The Cuckoo's Egg



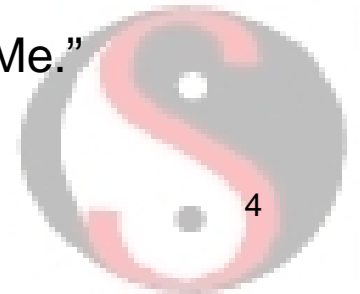
Originally published in 1989



## Screen Captures from PBS



In 1990, PBS' "Nova" aired "The KGB, the Computer, and Me."



# Cliff Stoll



Cliff Stoll was a Lawrence Berkeley National Laboratory astronomer assigned to be a Unix system administrator in his lab.



## It Started with 75 Cents



In August 1986, Stoll's supervisor Dave Cleveland asked Stoll to resolve a \$0.75 accounting error.



# Hunter

Starr	79907
Vine	67008
Treppasso	59099
Carlson	24517
Norman	34257
Hunter	
Benson	87459
Johnson	56739
Schlar	74578

Stoll determined the user "Hunter" was responsible for the \$0.75 discrepancy.



# First Response

Starr	79907
Vine	67008
Treppasso	59099
Carlson	24517
Norman	34257
Benson	87459
Johnson	56739
Schlar	74578

Stoll deleted the Hunter account.





## Third Party Notification

```
From: WAliff@dockmaster.ncsc.mil
To: root@ux4.lbl.gov

Subject: Breakin Attempt

Someone on your system ux4.lbl.gov
to our computer Saturday morning

We would appreciate you investigate
putting a stop to it.
```

Shortly thereafter Stoll's boss received an external notification from the owner of NSA's "dockmaster" computer that someone from LBNL was trying to log into dockmaster.



## Engage the Incident Response Team

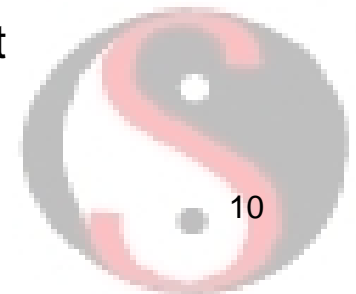
```
0x1-davec> forw
To: stoll
cc: davec
Subject: breakin

-----Enter initial text

Cliff,

Here's a problem for you!
```

Cleveland passed the issue to Stoll. Stoll realized that user “Sventek” was trying to log into dockmaster.



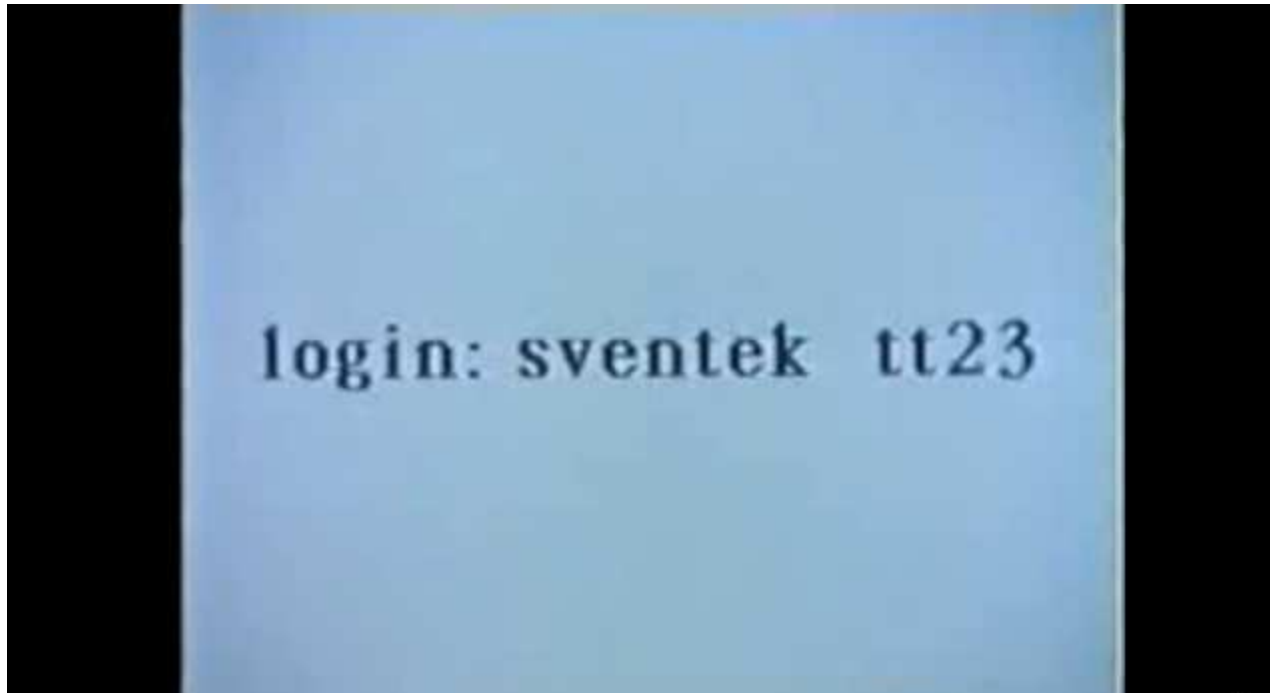
# The First Intrusion Detection System for LBNL



Stoll programmed his terminal to beep every time someone logs in!



## After 100s of Logins



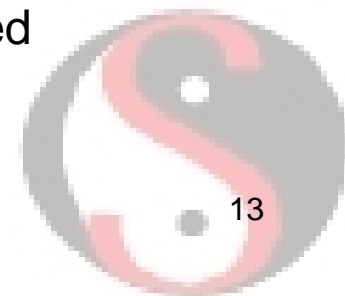
Stoll caught user Sventek logging into the LBNL network.



## Engage the Network Team



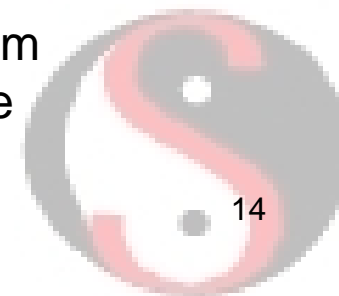
Working with the network team to trace the line associated with Sventek's login, they determined it is an outside connection with 50 possible lines.



## Instrumenting the Network



To instrument the network, Stoll borrowed 50 printers from LBNL users and attached one to each of the 50 lines he needed to monitor.



# The First Long Night



Surrounded by printers, Stoll stayed overnight hoping to catch Sventek logging into LBNL.



# Eighty Feet of Paper



During the night, Sventek logged in and generated eighty feet of logged activity!





# Local Privilege Escalation



Reading the logged activity, Stoll realized the intruder exercised a local privilege escalation vulnerability to become root. The problem resided in the movemail function in GNU Emacs.



## Improving the Instrumentation



Stoll bought equipment for monitoring at Radio Shack (of course).



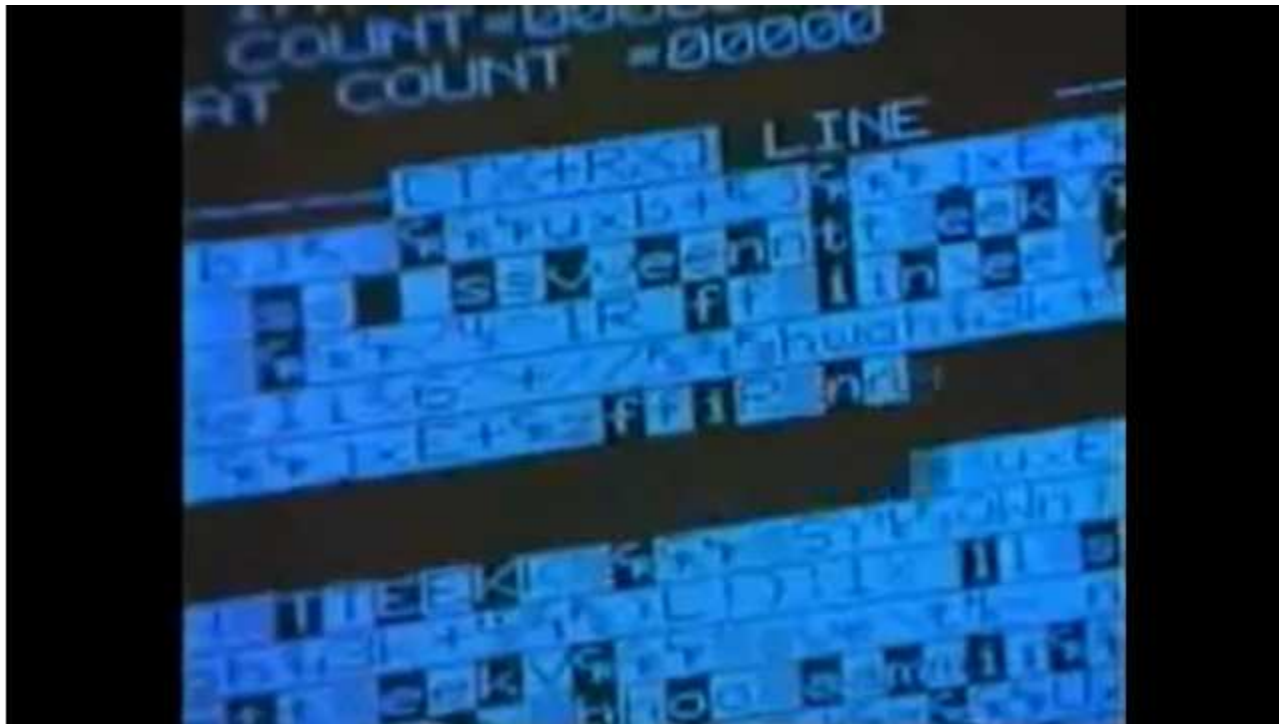
# Serial Line Intrusion Detection System



Stoll and colleague Lloyd Bellknap attached a logic analyzer to the lines, and programmed it to activate a dialer that will call Stoll.



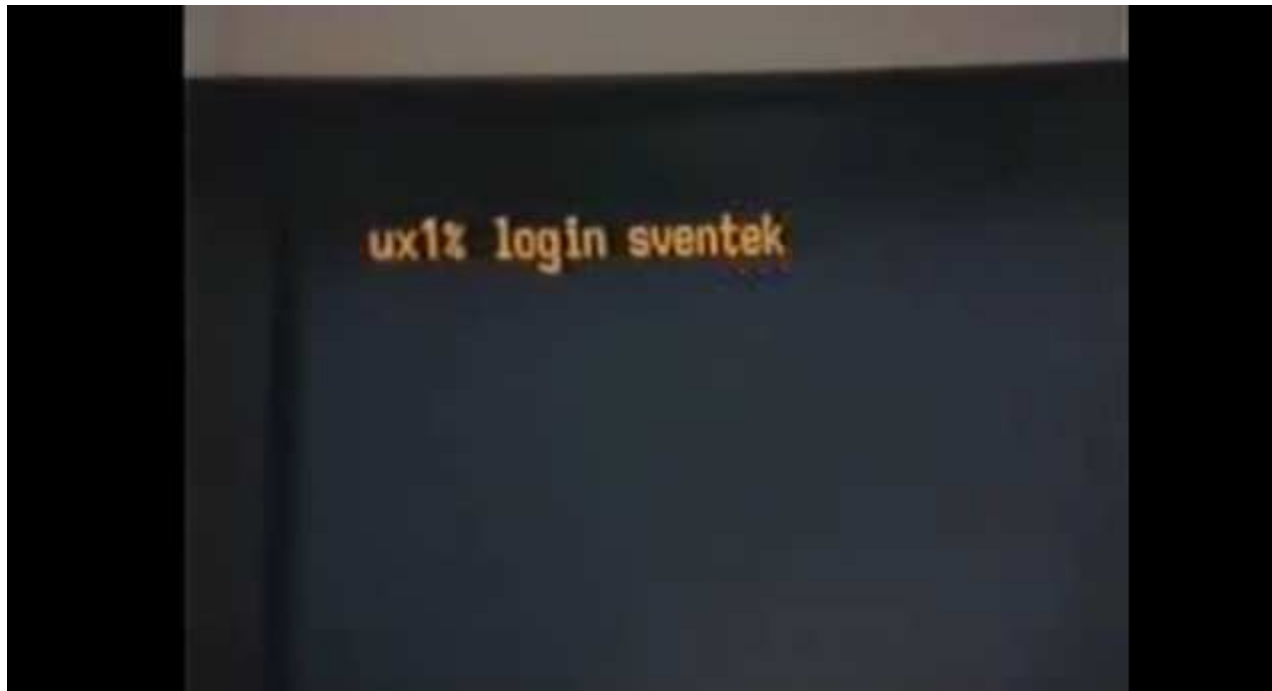
# Watch for Sventek



The logic analyzer watched for “sventek” on the serial lines.



# Stoll Tests the System



Rather than assuming the system just works, Stoll validated the alerting mechanism before Sventek returned.



## 24x7 Coverage



Now Stoll can wait for his LBNL IDS to call him at home when Sventek logs in.



## Additional Alerts



Stoll programmed a pager to sound when Sventek logs in. His girlfriend Martha disapproved.



## Stoll Gets Another Hit



Sventek logged in again and Stoll analyzed the activity.





# LBNL Is a Stepping Stone



Stoll observed logins to .mil and .gov computers.



## Accounts Created by Intruder



The intruder consistently created several accounts on compromised computers.



# Accounts Created by Intruder

Hedges\_



# Accounts Created by Intruder

Jaeger\_



# Accounts Created by Intruder

Benson\_



## Get the ISPs Involved



LBLN relies on Tymnet for connectivity, so Stoll asked them for help.



## More ISPs



Tymnet turned to Pacific Bell for assistance.



## Tracing the Next Login



Stoll enlisted the Oakland District Attorney to authorize tracing the calls to try to determine who is logging into LBNL.





## Sventek Returns

```
22 5377 56
23 6312 MS
24 4473 MS
25 4732 MS
26 10471 9.6
:pstat 2533 h0 0
HOST 0 PORT ARRAY 0 1
:trace 25_
REPORT PRT TEST LOG
```

When Sventek returned, Stoll and company began tracing him.



# Manual Effort



At least six parties were on the phone trying to determine the origin of the call.



# Stymied



Pacific Bell traced the call to VA, but the phone company said Stoll's search warrant is only good in CA. They wouldn't tell Stoll the origin of the phone call!



## Back to the Logs



Frustrated, Stoll decided to review the logs to identify affected parties.



# Enter the CIA

FOR  
-----  
SRI-NIC, TOPS-20  
@whois.cia  
Central Intelligence Agency  
Office of Data Process  
Washington, DC 20505  
There are 4 known mem  
Fischhoff, J. (JP27)  
Gresham, D.L. (DLG33)  
Manning, Edward J. (EM  
Sgler, Mary (MZ9)

Stoll noticed names, phone numbers, and email addresses of CIA netblocks in WHOIS data.



## Start Calling



Stoll decided to call the CIA points of contact directly to tell them Stoll has seen illicit activity involving CIA computers.



## Men in Suits



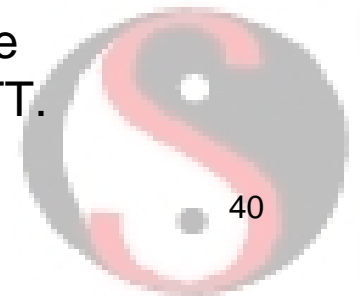
Officials from the CIA visited LBNL, but neither they nor the FBI offered help.



# Science

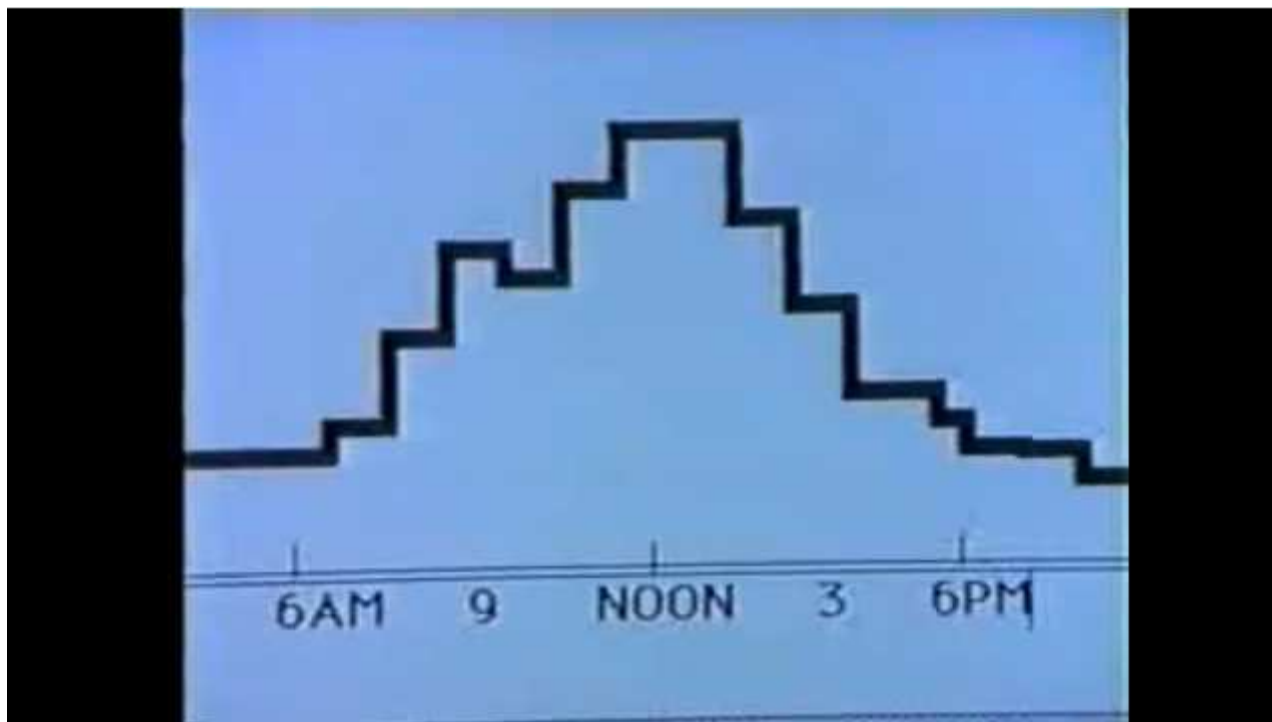


Stoll and friends tried to measure latency to determine the intruder's physical location. They measured 3 seconds RTT.





# Statistics



Statistical analysis of intruder login times showed he preferred accessing LBNL computers at mid-day, Pacific time.



# Star Trek

Scotty?



During one trace of Sventek activity, Stoll and friends identified activity originating from outside the US.



# The West German Connection

```
jay  
:SLOT 1 CORE SIZE IN KB  
:NO. OF LU FOR SLOT 1  
:V.24 DNIC 2624 ITT  
:V.24  
:V.24  
:V.24 Card
```

The trace lead to ITT, then to the Bundespost network in West Germany.



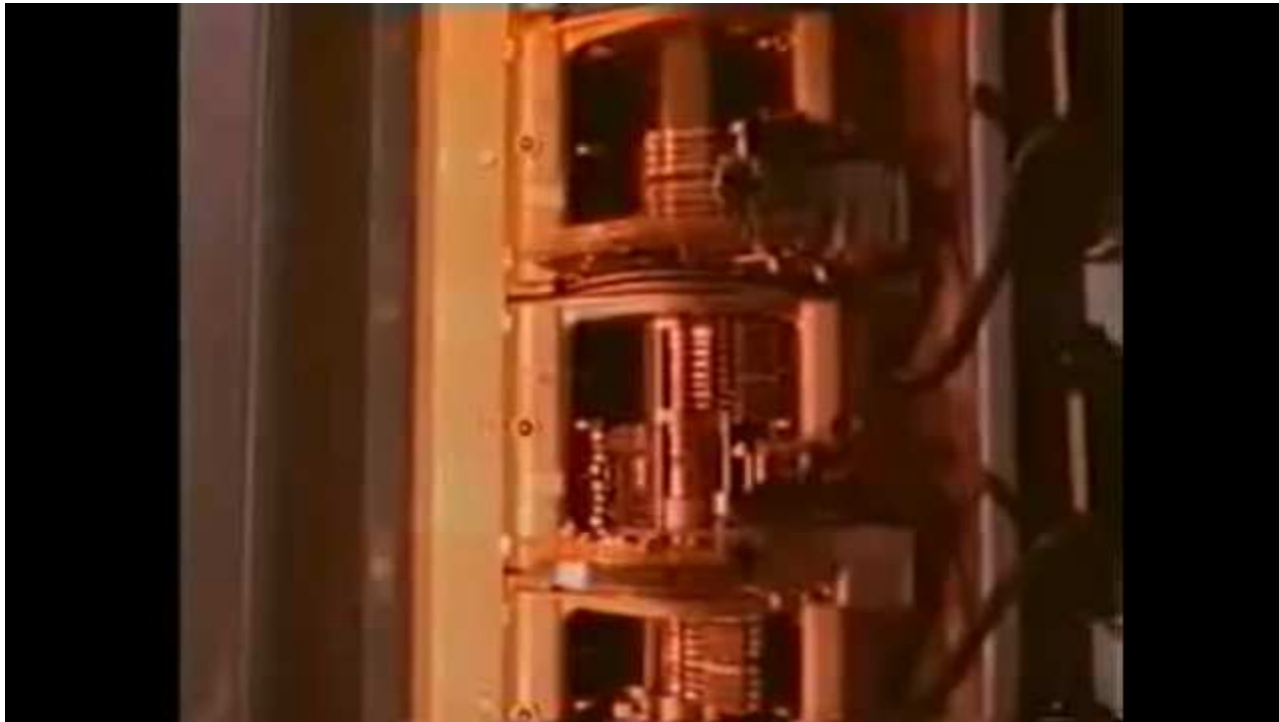
# Modern Germany



Unfortunately the Bundespost network used antique rotary switches from the 1950s.



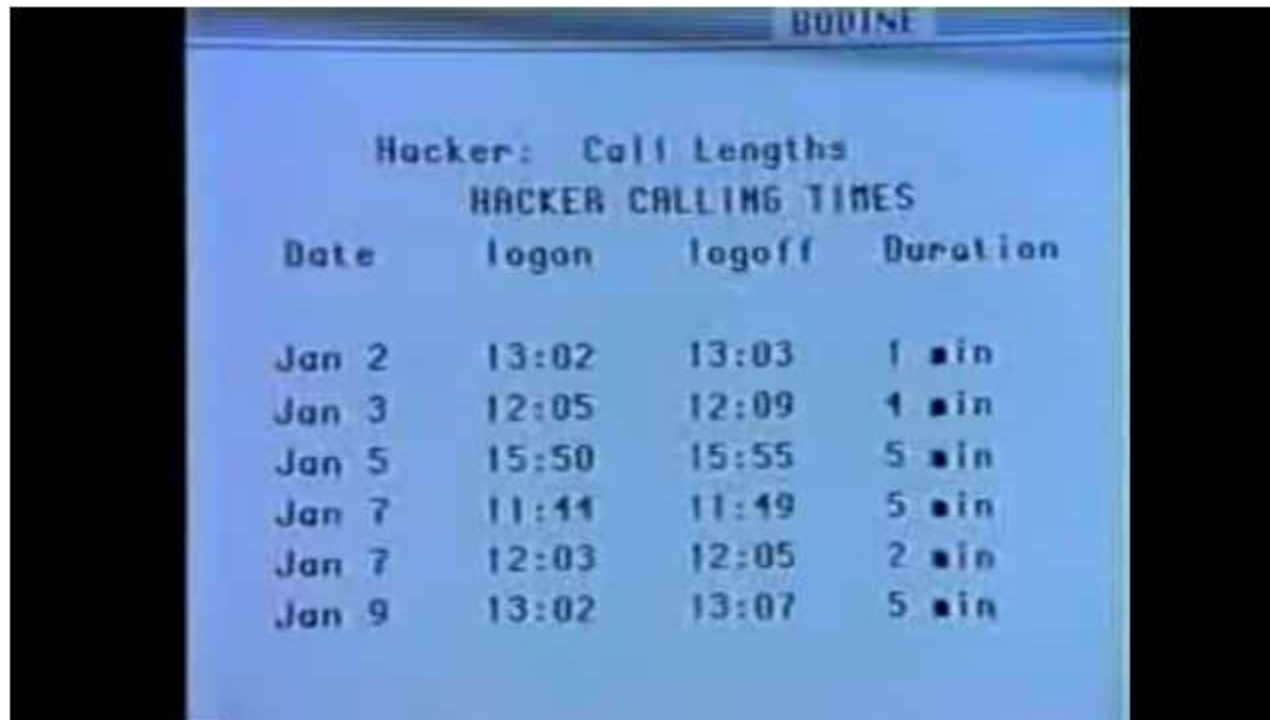
# Rotary Switches



Checking all of the rotary switches to determine the origin of a call required at least an hour!



# Too Little Time on Their Hands



The image shows a terminal window with a blue background and black text. The window title is 'BOITNE'. The text inside the window reads:

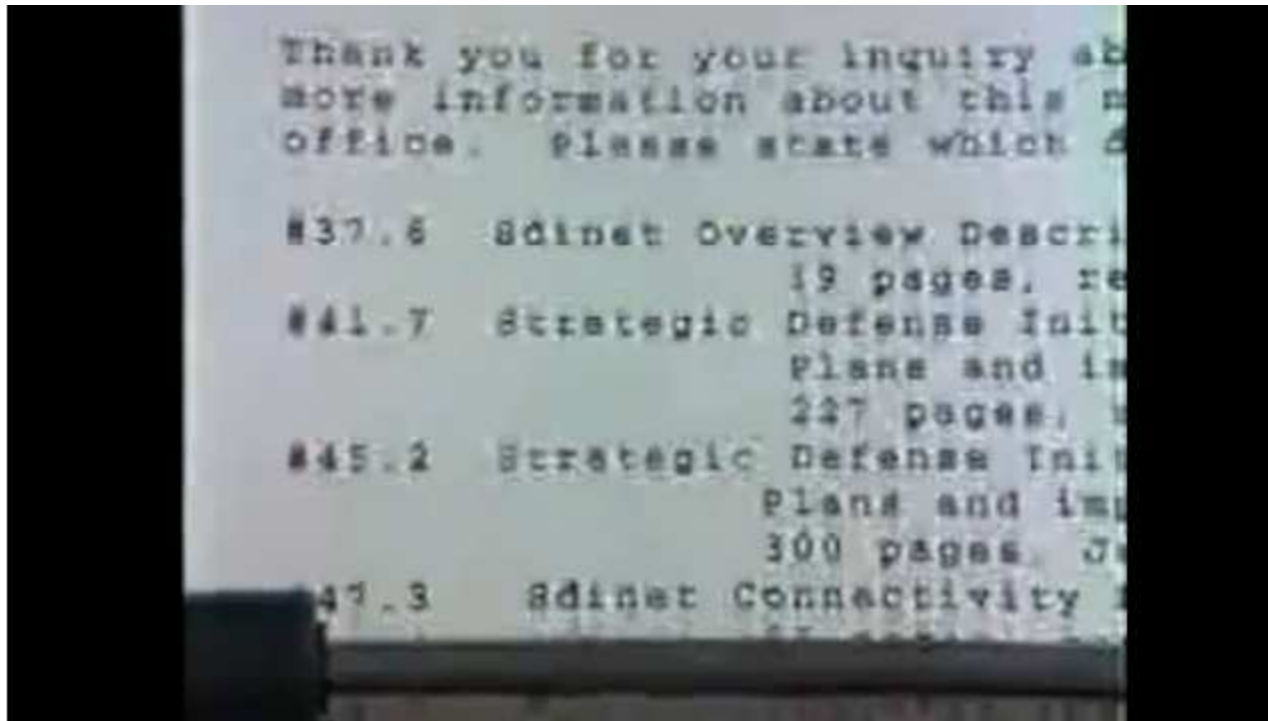
```
Hacker: Call Lengths
HACKER CALLING TIMES
```

Date	logon	logoff	Duration
Jan 2	13:02	13:03	1 min
Jan 3	12:05	12:09	4 min
Jan 5	15:50	15:55	5 min
Jan 7	11:44	11:49	5 min
Jan 7	12:03	12:05	2 min
Jan 9	13:02	13:07	5 min

The intruder spent too little time online. Stoll needed a way to keep the intruder online longer so the Bundespost could complete their manual trace.



# Building the Honeypot



Stoll's girlfriend Martha suggested creating fake documents to lure the intruder into wasting time reading and downloading them, thereby staying connected to LBNL longer.



## The Intruder Takes the Bait

```
lear'.  
#      TITLE  
=      =====  
      IG Inspections (Headquarters,  
      Department of the Army)  
      Nuclear, chemical, and biological  
      national security affairs  
      Nuclear, chemical and biological  
      warfare arms control  
      Nuclear and chemical strategy  
      formulations  
      Nuclear and chemical politico-  
      military affairs  
      Nuclear and chemical requirements
```

The ploy worked! In addition to downloading data, a Hungarian spy in the US wrote to an address planted by Stoll in friends, requesting information on the fake “SDINet.”





# Patience



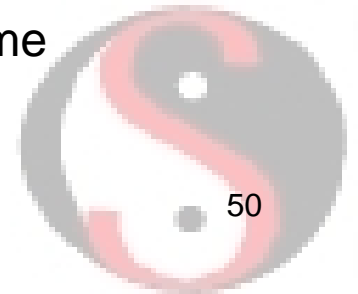
Six months after starting the investigation, Stoll kept the intruder online long enough for the Bundespost to trace the call to Hannover, West Germany.



## The FBI Takes Notice



Eventually the FBI became interested, but noted at that time there was no extradition treaty with West Germany.



## Stoll Goes to Germany



Three years after starting his investigation, Stoll went to Germany for a court case against the intruders.



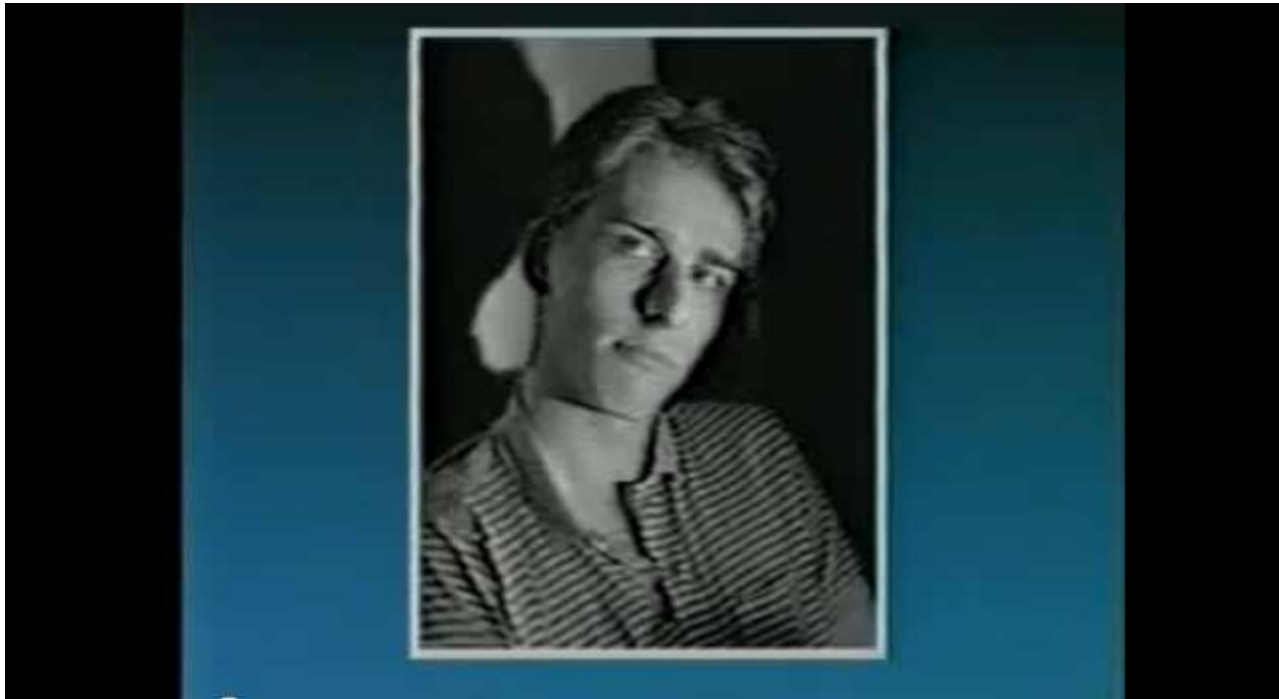
## Brezinski and Carl



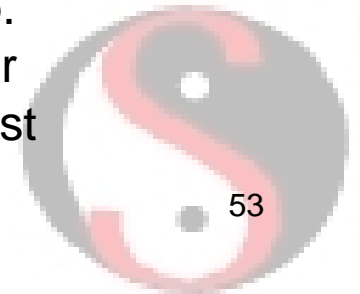
Dirk Brezinski (programmer) and Peter Carl (contact with KGB) were two of the group conducting espionage on behalf of the KGB.



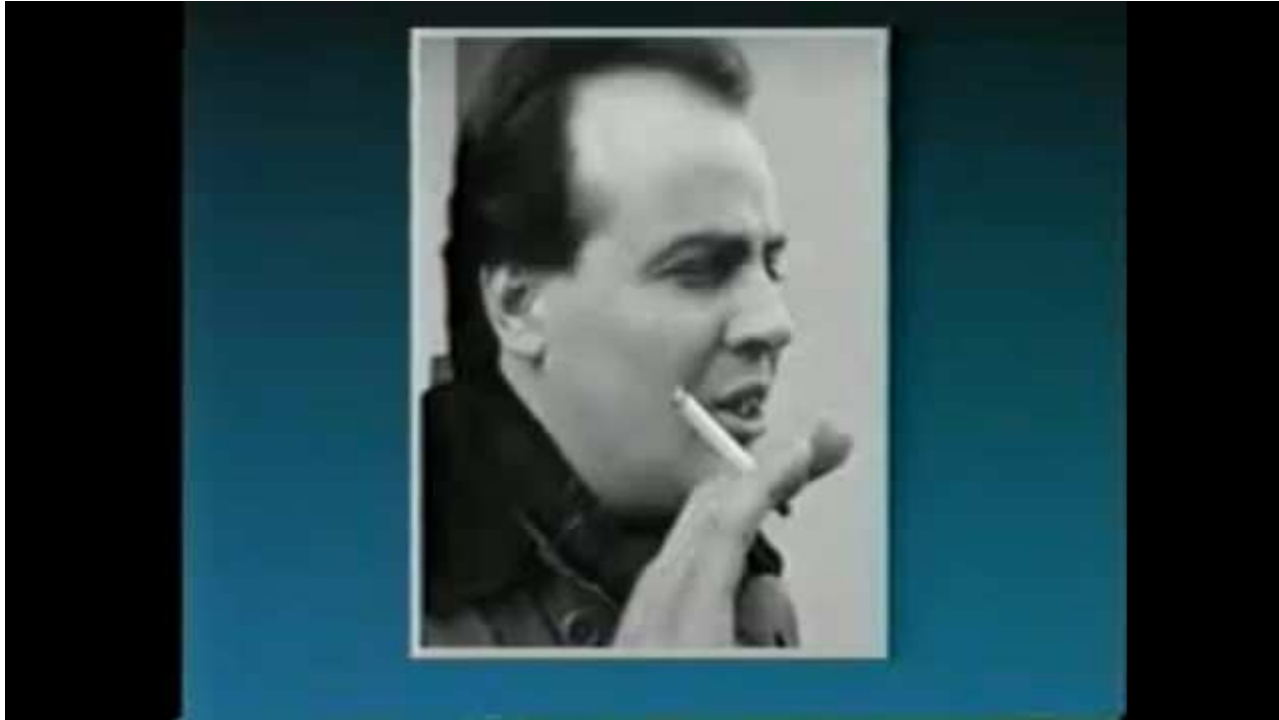
# Hagbard



Karl Koch, aka Hagbard, was a third member of the group. He died in May 1989 under suspicious circumstances after being charged. He supposedly committed suicide in a forest by setting himself on fire.



## Hunter Himself



Markus Hess, the fourth member of the group, was the intruder Stoll tracked.

The German court found the three survivors guilty but the defendants served less than two years probation.



Watch the Show Online!



<http://www.youtube.com/watch?v=v1swbLfrP6g>



## Lessons: Monitoring and Analysis

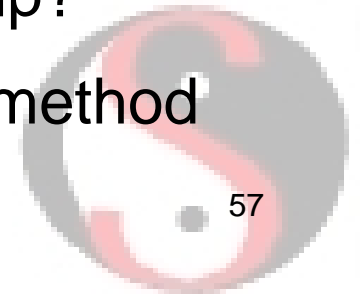
- “Build visibility in” with local accounting application
- Don’t rely on a single “source of truth”
- Centralized logging defeats intruders deleting local logs
- Passive full content monitoring captures all details without alerting intruder
- Document analysis in log book
- Key questions: scope of intrusion, depth of intrusion?
- Monitoring using discarded gear is better than nothing
- Writing custom tools for monitoring and alerting
- *Someone cares: analysis by a person who took the intrusion personally!*





## Lessons: Nature of the Intrusion

- Intruder exploits weak credentials to gain access
- Intruder leverages local privilege escalation vulnerability
- Intruder exploits trust relationships
- Intruder exploits poor configurations deployed by vendor
- Intruder exploits system monoculture (Unix in the '80s!)
- Sensitive data accessible from normal network, e.g., cancer treatment equipment
- Systems owners repeatedly told Stoll an intrusion was “impossible – our systems are secure!”
- Recover by reimaging, rebuilding, restore backup?
- External notification is most common detection method

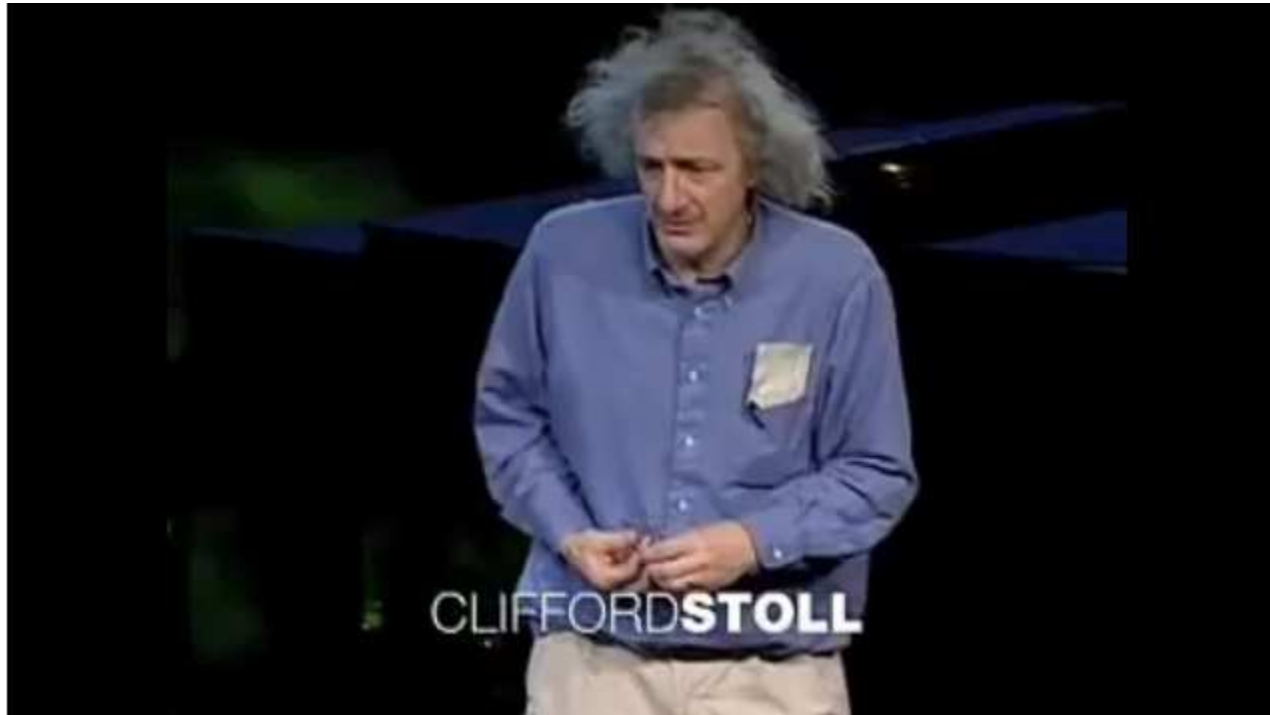


## Lessons: Enduring Truths

- Of at least 80 victims, only 2 noticed (LBNL, NSA)
- Agencies ask for information but provide little back
- Users communication about intrusion compromise opsec
- Intruders violate assumptions held by network owners
- When to monitor intruder, and when to contain him?
- How much is stolen data worth? What is incident cost?
- A variety of analysis techniques provides best results
- Cannot trust endpoints to defend themselves nor report their security state
- Intruders can be creative and persistent



## Watch Cliff Stoll's TED Appearance



<http://www.youtube.com/watch?v=Gj8IA6xOpSk>



# Questions?

## KNOW YOUR NETWORK BEFORE AN INTRUDER DOES

```
40.652146 10.145.15.100 -> 216.68.1.200 DNS Standard query A z3n.phatcamp.org
40.690278 10.142.1.89 -> 216.68.1.100 DNS Standard query A z3n.phatcamp.org
40.690291 10.142.1.89 -> 216.68.1.100 DNS Standard query A z3n.phatcamp.org
41.386313 10.145.15.98 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
43.386117 10.145.15.100 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
43.386248 10.145.15.100 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
44.568156 10.142.1.97 -> 10.145.15.100 DNS Standard query A z3n.phatcamp.org
46.258206 10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258210 10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258292 10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258306 10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
48.062938 10.142.1.97 -> 10.142.1.89 DNS Standard query A z3n.phatcamp.org
```

Richard Bejtlich

[richard@taosecurity.com](mailto:richard@taosecurity.com)

[taosecurity.blogspot.com](http://taosecurity.blogspot.com)

